О. І. Клесов

ЕЛЕМЕНТАРНА ТЕОРІЯ ЧИСЕЛ ТА ЕЛЕМЕНТИ КРИПТОГРАФІЇ

ПІДРУЧНИК

Рекомендовано Вченою радою НТУУ “КПІ”
як підручник для студентів вищих навчальних закладів,
які навчаються за спеціальністю “математика та статистика”

⟨⟨**ТВіМС**⟩⟩
Київ
2016

УДК 519.21
ББК 22.171
К–18

Рецензенти:

В. В. Гавриленко — доктор фізико-математичних наук, професор, завідувач кафедри інформаційних систем і технологій Національного транспортного університету

П. В. Задерей — доктор фізико-математичних наук, професор, завідувач кафедри вищої математики Київського університету технологій та дизайну

Затверджено Науковою радою Національного технічного університету "КПІ" (протокол № 8 від 30.06.2016 р.) як підручник для студентів вищих навчальних закладів, які навчаються за спеціальністю "111. Математика та статистика"

Клесов О. І.

К–18 ЕЛЕМЕНТАРНА ТЕОРІЯ ЧИСЕЛ ТА ЕЛЕМЕНТИ КРИПТОГРАФІЇ: Підручник. — К.: ТВіМС, 2016. — 412 стор.

Підручник містить відомості з теорії чисел, які необхідні для оволодіння елементами криптографії, а також класичні та сучасні методи шифрування інформації включно з методами RSA, Ель-Гамаля, цифрового підпису, які входять до навчального плану освітньо-кваліфікаційного рівня "*бакалавр*" зі спеціальності "*Математика та статистика*".

ББК 22.171
УДК 519.21

ISBN 978–966–8725–11–1

Зміст

ПЕРЕДМОВА

Глава 1. Зв'язок між теорією чисел та криптографією 1
1.1. "Апологія математика" 1
1.1.1. Чи правий Харді? 2
1.1.2. Чи існують застосування математики? 3
1.1.3. Чи існують застосування теорії чисел? 3
1.2. Як кодують повідомлення 4
1.2.1. Математичні шифри 9
1.3. Перевірка числа на простоту 10
1.4. Решето Ератосфена 12
1.5. Кілька відомих шифрів 16
1.5.1. Шифр перестановки 16
1.5.2. Рандомізований матричний шифр 17
1.5.3. Азбука Брайля 18
1.5.4. Азбука Морзе 19
1.6. Контрольні питання 20
1.7. Задачі 20
1.8. Біографії 27

Глава 2. Шифр Цезаря 37
2.1. Код клавіатури 38
2.2. Шифр Цезаря 38
2.2.1. Використання чисел у шифрі Цезаря 40
2.3. Подільність натуральних чисел 42

2.3.1. Ділення з остачею 43
2.4. Властивості конгруенції 44
2.5. Найбільший спільний дільник 46
2.6. Прості числа та основна теорема арифметики 46
2.6.1. Закон розподілу простих чисел 49
2.7. Шифр Віженера 50
2.8. Шифр Вернама 53
2.9. Контрольні питання 54
2.10. Задачі 55
2.11. Біографії 61

Глава 3. Мультиплікативні шифри 66
3.1. Означення мультиплікативних шифрів 66
3.1.1. M_2-шифр 67
3.1.2. Дешифрування M_2-шифру 68
3.1.3. Шифр M_3 69
3.2. Обернені числа в арифметиці за модулем ... 70
3.3. Властивості шифру $M_{a,n}$ 72
3.3.1. Дешифрування $M_{a,n}$ шифру 72
3.3.2. Криптоаналіз M_a шифру 72
3.3.3. Алгебраїчний спосіб дешифрування 73
3.3.4. Для яких a існують M_a шифри 74
3.3.5. Інші алфавіти 75
3.4. Контрольні питання 77
3.5. Задачі 78
3.6. Біографії 86

Глава 4. Алгоритми Евкліда 88
4.1. Алгоритм Евкліда знаходження найбільшого спільного дільника 89

4.2. Знаходження оберненого числа в арифметиці за модулем ... 92
4.2.1. Побудова оберненого за модулем ... 94
4.3. Розширений алгоритм Евкліда ... 98
4.4. Контрольні питання ... 101
4.5. Задачі ... 102
4.6. Біографії ... 107

Глава 5. Шифр Хілла ... 110
5.1. Дешифрування шифру Хілла ... 111
5.2. Системи лінійних конгруенцій ... 112
5.2.1. Одне рівняння ... 112
5.2.2. Система двох рівнянь ... 113
5.3. Дешифрування шифру Хілла: закінчення ... 115
5.3.1. Блоки іншого розміру ... 117
5.4. Криптоаналіз шифру Хілла ... 118
5.5. Системи лінійних рівнянь за модулем ... 118
5.6. Шифр Плейфера ... 122
5.7. Контрольні питання ... 125
5.8. Задачі ... 126
5.9. Біографії ... 134

Глава 6. Лінійні шифри ... 136
6.1. Дешифрування лінійного шифру ... 137
6.2. Скільки існує лінійних шифрів? ... 138
6.2.1. Випадок загального n ... 139
6.3. Функція Ойлера ... 140
6.3.1. Формула включення/виключення ... 141
6.3.2. Загальна формула для функції Ойлера ... 143
6.4. Теорема Ойлера ... 145
6.4.1. Обчислення оберненого за модулем ... 146

6.4.2. Мала теорема Ферма 147
6.5. Таблиця перших значень функції Ойлера . 147
6.6. Контрольні питання 148
6.7. Задачі 149
6.8. Біографії 154

Глава 7. Криптоаналіз лінійних шифрів 156
7.1. Алгебраїчний метод для $L_{a,b}$ шифрів 156
7.1.1. Як розв'язувати лінійні рівняння у модульній арифметиці 156
7.1.2. Як розв'язувати системи лінійних рівнянь у модульній арифметиці 158
7.2. Частотний аналіз 159
7.3. Надійність лінійних шифрів 163
7.3.1. Принцип Керкхоффса 164
7.3.2. Принцип складності обчислень 164
7.3.3. Лист Джона Неша 165
7.3.4. Найбільш загадковий рукопис 166
7.3.5. Час, потрібний для зламу лінійного шифру 167
7.4. Ще раз про знаходження оберненого за модулем 169
7.5. Контрольні питання 170
7.6. Задачі 171
7.7. Біографії 178

Глава 8. Експоненціальні шифри 180
8.1. Особливості експоненціального шифру 180
8.1.1. Яким має бути n 181
8.1.2. Експоненціальний шифр не є підстановкою 181
8.2. Властивість конгруенцій, необхідна для експоненціальних шифрів 183

8.3. Дешифрування експоненціального шифру . 183
8.3.1. Обчислення показника кореня 184
8.3.2. Обчислення показника кореня, коли $n = p$. 185
8.3.3. Обчислення показника кореня, коли $n = pq$ 186
8.3.4. Як створити свій експоненціальний код ... 188
8.4. Швидке піднесення до степеня 189
8.5. Швидке піднесення до степеня за модулем 190
8.5.1. Бінарне представлення 192
8.6. Контрольні питання 194
8.7. Задачі 196
8.8. Біографії 201

Глава 9. Криптоаналіз експоненціальних шифрів 202
9.1. Дешифрування у випадку коли степінь та модуль відомі 202
9.2. Дешифрування у випадку коли показник або модуль невідомі 205
9.3. Надійність експоненціальних шифрів 208
9.3.1. Метод факторизації Крайчика 211
9.4. Односторонні функції 214
9.4.1. Односторонні функції з секретом 214
9.4.2. Дискретний логарифм 215
9.4.3. Захист пароля 216
9.4.4. Алгоритм Шенкса 217
9.5. Контрольні питання 219
9.6. Задачі 221

Глава 10. Криптосистеми з відкритим ключем 229
10.1. Головоломки Меркла 230

10.2. Метод В. Діффі та М. Хеллмана 230
10.3. Шифр RSA 232
10.3.1. Що таке шифр RSA 232
10.3.2. Відкритий та приватний ключі для RSA . 234
10.3.3. Надійність RSA 235
10.3.4. Початок історії RSA 236
10.3.5. Припущення щодо RSA 238
10.3.6. Інший спосіб запису RSA 239
10.4. Доведення алгоритму RSA 240
10.5. Атаки на RSA 241
10.5.1. Факторизація n якщо відоме $\phi(n)$ 242
10.5.2. Факторизація n, якщо $|p-q|$ є малим 242
10.6. Задача про рюкзак в криптографії 244
10.6.1. Задача про рюкзак для суперзростаючих послідовностей 244
10.6.2. Криптосистема, основана на задачі про рюкзак 245
10.7. Метод Ель-Гамаля 247
10.7.1. Примітивний корінь числа 248
10.7.2. Криптосистема Ель-Гамаля 250
10.8. Контрольні питання 255
10.9. Задачі 256
10.10. Біографії 263

Глава 11. Цифровий підпис 269
11.1. Метод RSA для цифрового підпису 269
11.2. Дайджест 273
11.2.1. Хеш функції 275
11.3. Сліпий цифровий підпис 277
11.3.1. Вимоги до схеми сліпого підпису 278
11.3.2. Доведення алгоритму 1 280

11.4. Застосування схеми сліпого підпису 281
11.4.1. Електронні гроші 281
11.4.2. Таємне голосування 284
11.5. Цифровий підпис для схеми Ель-Гамаля . 287
11.5.1. Невдала хеш функція 290
11.5.2. Атака, якщо j є відомим 291
11.5.3. Атака, якщо j повторюється 291
11.6. Розподілення секретів 292
11.7. Контрольні питання 296
11.8. Задачі 297
11.9. Біографії 305

Глава 12. Перевірка чисел на простоту 306
12.1. Кілька відомих способів перевірки чисел на простоту 307
12.1.1. Формула Міллса 307
12.1.2. Критерій Вілсона 308
12.2. Псевдопрості числа 309
12.3. Числа Кармайкла 313
12.3.1. Найменше з чисел Кармайкла 314
12.3.2. Необмеженість множини чисел Кармайкла 315
12.3.3. Теорема Корселта 315
12.4. Тест Соловея–Штрассена 317
12.4.1. Тест Соловея–Штрассена 318
12.4.2. Оптимальність тесту Соловея–Штрассена 321
12.4.3. Обгрунтування тесту Соловея–Штрассена 323
12.4.4. Кілька ітерацій тесту Соловея–Штрассена 324
12.5. Тест Міллера 328
12.6. Тест Рабіна–Міллера 332
12.6.1. Рандомізований алгоритм 333
12.6.2. PRIMES is in P 336

12.7. Контрольні питання 336
12.8. Задачі 338
12.9. Біографії 345

Глава 13. Теорема Чебишова 351
13.1. Асимптотика кількості простих чисел 357
13.1.1. Про доведення теореми про прості числа . 357
13.2. Постулат Бертрана 358
13.2.1. Теорема Райта 363
13.3. Асимптотика функції Чебишова 364
13.4. Асимптотика n-ого простого числа 366
13.5. Контрольні питання 369
13.6. Задачі 372
13.7. Біографії 377

СПИСОК ЛІТЕРАТУРИ 385

ПРЕДМЕТНИЙ ПОКАЖЧИК 387

СПИСОК ПОЗНАЧЕНЬ 393

Передмова

Розкажи мені — я забуду.
Покажи мені — я запам'ятаю.
Зроби разом зі мною — я навчусь.
Конфуцій

В основу цього підручника покладено курс лекцій з такою ж назвою, який автор викладає на фізико-математичному факультеті Національного технічного університету України "Київський політехнічний інститут".

Назва курсу лекцій "*Елементарна теорія чисел та елементи криптографії*" правильно відображає його зміст: він дійсно містить лише найпростіші теми з теорії чисел та сучасної криптографії.

При написанні цього підручника автор не мав на меті викласти в повному обсязі (елементарну) теорію чисел або (елементарну) криптографію. Натомість мета полягала у тому, щоб показати, що навіть прості факти з теорії чисел можуть бути корисними у сучасних застосуваннях та у доступній формі описати такі застосування у криптографії.

Автор намагався представити матеріал в першу чергу для студентів, які вивчають математику. Тому в підручнику доведено багато простих, але необхідних фактів з елементарної теорії чисел, що є обов'язковою складовою освіти

математиків. Можливо, іншим студентам, які спеціалізуються, наприклад, у галузі захисту інформації, деякі з доведень будуть здаватися зайвими.

Майже всі теми, що увійшли до підручника, є достатньо простими (принаймні для математиків). Проте це не означає, що всі математичні методи криптографії (навіть ті, які представлені в цьому підручнику) є простими і легко доступними читачам без належної підготовки. Прикладом може служити глава 13, де розглянуто асимптотику кількості простих чисел.

Кілька слів до викладачів. Кожна з глав містить більше матеріалу, ніж лектор зможе викласти в нормальному темпі за 2 академічні години. Залежно від навчальної програми додатковий матеріал кожної глави можна пропонувати студентам для самостійної роботи або викладати на наступному занятті. Мені здається, що для того, щоб викласти весь матеріал цього підручника, вистачить 18–20 лекційних занять.

Уявлення про теми, представлені в підручнику, дає наступний перелік:

теми з криптографії	**теми з теорії чисел**
лінійні шифри	арифметика за модулем
мультиплікативні шифри	обернені за модулем
шифр Хілла	алгоритми Евкліда
експоненціальні шифри	функція Ойлера
метод RSA	перевірка чисел на простоту
криптосистема Ель-Гамаля	системи конгруенцій
“рюкзачна” криптосистема	примітивні корені
цифровий підпис	асимптотика простих чисел

Саме ці теми складають семестрову навчальну програму курсу на фізико-математичному факультеті КПІ.

В залежності від вподобань лектора курс лекцій можна доповнити однією або кількома наступними темами, які також досить детально викладено в підручник: системи конгруенцій, примітивні корені, рюкзачні системи, алгоритми факторизації натуральних чисел тощо. Крім цього, в підручнику обговорюються також інші застосування, які не мають прямого відношення до теорії чисел або криптографії, але які використовують ті ж результати та аналогічні протоколи, а саме: сліпий підпис, таємне голосування, розподілені секрети, електронні гроші тощо.

Хоча назви багатьох глав є "криптографічними", вони більше ніж наполовину складаються з результатів теорії чисел. Наприклад, назвою глави 2 є "*Шифр Цезаря*" хоча в ній, разом з шифрами Цезаря, Вернама та Віженера, розповідається також і про "*Подільність натуральних чисел*", "*Ділення з остачею*", "*Властивості конгруенції*", "*Найбільший спільний дільник*", "*Прості числа та основна теорема арифметики*", "*Закон розподілу простих чисел*".

Наприкінці кожної глави є розділ "*Контрольні питання*", які можна використати для оперативної перевірки рівня оволодіння матеріалом даної глави. Іншою важливою складовою кожної глави є задачі, яких достатньо і для практичних занять, і для домашньої роботи. Приблизно половина задач відноситься до теорії чисел, а інша — до криптографії. Виключенням є глави 11 та 13, де задач з теорії чисел 0% та 100% відповідно.

Всі формули і форматування підручника здійснено за допомогою програми TEX, автором якої є відомий американський математик Дональд Кнут. Ця програма зараз вва-

жається стандартним інструментом для підготовки математичних публікацій і тому нею користуються майже всі математики в усьому світі. Набагато менше відомі інші чудові властивості TEX'у, які нагадують засоби інших мов програмування для комп'ютерів. Майже всі обчислення, представлені в підручнику, виконано за допомогою макросів, написаних мною засобами TEX'у. Це дозволило мені під час підготовки цього підручника залишатись в комфортному "середовищі" TEX'а.

Кілька слів до студентів. В тексті підручника багато позначок типу ①, які рекомендують читачеві подумати над певним питанням. Питання не складні, але читачу важливо знайти відповіді на кожну з них, щоб зрозуміти міркування автора. Саме ці питання складають розділ "*Контрольні питання*" в кінці кожної глави.

Твердження та формули в кожній главі нумеруються за допомогою одного числа, наприклад в главі 8 є "теорема 1" і протягом цієї глави я посилаюсь на неї як на "теорему 1". Якщо ж вираз "теорема 8.1" зустрічається в іншій главі, то це означає, що автор посилається на "теорему 1 з глави 8". Аналогічне правило стосується номерів інших типів тверджень, а також формул.

В кінці кожної глави наведено вправи, які необхідно виконати під час практичного заняття в аудиторії або вдома. Я вважаю, що гарною стратегією для студентів є повторення матеріалу останньої лекції перед черговим практичним заняттям, а також перед черговою лекцією. Поганою ж стратегією є намагання відкласти оволодіння матеріалом

[1] це порада автора читачу здійснити певну дію.

лекцій на період безпосередньої підготовки до іспиту. ②

В кінці підручника на стор. 385–386 наведено перелік (далекий від повного) посилань на інші літературні джерела, якими я користався під час написання свого підручника або які я рекомендую для подальшого вивчення матеріалу. Для бажаючих розширити свої знання з теорії чисел я рекомендую підручники [3] або [18], [20] (більш складні питання обговорюються в [17]). Дружніми до читача підручниками з криптографії я вважаю [9] або [10], а також [15] та [21]. Багато цікавих історичних відомостей про криптографію міститься в [8]. Алгоритмічні питання теорії чисел та криптографії обговорюються в [13]. Додаткові задачі з криптографії можна знайти в [6] та [11].

Кілька загальних зауважень. Автор не вважає правильним, що надто багато розділів з теорії чисел, теорії графів, алгебри або дискретної математики "відносяться" до комп'ютерних наук або так званої "прикладної математики". Незрозумілою є й поведінка самих математиків, які добровільно відмовляються від цих розділів на підставі їх "занадто прикладного спрямування".

Неприродний (або "віртуальний", якщо вживати сучасний сленг) поділ на фундаментальну та прикладну науку існує не тільки в математиці і з'явився він не зараз. У часи І. Ньютона (XVII сторіччя) такого поділу ще не існувало. Через 300 років після Ньютона в своїй доповіді на Міжнародному симпозіумі з планування науки у 1959 році

[2] а тим більше до моменту безпосередньої відповіді на іспиті!

П. Л. Капіца сказав:

> “ ... У зв'язку із зростанням масштабів наукової роботи відбувається поділ науки на фундаментальну і прикладну. Я думаю, що цей поділ багато в чому слід вважати штучним, і важко вказати точку, де кінчається фундаментальна і починається прикладна наука ... ”

Таким чином, у другій половині XX сторіччя вже існував “штучний” (за висловлюванням Капіци) поділ науки на фундаментальну та прикладну складові. Але ще за сто років до Капіци, Луї Пастер, якого важко запідозрити у зайвій схильності до теоретичних досліджень, був більш категоричним у своїх висловлюваннях:

> “ ... Не існує жодних “прикладних наук”; є тільки одна Наука та її плоди — як дерево й плоди, ним породжені ... ”

Таким чином, в XIX сторіччі вчені вже дискутували з приводу поділу науки на дві складові. Мабуть неприродний поділ на фундаментальні та прикладні науки виник раніше, можливо у XVIII сторіччі.

Правильним, на думку автора, шляхом розвитку математики є генерація математичних ідей математиками і використання ними ж цих ідей для розв'язання практичних задач разом із спеціалістами зі сміжних галузей.

Варто також зазначити, що в математиці існують задачі, які самі математики вважають важливими, але інші спеціалісти з цим не погоджуються. Захопленість математиків абстрактними конструкціями та теоріями може навіть стати приводом для глузування з боку нематематиків. Тому одним з завдань, які стоять перед сучасними математиками,

є пошук порозуміння з іншими вченими шляхом пояснення актуальності своїх досліджень.

У цьому зв'язку характерною є позиція видатного російського математика В. І. Арнольда стосовно доведення великої теореми Ферма, яка протягом більше трьох століть не піддавалась розв'язанню. Весь цей час вона приваблювала майже кожного з математиків, але жодному з них не вдавалося її підкорити до 1994 року, коли Ендрю Вайлс показав, що гіпотеза Ферма є вірною. Більшість математиків вважали його результат одним з найвидатніших у XX сторіччі. З цього приводу В. І. Арнольд писав, що галас, здійснений навколо доведення великої теореми Ферма, може привести до припинення фінансування цієї науки урядами і суспільством, оскільки на цьому прикладі стає зрозумілим, якою "непотрібною" діяльністю займаються математики.

Якщо знизити полемічний запал В. І. Арнольда й викласти його висловлювання у більш зваженому вигляді, то можливою інтерпретацією його слів буде така: математики повинні представляти свої результати у публічній сфері, причому таким чином, щоб вони були зрозумілими широкому загалу, в тому числі й керівникам, від яких залежить фінансування науки.

В. І. Арнольд вважає, що це зробити можна й це завдання є здійсненним, оскільки

> " ... справжня математика геометрична й сильна зв'язками з фізикою ... "

Інша точка зору, яка належить видатному англійському математику Ґ. Харді і з якою автор цього підручника полемізує у главі 1, полягає в тому, що справжня математика

не має нічого спільного з застосуваннями, а ті формули, що використовуються для застосувань, не є математикою.

Схожі думки висловлював інший видатний математик Давід Гільберт на початку XX сторіччя: він вважав, що математика не мала, не має і ніколи не буде мати жодних застосувань.

Екстремальна точка зору належить сучасному російському математику Ю. І. Манінy, який працює в Німеччині: він вважає, що математика потрібна лише для того, щоб відволікати розумних людей від інших зайнять, які можуть нашкодити людству (наприклад, винаходами нових видів зброї).

Цю передмову я хочу завершити, навівши слова трьох видатних вчених, які додержуються іншої точки зору, ніж Харді, Гільберт чи Манін.

> “ ... Не існує нічого більш практичнішого, ніж хороша теорія ... ”
>
> Людвіґ Больцман

> “ ... Той, хто захоплюється практикою без науки, нагадує керманича, який ступив на корабель без керма та компаса: він ніколи не знає, куди пливе ... ”
>
> Леонардо да Вінчі

> “ ... Наука повинна бути найбільш піднесеним втіленням патріотизму, оскільки той народ буде завжди першим, який випередить інших в області розумової діяльності ... ”
>
> Луї Пастер

Ці промовисті цитати краще, ніж мої власні слова, пояснюють мою позицію.

Автор

Глава 1

ЗВ'ЯЗОК МІЖ ТЕОРІЄЮ ЧИСЕЛ ТА КРИПТОГРАФІЄЮ

1. "Апологія математика"

В 1940 році вийшла у світ маленька книжка видатного англійського математика Ґодфрі Харді під назвою "Апологія математика". Слово "апологія" має декілька значень, в тому числі й "прохання про прощення", але у назві книги автор вживає його у розумінні "пояснення".

У популярній формі Харді пояснює читачеві своє ставлення до математики, аналізує її значення та роль у суспільстві. Нагадаємо, що в 1940 році вже точилася Друга світова війна і це впливало на позицію Харді. Він, як справжній пацифіст, не міг виправдати людські смерті та страждання з будь-якої сторони конфлікту, звинувачуючи технічний прогрес у створенні засобів вбивства людей. Технічний прогрес, на думку Харді, відбувається завдяки розвитку природничих наук, таких як фізика або механіка.

На відміну від цих наук, математика, а за думкою Харді, є найбільш миролюбною та толерантною у тому розумінні, що справжня математика — це вид інтелектуальних зайнять, таких, наприклад, як шахи або мистецтво, а вони не можуть нанести шкоди людству. Застосування науки, вважав Харді, стимулює технічний прогрес, жорстокий та байдужий до страждань людей. Найбільш "чистим" від застосувань розділом математики він вважав свою улюбле-

ну теорію чисел, яку називав "непотрібною суспільству" на тій підставі, що теорія чисел не впливає на прогрес, не підвищує матеріальний добробут людства, але і не приносить йому страждань.

Свою позицію Харді підкріплював словами геніального німецького математика Карла Гаусса (1777–1855): "Математика — цариця наук, а теорія чисел — королева математики" (про англійську королеву кажуть, що вона править, але не володарює, тобто королева не впливає на розвиток суспільних процесів у країні). Харді пояснював слова Гаусса тим, що поняття та результати, які складають теорію чисел, є більш глибокими та елегантними у порівнянні з будь-яким іншим розділом математики, і тому мають виключне інтелектуальне значення.

Для Харді красивою є та математика, яка не має застосувань; а та, що має, — є гидкою, тривіальною та нудною. Прагнення до чистої математики пояснюється тим, що її "непотрібність" означає, що її не можна використати для причинення "шкоди" людству.

1.1. Чи правий Харді? Щоб наблизитись до відповіді на це питання, наведемо результат з теорії чисел, який називається *основною теоремою арифметики.*

Теорема 1 (*основна теорема арифметики*)**.** *Кожне натуральне число можна представити як добуток простих чисел. Таке представлення є єдиним з точністю до порядку множників.*

Чи може хто небудь уявити хоча б одне застосування теореми 1 у практичних задачах? Мабуть, ні. Здається, Харді мав рацію.

Звернімося до іншого факту теорії чисел, яким пишаються математики ще з часів Стародавньої Греції.

Теорема 2 (*про нескінченість множини простих чисел*)**.** *Для будь-якого простого числа p існує просте число $q > p$.*

У якій же галузі знань може знадобиться факт нескінченості множини простих чисел? Здається, що в жодній. Це ще раз свідчить на користь думки Харді (принаймні, по відношенню до теорії чисел).

1.2. Чи існують застосування математики? Схвальну відповідь на це питання дав і сам Харді, оскільки писав про "огидні" розділи математики, які розв'язують прикладні задачі. Але чи тільки "огидні" математичні результати мають практичні застосування?

Кілька років тому було опубліковано результати соціологічного дослідження, метою якого було з'ясувати, який з математичних результатів математики вважають найбільш красивим. Більшість опитуваних найкрасивішим математичним результатом назвали теорему Піфагора. Цей безсумнівно красивий геометричний факт має очевидні застосування, наприклад, у будівництві (починаючи з часів Древнього Єгипту). Більше того, геометрія (одним з тверджень якої є теорема Піфагора) виникла, а потім розвивалась, як відповідь на суто утилітарні запити суспільства. Дослідження геометрами V постулату Евкліда, які можуть здаватись схоластичними, врешті решт привели до виникнення геометричних моделей, які вважають адекватним описом нашого Всесвіту.

1.3. Чи існують застосування теорії чисел? Харді в

1940 році писав в "Апології":

> "Існує один втішний висновок, приємний для справжнього математика: справжня математика не має впливу на війну. Нікому ще не вдалося виявити жодну військову, або таку, що має відношення до війни, задачу, якій служила б теорія чисел або теорія відносності, і малоймовірно, що кому-небудь вдасться виявити щось подібне у майбутньому, на скільки б років ми не заглядали вперед у майбутнє."

За іронією долі через 5 років після появи "Апології", коли Харді був ще живий, вибухнула перша ядерна бомба, що стало практичним застосуванням теорії відносності ...

Метою цього підручника є показати чисельні застосування теорії чисел у сучасній криптографії, яку зараз вже не можна уявити без багатьох "непотрібних" результатів типу малої теореми Ферма. Все, про що ми будемо говорити нижче, є невтішним для мрії Харді про чисту науку. До речі, його підручник з математичного аналізу, перекладений також і російською (у 1949 році), має назву "*Курс чистой математики*"" (перше англійське видання вийшло в 1907 році).

2. Як кодують повідомлення

Криптографія (від грецького $\kappa\rho\upsilon\pi\tau o\zeta$ — прихований і $\gamma\rho\alpha\varphi\omega$ — писати) — наука про способи збереження конфіденційності інформації. Протягом усього часу, коли існує людство, люди намагались приховати певну інформацію, яку одна особа передавала іншій. Найпростішим способом приховування є тримання у секреті самого факту передачі інформації. Інший спосіб полягає у шифруванні інформації

та триманні у секреті ключа, за допомогою якого зашифровану інформацію можна відновити.

При шифруванні букви алфавіту замінюються іншими символами, наприклад номерами їх позицій в алфавіті. Багато систем шифрування описано у детективних та пригодницьких романах, сюжет яких будується навколо важливої зашифрованої інформації.

"Золотий жук". В оповіданні "Золотий жук" американського письменника Едгара Алана По (1809–1849), яке вийшло у 1843 році, головний герой намагається знайти скарб. Інформація про місце збереження скарба міститься у закодованому повідомленні:

```
53‡‡†305))6*;4826)4‡.)4‡);806*;48†8¶
60))85;1‡(;:‡*8†83(88)5*†;46(;88*96*
?;8)*‡(;485);5*†2:*‡(;4956*2(5*-4)8¶
8*;4069285);)6†8)4‡‡;1(‡9;48081;8:8‡
1;48†85;4)485†528806*81(‡9;48;(88;4(
‡?34;48)4‡;161;:188;‡?;
```

Головний герой оповідання Е. По зумів прочитати повідомлення, використовуючи дотепну систему аналізу знаків шифру, основану на частотах використання букв в англійській мові.

"Танцюючі чоловічки". У цьому оповіданні англійського письменника Артура Конана Дойля (1859–1930), яке вийшло у 1903 році, Шерлок Холмс запобіг злочину, прочитавши зашифровані повідомлення. У російськму перекладі оповідання наведено наступну таблицю, яку злодій використовув для шифрування повідомлень:

Рис. 1. Шифр “Танцюючі чоловічки”

Шерлок Холмс принаймні двічи мав справу з шифрами. В оповіданні “Долина страху” Конан Дойль описує історію, коли великий сищик отримав закодоване повідомлення від свого заклятого ворога, професора Моріарті. І в цьому випадку детектив виявився на висоті завдяки своїм здібностям до дедуктивного мислення.

“Жангада”. “Жангада. 800 льє вниз по Амазонці” — науково-фантастичний пригодницький роман французького письменника Жуля Верна (1828–1905), написаний в 1881 році. Головного героя роману, Жоама Гарраля, розшукують вже багато років за злочин, який він не скоював. У подорожі Амазонкою він отримав документ, в якому є свідчення його невинуватості, проте текст є зашифрованим. Поліція заарештовує Гарраля, відтак єдиною його надією є розшифрувати документ. За розгадку завзято береться суддя Жаррікес, але розшифрувати документ йому не вдається, Гарраля засуджують до страти. В останню мить стає відомим ім’я автора документа і ця підказка дозволяє Жаррікесу

закінчити розшифровку документа.

Основна теорема аналіза. Шифровані повідомлення, як засіб приховати свої відкриття, можна зустріти у листуванні між великими математиками. Перебуваючи у Лондоні протягом 1669 року, Ґотфрід Ляйбніц, тоді ще невідома молода людина, який згодом став видатним німецьким математиком, дізнався про математичні роботи іншої молодої особи, Ісаака Ньютона, який вже тоді був достатньо визнаним у наукових колах. Ляйбніц намагався зустрітися з Ньютоном, але той не бажав спілкуватись. Повернувшись додому, Ляйбніц згодом надіслав Ньютону листа, у якому просив розтлумачити йому основні методи англійського математика.

У відповіді до Г. Ляйбніца, датованій 24 жовтня 1677 року, І. Ньютон написав:

> *Насправді основні операції достатньо очевидні. Я не можу пояснити їх зараз; замість цього вважаю доцільним, приховати це так:*
>
> `6accdae13eff7i3l9n4o4qrr4s8t12ux`
>
> *На підставі цих операцій я намагався спростити теорію щодо квадратури кривих й зміг отримати декілька загальних результатів.*

В цьому листі Ньютон закодував свій метод дослідження функцій, який ми називаємо зараз *основною теоремою аналіза*. Закодованим був текст латиною:

```
Data aequatione quotcunque fluentes quantitates involvente,
fluxiones invenire; et vice versa
```

який можна наступним чином перекласти українською, якщо вживати сучасні математичні терміни:

`Маючи функцію, знайти її похідну і навпаки`

Ньютон застосував наступний підхід при шифруванні: в тексті латиною він підрахував кількість входжень окремих букв та їхніх сполучень і вказав це у зашифрованому тексті. Наприклад, `6a` на початку шифрованого тексту означає, що буква `a` зустрічається шість разів.

Важко сказати чи легко відновити справжній текст за інформацією, наданою Ньютоном. Настільки ж важко стверджувати напевно, чи дійсно розшифрований текст допомагає зрозуміти зміст операцій, про які писав Ньютон.

У липні 1678 року, Ляйбніц надіслав у відповідь ще одного листа Ньютону, у якому досить ясно і відкрито виклав свій метод з іншими позначеннями та назвами операцій. Зараз ми визнаємо, що обидва методи є еквівалентними.

Між Ньютоном та Ляйбніцем виникла суперечка відносно пріоритету у відкритті диференціального та інтегрального числення. Багато математиків з Англії на боці Ньютона і математиків з континентальної Європи на боці Ляйбніца долучились до суперечки.

Мабуть Ньютон приховував свій головний результат для того, щоб Ляйбніц не зміг, змінивши формулювання, приписати його собі. Підозри Ньютона могли грунтуватись на тій підставі, що Ляйбніц під час візиту до Лондона мав змогу ознайомитись з роботою Ньютона, яка з'явилась у 1669 році. Таке недалекоглядне ставлення не принесло Ньютону одноосібної слави відкриття, якої він так бажав. Ляйбніц виявився здатним дійти до усього самотужки і раніше за Ньютона почав популяризувати свої результати.

За іронією долі, зараз цей результат ми називаємо також *теоремою Ньютона–Ляйбніца*, поєднуючи імена цих геніальних вчених та антагоністів, з спілкування яких (хоча і не дуже приязненого) почалася нова ера у математичному аналізу.

2.1. Математичні шифри. До *математичних шифрів* відносяться такі, які використовують математичні формули для перетворення текстової інформації. Будь-який шифр починається з перетворення букв на числа, цей крок ми називаємо *кодуванням*. В залежності від складності шифру ці числа можуть перетворюватись і далі за допомогою спеціальних математичних алгоритмів. Чи можна зрозуміти принцип, за яким букви українського алфавіту перетворені на числа у наступній таблиці?

Таблиця 1. Загадковий принцип перетворення

А	Б	В	Г	Ґ	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П
2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71

Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
73	79	83	89	97	101	103	107	109	113	127	131	137

Можливо принцип перетворення стане зрозумілим, якщо придивитись до таблиці 2 на стор. 10, де наведено перші 50 простих чисел? ①

Якщо зупинитись на перетворенні букв, наведеному у таблиці 1, і не вживати додаткових математичних формул, то все рівно можна шифрувати будь-яке повідомлення, на-

приклад

У Р А ⟶ 89 73 2

Т а б л и ц я 2. Перші п'ятдесят простих чисел

2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59
61	67	71	73	79	83	89	97	101	103	107	109	113	127	131	137	139
149	151	157	163	167	173	179	181	191	193	197	199	211	223	227	229	

Якщо ж до таблиці 1 додати математичні перетворення, то "секретність" повідомлення стане більш надійною, наприклад

(1) У Р А ⟶ 89 73 2 ⟶ 183 151 9

Чи легко здогадатись, яким було останнє перетворення? ②

Дешифрування повідомлень є простим завданням, якщо відомою є таблиця відповідності букв і чисел. Більше того, сучасна криптографія не вважає цю задачу складною, навіть якщо таблиця є невідомою.

3. Перевірка числа на простоту

Як можна перевірити чи є дане число n простим? В медичній літературі описано випадок, коли брати-близнюки були здатні визначати без жодного пристрою, навіть без паперу та олівця, чи є назване число простим.* Спосіб, яким вони здійснювали обчислення, ми не знаємо (самі близнюки

*O. Sacs, The man who mistook his wife for a hat and other clinical stories, (1985) Harper & Row, New York

казали, що вони "*бачать*" прості числа), але найпростішим з відомих є наступний алгоритм.

Алгоритм 1. Перевірка числа на простоту

Вхідні дані: натуральне число n;

Вихідні дані: висновок стосовно простоти $n > 2$;

знайти остачу r_2 від ділення n на 2

якщо $r_2 = 0$, то n є складеним числом. STOP.

якщо ж $r_2 \neq 0$, то знайти остачу r_3 від ділення n на 3

якщо $r_3 = 0$, то n є складеним числом. STOP.

якщо ж $r_3 \neq 0$, то знайти остачу r_4 від ділення n на 4

якщо $r_4 = 0$, то n є .....

.....

якщо ж $r_{n-2} \neq 0$, то n є простим числом.

Алгоритм 1 покроково перевіряє подільність n на будь-яке число, менше ніж n. Якщо виявляється, що n ділиться на одне з чисел, то робиться висновок, що n є складеним числом. Останньою у цьому алгоритмі може стати перевірка подільності на $n-2$ (звичайно ж n не ділиться на $n-1$, ③ якщо $n > 2$): якщо остача від ділення n на $n-2$ не дорівнює 0, то алгоритм робить висновок, що n є простим числом.

Неважко здогадатись, що алгоритм 1 можна закінчувати вже на перевірці подільності на $[\sqrt{n}]$. ④ Навіть покращений алгоритм працює надто повільно для великих n.

Задача перевірки натурального числа на простоту є важливою для криптографії, тому пошуки ефективних алгоритмів тривають і досі. Хоча сучасні алгоритми значно перевищують за швидкодією алгоритм 1, їхня ефективність ще потребує подальшого покращення.

В розділі 12 ми познайомимось з кількома методами перевірки натуральних чисел на простоту, в тому числі й з сучасними методами, які спираються не тільки на властивості чисел, але й на певні результати теорії ймовірностей.

4. Решето Ератосфена

Порівняймо складність двох задач:

1. визначити чи є N простим числом;
2. знайти всі прості числа, які не перевищують N.

Яка з них є більш простою? Звичайно ж такою є перша задача, причому здається, що розв'язання другої задачі потребує набагато більше часу. ⑤ Але, якщо для розв'язання задачі 1 використати алгоритм 1, а для розв'язання задачі 2 використати так зване *решето Ератосфена*, то різниця у часі між двома способами буде майже непомітною.

Решето Ератосфена використовують для складання таблиці простих чисел, менших або рівних наперед заданого натурального числа N.

Свою назву "решето" цей метод отримав згідно легенді, за якою Ератосфен записував числа на дощечці, вкритій воском, і проколював дірочки в тих місцях, де були написані складені числа. Тому дощечка ставала подібною до решета, через яке "просівали" всі складені числа, а залишалися тільки числа прості. Ератосфен побудував таблицю простих чисел до 1000.

Алгоритм 2. Решето Ератосфена

Вхідні дані: натуральне число $N \geq 2$;
Вихідні дані: список всіх простих чисел до N;
запишемо числа $1, 2, 3, \ldots, N$ одне за другим;
першим простим числом є $p_1 = 2$;
викреслимо всі числа, кратні p_1, крім p_1;
визначимо перше невикреслене число після p_1;
воно і є другим простим числом $p_2 = 3$;
викреслимо всі числа, кратні p_2, крім p_2;
. . . . . .
визначимо перше невикреслене число після p_{k-1};
воно і є k-им простим числом p_k;
викреслимо всі числа, кратні p_k, крім p_k;
. . . . . .

Ми наводимо алгоритм Ератосфена у сучасній нотації. Замість того, щоб проколювати дірки на місці складених чисел, ми викреслюємо їх. Усі інші деталі цілком узгоджені з ідеєю Ератосфена.

Варто також зазначити, що хоча зараз існують й більш ефективні алгоритми, які краще враховують можливості сучасних комп'ютерів, свого значення решето Ератосфена не втратило й досі.

Зрозуміло, що алгоритм 2 не буде працювати безкінечно, він закінчиться не більше, ніж за N кроків. ⑥ Насправді ж він закінчиться не більше, ніж за $\sqrt{N}$ кроків. ⑦

Для прискорення роботи, можна скористатись наступним зауваженням: якщо на якомусь кроці визначено просте

число p_k, то процедуру викреслення можна починати з p_k^2, оскільки всі складені числа від p_k+1 до p_k^2-1 вже викреслено на попередніх кроках. ⑧

Зауваження 1. Метод Ератосфена не є ефективним алгоритмом, якщо число N є досить великим. Якщо ж n є доволі помірним числом, то його швидкість є прийнятною. Можна довести, що цей алгоритм потребує $N\log\log N + O(N)$ операцій.

Математики і до цього часу намагаються знайти більш ефективні алгоритми знаходження простих чисел. Розвиток нових способів пов'язано з величиною чисел, які необхідні сучасній криптографії. Для таких чисел обчислення можна здійснити тільки на комп'ютері, але не всі з комп'ютерів здатні це робити: їхні процесори мають бути достатньо потужними, оперативна пам'ять та ємність інших носіїв інформації повинні бути відповідними поставленій задачі.

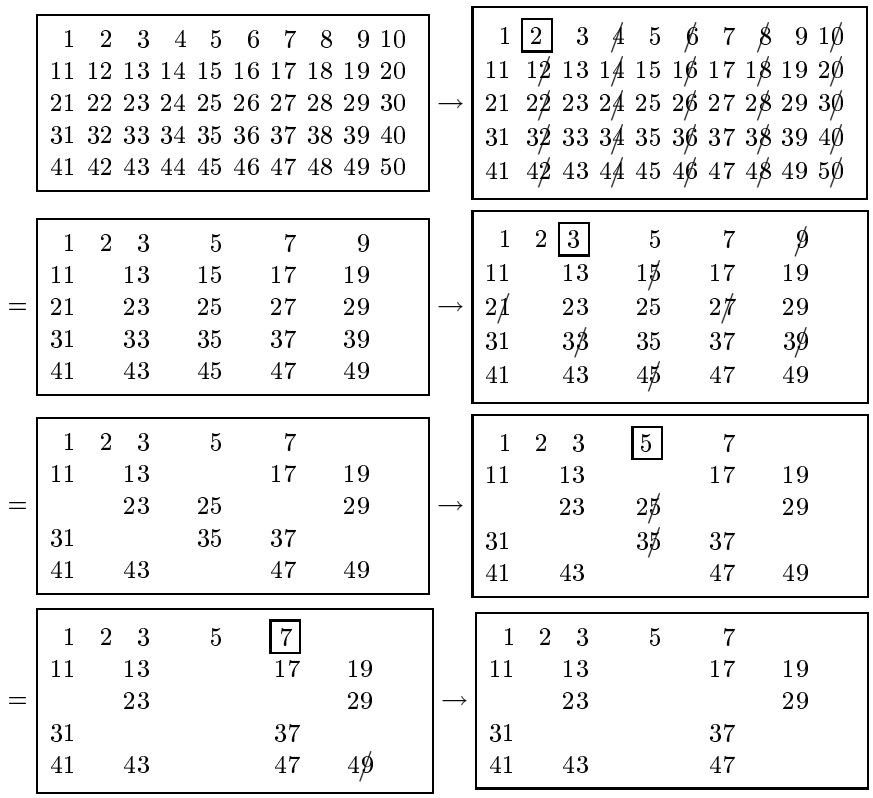
Математики пропонують не тільки покращені комп'ютерні алгоритми. Наведемо одне з тверджень, яке полегшує пошук простих чисел навіть і без комп'ютера.

Твердження 1 (*критерій Ойлера*)**.** *Нехай $N>1$ є непарним числом. Якщо N можна представити у вигляді різниці квадратів двох натуральних чисел єдиним способом, то N є простим. Одним з представлень різницею квадратів є $N=\left(\frac{N+1}{2}\right)^2-\left(\frac{N-1}{2}\right)^2$.* ⑨

Якщо ж таке представлення не є єдиним, то N є складеним

Приклад 1. Нижче показано роботу алгоритму 2 для $N=50$. Всі числа розташовано у матрицях: перша з них містить всі цілі числа від 1 до 50; остання — прості числа від 1 до 50.

Таблиця 3. Решето Ератосфена для $N = 50$



На кожному кроці ми викреслюємо всі числа кратні черговому простому числу, крім нього амого; квадратиком відмічено те просте число, для якого здійснюється викреслення його кратних.

У другій матриці викреслено усі парні числа, крім двійки; результат показано у третій матриці. У четвертій мат-

риці викреслено всі числа, які є кратними 3, крім трійки; результат показано у п'ятій матриці. У шостій матриці викреслено всі числа, які є кратними 5, крім п'ятірки; результат показано у сьомій матриці. У цій же матриці викреслено всі числа, які є кратними 7, крім семірки, (таких залишилось лише одне число 49). Зверніть увагу, що алгоритм Ератосфена завершився за 4 кроки, тобто менше, ніж за $\left[\sqrt{50}\right]$ кроків, як і передбачалось.

Всі числа, що залишились в останній матриці, є простими. Таким чином, простими числами, які не перевищують 50, є

$$2,\ 3,\ 5,\ 7,\ 11,\ 13, 17,\ 19,\ 23, 29,\ 31,\ 37,\ 41,\ 43,\ 47.$$

Таких чисел існує рівно 15.

5. Кілька відомих шифрів

5.1. Шифр перестановки. Так званий *шифр перестановки* або *перестановочний шифр*, відомий принаймні з часів Стародавньої Греції, визначається двома параметрами: натуральним числом n та перестановкою чисел $1, \ldots, n$.

Наприклад, якщо $n = 4$, а перестановкою є $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$, то шифром слова "`кіно`" є "`іонк`". Загальне правило шифрування цим методом таке: якщо перестановочний шифр визначається параметрами n та $\begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$, то першою буквою у шифрі буде буква з номером i_1 у звичайному тексті, другою — i_2-а і так далі.

Замість перестановки можна обрати *ключове слово*, яке визначає перестановку. Наприклад, перестановку $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$

визначає слово "якщо". Загальне правило таке: переставимо букви ключового слова згідно до їхнього порядку в українському алфавіті. Нехай перша буква у цій перестановці має позицію i_1 у початковому слові, друга — i_2, і так далі. Тоді послідовність $i_1, i_2, \ldots, i_n$ визначає перестановку $\begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$.

Якщо необхідно зашифрувати великий текст, то його розбивають на блоки довжини n й до кожного з блоків застосовують перестановочний шифр.

5.2. Рандомізований матричний шифр. Цей шифр визначається двома параметрами: натуральним числом n і перестановкою букв українського алфавіту. Слово "*рандомізований*" у назві цього шифру пояснюється тим, що другий параметр обирається випадковим чином.

Пояснімо процес шифрування на прикладі $n = 6$. Розташуємо букви українського алфавіту у матриці 6×6:

	1	2	3	4	5	6
1	а	б	в	г	ґ	д
2	е	є	ж	з	и	і
3	ї	й	к	л	м	н
4	о	п	р	с	т	у
5	ф	х	ц	ч	ш	щ
6	ь	ю	я			

Оскільки український алфавіт складається з 33 букв, то 3 останні позиції в останньому рядку матриці залишились вільними.

Переставимо тепер букви, враховуючи вільні місця, згідно до другого параметру шифру (перестановки букв алфавіту). Перестановка, яку ми застосували нижче у якості

прикладу, отримується з попередньої матриці розташуванням її рядків у порядку 642135, тобто шостий рядок став першим, четвертий — другим і так далі.

На три вільні позиції необхідно поставити довільні букви; для прикладу ми обрали “е”, “и”, “ї”:

(2)

	1	2	3	4	5	6
1	ь	ю	я			
2	о	п	р	с	т	у
3	е	є	ж	з	и	і
4	а	б	в	г	ґ	д
5	ї	й	к	л	м	н
6	ф	х	ц	ч	ш	щ

→

	1	2	3	4	5	6
1	ь	ю	я	[е]	[и]	[ї]
2	о	п	р	с	т	у
3	е	є	ж	з	и	і
4	а	б	в	г	ґ	д
5	ї	й	к	л	м	н
6	ф	х	ц	ч	ш	щ

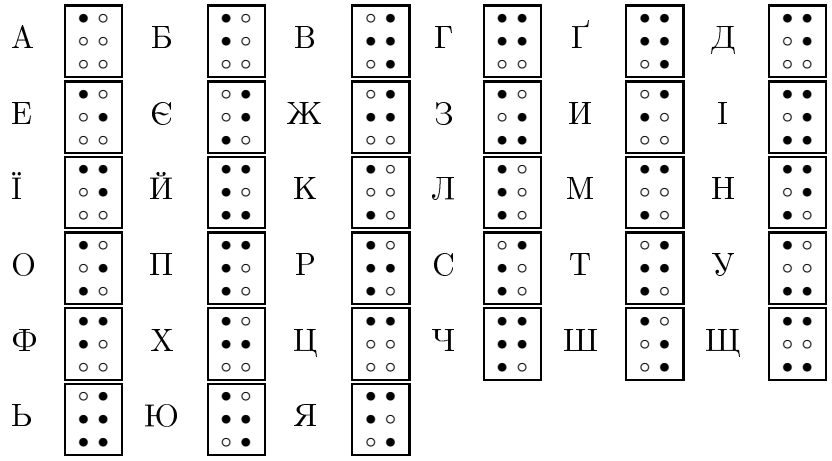
Таким чином, кожній букві алфавіту відповідає пара чисел (номер стовпчика-номер рядка), причому буквам “е”, “и” та “ї” відповідають по дві пари.

При шифруванні кожна буква замінюється відповідною парою чисел, причому пари для “е”, “и”, “ї” чергуються.

5.3. Азбука Брайля. Азбука Брайля — рельєфно-крапковий шрифт для написання і читання сліпими, розроблений французом Луїсом Брайлем (1829 р.). У віці трьох років Л. Брайль осліп, але, коли став дорослим, зміг викладати музику для сліпих. Саме для цих занять він розробив оригінальний спосіб кодування інформації.

В основі шрифту (в тому числі й для музичної нотації) лежить комбінація шести опуклих/увігнутих крапок, що використовується і дотепер в усьому світі. У таблиці, наведеній нижче, символом • позначено опуклі точки, а символом ∘ — увігнуті. Одна і та ж комбінація опуклих та увігнутих символів означає зовсім різне для різних мов. Нижче ми наводимо таблицю для українського алфавіту.

Шрифт Брайля для українського алфавіту



5.4. Азбука Морзе. *Азбука Морзе* — спосіб кодування букв, названий за ім'ям його розробника, американського інженера Семюела Морзе (1838 р.). За цим способом букви (знаки) кодуються за допомогою комбінацій коротких (крапок) і довгих (тире) імпульсів. За одиницю часу приймається тривалість передачі однієї точки. Тривалість тире дорівнює трьом точкам. Пауза між елементами одного знака дорівнює одній точці, між знаками в слові — 3 точки, між словами — 7 точок. Радист середньої кваліфікації передає 60–100 знаків на хвилину. Найкращі радисти у змозі передати 220–260 знаків за хвилину.

Першу провідну лінію для передачі повідомлень довжиною 61 км між містами Вашингтон та Балтимор у США було офіційно відкрито 2 травня 1844 року. Першою фразою, переданою проводами, була "*What hath God wrought*",

що є архаїчною цитатою з Біблії (відповідає виразу "*what has God created*" у сучасній англійській мові).

Наведемо азбуку Морзе для українського алфавіту.

Азбука Морзе для українського алфавіту

А ·−	Б −···	В ·−−	Г −−·	Ґ −−··
Д −··	Е ·	Є ··−··	Ж ···−	З −−··
И −·	І ··	Ї ·−−··	Й ·−−−	К −·−
Л ·−··	М −−	Н −·	О −−−	П ·−−·
Р ·−·	С ···	Т −	У ··−	Ф ··−·
Х −−−−	Ц −·−·	Ч −−−·	Ш −−·−	Щ −−·−−
Ь −··−	Ю ··−−	Я ·−·−		

Існує спеціальний сигнал SOS ...---... (три крапки, три тире, три крапки), який має однакове значення на всіх мовах. Сигнал SOS забороняється подавати, якщо немає неминучої загрози для життя людей або судна на морі.

6. Контрольні питання

1. Поясніть принцип, за яким букви у таблиці 1 перетворюються у числа. (стор. 9).

2. Довести, що перевореннням у формулі (1) є $2x + 5$ (стор. 10).

3. Чому n не ділиться на $n - 1$ для жодного $n > 2$? (стор. 11).

4. Чому алгоритм 1 можна закінчувати вже на перевірці подільності на $\lfloor\sqrt{n}\rfloor$? (стор. 11).

5. Пояснити чому здається правильним, що розв'язання другої задачі потребує набагато більше часу, ніж розв'язання першої задачі у розділі 4? (стор. 12).

6. Пояснити, чому алгоритм 2 закінчиться не більше, ніж за N кроків? (стор. 13).

7. Пояснити, чому алгоритм 2 насправді закінчиться не більше, ніж за $\sqrt{N}$ кроків? (стор. 13).

8. Чому всі складені числа від $p_k + 1$ до $p_k^2 - 1$ вже викреслено на попередніх кроках алгоритму 2? (стор. 13).

9. Перевірити представлення у твердженні 1. (стор. 14).

7. З А Д А Ч І

Задача 1. *Текст, який наведено нижче, зашифровано за допомогою так званого книжкового шифру*:

```
0408 0453 1020 1038 1101 0602 0150 0217 0636 0208 1306 0950
0421 0637 1110 0913 0708 0204 0404 1217 0708 0216 1107 0842
```

Кожне кодове слово складається з двох двозначних чисел. Перше з них вказує на рядок у іншому тексті, а друге — на стовпчик там же. На перетині рядка та стовпчика у тому тексті знаходимо символ оригінального повідомлення. Розшифрувати повідомлення, якщо іншим текстом є початок цієї лекції на сторінці 1.

Задача 2. *У книзі рекордів Гінесса написано, що найбільшим відомим простим числом є* $23021^{377} - 1$. *Довести, що*

a) *це є помилкою*;
b) *вказане число ділиться на 10.*

Задача 3. *Л. Ойлер, геніальний математик XVIII сторіччя, вважав, що значеннями полінома* $P_-(x) = x^2 - x + 41$ *при всіх натуральних* x *є прості числа.*

a) *перевірити його гіпотезу для* $x = 1, 2, \ldots, 15$ (*використати решето Ератосфена* 16×16).
b) *чи вірною є гіпотеза Ойлера?* Вказівка. Обрати $x = 41$.

Задача 4. *Нехай* $P_+(x) = x^2 + x + 41$.

a) *перевірити, що* $P_+(x)$ *є простим числом для* $x = 1, 2, \ldots, 15$;
b) *довести, що серед значень* $P_+(x)$, $x = 1, 2, \ldots$, *зустрічаються складені числа.*

Задача 5. *Нехай* p — *просте число. Довести, що*

a) *обидва числа* $p - 1$ *та* $p + 1$ *є парними, якщо* $p > 2$;
b) *одне з чисел* $p - 1$ *або* $p + 1$ *ділиться на* 3, *якщо* $p > 3$.

Задача 6. *Нехай $p \geq 5$ — просте число. Довести, що або $p = 6k+1$, або $p = 6k-1$ для деякого натурального k.*

Задача 7. *Нехай $p \geq 3$ — просте число. Довести, що*

a) *одне з чисел $p-1$ або $p+1$ ділиться на 4;*
b) *невірним є твердження, що одне з чисел $p-1$ або $p+1$ ділиться на 5.*

Задача 8. *Записати слово* `МОРЗЕ` *за допомогою азбуки Морзе.*

Задача 9. *Записати слово* `БРАЙЛЬ` *за допомогою шифра Брайля.*

Задача 10. a) *Скільки існує перестановочних шифрів для фіксованого параметру n?*

b) *Яким чином дешифруються повідомлення у випадку шифру перестановки?*

c) *Дешифрувати секретне повідомлення*

`емічпо ␣урнка низї␣␣утофбл ␣␣␣у␣␣`

якщо ключовим словом є "`динамо`*".*

Задача 11. a) *Скільки існує рандомізованих матричних шифрів з параметром n?*

b) *Дешифрувати секретне повідомлення*

```
55 41 25 23 35 64 56 35 52 65 35 61 23
```

якщо другий параметр шифру визначається перестановкою (2) *на стор. 18.*

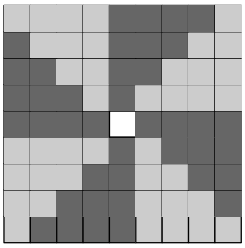
Задача 12. *Число*

$$t_n = \sum_{i=1}^{n} i, \qquad n \geq 1,$$

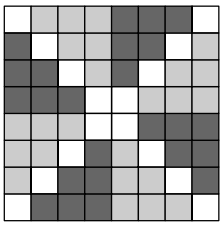
називається n-им трикутним числом.

a) *Пояснити цю назву геометрично.*
b) *Довести рекурентну формулу: $t_n = t_{n-1} + n$, $n \geq 2$.*
c) *Знайти простий вираз для t_n.*

Задача 13. *Пояснити наступне ілюстративне доведення формул Діофанта. Довести їх у загальному випадку*:



$8t_n + 1 = (2n+1)^2$



$8t_{n-1} + 4n = (2n)^2$

Задача 14. *Нехай*

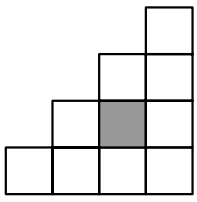
$$s_n = 1,$$
$$s_n = s_{n-1} + 2n - 1, \qquad n \geq 2.$$

Число s_n називається n-м квадратним числом.

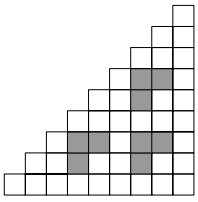
a) *Пояснити назву геометрично.*
b) *Знайти просту формулу для s_n.*

Задача 15. *В 1775 році Л. Ойлер довів, що якщо n є трикутним числом, то $9n+1$, $25n+3$ та $49n+6$ також є трикутними числами. Перевірити це.*

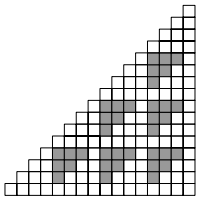
Задача 16. *Нижче наведено ілюстрацію до доведення властивості трикутних чисел для чотирьох значень n. Знайти формулу, яка описує цю властивість, і довести її у загальному випадку.*



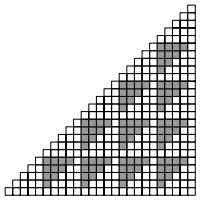
$t_1^2 + t_2^2 = t_4$



$t_2^2 + t_3^2 = t_9$



$t_3^2 + t_4^2 = t_{16}$



$t_4^2 + t_5^2 = t_{25}$

Задача 17. *Довести, що існує* $\left[\frac{a}{b}\right]$ *натуральних чисел, які не перевищують* a *і діляться на* b.

Задача 18. *Високосний рік — це такий, кількість днів у якому становить* 366 *— на одну добу більше, ніж у звичайному (невисокосному) році. У такий рік місяць лютий має не* 28, *а* 29 *днів. Високосні роки визначаються за наступним правилом: рік є високосним, якщо з нього починається сторіччя і його порядковий номер ділиться на* 400, *або з нього сторіччя не починається, але його порядковий номер ділиться на* 4. *Скільки високосних років до* 2016 *було після* 1600?

Задача 19. *У древньому Єгипті використовували своєрідний метод множення чисел, який ми продемонструємо на прикладі множення* 23 *на* 45. *Перш за все, запишемо перше з цих чисел у вигляді суми степенів двійки:* $23 = 1 + 2 + 4 + 16 = 2^0 + 2^1 + 2^2 + 2^4$. *Тоді*

$$23 \cdot 45 = 1 \cdot 45 + 2 \cdot 45 + 4 \cdot 45 + 16 \cdot 45.$$

Тепер побудуємо таблицю:

1	2	4	8	16
45✓	90✓	180✓	360	720✓

Перший рядок містить всі степені двійки, які не перевищують 23; *елементи другого дорівнюють добутку* 45 *та відповідного степеня двійки у тому ж стовпчику (легше обчислювати, якщо помітити, що кожний наступний елемент це подвоєний попередній). Знаком* ✓ *відмічено ті елементи другого стовпчика, які відповідають двійковому розкладу* 23. *Потрібний результат дорівнює сумі елементів з символом* ✓:

$$23 \cdot 45 = 45 + 90 + 180 + 720 = 1035.$$

Використовуючи єгипетський метод множення, перемножити 25 *та* 33.

Задача 20. *Так званий "селянський" метод множення двох чисел схожий на египетський. Для ілюстрації цього методу перемножимо* 24 *та* 43. *Спочатку складемо таблицю*:

24	12	6	3	1
43	86	172	344✓	688✓

Перший її рядок починається з 24, *а кожний наступний елемент є часткою від ділення попереднього на* 2. *Другий рядок починається з* 43, *а кожний наступний елемент вдвічи більший за попередній. Ми позначили знаком* ✓ *ті елементи другого рядка, які відповідають непарним числам у першому рядку. Результат множення є сума елементів з символом* ✓:

$$24 \cdot 43 = 344 + 688 = 1032.$$

Довести "селянський" метод множення натуральних чисел.

Задача 21. *Нескладно підрахувати, що* $123 \cdot 7 \cdot 11 \cdot 13 = 123123$. *Довести, що* $(abc)_{10} \cdot 7 \cdot 11 \cdot 13 = (abcabc)_{10}$, *де* a, b, c *— довільні цифри, а* $(xyz\dots)_{10}$ *означає десяткове число, складене з цифр* $x, y, z, \dots$.

Задача 22. *Репьюнітом* (*repeated unit*, *англ.*) *називається число, всі десяткові цифри якого дорівнюють одиниці. Якщо репюніт складається з* n *одиниць, то він позначається* R_n. *Довести, що якщо* R_n *є простим, то* n *також є простим.*

Задача 23. *Нехай* n *є простим числом. Чи обов'язково репюніт* R_n (*див. задачу* 22) *є простим*?

Задача 24. *Довести, що сума двух послідовних непарних чисел є добутком принаймні трьох* (*не обов'язково різних*) *простих чисел.*

Задача 25. *Довести, що квадрат будь-якого непарного числа* $n > 1$ *можна записати у вигляді* $8m+1$ *для деякого натурального числа* m.

Задача 26. *Числами Фібоначчі називають члени послідовності* $F_1 = 1$, $F_2 = 1$,

$$F_n = F_{n-1} + F_{n-2}, \qquad n \geq 3.$$

Довести, що F_n *є парним тоді і тільки тоді, коли* n *ділиться на* 3.

Задача 27. *Нехай* $\{F_n\}$ *— це послідовність чисел Фібоначчі (задача* 26*). Знайти* $\sum_{i=1}^{n} F_i$.

Задача 28. *Довести, що якщо* $2^m - 1$ *є простим, то й* m *є простим.*

Задача 29. *Числами Ферма називають члени послідовності*

$$f_n = 2^{2^n} + 1, \qquad n \geq 1.$$

Довести, що

$$f_n = f_{n-1}^2 - 2f_{n-1} + 2, \qquad n \geq 2.$$

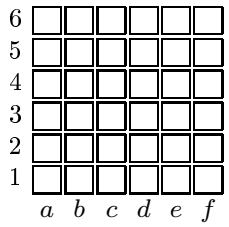
Задача 30. *Нехай* $\{f_n\}$ *— це послідовність чисел Ферма (задача* 29*). Нескладно підрахувати, що* $f_2 = 17$, $f_3 = 257$, $f_4 = 65537$. *Можна також продовжити цей ланцюжок*:

$$f_5 = 4294967297, \qquad f_6 = 18446644033331951617.$$

Таким чином, кожне число Ферма F_n, $2 \leq n \leq 6$, *закінчується на* 7. *Довести це твердження для всіх* $n \geq 2$ (*використайте задачу* 29).

Задача 31. *Довести, що* C_{2n}^n *є парним числом.*

Задача 32 (Ю. Б. Чураченко)**.** *У кожній горизонталі та в кожній вертикалі квадрата* 6×6



розмістити числа $1, 2, 3, 4, 5, 6$ *так, щоб для чисел із відповідними координатами одночасно виконувались десять рівностей*:

$$d_4 + e_4 = 4, \qquad a_3 + b_3 = 6, \qquad b_5 + c_5 = 6, \qquad e_5 + f_5 = 6$$
$$a_1 + a_2 + a_3 = 7, \qquad c_1 + d_1 + e_1 = 8, \qquad a_6 + b_6 + c_6 = 9,$$
$$f_1 + f_2 + f_3 = 9, \qquad b_3 + b_4 + b_5 = 10, \qquad e_4 + e_5 + e_6 = 12.$$

8. БІОГРАФІЇ

Харді, *Ґодфрі Ґарольд* (1877–1947), англійський математик, відомий своїми досягненнями в теорії чисел і математичному аналізі.

Ґ. Харді у 1890-х роках

Ґ. Харді у 1930-х роках

Неабиякий математичний хист Харді був помітним ще в дитинстві. Йому виповнилося всього два роки, а він вже міг записати числа до мільйонів, а коли його брали до церкви, він розважався тим, що розкладав на множники кількість церковних гімнів. Під час навчання в школі він був найкращим у своєму класі з більшості предметів, і виграв багато призів і нагород, але ненавидів отримувати їх перед усією школою.

З 1906 р. він обіймав посаду лектора в університеті Кембриджа, на якій викладання займало шість годин на тиждень, що залишило йому достатньо часу на дослідження. Харді приписують реформування британської математики шляхом впровадження в ній строгості, яка раніше була характерна для французької, швейцарської та німецької математики.

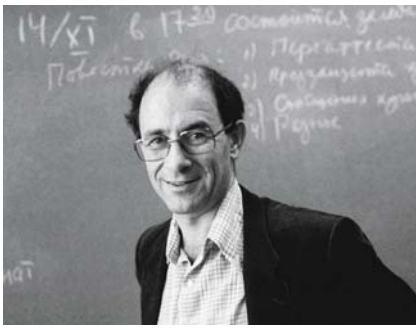
Багато працював разом з Джоном Літльвудом та Срінівасою Рамануджаном. Результати у математичному аналізі, отримані разом з Літльвудом, вразили відомого данського математикп Ґаральда Бора

настільки, що він якось афористично висловився: "*Сьогодні є тільки три дійсно великих англійських математики*: *Харді*, *Літльвуд і Харді–Літльвуд*."

Сам Харді високо цінував результати з теорії чисел, отримані ним разом з індійським самородком Рамануджаном, який формально не мав університетської освіти. Якось Харді сказав, що найвищим досягненням його життя було відкриття Рамануджана.

"*Індійський клерк*" ("*The Indian Clerk*") — роман американського письменника Девіда Лівітта, виданий 2007 р., написано за мотивами життя Харді в Кембриджі.

Арнольд, *Володимир Ігоревич* (1937–2010), російський математик, народився в Одесі, закінчив Московський державний університет.



В. І. Арнольд у 1982 році

Автор робіт у галузі топології, теорії диференціальних рівнянь, теорії особливостей гладких відображень та теоретичної механіки, відомий своїм ясним стилем викладання. Він вмів майстерно комбінувати математичну строгість і фізичну інтуїцію, його стиль викладання був простим і дохідливим. Публікації Арнольда являли собою завжди свіжий і зазвичай геометричний підхід до традиційних розділів математики.

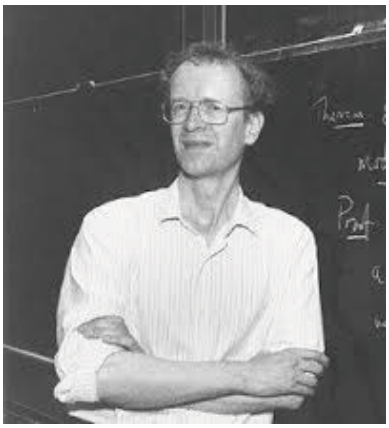
Він був відомим критиком існувавших в середині XX століття спроб створити замкнутий виклад математики в строгій аксіоматичної формі з високим рівнем абстракції.

Він довів (1956), що довільна неперервна функція є композицією скінченої кількості неперервних функцій однієї або двох змінних, що розв'язувало 13-ту проблему Гильберта в одній з можливих її інтерпретацій (сам Арнольд вважав, що основний внесок у доведення належить його вчителю А. М. Колмогорову, а сам він лише уточнив результати Колмогорова). Він є (1963) співатором теореми Колмогорова–Арнольда–Мозера про стабільність інтегрованих гамільтонових систем, яку довів ще на початку своєї кар'єри математика.

Неодноразово підкреслював, що математична освіта у країнах з екс-СРСР залишається на більш високому рівні, ніж на заході, а студенти є більш мотивованими і підготовленими, проте

> "... *В усьому світі катастрофічно падає рівень освіти. Приходить нове покоління дітей, які нічого не знають: ані таблиці множення, ані евклідової геометрії — нічого не знають, не розуміють і не хочуть знати. Вони тільки хочуть натискати на кнопки комп'ютера, і більше нічого. Що робити, як тут бути?*"

Вайлс, *Ендрю Джон* (нар. 1953 р.), англійський та американський математик, професор математики Принстонського університету.



Ендрю Вайлс

Одною з головних подій у його кар'єрі стало доведення *великої теореми Ферма*, про яку він дізнався у віці десяти років. Тоді він зробив першу спробу довести її, використовуючи методи зі шкільного підручника; природньо, що у нього нічого не вийшло.

В 1986 році він повернувся до доведення великої теореми Ферма, якій присвячував майже весь час протягом 6 років в майже повній секретності. У 1993 році він публічно представив своє доведення, але трохи згодом у ньому було виявлено недолік.

Протягом усього наступного року Уайлс безуспішно намагався усунути недолік. 19 вересня 1994 року, коли він був вже готовий визнати поразку, йому вдалося досягти своєї мети. Разом зі своїм колишнім студентом Річардом Тейлором він опублікував статтю, у якій було пояснено, як можна усунути недолік, помічений у його першому доведенні. Таким чином, велику теорему Ферма було доведено.

Ферма, *П'єр* (1601–1665), французький математик, засновник аналітичної геометрії, математичного аналізу, теорії ймовірностей та алгебраїчної теорії чисел. П'єр де Ферма — одна з найзагадковіших постатей у науковому світі XVII століття.

П'єр Ферма

Досягнення Ферма у математиці є багаточисельні та фундаментальні, хоча математикою він займався лише у вільний час, який знаходив у перервах між засіданнями у суді, де він обіймав посаду судді.

В аналітичній геометрії раніше від Декарта і більш систематизовано він ввів метод координат із його застосуваннями до рівнянь прямої та кривих 2-го порядку. Є одним із засновників математичного аналізу, де першим почав оперувати поняттям змінної величини, встановив правило диференціювання та інтегрування степеня з довільними показниками, вивів формулу інтегрування частинами, з'ясував методи знаходження екстремуму функцій.

Ферма разом з Паскалем були першотворцями математичної теорії ймовірностей.

Він ніколи не публікував результати своїх досліджень у наукових журналах, оскільки тоді вони не існували. Майже все, що ми знаємо про його творчий доробок, міститься у його листах до видатних математиків того часу. Як було прийнято у ті часи, листи Ферма не містять доведень, а лише формулювання результатів. Винятком стала велика теорема Ферма, доведення часткового випадку якої (для $n = 4$) було пізніше знайдено у його паперах:

> *якщо* $n > 2$, *то рівняння* $x^n + y^n = z^n$ *відносно невідомих* x, y, z *не має такого розв'язку, що кожне з цих трьох чисел є натуральним.*

Згодом він написав на полях книги Евкліда, що має доведення цього результату, але " ... *навести його не можу, оскільки воно потребує більше місця, ніж дозволяють поля цієї книги ... воно випливає з багатьох різноманітних і таємничих властивостей чисел ...* "

Після Ферма доведення його теореми безуспішно шукали сотні найвидатніших математиків світу аж до наших днів. Магія великої теореми Ферма у зовнішній простоті її формулювання, яка уже більше трьохсот років породжувала нав'язливу ідею фікс — довести цей результат. Саме через цю таємничо-зрадливу простоту позбулися спокою тисячі і тисячі аматорів. У місті Дортмунд (Німеччина) зараз функціонує Музей доведень великої теореми Ферма.

Визнане всім науковим світом доведення великої теореми Ферма здійснено нарешті у 1994 році Ендрю Вайлсом.

Ератосфен, *грец.* $Ερατοσθενης$ (бл. 275–194 до Р. Х.), давньогрецький вчений і письменник. Серед математичних творів Ератосфена

виділяється твір "*Платоники*", свого роду коментар до діалогу "*Тімей*" Платона, у якому розглядалися питання з математики і музики.

Ератосфен

У "*Платониках*" Ератосфен звертається до математичних і музичних основ платонівської філософії. Вихідним пунктом було так зване делійське питання, тобто подвоєння куба, якому автор присвятив трактат "*Подвоєння куба*".* Ератосфен запропонував один з розв'язків цієї задачі, в якому використовується спеціальний механічний інструмент — мезолябія.

Геометричний зміст мав його твір "*Про середні величини*" у 2 частинах, присвячений розв'язуванню геометричних та арифметичних задач. Широко відомий інший його трактат "*Решето*". В ньому вчений виклав спрощену методику визначення простих чисел. (так зване "решето Ератосфена").

**Подвоєння куба* — класична антична задача на побудову циркулем та лінійкою ребра куба, об'єм якого вдвічі більший за об'єм заданого куба. Згідно з античною легендою, одного разу на острові Делос почалася епідемія чуми. Мешканці острова звернулись до дельфійського оракула, і той повідомив, що необхідно подвоїти жертовне святилище, яке мало форму куба. Мешканці Делоса спорудили ще один такий же куб та поставили його на перший, але епідемія не припинилася. Після повторного звернення оракул роз'яснив, що подвоєний жертовник також повинен мати форму куба.

Ляйбніц, *Ґотфрід Вільгельм* (1646–1716), видатний німецький математик, логік, філософ. Незалежно від Ньютона створив диференціальне й інтегральне числення; заклав основи двійкової системи числення.

Ґ. В. Ляйбніц

У 1675 році Лейбніц опублікував головні результати свого відкриття стосовно інтегрального та диференціального числення, випередивши Ньютона, який ще раніше прийшов до схожих результатів і писав про них Лейбніцу у приватному листуванні. Лейбніц виклав свої дослідження з математичного аналізу у декількох мемуарах, починаючи з 1684 р. Зокрема, його перший мемуар містить нотацію dx для диференціалу і правила для діференціювання добутків, часток і степенів. Він ввів позначення $\int$ для інтегралу і вказав, що ця операція обернена диференціюванню. Хоча Ньютон зневажливо поставився до результатів Ляйбніца, зауваживши, що в них " ... *не розв'язане жодне попередньо відкрите питання* ... ", ідеї Лейбніца та його нотація мали набагато більший вплив на розвиток математичного аналізу протягом наступного століття, особливо на континенті.

Ляйбніц відомий також своїми численними винаходами, зокрема він створив механічний калькулятор (арифмометр), який міг виконувати додавання, віднімання, множення і ділення чисел, а також добування коренів і піднесення до степеня. Спеціально для своєї машини Лейбніц застосував двійкову систему числення.

На прохання Петра I розробив проекти розвитку освіти і державного керування в Російській імперії.

Ньютон, *Ісаак* (1642–1727), англійський учений, який заклав основи сучасного природознавства, творець класичної фізики та один із засновників числення нескінченно малих.

І. Ньютон

Його математичні дослідження почалися ще під час навчання в університеті із узагальнення біному на випадок раціональних показників, що привело його до числових рядів. Згодом Ньютон зміг перетворити цей метод у теорію, яку зараз називають інтегральним та диференціальним численням. Похідні функцій Ньютон позначав $\dot{x}$, $\ddot{y}$, ... й називав їх *флюксіями*. Змінні величини він називав *флюентами*.

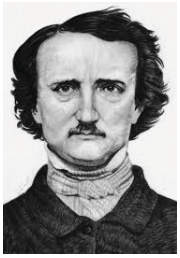
Ньютону належить також ідея використання похідних для знаходження кореня нелінійного рівняння, яка є вагомим внеском у чисельний аналіз. Запропонований ним метод називають методом дотичних або методом Ньютона.

Найвидатнішими його творами вважаються "*Математичні начала натуральної філософії*" (1687) та "*Оптика*" (1704).

Він є автором закону всесвітнього тяжіння. Загальновідомою є легенда про те, що закон тяжіння Ньютон відкрив, спостерігаючи падіння яблука з гілки дерева. Легенда стала популярною завдяки Вольтеру, хоча з його записів зрозуміло, що він поступово наближався до цієї ідеї.

На честь Ісаака Ньютона названо одиницю сили в Міжнародній системі одиниць — *ньютон*. Він був першим в Англії, кого висвятили в лицарі за наукові заслуги.

Конан Дойль, *Артур* (1859–1930), англійський письменник, відомий насамперед своїми творами про Шерлока Холмса. Крім детективних романів про Шерлока Холмса, відомими є його науково-фантастичні про професора Челленджера, а також історичні романи. Крім того, він писав п'єси та вірші. "Скандал у Богемії", перше оповідання із серії "Пригоди Шерлока Холмса", було надруковано 1891 року. Прототипом головного героя, котрий став невдовзі легендарним детективом-консультантом, був Дж. Белл, професор Единбурзького університету, який славився здатністю по найдрібніших деталях вгадувати характер і минуле людини. Протягом двох років Дойль створював розповідь за розповіддю, і врешті-решт почав перейматися власним персонажем. Його спроба "покінчити" з Холмсом у сутичці з професором Моріарті ("Остання справа Холмса", 1893 рік) виявилася невдалою: він полюбився читачам і героя довелося "воскресити". Холмсовська епопея увінчалася романом "Собака Баскервілів" (1900), який відносять до класики детективного жанру.



По, *Едгар Аллан* (1809–1849), американський письменник, поет, есеїст, драматург, літературний редактор і критик, один із провідних представників американського романтизму. Оповідання "Золотий жук" є одним з ранніх зразків детективного жанру. Як редактор однієї з газет, По у своїй рубриці просив читачів надсилати йому зашифровані тексти, які він пропонував іншим читачам. Він обіцяв розшифрувати будь-який текст і опублікувати його у наступному випуску газети. Один з текстів, який По не зміг розшифрувати, було розгадано тільки у 2000 (!) році. Метод дешифрації спирався на поліалфавітний підстановочний шифр, який використовув шість різних символів для кожної буква англійського алфавіту.

В 1841 році По написал кілька статей по криптографії з назвою "Кілька слів про секретне письмо". В цих статтях По розповідав про найпростіші підстановочні шифри, які використовують ключову фразу. Саме цей спосіб шифрування він кілька разів вживав у своїх творах

Верн, *Жуль* (1828–1905), відомий французький письменник; разом з Г. Уеллсом вважається засновником жанру наукової фантастики. Однією з найвідоміших є його трилогія "20 000 льє під водою", "Таємничий острів" і "Діти капітана Гранта", об'єднана спільними героями. Один з них — капітан Немо — спочатку був задуманий як польський революціонер, що шукав можливостей помститися Росії після жорстокого придушення польського повстання 1863 року. Пізніше Верн перетворив його в бунделкхандського принца Даккар.

Немо у романах Верна подорожував під водою у спеціальному підводному човні, який пересувався під дією електричних сил. На час створення роману нічого подібного не існувало у жодній країні світу! Перший електричний підводний човен, побудований у 1886 році двома англійцями, було названо "Наутілусом" на честь вернівського судна. Перший атомний підводний човен, спущений на воду в 1955, також називався "Наутілус".

Не маючи освіти вченого, Верн проводив більшу частину свого часу у дослідженнях для своїх творів та намагався бути реалістичним і дотримуватися фактів у деталях. Із 108 наукових передбачень письменника-провидця на сьогодні не справдилось лише 10!

Глава 2

ШИФР ЦЕЗАРЯ

Шифрування використовують у тих випадках, коли потрібно зберегти певну інформацію в секреті від інших осіб. Відомі і інші способи захисту інформації. Наприклад, текст, написаний на на поштовій картці, може прочитати будь-хто, але якщо вкласти картку у конверт, то можна сподіватись на певну захищеність своєї інформації. Зрозуміло, що цей спосіб збереження інформації не є надійним.

Засоби приховування самого факту існування таємного повідомлення вивчає *стеганографія*. До засобів, які вивчає стеганографія, належать *невидиме чорнило* або *цифрові водяні знаки*. Методи стеганографії використовують й шахраї. Наприклад, відомий грецький мультиміліонер Аристотель Онассіс кілька контрактів підписав ручкою з симпатичним чорнилом, що згодом зникало.

Ще один спосіб стеганографії називається *мікрокрапки*: повідомлення записується на дуже маленький носій (мікрокрапку), який пересилається під маркою або в іншому зумовленому місці на конверті.

Оригінальний спосіб приховування інформації використовувся під час першої світової війни: написаний на оболонці курячого яйця текст зникає, якщо яйце вкинути в окріп. В той же час, чорнила проходять скрізь пори оболонки й утворюють копію текста на звареному білку.

У сучасному світі засоби стеганографії застосовують лише у комбінації з використанням математичних методів за-

безпечення конфіденційності та автентичності інформації. Наука, яка вивчає ці методи, називається *криптографією*.

1. Код клавіатури

Один з способів кодування широко використовується в наш час і полягає у наступному. Запишемо у рядок всі букви українського алфавіту. У другому рядку запишемо букви, які отримуються послідовним натисканням клавіш клавіатури. Отримаємо наступну таблицю:

Таблиця 1. Шифр клавіатури

А	Б	В	Г	Ґ	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
Й	Ц	У	К	Е	Н	Г	Ш	Щ	З	Х	Ї	Ф	І	В	А	П	Р	О	Л	Д	Ж	Є	Ґ	Я	Ч	С	М	И	Т	Ь	Б	Ю

Кожній букві з першого рядка поставимо у відповідність букву з другого рядка, що записана під нею. Зауважимо, що коди трьох букв у цій таблиці співпадають з самими буквами.

При шифруванні повідомлення будемо замість справжньої букви писати ту, яка їй відповідає у наведеній таблиці. Наприклад,

ПРИКЛАД ⟶ ЛДХВАЙН

Код клавіатури відносить до так званих *підстановочних шифрів*, серед яких є і шифр Цезаря.

2. Шифр Цезаря

Мабуть найдревнішим серед підстановочних є *шифр Цезаря*. Підстановочні шифри відомі також під назвою *моноалфавітних* або *простої заміни*. Цей шифр характеризується параметром $0 < b \leq 33$, який є натуральним числом. Обмеження зверху пояснюється кількістю букв в українському алфавіті. Смисл цього параметра у наступному: у повідомленні кожна буква замінюється на ту, яка в алфавіті відстоїть від неї на b позицій вправо. Нижче наведено таблицю для шифра Цезаря при $b = 3$ (саме це значення вживав Юлій Цезарь, але для іншого алфавіту!):

Таблиця 2. Шифр Юлія Цезаря

А	Б	В	Г	Ґ	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
Г	Ґ	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я	А	Б	В

Наприклад, за допомогою шифра Цезаря повідомлення ПРИКЛАД перетворюється у повідомлення ТУЙНОГЖ.

Для дешифрування можна використати ту ж таблицю. Алгоритм дешифрування складається з двох дій:

(i) знайти шифр-букву у другому рядку таблиці 2;
(ii) оригінал-буквою буде та, яка стоїть у першому рядку відповідного стовпчика.

Пошук шифр-букви стане простішим, якщо стовпчики таблиці 2 переставити так, щоб букви у другому рядку були розташовані в алфавітному порядку:

Таблиця 3. Таблиця для дешифрування шифру Цезаря

Ь	Ю	Я	А	Б	В	Г	Ґ	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
А	Б	В	Г	Ґ	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я

Тепер нескладно дешифрувати закодоване слово:

$$\text{ТУЙНОГЖ} \longrightarrow \text{ПРИКЛАД}$$

Нескладно вивести правила, які пов'язують між собою рядки таблиць 2 та 3:

(a) другий рядок таблиці 2 є циклічним зсувом першого рядка вліво на 3 позиції;
(b) перший рядок таблиці 2 є циклічним зсувом другого рядка вліво на 30 позицій (або вправо на 3 позиції);
(c) другий рядок таблиці 3 є циклічним зсувом першого рядка вліво на 3 позиції;
(d) перший рядок таблиці 3 є циклічним зсувом другого рядка вправо на 3 позиції (або вліво на 30 позицій). ①

Якщо шифр Цезаря використовується з параметром $0 < b \leq 33$ замість 3, то в усіх правилах 3 необхідно замінити на b, а 30 на $33 - b$.

Варто також відзначити, що шифр Цезаря з $b = 0$ є еквівалентним шифру з $b = 33$. Його можна вживати й для $b < 0$ або $b > 33$, але ці випадки є еквівалентними до вивчених вище. ②

2.1. Використання чисел у шифрі Цезаря. Процес шифрування при використанні шифра Цезаря можна алго-

ритмізувати, якщо використати номер позиції кожної букви. Наведемо номери позицій для букв українського алфавіту.

Таблиця 4. Номери позицій букв українського алфавіту

А	Б	В	Г	Ґ	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
21	22	23	24	25	26	27	28	29	30	31	32	33

Часто нумерацію позицій букв алфавіту починають з 0 і закінчують 32, але ми починаємо з 1 і закінчуємо 33.

Алгоритм шифрування за допомогою шифру Цезаря з $b = 3$ можна представити наступним чином:

$$\begin{aligned} \text{ПРИКЛАД} &\longrightarrow 20\ 21\ 11\ 15\ 16\ 1\ 6 \\ &\qquad \text{перевели у числа} \\ &\longrightarrow 23\ 24\ 14\ 18\ 19\ 4\ 9 \\ &\qquad \text{додали } b{=}3 \\ &\longrightarrow \text{ТУЙНОГЖ} \\ &\qquad \text{перевели у букви} \end{aligned}$$

Цей же алгоритм можна використати і для дешифрування, але з $33 - b$ замість b (у нашому випадку $b = 3$):

$$\begin{aligned} \text{ТУЙНОГЖ} &\longrightarrow 23\ 24\ 14\ 18\ 19\ 4\ 9 \\ &\qquad \text{перевели у числа} \\ &\longrightarrow 53\ 54\ 44\ 48\ 49\ 34\ 39 \\ &\qquad \text{додали } 30 \\ &\longrightarrow 20\ 21\ 11\ 15\ 16\ 1\ 6 \\ &\qquad \text{операція } \mathrm{mod}\,33 \\ &\longrightarrow \text{ПРИКЛАД} \\ &\qquad \text{перевели у букви} \end{aligned} \tag{1}$$

Відмінність між цими двома схемами у тому, що у другій використано додаткову операцію $\bmod 33$:

$$k \bmod 33 = \begin{cases} k, & k \le 33, \\ k - 33, & k > 33. \end{cases} \tag{2}$$

Необхідність цієї операції пояснюється тим, що в алгоритмі (1) після другого кроку з'явились числа, які перевищують кількість букв в алфавіті. Щоб знайти справжню позицію відповідної букви, ми застосовуємо операцію $\bmod 33$.

Зауважимо, що ця ж операція фактично є необхідною і для шифрування за допомогою шифру Цезаря. Наприклад,

ЮЛІЯ $\longrightarrow$ 32 16 12 33
(перевели у числа)
$\longrightarrow$ 35 19 15 36
(додали 3)
$\longrightarrow$ 2 19 15 3
(операція mod 33)
$\longrightarrow$ БОКВ
(перевели у букви)

Операція $k \bmod 33$ — це математичний еквівалент виразу "циклічний зсув на 33".

3. Подільність натуральних чисел

Насправді операція $\bmod 33$, означена в (2), є більш загальною. Означення в (2) спирається на ту властивість, що після зсуву номер позиції не перевищує 66.

Приклад 1. Якщо ми б обрали $b = 34$ у шифрі Цезаря, то буква Я шифрувалась би буквою А. Але правило (2) дало б невірну відповідь $67 \bmod 33 = 34$, що не відповідає жодній букві українського алфавіту. Щоб отримати

вірну відповідь, необхідно застосувати правило (2) ще раз: $34 \mod 33 = 1$.

Розглянемо цю важливу операцію більш детально.

3.1. Ділення з остачею. Будемо позначати через $\mathbf{N}$ множину натуральних чисел, $\mathbf{N} = \{1, 2, 3, \dots\}$, а через $\mathbf{Z}$ — множину цілих чисел, $\mathbf{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$.

Означення 1. Ми кажемо, що ціле число m *ділиться* на ціле число $n \neq 0$, якщо існує $q \in \mathbf{Z}$, для якого $m = qn$.

Якщо m не ділиться на n, то $m = qn + r$ для деяких $q \in \mathbf{Z}$ та $0 < r < n$. Ми доводимо це у наступній теоремі.

Теорема 1. *Нехай $m \in \mathbf{Z}$, $n \in \mathbf{N}$. Тоді знайдуться такі два числа $q \in \mathbf{Z}$ та $0 \leq r < n$, що*

$$m = qn + r.$$

Таке представлення m через n є єдиним.

Доведення. Теорема є вірною для $m = 0$, тому далі розглядаємо випадок $m \neq 0$. ③ Розглянемо множину

$$M = \{x \in \mathbf{Z} : m - nx \geq 0\}.$$

Зрозуміло, що число $-|m|$ належить множині M, ④ причому жоден елемент M не перевищує $|m|$ ⑤. Позначимо через q найбільший елемент множини M і покладемо $r = m - nq$. Оскільки $q \in M$, то $r \geq 0$. ⑥ Якби $r \geq n$, то $q + 1 \in M$, ⑦ що неможливо згідно вибору q. Це доводить існування чисел q та r з потрібними властивостями.

Щоб довести єдиність такого представлення, припустимо, що існує ще одна пара цілих чисел q' та r', для якої

$m = q'n + r'$. Тоді $n(q' - q) = r - r'$. Оскільки $-n < r - r' < n$, ⑧ то $n|q' - q| < n$, звідки $q' = q$ ⑨ і тому $r' = r$. Єдиність також доведено. □

Означення 2. Числа q та r, визначені в теоремі 1, називаються *часткою* та *остачею* від ділення m на n. Зрозуміло, що $r = 0$, якщо m ділиться на n.

Означення 3. Нехай $m \in \mathbf{Z}$, $n \in \mathbf{N}$. Нехай пару q та r означено згідно теоремі 1. Тоді ми позначаємо

$$r = m \pmod{n}.$$

Зауваження 1. Нескладно переконатись, що $k \pmod{33}$ для $1 \leq k < 66$ співпадає з результатом операції (2). ⑩ Також нескладно впевнитись, що в прикладі 1 можна один раз застосувати операцію $k \pmod{33}$ замість того, щоб двічи застосовувати операцію $k \bmod 33$.

Означення 4. Два числа $m_1, m_2 \in \mathbf{Z}$ називаються *конгруентними* за модулем n, якщо $m_1 \pmod{n} = m_2 \pmod{n}$ (іншими словами, якщо остачі від ділення на n є однаковими). В цьому випадку ми пишемо $m_1 \equiv m_2 \pmod{n}$.

4. Властивості конгруенції

Наведемо кілька властивостей конгруенції, які знадобляться у подальшому.

Теорема 2. *Нехай $n \in \mathbf{N}$. Наступні три властивості виконуються для будь-яких $r, s, t \in \mathbf{Z}$.*

Властивість 1. $r \equiv r \pmod{n}$.

Властивість 2. $r \equiv s \pmod{n}$ *тоді і тільки тоді, коли* $s \equiv r \pmod{n}$.

Властивість 3. *Якщо* $r \equiv s \pmod{n}$ *і разом з цим* $s \equiv t \pmod{n}$, *то* $r \equiv t \pmod{n}$.

Ці властивості мають спеціальні назви: властивість 1 називається *відношення рефлексивності*, властивість 2 – *симетричністю*, властивість 3 – *транзитивністю*.

Доведення. Всі три властивості випливають безпосередньо з означення 4. ⑪ □

Зауваження 2. У математичній логіці розглядають булеві функції двох аргументів, тобто такі, які приймають тільки два значення, `true` та `false`, якими б не були їхні аргументи. Нехай $h(i, j)$ довільна булева функція двох аргументів. Вона називається *еквівалентністю*, якщо вона є рефлексивною, симетрично та транзитивною, тобто якщо

(a) $h(i, i) =$`true` для будь-яких i;
(b) якщо $h(i, j) =$`true`, то $h(j, i) =$`true`;
(c) якщо $h(i, j) =$`true` та $h(j, k) =$`true`, то $h(i, k) =$`true`.

Таким чином, теорема 2 стверджує, що операція mod є еквівалентністю.

Теорема 3. *Нехай* $n \in \mathbf{Z}$. *Тоді*

Властивість 4. $n \equiv 0 \pmod{n}$;

Властивість 5. $nq \equiv 0 \pmod{n}$ *для будь-якого* $q \in \mathbf{Z}$.

Доведення. Обидві властивості випливають з означення 4. ⑫ □

Теорема 4 (*арифметичні властивості*)**.** *Припустимо, що* $m_1 \equiv l_1 \pmod{n}$ *та* $m_2 \equiv l_2 \pmod{n}$. *Тоді*

Властивість 6. $m_1 + m_2 \equiv l_1 + l_2 \pmod{n}$;
Властивість 7. $m_1 - m_2 \equiv l_1 - l_2 \pmod{n}$;
Властивість 8. $m_1 m_2 \equiv l_1 l_2 \pmod{n}$.

Доведення. За умовою теореми $m_1 - l_1 \equiv 0 \pmod{n}$, тобто

$$m_1 - l_1 = in \qquad \text{для деякого } i \in \mathbf{Z}.$$

Аналогічно $m_2 - l_2 \equiv 0 \pmod{n}$, тобто $m_2 - l_2 = jn$ для деякого $j \in \mathbf{Z}$. Звідси випливає, що $(m_1 + m_2) - (l_1 + l_2) = (i + j)n$, що є еквівалентним властивості 6.

Властивості 7 та 8 доводяться таким же чином. ⑬ □

5. Найбільший спільний дільник

Означення 5. Нехай $m, n \in \mathbf{Z}$, причому хоча б одне з цих чисел не дорівнює 0. Число $d \in \mathbf{N}$ називається їхнім *найбільшим спільним дільником*, якщо

(1) m ділиться на d та n ділиться на d;
(2) якщо $d' > d$, то або m не ділиться на d', або n не ділиться на d', або обидва не діляться на d'.

Найбільший спільний дільник чисел m та n позначається (m, n). Якщо $(m, n) = 1$, то m та n називаються *взаємно простими числами.*

6. Прості числа та основна теорема арифметики

В цьому розділі наведено доведення теорем 1.1 та 1.2 про канонічне представлення натуральних чисел та нескінченість множини простих чисел.

Число $p \neq 1$ називається *простим*, якщо $(p, n) = 1$ або $(p, n) = p$ для будь-якого $n \in \mathbf{Z}$. Число $p = 1$ не вважається простим. Число, яке не є простим, називається *складеним*.

Приклад 2. Кожне натуральне число n можна записати одним з трьох можливих способів:

1) $n = 3a$, $a \in \mathbf{N}$;
2) $n = 3b + 1$, $b \in \mathbf{N}$;
3) $n = 3c + 2$, $c \in \mathbf{N}$.

В першому випадку $(n, 3) = 3$, а в решті — $(n, 3) = 1$. Тому число 3 є простим.

Зауваження 3. Якщо число p є простим, то воно не ділиться на жодне число $1 < a < p$. Якщо це було б не так, то $(p, a) = a$, що протирічіть простоті p. Це означає, що просте число ділиться тільки на себе та на 1.

Теорема 5 (*основна теорема арифметики*)**.** *Кожне натуральне число $n \geq 2$ розкладається у добуток простих чисел, причому цей розклад є єдиним з точністю до перестановки множників.*

Доведення існування розкладу. Доведення проведемо методом математичної індукції. Для $n = 2$ твердження є очевидним. ⑭ Нехай твердження є справедливим для всіх $n < m$, доведемо його також і для m. Якщо m є простим числом, то твердження є справедливим. ⑮ Якщо ж m не є простим числом, то знайдуться натуральні числа $a \neq 1$ та $b \neq 1$, для яких $n = ab$. ⑯ За припущенням індукції і a, і b дорівнюють добутку простих чисел. Звідси і випливає, що m також дорівнює добутку простих чисел. □

Для доведення єдиності розкладу на прості множники нам потрібен наступний допоміжний результат.

Лема 1. *Якщо розклад числа m на прості множники є єдиним, то кожний простий дільник m входить в цей розклад.*

Доведення. Нехай m ділиться на просте число p. Тоді $m = p \cdot m'$, де m' — деяке натуральне число. Таким чином розклад m складається з розкладу числа m' з додатковим множником p. За припущенням існує тільки один розклад числа m, звідки і випливає, що p зустрічається у цьому розкладі. Лему доведено. □

Доведення єдиності розкладу в теоремі 5. Єдиність розкладу натурального числа у добуток простих множників доведемо методом математичної індукції. Нехай єдиність доведено для всіх чисел, менших за n, доведемо її для n. Якщо число n є простим, то єдиність є очевидною. Якщо ж n не є простим, то припустимо, що існують два різних розклади числа n у добутки простих множників:

$$n = p_0 \cdot p_1 \cdot p_2 \cdot p_3 \cdot \dots = q_0 \cdot q_1 \cdot q_2 \cdot q_3 \cdot \dots, \tag{3}$$

де p_i, q_i — прості числа. Жодне просте число не може входити в обидва розклади, оскільки в цьому випадку ми б сократили на нього й отримали два різних розклади для числа, що є меншим за n, а це протирічить припущенню індукції.

Вважатимемо, що множники $p_0, p_1, p_2, \dots$ та $q_0, q_1, q_2, \dots$ розташовано в порядку зростання. Оскільки n не є простим числом, то, крім p_0, в першому розкладі існує ще хоча б один множник. Оскільки p_0 є наименшим з усіх множників, то $n \geq p_0^2$. Аналогічні міркування для другого розкладу приводять до нерівності $n \geq q_0^2$. Оскільки $p_0 \neq q_0$, то одна з цих нерівностей є строгою, тобто $p_0 \cdot q_0 < n$.

Оскільки $n - p_0 \cdot q_0$ — є натуральним числом, меншим за n, то його розклад у добуток простих є єдиним за припущенням індукції. Число n ділиться на p_0, тому й $n - p_0 \cdot q_0$ ділиться на p_0. Згідно до леми, p_0 входить у розклад числа $n - p_0 \cdot q_0$. Аналогично, q_0 також входить у розклад цього числа.

Звідси випливає, що число n ділиться на $p_0 \cdot q_0$. ⑰ Тому $k \stackrel{\text{def}}{=} p_1 \cdot p_2 \cdot p_3 \cdot \ldots$ також ділиться на q_0, тобто $k = q_0 l$ для деякого $l \in \mathbf{N}$. Оскільки $l < n$, то розклад $l = r_1 \cdot r_2 \cdot \ldots$ у добуток простих співмножників є єдиним за припущенням індукції. Аналогічно, оскільки $k < n$, то і його розклад у добуток простих співмножників є єдиним. Таким чином,

$$n = p_0 k = p_0 \cdot q_0 \cdot r_1 \cdot r_2 \cdot \ldots,$$

тобто q_0 входить в обидва розклади в (3). Але це неможливо, що було доведено вище. Отримане протиріччя доводить єдиність розкладу числа n на прості множники. □

Теорема 6 (*необмеженість простих чисел*)**.** *Нехай p — просте число. Тоді існує натуральне $p' > p$, яке також є простим.*

Доведення. Позначимо всі прості числа, які не перевищують p, через $p_1, \ldots, p_k$. Нехай $n = p_1 p_2 \ldots p_k + 1$. Якщо n є простим, то теорему доведено. Якщо ж воно не є простим, запишемо його розклад у добуток простих чисел: $n = q_1 \ldots q_m$.

Жодне з чисел $q_1, \ldots, q_m$ не може дорівнювати жодному з чисел $p_1, \ldots, p_k$. ⑱ Тому всі вони більші за p. ⑲ □

6.1. Закон розподілу простих чисел. З доведеної теореми випливає, що на кожному з проміжків $[n, n!+1]$ ряду натуральних чисел є принаймні одне просте число. ⑳

Зауваження 4. Набагато більш сильне твердження називається постулатом Бертрана: *якщо* $n \geq 2$, *то у проміжку* $(n, 2n)$ *знайдеться принаймні одне просте число* (див. розділ 13.2).

З іншого боку, існують як завгодно великі проміжки ряду натуральних чисел, які не містять простих чисел.

Твердження 1. *Нехай* N *є натуральним числом. Тоді будь-яке з чисел*

$$N!+2,\ N!+3,\ \ldots,\ N!+(N-1),\ N!+N \tag{4}$$

є складеним.

Доведення. Дійсно, оскільки $N! = 1 \cdot 2 \cdot \ldots \cdot N$, то $N!$ ділиться на 2, звідки випливає, що й $N!+2$ ділиться на 2. ㉑. Далі, оскільки $N! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot N$ то $N!$ ділиться на 3, звідки випливає, що й $N!+3$ ділиться на 3. Таким же чином доводимо, що $N!+k$ ділиться на k для будь-якого $k \leq N$. ㉒ Таким чином, кожне з чисел в (4) є складеним. □

Якщо в твердженні 1 обрати $N = 1,000,000$, то виявиться, що існує проміжок довжиною 1,000,000 у ряді натуральних чисел, який не містить простих чисел. Оскільки N у твердженні 1 обрати ще більшим, то все рівно знайдеться інтервал довжини N, який не містить простих чисел.

Одну з найважливіших закономірностей, яка описує частоту простих чисел у множині $\mathbf{N}$ і називається *законом розподілу простих чисел*, ми вивчаємо в главі 13.

7. Шифр Віженера

Шифр Віженера — це один з *поліалфавітних шифрів*.

Таблиця 5. Tabula recta для шифру Віженера

	а	**б**	**в**	**г**	**ґ**	**д**	**е**	**є**	**ж**	**з**	**и**	**і**	**ї**	**й**	**к**	**л**	**м**	**н**	**о**	**п**	**р**	**с**	**т**	**у**	**ф**	**х**	**ц**	**ч**	**ш**	**щ**	**ь**	**ю**	**я**
а	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я
б	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а
в	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б
г	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в
ґ	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г
д	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ
е	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д
є	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е
ж	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є
з	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж
и	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з
і	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и
ї	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і
й	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї
к	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й
л	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к
м	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л
н	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м
о	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н
п	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о
р	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п
с	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р
т	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с
у	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т
ф	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у
х	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф
ц	ц	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х
ч	ч	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц
ш	ш	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч
щ	щ	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш
ь	ь	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ
ю	ю	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь
я	я	а	б	в	г	ґ	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю

Поліалфавітні шифри циклічно використовують кілька моноалфавітних шифрів. Цей принцип пояснімо на прикладі шифра Віженера.

Перед початком шифрування за Віженером зручно створити таблицю (tabula recta, таблиця 5), кожний наступний рядок якої є попереднім рядком, циклічно зсунутим вліво на одну позицію. У першому рядку записано всі букви українського алфавіту у їхньому природному порядку. Таким чином, в кожному рядку записано букви чергового моноалфавіту для шифру Віженера.

Кожен шифр Віженера має ключ; ним є певне слово, яке обирається довільним чином. Утворимо тепер *шифр-матрицю* з двох рядків: перший рядок складається з фрази, яку необхідно зашифрувати. У другому рядку записуємо ключове слово стільки разів, скільки необхідно, щоб він став довшим за перший. Якщо на певній позиції у першому рядку стоїть буква `Х`, а в шифр-матриці під нею розташовано букву `Ү`, то для шифрування букви `Х` знаходимо символ у tabula recta, який стоїть на перетині рядка `Ү` та стовпчика `Х`. Саме цей символ і є шифром Віженера букви `Х`.

Наприклад, якщо текст починається з букви `Б`, а першою буквою ключового слова є `Г`, то першим символом шифрованої фрази є буква, яка знаходиться у tabula recta на перетині рядка `Г` та стовпчика `Б`, тобто `Ґ`.

Приклад 3. Зашифруємо повідомлення `ШИФР ВІЖЕНЕРА` за допомогою ключового слова `ШИФР ВІЖЕНЕРА`, тобто шифр-матрицею є

Ш И Ф Р В І Ж Е Н Е Р А
Ш И Ф Р В І Ж Е Н Е Р А

Особливістю цього прикладу є те, що всі шифр-букви визначаються перетином рядків та стовпчиків з однаковими номерами. Оскільки на перетині рядка Ш та стовпчика Ш в таблиці 5 розташовано У, то шифром Ш є У. Аналогічно шифруємо інші букви повідомлення:

Ш	И	Ф	Р	В	І	Ж	Е	Н	Е	Р	А
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
У	Р	Л	Є	Ґ	Т	М	Ї	Б	Ї	Є	А

8. Шифр Вернама

Шифр Вернама або схема *одноразового блокноту* (англ. one-time pad) — система *симетричного шифрування*, винайдена в 1917 році співробітниками AT&T М. Моборном і Г. Вернамом. Шифр Вернама є єдиною системою шифрування, для якої доведена абсолютна *криптографічна стійкість*. Під криптографічною стійкістю ми розуміємо властивість системи шифрування протистояти спробам дешифрування навіть при наявності усіх існуючих комп'ютерних ресурсів.

Принцип шифрування за Вернамом подамо на прикладі шифру Віженера. В цьому випадку єдиною відмінністю між ними є принцип, за яким обирається ключове слово. Якщо у шифрі Віженера воно обирається так, щоб його легко було запам'ятати, то у шифрі Вернама ключове слово

(a) має бути випадковим;
(b) має довжину, яка дорівнює довжині повідомлення;
(c) застосовується лише один раз.

До речі, ключове слово у прикладі 3 задовольняє умову (b).

Слово "*блокнот*" у назві шифру пояснюється такою схемою утворення випадкового ключа: шифрувальник забезпечується блокнотом, кожна сторінка якого містить новий ключ. Такий же блокнот є і у дешифрувальника. Використані сторінки знищуються.

Проблемою у застосуванні шифру Вернама є таємна передача блокноту з ключовими словами та збереження його у таємниці. Для цього необхідно мати надійно захищений канал для спілкування між шифрувальником та отримувачем інформації. Але, якщо існує надійно захищений канал передачі повідомлень, то шифри взагалі не потрібні: секретні повідомлення можна передавати через цей канал.

9. КОНТРОЛЬНІ ПИТАННЯ

1. Впевнитись, що перший рядок таблиці 3 є циклічним зсувом другого рядка вправо на 3 позиції (або вліво на 30 позицій). (стор. 40).

2. Як випадки $b < 0$ або $b > 33$ для шифру Цезаря зводяться до $0 \le b \le 33$? (стор. 40).

3. Чому теорема 1 є вірною для $m = 0$? (стор. 43).

4. Чому у доведенні теореми 1 стверджується, що число $-|m|$ належить множині M. (стор. 43).

5. Чому у доведенні теореми 1 жоден елемент M не перевищує $|m|$? (стор. 43).

6. Чому $r \ge 0$ у доведенні теореми 1? (стор. 43).

7. Пояснити, чому у доведенні теореми 1 стверджується, що $q+1 \in M$, якщо $r \ge n$? (стор. 43).

8. Пояснити оцінки $-n < r - r' < n$, які використано у доведенні теореми 1. (стор. 43).

9. Чому з $n|q' - q| < n$ у доведенні теореми 1 випливає, що $q' = q$? (стор. 43).

10. Переконатись, що $k \pmod{33} = k \bmod 33$ для $1 \le k < 66$. (стор. 44).

11. Перевірити, що властивості 1, 2 та 3 випливають з означення 4. (стор. 45).

12. Довести, що властивості 4–5 випливають з означення 4 (стор. 45).

13. Перевірити, що доведення властивостей 7 та 8 є таким же, як і доведення властивості 6. (стор. 46).

14. Чому теорема 5 є очевидною для $n = 2$? (стор. 47).

15. Чому існування розкладу, про який йдеться у теоремі 5, є справедливим для простих чисел? (стор. 47).

16. Пояснити, чому знайдуться натуральні числа $a \neq 1$ та $b \neq 1$, для яких $m = ab$, якщо m не є простим числом? (стор. 47).

17. Чому n ділиться на $p_0 \cdot q_0$ у доведенні теореми 5? (стор. 49).

18. Чому жодне з чисел $q_1, \ldots, q_m$ не може дорівнювати жодному з чисел $p_1, \ldots, p_k$ у доведенні теореми 6? (стор. 49).

19. Чому кожне з чисел $q_1, \ldots, q_m$ є більшим за p у доведенні теореми 6? (стор. 49).

20. Пояснити чому з теореми 6 випливає, що на кожному з проміжків $[n, n! + 1]$ ряду натуральних чисел є принаймні одне просте число. (стор. 49).

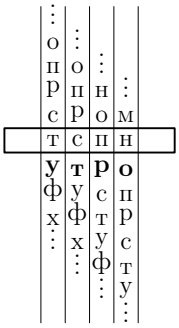
21. Чому $N! + 2$ ділиться на 2? (стор. 50).

22. Довести, що $N!+k$ ділиться на k для будь-якого $k \leq N$. (стор. 50).

10. З А Д А Ч І

Задача 1. *Використати шифр Цезаря з $b = 5$ й зашифрувати слово* ЧИСЛО.

Задача 2. *Дешифрувати фразу* ЮІФХУЦЧУ, *яку зашифровано за допомогою шифру Цезаря з $b = 5$.*



Задача 3. *Для шифру Цезаря існує простий спосіб дешифрації — так званий метод смужок. Щоб дешифрувати текст, на кожну зі смужок записують у природному порядку букви українського алфавіту. Нехай слово* ТСПН *зустрічається в повідомленні, зашифрованому шифром Цезаря. Суміщаємо смужки так, щоб утворилось "слово"* ТСПН. *Зафіксувавши таке положення смужок, тепер читаємо одне за іншим "слова" у рядках цієї "таблиці". У прикладі з* ТСПН *виявляється, що єдиним змістовним словом є* УТРО. *Це*

дозволяє обчислити параметр b та прочитати все повідомлення. Яким є параметр b у цьому прикладі? Пояснити чому цей прийом є універсальним?

Задача 4. *Відомо, що текст зашифровано спочатку шифром Цезаря з параметром b_1, а потім ще раз шифром Цезаря з іншим параметром b_2. Чи є такий спосіб шифрування більш стійким, ніж спосіб, коли шифр Цезаря використовується тільки один раз?*

Задача 5. *Зашифрувати слово* `МАТЕМАТИКА` *за допомогою шифра Віженера та ключового слова* `ФІЗМАТ`.

Задача 6. *Замість зсуву алфавіту на певну величину, як у шифрі Цезаря, можна застосувати перестановку його букв.*

(a) *Скільки існує різних шифрів перестановки для українського алфавіту?*

(b) *Чи є метод грубої сили ефективним, якщо відомо, що при шифрації використано один з шифрів перестановки?*

Задача 7. *Моноалфавітні шифри легко зламати, бо вони містять дані про частоту букв алфавіту. Контрзаходом є використання декількох замінників, відомих як гомофони, для однієї і тієї ж букви. Наприклад, букві* `Е` *можна призначено кілька різних символів при шифруванні, наприклад, 7, 35, 56 і 89. Кожен гомофон використовується циклічно або обирається випадковим чином. Якщо кількість гомофонів, призначених кожній букві, є обернено пропорційною до відносної частоті цієї букви, то однобуквені частоти у повідомленні є абсолютно однаковими. Великий математик Гаусс вважав, що, використовуючи гомофони, ми маємо незламний шифр. Тим не менше, у сучасній криптографії вважається, що криптоаналіз шифрів з гомофонами є відносно простим. Поясніть це.*

Задача 8. *Довести, що шифр Цезаря є частковим випадком шифра Віженера (див. розділ 7) й знайти відповідне ключове слово.*

Задача 9. *Нехай черговою буквою у фразі, яку необхідно зашифрувати за допомогою шифру Віженера (див. розділ 7), є* `Х`, *а їй відповідає буква* `Ү` *у шифр-матриці. Нехай буква* `Ү` *має позицію i, в*

алфавіті, а `X` *— позицію* j. *Довести, що елементом* (i, j) *в tabula recta є*

$$i + j - 1 \pmod{33}.$$

Задача 10. *Зашифрувати фразу* `ШИФРВЕРНАМА` *за допомогою шифру Вернама (див. розділ* 8*). Для цього використати ключове слово* `ІБФКҐЧНЄЬРИ`.

Задача 11. *Ключове слово у задачі 10 утворено за правилом*:

$$\mathtt{X}_{n+1} = 23 + \mathtt{X}_n \pmod{33}, \qquad X_0 = 23,$$

тобто кожна наступна буква обчислюється через попередню за допомогою зсуву на 23 *та обчислення конгруенції за модулем* 33. *Перевірити це.*

Задача 12. *Вернам фактично запропонував наступну процедуру. Спочатку перевести букви (як повідомлення, так і ключового слова) у десяткові числа; потім записати двійкове представлення для кожного числа, отримавши дві довгі послідовності* 0 *та* 1 *(бітів); нарешті, до кожного біта* m_i *повідомлення застосувати операцію* $m_i \oplus k_i$, *де* m_i *та* k_i *— це відповідні біти повідомлення та ключового слова. Тут* $x \oplus y = 0$ *або* 1 *в залежності від* $x = y$ *чи* $x \neq y$. *Зашифрувати повідомлення* `КІТ`, *якщо ключовим словом є* `ПЕС`.

Задача 13. *Підрахувати суми*

$$\sum_{d|12} d, \qquad \sum_{d|12} 1, \qquad \sum_{d|18} \frac{1}{d}, \qquad \sum_{d|18} \frac{18}{d}.$$

Задача 14. *Довести, що якщо*

a) $a|b$ *та* $b|a$, *то* $a = b$;
b) $a|b$ *та* $c|d$, *то* $ac|bd$.

Задача 15. *Довести, що якщо квадрат цілого числа*

a) *є парним, то і саме число є парним*;
b) *є непарним, то і саме число є непарним.*

Задача 16. *Довести, що*

a) *добуток двох послідовних цілих чисел є парним*;
b) $n^2 + n$ *є парним для будь-якого натурального числа* n.

Задача 17. *Довести, що* $2n^3 + 3n^2 + n$ *є парним для будь-якого натурального числа* n.

Задача 18. *Довести, що* $30|(n^5 - n)$ *для будь-якого натурального* n.

Задача 19. *Довести, що різниця квадратів двох натуральних чисел не може дорівнювати* 1.

Задача 20. *Довести, що якщо сума кубів трьох послідовних натуральних чисел є кубом* k^3, *то* $3|k$.

Задача 21. *Які з наступних тверджень є вірними, якщо* a, b, c — *натуральні числа, а* p — *просте?*

a) $(a, b) = (b, a)$; *b)* $(a, b) = (a, a - b)$; *c)* $(a, b) = (a, a - 2b)$;
d) $(a, a + 2) = 1$; *e)* $(p, p + 2) = 1$; *f)* $(ac, bc) = c(a, b)$.

Задача 22. *Знайти* (a, b), *якщо*

a) $b = 1$; *b)* $b = a$; *c)* $b = a + 1$; *d)* $b|a$;
e) $b = a^2$; *f)* $b = a^n$; *g)* $b = na$; *h)* $b = (b, a)$.

Задача 23. *Нехай* $a > b$. *Знайти*

a) $(a + b, a^2 - b^2)$; *b)* $(a^2 - b^2, a^4 - b^4)$; *c)* $(a^2 - b^2, a^3 - b^3)$.

Задача 24. *Спростувати твердження*:

a) *якщо* $(a, b) = 1$ *та* $(b, c) = 1$, *то* $(a, c) = 1$;
b) *якщо* $(a, b) = 2$ *та* $(b, c) = 2$, *то* $(a, c) = 2$.

Задача 25. *Довести, що* $(a, a - b) = 1$ *тоді і тільки тоді, коли* $(a, b) = 1$.

Задача 26. *Довести, що якщо* $(a,b)=1$ *та* $(a,c)=1$, *то* $(a,bc)=1$.

Задача 27. *Нехай* n *— будь-яке чотиризначне число, утворене з перестановки десяткових цифр* $0\le d\le c\le b\le a\le 9$, *не всі з яких є однаковими. Покладемо* $n'=(abcd)_{10}$ *та* $n''=(dcba)_{10}$. *Значенням функції Капрекара для аргумента* n *називається* $K(n)=n'-n''$. *Наприклад,* $K(1995)=9951-1599=8352$.

(a) *Обчислити* $K(K(1995))$;
(b) *довести, що* $K(6174)=6174$;
(c) *чи існують інші числа* n, *крім* 6174 (*константа Капрекара*), *для яких* $K(n)=n$?

Задача 28. *Нехай* $K^1(n)=K(n)$, *де* K *— це функція, означена в задачі* 27. *Покладемо тепер* $K^2(n))=K(K(n))$ *і взагалі* $K^m(n)=K(K^{m-1}(n))$ *для довільного* $m\ge 2$. *Перевірити, що* $K^7(2016)=6174$.

Задача 29. *Абсолютно простим числом називають таке просте число, що кожна перестановка його цифр також є простим числом. Наприклад,* 2, 3 *та* 5 *є абсолютно простими числами.*

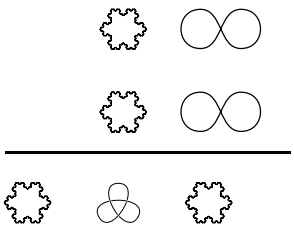
(a) *Існує вісім абсолютно простих чисел, які складаються з двох різних десяткових цифр. Знайти їх.*
(b) *Існує дев'ять абсолютно простих чисел, які складаються з трьох різних десяткових цифр. Знайти їх.*
(c) *Довести, що абсолютно просте число, яке складається з двох або більших десяткових цифр, може складатися лише з десяткових цифр* 1, 3, 7 *або* 9.

Задача 30. *Англійський математик де Морган, який жив у XIX сторіччі, одного разу сказав, що у році* x^2 *йому виповнилось* x *років.*

a) *Коли він народився?*
b) *Чи може таке ж стверджувати математик, який жив у XX сторіччі?*

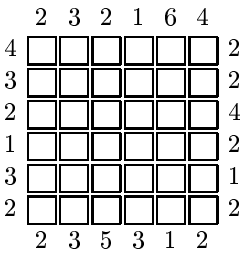
Задача 31. *Цю задачу в* 1968 *році опублікував М. Гарднер, відомий популяризатор математики, автор численних книг. Ми подаємо переклад оригінального формулювання задачі.*

Астронавти, які досліджують Венеру, знайшли запис домашнього завдання з математики, виконане венеріанським школяром на тему додавання двох чисел у стовбчик:



Числова система венеріанців є схожою на нашу, а основою для неї служить кількість пальців на руці венеріанців. Визначити кількість пальців на руці венеріанських аборигенів.

Задача 32 (Ю. Б. Чураченко)**.** *У кожній клітинці кварталу* 6×6 *стоїть будинок (в кожній горизонталі та кожній вертикалі є будинки з кількістю поверхів* $1, 2, 3, 4, 5, 6$*).*



Цифри вздовж периметра квадрата вказують на кількість будинків, які спостерігач може побачити у відповідному рядку або стовбчику, якщо буде дивитись у відповідному напрямку з позиції, де зображено цифру. Наприклад, біля сторін лівої верхньої клітинки записано цифри 4 та 2. Цифра 4 (зліва від клітинки) означає, що, якщо дивитись на перший рядок з позиції, на якій зображено цифру 4, то можна побачити 4 будинки. Аналогічно, цифра 2 (зверху клітинки) означає, що, якщо дивитись на перший стовбчик з позиції, на якій зображено цифру 2, то можна побачити 2 будинки.

Побудуйте таку конфігурацію будинків.

11. БІОГРАФІЇ

Вернам, *Гилберт Сендфорд* (1890–1960), американський інженер, співробітник Bell Laboratories.

Гилберт Вернам

Найбільш відомий тим, що в 1917 році винайшов вдосконалений поліалфавітний потоковий шифр і ввів в обіг успішну інновацію — шифроблокнот з одноразовими ключами, який базується на так званому шифрі Вернама. Для шифра Вернама доведена абсолютна криптографічна стійкість.

де Віженер, *Блез* (1523–1596), французький дипломат і криптограф, алхімік і астролог.

Його іменем названо шифр Віженера, який насправді винайшов Джованні Баттіста Беллазо, але цей шифр був помилково приписаний у 19 столітті саме Віженеру.

В 1554 році Віженер перебував у Римі з дворічною дипломатичною місією. Там він познайомився з літературою з криптографії. У книзі "*Traicte des Chiffres*" ("*Трактат про шифри або таємні способи письма*") він описав шифрування з автоматичним вибором ключа, який він винайшов. Це був перший шифр після Беллазо, який неможливо було

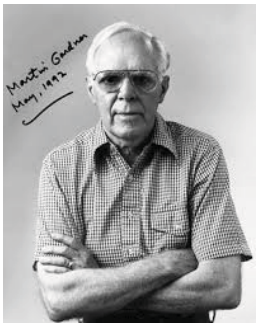
тривіально зламати. Метод зламу шифру Віженера був опублікований лише у 1863 році Ф. В. Касіскі. Проте цифровий варіант шифра Віженера, *Cifrario tascabile* (кишеньковий шифр), використовували з початку жовтня 1915 р. в італійських військових силах часів Першої Світової війни. Був успішно зламаний австрійською криптографічною службою.

Блез де Віженер

Перші задокументовані згадки поліалфавітних шифрів історики знайшли у роботах Леона Батісти Альберті у 1467 році. У 1518 році Йоганн Трисемус описав tabula recta — таблицю підстановки для шифра Віженера. Джованні Батіста Беллазо використав таблицю Трисемуса та додав ключ. У 1586 році Блез Віженер запропонував цей шифр Генриху III, тодішньому королю Франції, що і стало (помилковою) причиною для назви.

Ґарднер, *Мартін* (1914–2010), американський математик, письменник, популяризатор науки. Засновник (середина 50-х рр.), автор й ведучий (до 1983) рубрики "Математичні ігри" журналу "Scientific American". В ній, зокрема, була представлена широкому загалу гра "Життя", придумана Джоном Конвеєм, а також багато інших цікавих ігор, завдань, головоломок. Ґарднеру вдалося більш-менш самотужки відродити та підживлювати інтерес до цікавої математики. Ґарднер трактує цікавість як синонім захоплюючого, цікавого в пізнанні, але чужого дозвільної розважальності. Особливу популярність серед читачів здобули статті та книги Ґарднера з математики. "Ґарднерівсь-

кий" стиль характеризують дохідливість, яскравість переконливість викладу, парадоксальність думок, новизна і глибина наукових ідей, багато з яких почерпнуті з сучасних наукових публікацій і в свою чергу стали стимулом проведення серйозних досліджень, активного залучення читача до самостійної творчості.



Мартін Ґарднер

Нижче наведено назви лише кількох книжок Ґарднера, перекладених на російську:

- "*Математические головоломки и развлечения*", М., "Мир", 1971;
- "*Математические досуги*", М., "Мир", 1972;
- "*Математические новеллы*", М., "Мир", 1974;
- "*Математические чудеса и тайны*", М., "Мир", 1977.

де Морган, *Ауґустус* (1806–1871), британський математик та логік, перший президент (1866) Лондонського математичного товариства. З його ім'ям пов'язано відомі теоретико-множинні співвідношення (закони де Моргана).

У творчій діяльності Моргана відзначають роботи з теорії рядів, в якій йому належить відкриття критеріїв збіжності, що значно перевершують за своєю строгістю всі критерії того ж роду, відомі до нього. Відомими є його роботи з теорії ймовірностей та історії математики. Дуже багато було зроблено Морганом в області дедуктивної

логіки взагалі і математичної логіки зокрема. На думку багатьох видатних діячів цієї науки, Морган є "одним з найдотепніших логіків, які коли-небудь існували".

З творів Моргана вирізняється книга "*A budget of paradoxes*", яка вийшла вже після його смерті.

Ауґустус де Морган

В цій книзі автор запропонував класифікацію вчених, які займали абсурдні позиції стосовно наукових знань. За Морганом такі вчені належать до одного з класів

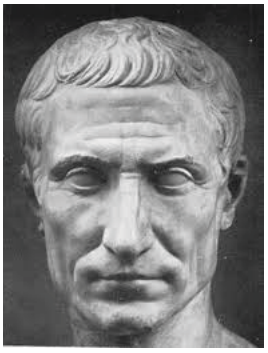
1) антикоперніканців,
2) алхіміків,
3) антиньютоніанців,
4) астрологів,
5) квадратурщиків кола,*
6) містиків,
7) трисекторщиків кута.**

---

* *Квадратура колі* — задача про побудову циркулем та лінійкою квадрата, який має таку ж площу, як і задане коло. І. Г. Ламберт в 1766 році довів, що це зробити неможливо.

** *Трисекція кута* — задача, яка полягає у розділенні кута на три рівні частини за допомогою циркуля та лінійки. П. Л. Ванцель довів в 1837 році, что цю задачу можна розв'язати тоді і тільки тоді, коли рівняння $x^3 - 3x - 2\ \cos\alpha = 0$ можна розв'язати у радикалах. Наприклад, трисекція можлива для кутів $\frac{360^\circ}{n}$, якщо ціле число n не делится на 3.

За великі математичні досягнення, штаб-квартира Лондонського математичного товариства була названа De Morgan House, а студентське суспільство математичного факультету університету Лондона називають Аугустус де Морганським товариством.



Цезар, *Гай Юлій* (100 до н.е.–44 до н.е.), давньоримський державний і політичний діяч, полководець, письменник. Діяльність Цезаря докорінно змінила культурний і політичний вигляд Європи та Середземномор'я і залишила визначний слід в житті наступних поколінь.

Згідно "*Життя дванадцяти цезарів*" Светонія, щоб захищати військові повідомлення, Цезар використовував (зі здвигом 3) шифр, який зараз називають його ім'ям. Відомо, що інші підстановочні шифри використовувались і раніше, але Цезар був першим, про кого залишилась згадка у літературному джерелі як про користувача певного шифру.

Існують свідчення про те, що Юлій Цезар користувався також і більш складними схемами. Невідомо, наскільки ефективним шифр Цезаря був у його часи, але, ймовірно, він був розумно безпечним (не в останню чергу завдяки тому, що більшість ворогів Цезаря були неписьменними). Багато хто з тих, хто бачив зашифровані Цезарем повідомлення, вважав, що вони написані на невідомій іноземній мові.

Зараз немає жодних свідчень щодо методів злому простих шифрів підстановки, відомих у часи Цезаря. Найбільш ранніми (IX сторіччя) є твори Ал-Кінді про частотний аналіз.

Глава 3

МУЛЬТИПЛІКАТИВНІ ШИФРИ

Через $\mathcal{P}_{\mathtt{X}}$ будемо позначати номер позиції букви X в українському алфавіті, а через $\mathcal{C}_{\mathtt{X}}$ — позицію букви, в яку X переходить при кодуванні. В цих позначеннях алгоритм шифрування для шифру Цезаря можна записати наступним чином

$$\mathcal{C}_{\mathtt{X}} \equiv \mathcal{P}_{\mathtt{X}} + b \pmod{33}$$

або

$$\mathcal{P}_{\mathtt{X}} + b \equiv \mathcal{C}_{\mathtt{X}} \pmod{33}.$$

Через спосіб, яким параметр b входить до цих формул, цей шифр іноді називають *адитивним*.

1. Означення мультиплікативних шифрів

Інший клас утворюють *мультиплікативні* шифри. Нехай $1 < a < 33$ — натуральне число. Тоді алгоритм шифрування мультиплікативним шифром записують так

$$\mathcal{C}_{\mathtt{X}} \equiv a \cdot \mathcal{P}_{\mathtt{X}} \pmod{33} \tag{1}$$

або

$$a \cdot \mathcal{P}_{\mathtt{X}} \equiv \mathcal{C}_{\mathtt{X}} \pmod{33}. \tag{2}$$

Скорочено мультиплікативний шифр з множником a називають також M_a-*шифром* і позначають M_a.

Зауваження 1. Формули (1) та (2) можна використати також і для $a = 1$ або $a = 33$. В першому випадку шифрування не відбувається, а у другому всі шифр-букви будуть однаковими. ① Шифр M_a з $a > 33$ зводиться до еквівалентного шифру $M_{a \pmod{33}}$. ②

Зауваження 2. При щифруванні ми використовуємо конгруенцію $33 \equiv 33 \pmod{33}$ замість $33 \equiv 0 \pmod{33}$, щоб уникнути проблеми з "нульовою" буквою. В цьому випадку не виникає невизначеності при шифруванні букви Я, тобто ми вважаємо, що $\mathcal{C}_{\text{Я}} = 33$ для будь-якого шифру M_a.

1.1. M_2-шифр. Кілька прикладів шифрування з використанням M_2-шифру:

X	$\mathcal{P}_{\text{X}}$	$2 \cdot \mathcal{P}_{\text{X}}$	$\mathcal{C}_{\text{X}}$	код X
А	1	2	2	Б
З	10	20	20	П
Н	18	36	3	В

Нижче наведено повну таблицю відповідності букв та їхніх кодів для M_2-шифру.

Таблиця 1. M_2-шифр

А	Б	В	Г	Ґ	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
Б	Г	Д	Є	З	І	Й	Л	Н	П	С	У	Х	Ч	Щ	Ю	А	В	Ґ	Е	Ж	Є	З	К	М	Щ	Р	Т	Ф	Ц	Ш	Ь	Я

Наведемо також частину розширеної таблиці відповідності для мультиплікативного шифру, яка включає додатково номери позицій букв та їхніх кодів, які використовуються для шифрування повідомлень.

Таблиця 2. Частина розширеної таблиці M_2-шифра

А	Б	В	Г	Ґ	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	М	Н	О	П	Р	С	...
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	...
2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	1	3	5	7	9	11	...
Б	Г	Д	З	З	І	Й	Л	Н	П	С	У	Х	Ч	Щ	Ю	А	В	Ґ	Е	Ж	Є	...

Нижче наведено приклад шифрування повідомлення для M_2-шифру:

$$\texttt{РОЗА} \to 21\ \ 19\ \ 10\ \ 1 \to 9\ \ 5\ \ 20\ \ 2 \to \texttt{ЖҐПБ}$$

1.2. Дешифрування M_2-шифру. Здається, що формулу (2) можна використати для дешифрування. У випадку $a = 2$ вона перетворюється у формулу

$$2 \cdot \mathcal{P}_{\texttt{Х}} \equiv \mathcal{C}_{\texttt{Х}} \pmod{33}, \tag{3}$$

поділивши обидві частини якої на 2, отримаємо

$$\mathcal{P}_{\texttt{Х}} \equiv \frac{1}{2} \cdot \mathcal{C}_{\texttt{Х}} \pmod{33}. \tag{4}$$

Проте $\frac{1}{2} \cdot \mathcal{C}_{\texttt{Х}}$ не має смислу, якщо $\mathcal{C}_{\texttt{Х}}$ є непарним числом, тому в арифметиці за модулем застосовується інший спосіб.

Конгруенція не зміниться, якщо обидві її частини домножити на одне і те ж число (властивість 2.8). Використаємо цю властивість, помноживши обидві частини (3) на число 17:

$$17 \cdot 2 \cdot \mathcal{P}_{\mathtt{X}} \equiv 17 \cdot \mathcal{C}_{\mathtt{X}} \pmod{33}.$$

Оскільки $34 \equiv 1 \pmod{33}$, то застосуємо ще раз властивість 2.8:

$$1 \cdot \mathcal{P}_{\mathtt{X}} \equiv 17 \cdot \mathcal{C}_{\mathtt{X}} \pmod{33}$$

або

$$\mathcal{P}_{\mathtt{X}} \equiv 17 \cdot \mathcal{C}_{\mathtt{X}} \pmod{33}. \tag{5}$$

Це означає, що відновити повідомлення можна, якщо застосувати M_{17}-шифр. Наприклад, закодоване повідомлення ЖҐПБ можна дешифрувати наступним чином (ми використовуємо таблицю 2):

X	$\mathcal{C}_{\mathtt{X}}$	$17 \cdot \mathcal{C}_{\mathtt{X}}$	$17 \cdot \mathcal{C}_{\mathtt{X}} \pmod{33}$	розкодоване X
Ж	9	153	21	Р
Ґ	5	85	19	О
П	20	180	7	З
Б	2	34	1	А

1.3. Шифр M_3. Розглянемо шифр M_3. Частину таблиці відповідності для нього наведено нижче.

Таблиця 3. Частина розширеної таблиці M_3-шифра

А	Б	В	Г	Ґ	Д	Е	Є	Ж	З	И	І	Ї	Й	К	Л	...	Т	У	...
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	...	23	24	...
3	6	9	12	15	18	21	24	27	30	33	3	6	9	12	15	...	3	6	...
В	Д	Ж	І	К	Н	Р	У	Ц	Щ	Я	В	Д	Ж	І	К	...	В	Д	...

Нескладно побачити, що букви Б, Ї та У мають однакове значення Д при шифруванні M_3-шифром. Аналогічна ситуація і для букв А, І та Т, а також для деяких інших трійок букв. Це означає, що такий шифр не можна вживати для шифрування інформації, оскільки букву Д (а також букву В і деякі інші) неможливо однозначно дешифрувати.

Зауваження 3. В §1.2 ми здійснили процедуру дешифрування для $a = 2$, знайшовши таке c (ним виявилось число $c = 17$), що

$$ac \equiv 1 \pmod{33}.$$

Це рівняння відносно c не має розв'язків, якщо $a = 3$. ③ Як ми побачимо нижче ця властивість і відрізняє шифри M_2 та M_3.

2. Обернені числа в арифметиці за модулем

У звичайній арифметиці число c називається *оберненим* до a, якщо

$$ca = 1.$$

Обернене число позначається також $1/a$, $\frac{1}{a}$ або a^{-1}. Зауважимо, що обернене число c у звичайній арифметиці не є

натуральним, якщо $a \neq 1$.

Означення 1. Нехай a та n натуральні числа. В арифметиці за модулем n натуральне число $1 \leq c < n$ називається *оберненим до a за модулем n*, якщо

$$ca \equiv 1 \pmod{n}.$$

Обернене за модулем n число позначається $a^{-1} \pmod{n}$.

Підкреслимо ще раз, що, на відміну від звичайної арифметики, $a^{-1} \pmod{n}$ є натуральним числом, причому меншим за n.

Як ми бачили вище, обернене за модулем число існує не для довільної пари a, n.

Теорема 1 (*про існування оберненого за модулем*). *Нехай n та $1 \leq a < n$ є натуральними числами. Якщо $(a, n) = 1$, то $a^{-1} \pmod{n}$ існує. Якщо ж $(a, n) \neq 1$, то $a^{-1} \pmod{n}$ не існує. Іншими словами, $a^{-1} \pmod{n}$ існує тоді і тільки тоді, коли $(a, n) = 1$.*

Доведення. Нехай $(a, n) = 1$, але обернене $a^{-1} \pmod{n}$ не існує. Розглянемо остачі r_k, $1 \leq k < n$, від ділення чисел ka на n, тобто $ka = s_k n + r_k$ для деякого $s_k \in \mathbf{N}$. З $(a, n) = 1$ випливає, що $0 \notin \{r_1, \ldots, r_{n-1}\}$, ④ а з припущення про неіснування $a^{-1} \pmod{n}$ — що $1 \notin \{r_1, \ldots, r_{n-1}\}$. ⑤ Звідси отримуємо, що серед $\{r_1, \ldots, r_{n-1}\}$ знайдуться два однакових числа, скажімо r_i та r_j, $i > j$. ⑥ Тоді $(i-j)a \equiv 0 \pmod{n}$, що неможливо. ⑦ Отримане протиріччя доводить, що обернене $a^{-1} \pmod{n}$ існує.

Розглянемо тепер випадок $(a, n) \neq 1$. Якби при цьому обернене $a^{-1} \pmod{n}$ існувало, то $ka \equiv 1 \pmod{n}$ для

деякого $1 \le k < n$, тобто $ka = ns + 1$ або $ka - ns = 1$ для деякого цілого числа s. Але остання рівність неможлива, оскільки її ліва частина ділиться на $(a, n) > 1$. $\square$

Наслідок 1. *Нехай n та $1 \le a < n$ є натуральними числами. Обернене $a^{-1} \pmod{n}$ існує тоді і тільки тоді, коли всі остачі $ka \pmod{n}$, $1 \le k \le n$, є різними.* ⑧

Зауваження 4. Згідно з наслідком 1, якщо $(a, n) \ne 1$, то знайдуться дві однакові остачі. Для шифру M_a це означає, що відповідні букви мають однакові коди, тобто повідомлення неможливо відновити однозначно по його коду. Саме з цієї причини код M_3 не можна вживати для українського алфавіту, а код M_2 — можна.

Цікаво також відзначити, що оскільки в англійському алфавіті 26 букв, то для нього навпаки код M_2 вживати не можна, а M_3 — можна.

3. Властивості шифру $M_{a,n}$

3.1. Дешифрування $M_{a,n}$ шифру. Мультиплікативні шифри вживають для алфавітів, відмінних від українського. Нехай $(a, n) = 1$. Тоді шифрування згідно до мультиплікативного шифру $M_{a,n}$ з множником a та модулем n здійснюється за формулою

$$\mathcal{C}_{\mathtt{X}} \equiv a \cdot \mathcal{P}_{\mathtt{X}} \pmod{n}. \tag{6}$$

Дешифрування здійснюється за правилом

$$\mathcal{P}_{\mathtt{X}} \equiv a^{-1} \cdot \mathcal{C}_{\mathtt{X}} \pmod{n}. \tag{7}$$

Для скорочення запису ми, як і раніше, пишемо M_a замість $M_{a,33}$ у випадку $n = 33$.

3.2. Криптоаналіз M_a шифру. Нескладно підрахувати, що в інтервалі $[1, 33]$ існує 19 взаємно простих чисел з 33. ⑨ Тому, маючи закодоване повідомлення, знайти a нескладно *методом повного перебору*, який ще називається *методом грубої сили*.

Приклад 1. Нижче показано дію методу грубої сили на простому прикладі закодованого повідомлення `18 24 20`:

код	a^{-1}	$a^{-1} \cdot$ код	$a^{-1} \cdot$ код (mod 33)	текст
18 24 20	2	36 48 40	3 15 7	ВКЕ
18 24 20	3	54 72 60	21 6 27	РДЦ
18 24 20	4	72 96 80	6 30 14	ДЩЙ
18 24 20	5	90 120 100	24 21 1	УРА

В наведеній таблиці показано результат дешифрування за формулою (7) для кожного з "кандидатів" $a^{-1} \pmod{33} = 2, 3, 4, 5$. ⑩ Результат дешифрування є осмисленим словом тільки для $a^{-1} \pmod{33} = 5$. Тому ми вважаємо, що це і є ключ для дешифрування вказанного закодованого слова. До речі, якщо $a^{-1} \pmod{33} = 5$ то $a = 20$. ⑪

3.3. Алгебраїчний спосіб дешифрування. Метод прямого перебору, пояснений у прикладі 1, є достатньо ефективним для M_a кодів. Розглянемо один з його варіантів, який починається з припущення про рівність $\mathcal{C}_{\mathtt{X}} = \mathcal{P}_{\mathtt{Y}}$ для двох фіксованих букв X та Y.

Приклад 2. Припустимо, що повідомлення закодовано за допомогою шифру M_a. Якщо зробити припущення $\mathcal{C}_{\mathtt{Й}} = \mathcal{P}_{\mathtt{П}}$, то чи можна визначити a?

Ми знаємо, що для будь-якої букви `X`

$$\mathcal{C}_{\mathtt{X}} \equiv a \cdot \mathcal{P}_{\mathtt{X}} \pmod{33} \quad \text{та} \quad \mathcal{P}_{\mathtt{X}} \equiv a^{-1} \cdot \mathcal{C}_{\mathtt{X}} \pmod{33}.$$

Крім того, оскільки $\mathcal{P}_{\text{Й}} = 14$ та $\mathcal{P}_{\text{П}} = 20$, то

$$20 \equiv a \cdot 14 \pmod{33}.$$

Щоб розв'язати це рівняння відносно a, домножимо цю рівність на $26 = 14^{-1} \pmod{33}$: ⑫

$$520 \equiv a \pmod{33} \quad \text{або} \quad a = 25.$$

3.4. Для яких a існують M_a шифри. Це питання не є коректним, оскільки насправді M_a шифр існує для будь-якого $1 \le a \le 33$, але не для всіх a його можна однозначно дешифрувати. З теореми 1 випливає, що якщо a не ділиться на 3 та на 11, то M_a шифр можна однозначно дешифрувати. Іншими словами, для того, щоб M_a шифр можна було однозначно дешифрувати, необхідно, щоб існувало обернене $a^{-1} \pmod{33}$.

З іншого боку, для дешифрування M_a шифру необхідно знати саме обернене $a^{-1} \pmod{33}$ (див. (7)). Для зручності наведемо таблицю всіх чисел, взаємно простих з 33, та їхніх обернених. В таблиці 4 ми позначили $c = a^{-1} \pmod{33}$.

Таблиця 4. Взаємно прості з 33 та їхні обернені

a	2	4	5	7	8	10	13	14	16	17	19	20	23	25	26	28	29	31	32
c	17	25	20	19	29	10	28	26	31	2	7	5	23	4	14	13	8	16	32

⑬ Зверніть увагу на співпадіння:

$$10^{-1} \pmod{33} = 10, \qquad 23^{-1} \pmod{33} = 23,$$
$$32^{-1} \pmod{33} = 32.$$

До трійки 10, 23, 32 можна додати число 1, яке має ту ж властивість. Наявність чотирьох чисел a з властивістю $a^{-1} \pmod{33} = a$ відрізняє арифметику по модулю 33 від звичайної арифметики, в якій $a^{-1} = a$ тільки для двох чисел $a = \pm 1$.

3.5. Інші алфавіти. Ми вже відзначили, що зламати мультиплікативний шифр нескладно методом перебору. Цей метод стає менш ефективним, якщо параметр a стає достатньо великим. Нижче ми обговоримо декілька способів, ще далеких від практичного застосування, але які ускладнюють злам M_a шифру.

3.5.1. Перехід до "ширшого" алфавіту. Якщо в таблицю дешифрування включити цифри, то загальна кількість такого алфавіту сягне 43 символів. Для цього алфавіту можна обрати, наприклад, $a = 37$. Для методу грубої сили це означає витрати часу на 20% більші, ніж для звичайного алфавіту (необхідний час все одно є мізерним). ⑭ Іншим способом є включити в алфавіт інші символи, наявні на клавіатурі комп'ютера.

Найбільш радикальним є використання ASCII коду, який включає всі символи клавіатури, букви українського алфавіту, а також всі латинські букви. За допомогою ASCII можна кодувати 256 символів. ⑮

3.5.2. Групування. Суть цього способу пояснімо на прикладі. При шифруванні повідомлення

ЗУСТРІЧАЄМОСЬ О ВОСЬМІЙ

першою (додатковою) дією є групування букв по дві

(8) ЗУ СТ РІ ЧА ЄМ ОС Ь␣ О␣ ВО СЬ МІ Й␣

Тут використано символ ␣ для позначення проміжку між словами, а також для доповнення (якщо це є необхідним) останньої групи. Символ ␣ ми додаємо до алфавіту після Я.

Розглянемо "алфавіт", "буквами" якого є пари букв українського алфавіту з доданим символом ␣ . Цей "алфавіт" містить 1156 "букв". ⑯ Розташування "букв" в "алфавіті" може бути довільним.

Для шифрування повідомлення (8), кожну з його "букв" зашифруємо тепер за допомогою мультиплікативного шифру $M_{a,1156}$ з властивостями $1 < a < 1156$ і $(a, 1156) = 1$.

Цілком аналогічно попередньому аналізу $M_{a,33}$ шифру для звичайного алфавіту, дешифрування тепер також здійснюється за допомогою $M_{c,1156}$ шифру з $c = a^{-1} \pmod{1156}$.

Шифр стає ще більш захищеним, якщо попередньо групувати букви повідомлення у групи по три:

ЗУС ТРІ ЧАЄ МОС Ь␣О ␣ВО СЬМ ІЙ␣

⑰ У великих повідомленнях групи можуть складатись з більшої кількості "букв".

Зауваження 5. Припустимо, що кожна група складається з 10 букв. Тоді "алфавіт" містить $n = 33^{10} \approx 10^{13}$ (тобто, 10^4 мільярдів) "букв". При шифруванні повідомлень оберемо $a \approx 33^{10}$. Припустимо, що за одну секунду можна дешифрувати мільярд шифрів $M_{a,n}$. Тоді на повний перебір необхідно 10^4 секунд або 2 години та 37 хвилин. Чи є ефективним метод грубої сили в цьому випадку? Чи змінилась би відповідь на це питання, якщо групи складались з 11 символів?

Зауваження 6. Хоча порядок "букв" в "алфавіті" не є критичним для застосування мультиплікативних шифрів,

часто застосовують так званий *лексикографічний порядок*, який полягає у наступному: спочатку в цьому "алфавіті" розташовано "букви", які починаються з символа `А`, тобто `АА,АБ, ... ,А␣`; потім розташовано букви, які починаються з `Б`, тобто `БА,ББ, ... ,Б␣`; ... ; останніми "буквами" є `␣А,␣Б, ... ,␣␣`.

Лексикографічний порядок в "алфавіті" можна описати еквівалентним чином: "букву" `UV` розташовано в "алфавіті" раніше за "букву" `XY`, якщо $\mathcal{L}_{\mathtt{UV}} < \mathcal{L}_{\mathtt{XY}}$, де $\mathcal{L}_{\mathtt{UV}} = 100\mathcal{P}_{\mathtt{U}} + \mathcal{P}_{\mathtt{V}}$, $\mathcal{L}_{\mathtt{XY}} = 100\mathcal{P}_{\mathtt{X}} + \mathcal{P}_{\mathtt{Y}}$. ⑱

Найбільшим числом вигляду $100m + n$ з $1 \le m, n \le 34$, є 3434. Це означає, що не кожному числу з діапазону від 1 до 3434 можна поставити у відповідність певну "букву" з "алфавіту", але це не впливає на лексикографічний порядок.

Зрозуміло, що пара `АА` є першою в "алфавіті", а пара `␣␣` — останньою. Це підтверджується відповідними числами $\mathcal{L}_{\mathtt{АА}} = 100 * \mathcal{P}_{\mathtt{А}} + \mathcal{P}_{\mathtt{А}} = 101$ та $\mathcal{L}_{\text{␣ ␣}} = 100 * \mathcal{P}_{\text{␣}} + \mathcal{P}_{\text{␣}} = 3434$.

4. КОНТРОЛЬНІ ПИТАННЯ

1. Чому при $a = 33$ всі шифр-букви є однаковими для шифру M_a? (стор. 66).

2. Чому шифр M_a є еквівалентним шифру $M_{a \pmod{33}}$? (стор. 66).

3. Чому рівняння $ax \equiv 1 \pmod{33}$ не має розв'язків, якщо $a = 3$? (стор. 70).

4. Чому у доведенні теореми 1 з умови $(a, n) = 1$ випливає, що $0 \notin \{r_1, \ldots, r_{n-1}\}$? (стор. 71).

5. Пояснити, чому у доведенні теореми 1 стверджується, що якщо $a^{-1} \pmod{n}$ не існує, то $1 \notin \{r_1, \ldots, r_{n-1}\}$? (стор. 71).

6. Пояснити, чому у доведенні теореми 1 стверджується, що якщо $0, 1 \notin \{r_1, \ldots, r_{n-1}\}$, то знайдуться $1 \le j < i < n$, для яких $r_i = r_j$? (стор. 71).

7. У доведенні теореми 1 стверджується, що якщо $0 < i < j < n$, то конгруенція $(i-j)a \equiv 0 \pmod{n}$ неможлива. Чому це так? (стор. 71).

8. Довести наслідок 1. (стор. 72).

9. Підрахувати кількість взаємно простих чисел з 33 в інтервалі $[1, 33]$. (стор. 72).

10. Пояснити, чому у прикладі 1 випадок $a^{-1} \pmod{33} = 3$ можна не розглядати. (стор. 73).

11. Перевірити, що $a = 20$, якщо $a^{-1} \pmod{33} = 5$ у прикладі 1. (стор. 73).

12. Перевірити рівність $26 = 14^{-1} \pmod{33}$. (стор. 74).

13. Перевірте дані в таблиці 4. (стор. 74).

14. Оцінити час, необхідний для методу грубої сили у випадку алфавіту, який складається з 43 символів. (стор. 75).

15. Довести, що за допомогою ASCII можна кодувати 256 символів. (стор. 75).

16. Пояснити, чому "алфавіт", "буквами" якого є пари букв українського алфавіту з доданим символом ␣, містить 1156 "букв"? (стор. 76).

17. Проаналізувати спосіб шифрування за допомогою групування по три символи. (стор. 76).

18. Пояснити, чому правило $\mathcal{L}_{\mathtt{UV}} < \mathcal{L}_{\mathtt{XY}}$ є еквівалентним до лексикографічного порядку? (стор. 77).

5. З А Д А Ч І

Задача 1. *Довести, що формули* (4) *та* (5) *дають однаковий результат, якщо* $\mathcal{C}_{\mathtt{X}}$ *є парним.*

Задача 2. *Зашифрувати слово* `БУКВА` *за допомогою мультиплікативного шифру* M_{16}.

Задача 3. *Дешифрувати слово* `ИҐЄВЄ`, *яке було зашифровано за допомогою мультиплікативного шифру* M_{23}.

Задача 4. *Дешифрувати слово* `ЕЦЧЛЧ`, *яке спочатку було зашифровано за допомогою шифру* M_4, *а після цього — за допомогою шифру* M_7.

Задача 5. *Застосувати метод грубої сили і дешифрувати повідомлення українською мовою*

УҐКЦЛТОБ ЛШЩПДРЗШ ЮИСЙСЕЩШ ИЛҐЛУТШБ ХБЖЛСКУС
ОРКСАҐЩЖ РОРЙТЛСА ЙЦЖҐЛСКУ ШПШЇСХДР

яке було зашифровано мультиплікативним шифром $M_{a,33}$.

Задача 6. *Чи є мультиплікативний шифр* M_a *однозначним, якщо відомо, що*

(a) $\mathcal{P}_{\text{С}} = \mathcal{C}_{\text{И}}$?
(b) $\mathcal{P}_{\text{И}} = \mathcal{C}_{\text{С}}$?

Задача 7. *Чи існує* M_a *шифр, при якому*

a) $\mathcal{P}_{\text{Й}} = \mathcal{C}_{\text{Р}}$; b) $\mathcal{P}_{\text{Г}} = \mathcal{C}_{\text{С}}$; c) $\mathcal{P}_{\text{Е}} = \mathcal{C}_{\text{Є}}$;
d) $\mathcal{P}_{\text{В}} = \mathcal{C}_{\text{Б}}$; e) $\mathcal{P}_{\text{Ж}} = \mathcal{C}_{\text{М}}$; f) $\mathcal{P}_{\text{И}} = \mathcal{C}_{\text{Ж}}$.

Задача 8. *Відомо, що* $\mathcal{P}_{\text{О}} = \mathcal{C}_{\text{Х}}$, *якщо застосувати шифр* M_a. *Знайти* a.

Задача 9. *Розглянемо наступну систему шифрування, яка базується на алфавіті з 30 букв. Перед шифруванням кожне повідомлення змінюється так, щоб три обрані букви перейшли у три інші, а саме*

К → И, В → І, Р → Т.

Наприклад,

СЛОВО → СЛОІО

Після такої заміни у повідомленні використовується лише 30 букв українського алфавіту (всі, крім К, В *та* Р*). Змінене повідомлення шифрується за допомогою шифру* M_a. *Нижче показано процедуру шифрування слова* РЕЧЕННЯ *для шифру* M_7*:*

повідомлення	Р	Е	Ч	Е	Н	Н	Я
змінене повідомлення	Т	Е	Ч	Е	Н	Н	Я
числовий формат	23	7	28	7	18	18	33
$2 \cdot \mathcal{P}_{\text{Х}} \pmod{30}$	11	19	16	19	6	6	21
буквенний формат	И	О	Л	О	Д	Д	Р

Таким чином,

РЕЧЕННЯ → ИОЛОДДР

a) *Яким чином відбувається дешифрація повідомлення для описаного способу?*
b) *Чому шифр M_5 можна вживати для звичайного алфавіту, але небажано для розглянутого способу? З іншого боку, чому M_{11} можна вживати для описаної схеми, а для звичайного алфавіту ні?*
c) *Зашифрувати повідомлення* БУКВА, *використовуючи описану схему.*
d) *Пояснити, чому з точки зору криптоаналізу описана схема є більш стійкою, ніж мультиплікативний шифр для звичайного алфавіту?*

Задача 10. *Наступний спосіб допомагає зробити мультиплікативний шифр більш стійким. Обравши ключове слово, наприклад* ШОЛОМ, *переводимо його букви у цифровий формат. У нашому випадку цифровим ключем є* 29 19 16 19 17. *Під кожною буквою повідомлення запишемо відповідне число цифрового ключа з циклічним повтором. Наприклад, для повідомлення "*ЧЕКАЮ СЬОГОДНІ*" ми запишемо*

Ч	Е	К	А	Ю	С	Ь	О	Г	О	Д	Н	І
29	19	16	19	17	29	19	16	19	17	29	19	16

Тепер кожну букву повідомлення зашифруємо мультиплікативним шифром з параметром, що визначається другою строкою. Для нашого прикладу шифром буде

Ч	Е	К	А	Ю	С	Ь	О	Г	О	Д	Н	І
29	19	16	19	17	29	19	16	19	17	29	19	16
П	А	Ж	О	Л	И	Ч	Е	З	Х	Ж	І	Ц

a) *Як дешифрувати повідомлення, якщо ключове слово є відомим?*
b) *Дешифрувати повідомлення* ОВИКІХОКЄЦШ, *яке було зашифровано за допомогою ключового слова* ШОЛОМ.

Задача 11. *Нехай a та n є взаємно простими, а $1 \le m < n$. Довести, що рівняння $ax \equiv m \pmod{n}$ має розв'язок.*

Задача 12. *Нехай $i \ge 1$, а $n = (a_k a_{k-1} \dots a_1 a_0)_{10}$, причому $k \ge i$. Позначимо $n_i = (a_{i-1} \dots a_1 a_0)_{10}$ (n_i — це число, складене з останніх i десяткових цифр числа n).*

a *Довести, що n ділиться на 2^i тоді і тільки тоді, коли n_i ділиться на 2^i.*

b *Чи ділиться число* 343506076 *на* 4? *А на* 8?

Задача 13. *До 2007 року для ідентифікації друкованих видань використовувалась система ISBN–10, згідно до якої кожна книжка отримувала код, що складався з 10 символів, розбитих на блоки: перший блок ідентифікує мову видання, другий — видавництво, третій — номер книги. Четвертий блок відповідає за коректність запису номеру ISBN. Перші дев'ять символів у цьому номері є десятковими цифрами, а десятий — цифрою у системі за основою 11, тобто приймає значення* `0`, `1`, ... , `9` *або* `X`. *Якщо позначити через $x_1, x_2, \dots, x_{10}$ десяткові числа в номері ISBN, то x_{10} визначається формулою*

$$\sum_{i=1}^{10} i x_i \equiv 0 \pmod{11}.$$

a) *Довести*`0`, *що*

$$x_{10} \equiv \sum_{i=1}^{9} i x_i \pmod{11}.$$

b) *Обчислити контрольну цифру x_{10} для книжкового номера ISBN–10, який починається* `2-113-54001`.

Задача 14. *Доведіть, що помилку можна помітити, якщо у номері ISBN–10 (див. задачу* 13) *невірно записали один символ.*

Задача 15. *Доведіть, що помилку можна помітити, якщо у номері ISBN–10 (див. задачу* 13) *два символи випадково поміняли місцями.*

Задача 16. *З 2007 року діє система ISBN–13 ідентифікації книжок, яка використовує 13 символів. Останній символ використовується для перевірки коректності і визначається умовою*

$$\sum_{i=1}^{6}(x_{2i-1}+3x_{2i})+x_{13} \equiv 0 \pmod{10}.$$

Доведіть, що і ця система дозволяє помітити помилку, якщо у номері ISBN–13 невірно записали один символ.

Задача 17. *Показати, що система ISBN–13 не може розпізнати всі перестановки двох символів у номері.*

Задача 18. *Припустимо, що для перевірки коректності запису номеру використовується система запису десяти десяткових цифр, остання з яких визначається співвідношенням*

$$\sum_{i=1}^{10} x_i \equiv 0 \pmod{11}.$$

a) *Чи визначає ця система помилки в одному символі?*
b) *Чи визначає ця система помилку у зміні порядку двох символів?*

Задача 19. *Нескладно довести, що* $6! \equiv -1 \pmod 7$. *Дійсно* $6! = 1\cdot2\cdot3\cdot4\cdot5\cdot6 = 1\cdot(2\cdot4)\cdot(3\cdot5)\cdot6$. *Ми здійснили групування, об'єднавши у групи обернені за модулем:* $4 = 2^{-1} \pmod 7$, $5 = 3^{-1} \pmod 7$. *Тому* $6! \equiv 1\cdot6 \pmod 7 \equiv -1$.

Використовуючи цю ідею, довести теорему Вільсона: якщо p *є простим числом, то* $(p-1)! \equiv -1 \pmod p$.

Задача 20. *Метод факторизації натуральних чисел, який ми зараз опишемо, належить Д. Полларду й називається* ρ*-методом Полларда.*

Нехай задано число n*, яке має нетривіальний дільник. Розглянемо поліном* $f(x) = x^2+1$ *й натуральне число* x_0. *Побудуємо рекурентно послідовність натуральних чисел* $x_{k+1} \equiv f(x_k) \pmod n$, $k \geq 0$. *Якщо* $(x_j - x_i, n) \neq 1$ *для хоча б однієї пари* x_i *та* x_j, *то дільник* n *дорівнює* $(x_j - x_i, n)$.

Довести, що це дійсно так.

Задача 21. *За допомогою ρ-методу Полларда (задача 20) знайти дільник числа $n = 7943$, обравши $x_0 = 2$. Обчислені значення членів послідовності $\{x_i\}$ наведено нижче:*

$$x_1 = 5,\ x_2 = 26,\ x_3 = 677,\ x_4 = 5579,\ x_5 = 4568,\ x_6 = 364,\ \ldots .$$

Задача 22. *Довести, що обернене твердження до теореми Вільсона також є вірним: якщо $(n-1)! \equiv -1 \pmod{n}$, то n є простим числом.*

Задача 23. *Нехай $m = (a_k a_{k-1} \ldots a_1 a_0)_{10}$, де $a_0, a_1, \ldots, a_{k-1}, a_k$ — це цифри у десятковому записі числа m.*

a) *Довести, що $m \equiv (a_0 + a_1 + a_2 + \cdots + a_k) \pmod{9}$.*
b) *Використовуючи цю властивість перевірити, чи є $78,464$ сумою чисел 3569, $24,387$ та $49,508$?*

Задача 24. *Назвемо цифровим коренем натурального числа m число $1 \le \rho(m) \le 9$, яке утворено за наступним правилом: знайдемо суму цифр числа m, позначимо її s_1. Якщо $s_1 \le 9$, то $\rho(m) = s_1$; якщо ж $s_1 > 9$, то знайдемо суму цифр числа s_1, позначимо її s_2. Якщо $s_2 \le 9$, то $\rho(m) = s_2$; якщо ж $s_2 > 9$, то знайдемо суму цифр числа s_2, позначимо її s_3. Далі діємо за описаним правилом до тих пір, поки не дістанемо число, яке не перевищує 9; воно і є числовим коренем для m. Наприклад, числовим коренем числа 2015 є 8, а 1999 — є 1.*

Нехай $m = (a_1 a_2 \ldots a_k)_{10}$. Довести, що

$$\rho(m) = \begin{cases} (a_1 + \cdots + a_k) \pmod{9}, & (a_1 + \cdots + a_k) \not\equiv 0 \pmod{9}, \\ 9, & (a_1 + \cdots + a_k) \equiv 0 \pmod{9}. \end{cases}$$

Задача 25. *Нехай $\rho(n)$ — це числовий корень натурального числа n (див. задачу 24). Довести, що для будь-яких натуральних чисел m та n*

a) $\rho(\rho(n)) = \rho(n)$;
b) $\rho(m+n) = \rho(\rho(m) + \rho(n))$;
c) $\rho(mn) = \rho(\rho(m)\rho(n))$.

Задача 26.

a) *Знайти всі можливі числові корені для квадратів натуральних чисел (див. задачу* 24).

b) *Використовуючи отриманий результат, довести, що число* $n = 16\,151\,613\,924$ *не є квадратом.*

Задача 27. *Чи є вірним твердження, яке є оберненим до результату задачі 26? Іншими словами, чи обов'язково число є квадратом, якщо його числовий корінь дорівнює* 1, 4, 7 *або* 9?

Задача 28. *Нехай* $p > 3$ *та* $p + 2$ *— числа близнюки.*

a) *Довести, що числовий корінь їхнього добутку дорівнює* 8 *(див. задачу 24 стосовно означення числового кореня).*

b) *Чому це твердження є невірним для* $p = 3$?

Задача 29. *Номер кожної кредитної карти MasterCard складається з 16 десяткових цифр, які позначимо* $d_1, \ldots, d_{16}$. *Остання цифра* d_{16} *використовується для контролю. Вона обчислюється за правилом*

$$d_{16} \equiv -\left[\sum_{i=1}^{8} \rho(2d_{2i-1}) + \sum_{i=1}^{7} d_{2i}\right] \pmod{10},$$

де $\rho(m)$ *— це числовий корень числа* m *(див. задачу 24). Підрахувати* d_{16} *для карти, першими 15 цифрами якої є*

a) 5300–7402–4001–638 b) 5329–0419–4253–736.

Задача 30. *Діофантовим рівнянням першого степеня називають задачу знаходження натуральних* x *та* y, *при яких* $ax + by = c$, *де* a, b *та* c *— задані натуральні числа. Рівняння такого типу названо на честь грецького математика Діофанта, про якого мало що є відомим за винятком його творів, одним з яких є "Арифметика". Навіть дати його життя є невідомими, хоча зберігся старий текст, у якому про Діофанта написано*:

> дитинство тривало $\frac{1}{6}$ життя; через $\frac{1}{12}$ життя він завів бороду; ще через $\frac{1}{7}$ життя він оженився; син його народився через 5 років після одруження; син прожив $\frac{1}{2}$ життя батька, який помер через 4 роки після сина.

Першою задачею, розв'язаною в "Арифметиці", була така:

> 1. Задане число розкласти на два, різниця між якими є заданою.

"Арифметика" була добре відомою у Китаї. У книзі "Класична математика" Чан Чіу Чена (VI сторіччя) зустрічається така задача:

> Якщо півень коштує 5 монет, курка 3 монети, а три курчати разом 1 монету, то скільки півнів, кур та курчат (у загальній кількості 100), можна придбати за 100 монет?

a) *Скільки років прожив Діофант?*
b) *Розв'язати першу задачу з "Арифметики" Діофанта.*
c) *Звести задачу Чан Чіу Чена до діофантового рівняння та знайти її розв'язок.*

6. БІОГРАФІЇ

Діофант, *(др. грецькою* $\Delta\iota o\varphi\alpha\nu\tau o\varsigma$*)* (між 200 та 214 – між 284 та 298), давньогрецький математик, жив в III столітті в Александрії (Єгипет).

Обкладинки перекладів "Арифметики" Діофанта на латинську (зліва) та російську (справа) мови

Дати життя Діофанта точно не відомі. Наближені дати його життя отримано наступним чином. Теон Олександрійський в своїх коментарях до "Альмагесту" Птолемея навів уривок з творів Діофанта. Оскільки діяльність Теона падає на другу половину IV століття н. е., то Діофант не міг жити пізніше середини IV століття. Цим визначається верхня межа життя Діофанта.

З іншого боку, сам Діофант у своїй роботі "Про багатокутні числа" двічі згадує Гіпсікла (математика, який жив в Олександрії в середині

II століття до н. е.). Отже, нижньою межею є друга половина II століття до н. е. Таким чином, отримуємо проміжок в 500 років!

Діофант був останнім великим математиком античності. Разом з тим він був одним з перших творців нової алгебри, яка грунтується не так на геометрії (як це було у Евкліда, Архімеда і Аполлонія), а на арифметиці. Саме Діофант ввів негативні числа і користувався буквеною символікою.

З творів Діофанта до нас дійшло два: "Арифметика" ($Αριθμητικα$) і "Про багатокутні числа", проте обидва вони збереглися не повністю. З 13 книг "Арифметики", про які говорить Діофант у вступі до своєї роботи, до 1972 року були відомі тільки 6. У 1972 р. в Ірані був знайдений арабський переклад ще чотирьох книг. У "Арифметиці", коли мова йде про теоретико-числові твердження, Діофант зазвичай відсилає до своїх "Поризмів". Невідомо, чи була то окрема книга, або доведення у "Поризмах" були включені в саму "Арифметику". У всякому разі, жодного доведення теоретико-числового твердження від Діофанта до нас не дійшло.

Залишається також абсолютно незрозумілим питання про зв'язок "Арифметики" з дослідженнями конічних перетинів, проведеними з такою повнотою Аполлонієм, і кривих вищих порядків, якими займалися наступні математики. Багато задач Діофанта еквівалентні знаходженню раціональних точок на окружності або гіперболи, а підстановки, які він робить, відповідають проведенню прямої через деяку точку кривої і знаходженню другої точки перетину з нею. Чи здогадувався про це Діофант? Чи користувався він геометричною інтерпретацією? Його твори не дозволяють нам відповісти на це питання, хоча, звичайно, малоймовірно, щоб він не вбачав зв'язку рівнянь з відповідними алгебраїчними кривими.

"Арифметика" Діофанта — це збірник задач (їх всього 189), для кожної з яких наведено розв'язання (або декілька розв'язань, отриманих різними способами) і необхідними поясненнями. Тому з першого погляду здається, що вона не є теоретичним твором. Однак при уважному читанні видно, що завдання ретельно підібрані і розташовані так, що служать ілюстрацією цілком певних загальних методів. Як це було прийнято в античній математиці, методи не формулюються загальним чином, окремо від завдань, але розкриваються в процесі розв'язання.

Глава 4

АЛГОРИТМИ ЕВКЛІДА

В розділі §3.1 глави 3 ми з'ясували, що умова $(a, n) = 1$ є важливою для однозначності дешифрування мультиплікативних шифрів. Ми також встановили, що для дешифрування $M_{a,n}$ шифра необхідно знати число, обернене до множника шифру за його модулем, тобто $a^{-1} \pmod{n}$. В цій главі ми навчимося обчислювати $a^{-1} \pmod{n}$.

Але почнемо ми з алгоритму знаходження частки та остачі від ділення натуральних чисел на натуральні. Хоча цей алгоритм був відомий ще у Древній Греції, він й досі залишається одним з найбільш ефективних. Згадку про нього можна знайти в книзі VII (твердження 1) "*Елементів*" (грец. $\Sigma\tau o\iota\chi\varepsilon\tilde{\iota}\alpha$, лат. *Elementa*, рос. "*Начала*") Евкліда, написаних за 300 років до н. е. Тому його також називають *алгоритмом Евкліда*, хоча про цей алгоритм згадував ще Аристотель за кілька десятиріч до появи твору Евкліда. "*Елементи*" найстаріший грецький математичний трактат, що зберігся до наших часів. Хоча подібні твори існували й до Евкліда, усі вони були втрачені з плином часу.

В алгоритмі 1 для заданих натуральних чисел n та $a < n$ знаходяться цілі невід'ємні числа q та r, при яких $n = aq + r$. Ці числа називаються *часткою* та *остачею* від ділення n на a. Для знаходження q та r алгоритм рекурентно визначає члени арифметичної послідовності $\{v_k\}$ за правилом $v_k = v_{k-1} - a$. Першим членом цієї послідовності є $v_1 = n - a$.

Алгоритм 1. Знаходження частки та остачі від ділення

Вхідні дані: $a, n \in \mathbf{N}$, $1 \le a < n$;

Вихідні дані: натуральні $q \ge 0$ та $0 \le r < n$, для яких $n = aq + r$;

покласти $v_1 = n - a$;

якщо $v_1 < a$, то $r = v_1$, $q = 1$ STOP..

якщо ж $v_1 \ge a$, то покласти $v_2 = v_1 - a$;

якщо $v_2 < a$, то $r = v_2$, $q = 2$ STOP..

якщо ж $v_2 \ge a$, то покласти $v_3 = v_2 - a$;

якщо $v_3 < a$, то .....

.....

Якщо $v_k < n$ для якогось k, то на цьому кроці алгоритм закінчується визначенням двох чисел $r = v_k$ та $q = k$. Оскільки $v_k = v_{k-1} - a$, то $n = ka + r$, ① тобто r — це остача, а q — це частка від ділення n на a.

Алгоритм 1 закінчується за скінчену кількість кроків, оскільки на кожному кроці члени послідовності $\{v_k\}$ зменшуються на a. На певному кроці v_k стане меншим за n ② і саме тоді дія алгоритму закінчиться.

1. Алгоритм Евкліда знаходження найбільшого спільного дільника

Для знаходження найбільшого спільного дільника (a, n), $1 \le a < n$, можна використати *алгоритм Евкліда*. Позначимо $d = (n, a)$.

Алгоритм 2. Знаходження найбільшого спільного дільника

Вхідні дані: $a, n \in \mathbf{N}$, $1 \le a < n$;

Вихідні дані: найбільший спільний дільник $d = (a, n)$;

Поділити з остачею: $n = q_1 a + r_1$, $0 \le r_1 < n$;

якщо $r_1 = 0$, то $d = a$ `STOP`..

якщо ж $r_1 \neq 0$, то поділити з остачею a на r_1:

$$a = q_2 r_1 + r_2,\ 0 \le r_2 < r_1;$$

якщо $r_2 = 0$, то $d = r_1$ `STOP`..

якщо ж $r_2 \neq 0$, то поділити з остачею r_1 на r_2:

$$r_1 = q_3 r_2 + r_3,\ 0 \le r_3 < r_2;$$

якщо $r_3 = 0$, то $d = r_2$ `STOP`..

якщо ж $r_3 \neq 0$, то поділити з остачею r_2 на r_3:

$$r_2 = q_4 r_3 + r_4,\ 0 \le r_4 < r_3;$$

якщо $r_4 = 0$, то .....

.....

Алгоритм починається діленням n на a. Якщо n ділиться на a, то остача r_1 від ділення дорівнює 0. Тому $(n, a) = a$. Це зауваження реалізовано у другому рядку алгоритму 2.

Якщо ж n не ділиться на a, то в третьому рядку a ділимо на r_1. Якщо остача r_2 від ділення дорівнює 0, то в четвертому рядку стверджується, що $(n, a) = r_1$.

Далі дія алгоритму є цілком аналогічною: якщо остача від попереднього ділення не дорівнює 0, то на цю остачу ділиться попередня остача і здійснюється перевірка чи дорів-

нює нулеві нова остача. Якщо позначити

$$r_{-1} = n \quad \text{та} \quad r_0 = a, \tag{1}$$

то на i-ому кроці, $i \geq 1$, алгоритм 2 знаходить частку q_i та остачу r_i від ділення r_{i-2} на r_{i-1}, тобто представлення

$$r_{i-2} = q_i r_{i-1} + r_i, \qquad 0 \leq r_i < r_{i-1}. \tag{2}$$

③ Дія алгоритму завершується, якщо на певному кроці

$$r_{k-1} = r_k q_{k+1}. \tag{3}$$

В цьому випадку алгоритм стверджує, що $(n, a) = r_k$.

Чи закінчується алгоритм 2 за скінчену кількість кроків? Якщо так, то чи дійсно знайдене r_k дорівнює (n, a)?

Теорема 1. *Дія алгоритму* 2 *закінчується за скінчену кількість кроків. Якщо алгоритм* 2 *закінчується після обчислення* q_{k+1} (*див. рівність* (3)), *то* $(a, n) = r_k$.

Доведення. На i-ому кроці алгоритм 2 обчислює остачу r_i від ділення r_{i-2} на r_{i-1} (див. рівність (2)). Цей процес не може тривати безкінечно, оскільки остачі зменшуються, ④ залишаючись невід'ємними. Таким чином, на певному кроці остача стане рівною 0, тобто буде виконано умову (3). Наступна перевірка завершить дію алгоритму, при цьому $d = r_k$.

Для доведення рівності $(n, a) = r_k$ доведемо спочатку наступну лему.

Лема 1. *Якщо* $i = qj + r$, $r \neq 0$, *то* $(i, j) = (j, r)$.

Доведення леми 1. Зрозуміло, що якщо i та j діляться на якесь натуральне число m, то й r повинно ділитися на m. ⑤ Це означає, що r ділиться на (i, j), тобто (j, r) ділиться на (i, j). ⑥

Аналогічно, якщо j та r діляться на якесь наткральне число m, то й i повинно ділитися на m. Звідси випливає, що (i, j) ділиться на (j, r). Це і доводить лему. □

Тепер ми в змозі закінчити доведення теореми 1. На підставі леми 1, з першого рядка алгоритму Евкліда отримуємо $(n, a) = (a, r_1)$, а з другого — що $(a, r_1) = (r_1, r_2)$. Третій та четвертий рядки нам дають: $(r_1, r_2) = (r_2, r_3)$ та $(r_2, r_3) = (r_3, r_4)$. На підставі цих міркувань $(n, a) = (r_3, r_4)$.

Останній рядок (3) дає $(r_{k-1}, r_k) = r_k$. Повертаючись назад на один крок від рядка (3), отримуємо $(r_{k-2}, r_{k-1}) = (r_{k-1}, r_k) = r_k$. Якщо діяти таким же чином і далі, ми доведемо, що $(a, n) = r_k$. ⑦ □

Зауваження 1. Як довго продовжується дія алгоритму 2? Одна з можливих оцінок є такою:

$$k \leq 5[\log_{10} a] + 5.$$

Цей результат, доведений в 1844 році Г. Ламе, називається *теоремою Ламе*. Коефіцієнт 5 можна зменшити до

$$\frac{\ln(10)}{\ln(\phi)} \approx 4.785, \qquad \phi = \frac{1 + \sqrt{5}}{2},$$

де ϕ — це *золотий переріз*.

Зауважимо, також, що кількість кроків, необхідних для завершення алгоритму Евкліда, не залежить від найбільшого з чисел (у нашому випадку, від n): вона зростає дуже

повільно у порівнянні з ростом найменшого з двох чисел (у нашому випадку, з ростом a).

2. Знаходження оберненого числа в арифметиці за модулем

Якщо позначити $c = a^{-1} \pmod{n}$, то $ac \equiv 1 \pmod{n}$ за означенням оберненого числа, причому $1 \leq c < n$. Цю конгруенцію можна преписати у вигляді

$$ac - 1 = nj \qquad \text{або} \qquad ac + n \cdot (-j) = 1$$

для деякого j. Це означає, що рівняння

$$ax + ny = 1 \tag{4}$$

має розв'язок у цілих числах: $x = c$, $y = -j$.

Нескладно побачити, що і навпаки, якщо рівняння (4) має розв'язок у цілих числах, то $(a, n) = 1$. Більше того, одним з розв'язків є $x = a^{-1} \pmod{n}$.

Теорема 2 (*про знаходження оберненого за модулем*)**.** *Рівняння* (4) *має розв'язок у цілих числах тоді і тільки тоді, коли* $(a, n) = 1$. *Якщо* $(a, n) = 1$, *то для скорочення запису позначимо* $c = a^{-1} \pmod{n}$. *Тоді кожен розв'язок рівняння* (4) *має вигляд*

$$x = c + \lambda n, \tag{5}$$

$$y = y_0 - a\lambda, \quad \textit{де} \quad y_0 = \frac{1 - ac}{n} \tag{6}$$

при деякому $\lambda \in \mathbf{Z}$. ⑧ *Один з розв'язків є таким, що*

$$x = a^{-1} \pmod{n}. \tag{7}$$

Доведення. Першу частину твердження теореми 2 про розв'язність рівняння (4) у випадку $(a, n) = 1$ ми вже довели вище, тому зосередимось на доведенні другої частини.

Якщо позначити через x, y розв'язок рівняння (4), то $ax \equiv 1 \pmod{n}$, звідки робимо висновок, що $x = c + \lambda n$ для деякого $\lambda \in \mathbf{Z}$, тобто представлення (5) доведено. ⑨ Тоді для кожного розв'язку x, y

$$1 = ax + ny = ac + a\lambda n + ny \pm ny_0 = 1 + n(a\lambda + y - y_0),$$

тобто $y = y_0 - a\lambda$, ⑩ що і закінчує доведення представлення (6).

Зрозуміло, що рівність (7) виконується при $\lambda = 0$. Більше того, якщо розв'язок x має вигляд (5), то $c = x \pmod{n}$, тобто обернене число c можна легко знайти, якщо знати один з розв'язків рівняння (4). ⑪ □

2.1. Побудова оберненого за модулем. Алгоритм Евкліда 2 можна пристосувати для знаходження оберненого числа в арифметиці за модулем. Пояснімо це спочатку на прикладі.

Приклад 1. Нехай $a = 16$, а $n = 75$. Тоді алгоритм Евкліда для знаходження найбільшого спільного дільника записується таким чином:

$$\begin{aligned} 75 &= 16 \cdot 4 + 11, \\ 16 &= 11 \cdot 1 + 5, \\ 11 &= 5 \cdot 2 + 1, \\ 5 &= 1 \cdot 5 + 0. \end{aligned}$$

Таким чином, $(16, 75) = 1$, тобто $16^{-1} \pmod{75}$ існує. У символьних позначеннях: $q_3 = 2$, $q_2 = 1$, $q_1 = 4$. Побудуємо

таблицю для знаходження $16^{-1} \pmod{75}$, почавши з такої

(8)

			q_3	q_2	q_1
0	1				

$=$

			2	1	4
0	1				

Ми будемо виконувати для фрагментів

		i_3
i_1	i_2	

таблиці (8) таке перетворення:

(9)

		i_3
i_1	i_2	

$\longrightarrow$

		i_3
i_1	i_2	i_4

, де $i_4 = i_3 i_2 + i_1$.

Починаємо з фрагменту

		q_3
0	1	

, потім таке ж перетворення здійснюємо з фрагментом, який отримується з попереднього зсуненням на одну позицію вправо, і так далі. Послідовність перетворень є такою:

		2	1	4
0	1			

$\to$

		2	1	4
0	1	2		

$\to$

		2	1	4
0	1	2	3	

$\to$

		2	1	4
0	1	2	3	14

Тепер таблиця є заповненою. Нескладно перевірити, що

$$n \cdot 3 - a \cdot 14 = 1 \quad \text{або} \quad a \cdot (-14) + n \cdot 3 = 1.$$

Коефіцієнтом при a обрано останній елемент другого рядку, а коефіцієнтом при n — передостанній її елемент. Таким чином, пара чисел $-14, 3$ є розв'язком рівняння (4). Згідно до теореми 2 маємо $-14 = c + \lambda \cdot 75$ при деякому $\lambda \in \mathbf{Z}$. При $\lambda = -1$ отримуємо $c = 61$, тобто $16^{-1} \pmod{75} = 61$ Тепер цей результат можна перевірити безпосередньо. ⑫

Загальний випадок розглянуто у наступному результаті.

Теорема 3 (*алгоритм знаходження оберненого за модулем*)**.** *Нехай* $n \in \mathbf{N}$, $1 < a < n$ *та* $(a, n) = 1$. *Припустимо, що алгоритм Евкліда завершився на* $(k+1)$*-му кроці рядком* (3). *Починаючи з наступної таблиці з незаповненим другим рядком*

(10)

	q_k	$\dots$	q_2	q_1
0	1	$\dots$		

,

здійснимо послідовно перетворення (9) *й повністю заповнимо другий рядок таблиці* (10):

(11)

	q_k	$\dots$	q_2	q_1
0	1	u_k $\dots$	u_2	u_1

.

Тоді

$$nu_2 - au_1 = \pm 1. \tag{12}$$

Тому рівняння (4) *має розв'язок* $x = -u_1$, $y = u_2$, *якщо* $nu_2 - au_1 = 1$; *або* $x = u_1$, $y = -u_2$, *якщо* $nu_2 - au_1 = -1$.

Крім того,

$$c = u_1 \pmod{n}, \quad \textit{якщо} \quad nu_2 - au_1 = -1;$$
$$c = -u_1 \pmod{n}, \quad \textit{якщо} \quad nu_2 - au_1 = 1.$$

Доведення. Позначимо $u_{k+1} = 1$ та $u_{k+2} = 0$. Тоді зрозуміло, що

$$u_i = q_i u_{i+1} + u_{i+2}, \qquad i = k, k-1, \dots, 1. \tag{13}$$

Покладемо, як і вище, $r_0 = a$, $r_{-1} = n$. Тоді алгоритм 2 здійснить такі обчислення:

$$\begin{aligned} r_{-1} &= r_0 q_1 + r_1, \\ r_0 &= r_1 q_2 + r_2, \\ &\dots\dots\dots\dots\dots\dots\dots \\ r_{k-2} &= r_{k-1} q_k + r_k, \\ r_{k-1} &= r_k q_{k+1}. \end{aligned}$$

Ясно, що кожен з рядків включно з передостаннім можна записати так

$$r_i = r_{i+1} q_{i+2} + r_{i+2}, \qquad 1 \le i < k-1. \tag{14}$$

Використавши (14), обчислимо $nu_2 - au_1$:

$$nu_2 - au_1 = nu_2 - a(q_1 u_2 + u_3) = u_2(n - aq_1) - au_3.$$

Оскільки $r_{-1} = n$, $r_0 = a$ (див. (1)), то $n - aq_1 = r_1$ й тому

$$r_i u_{i+3} - r_{i+1} u_{i+2} = -r_{i+1} u_{i+4} + r_{i+2} u_{i+3} \tag{15}$$

при $i = -1$. Доведемо цю властивість також і для всіх $i = 0, \dots, k-1$. Дійсно, з (13) та (14) випливає, що

$$\begin{aligned} r_i u_{i+3} - r_{i+1} u_{i+2} &= r_i u_{i+3} - r_{i+1}(q_{i+2} u_{i+3} + u_{i+4}) \\ &= u_{i+3}(r_i - r_{i+1} q_{i+2}) - r_{i+1} u_{i+4} \\ &= r_{i+2} u_{i+3} - r_{i+1} u_{i+2}, \end{aligned}$$

що й доводить (15) для всіх $i = -1, 0, \dots, k-1$.

Ланцюжок рівностей (15) починається при $i = -1$ і закінчується при $i = k - 1$. Таким чином,

$$\begin{aligned} nu_2 - au_1 &= r_{-1}u_2 - r_0u_1 = -(r_0u_3 - r_1u_2) \\ &= r_1u_4 - r_2u_3 = -(r_2u_5 - r_3u_4) \\ &= \cdots = \pm(r_{k-1}u_{k+2} - r_ku_{k+1}) = \mp r_k, \end{aligned}$$

оскільки $u_{k+2} = 0$ та $u_{k+1} = 1$. Згідно до теореми 1 маємо $r_k = (n, a) = 1$, що і закінчує доведення. $\square$

Зауваження 2. Знак правої частини (12) змінюється при збільшенні k на одиницю. Тому цю формулу можна переписати таким чином:

$$nu_2 - au_1 = (-1)^k.$$

3. Розширений алгоритм Евкліда

Обернене число в арифметиці за модулем можна також знайти за допомогою так званого *розширеного алгоритма Евкліда.* Цей алгоритм вперше було опубліковано в 1740 році англійським математиком Н. Саундерсом, але він сам віддавав пріоритет іншому англійському математику Р. Коетсу, який застосовув алгоритм для розкладу дійсних чисел у ланцюгові дроби.

У той час, коли "звичайний" алгоритм Евклида (алгоритм 2) знаходить найбільший спільний дільник двох чисел a та b, розширений алгоритм Евклида додатково знаходить коефіцієнти x та y, для яких

$$a \cdot x + b \cdot y = (a, b).$$

Знайдені коефіцієнти x та y визначають обернене число за модулем у випадку $(a, b) = 1$.

Алгоритм 3. Розширений алгоритм Евкліда

Вхідні дані: $n \in \mathbf{N}$, $1 \le a < n$;

Вихідні дані: $\{u'_k\}$, $\{v_k\}$, $\{u_k\}$, $\{v'_k\}$, $\{s_k\}$, $\{t_k\}$, $\{q_k\}$, $\{r_k\}$;

покладемо $u'_1 = 0$, $v_1 = 0$, $u_1 = 1$, $v'_1 = 1$, $s_1 = n$, $t_1 = a$;

ділимо s_1 на t_1: $s_1 = t_1 q_1 + r_1$, $0 \le r_1 < t_1$;

якщо $r_1 = 0$, то $u'_1 a + v'_1 n = s_1$, $u_1 a + v_1 n = t_1$ STOP..

якщо ж $r_1 \ne 0$, то покладемо $u'_2 = u_1$, $v_2 = v'_1 - q_1 v_1$,

$u_2 = u'_1 - u_1 q_1$, $v'_2 = v_1$,

$s_2 = t_1$, $t_2 = r_1$;

ділимо s_2 на t_2: $s_2 = t_2 q_2 + r_2$, $0 \le r_2 < t_2$;

якщо $r_2 = 0$, то $u'_2 a + v'_2 n = s_2$, $u_2 a + v_2 n = t_2$ STOP..

якщо ж $r_1 \ne 0$, то покладемо .....

.....

В алгоритмі 3 покроково обчислюються послідовності

$$\{u'_k\}, \quad \{v_k\}, \quad \{u_k\}, \quad \{v'_k\}, \quad \{s_k\}, \quad \{t_k\}, \quad \{q_k\}, \quad \{r_k\}.$$

Зауваження 3. Якщо не обчислювати послідовності

$$\{u'_k\}, \quad \{v_k\}, \quad \{u_k\}, \quad \{v'_k\}, \tag{16}$$

то розширений алгоритм Евкліда є цілком ідентичним до алгоритму 2. ⑬ Це означає, що алгоритм 3 закінчується через скінчену кількість кроків.

Умовою завершення алгоритму 3 на кроці k є

$$r_k = 0. \tag{17}$$

В алгоритмі 3 стверджується, що при $i = k$

$$u'_i a + v'_i n = s_i, \qquad u_i a + v_i n = t_i. \tag{18}$$

Насправді ж ці рівності виконуються на кожному кроці до завершення алгоритму.

Лема 2. *Умови* (18) *виконано на кожному кроці до завершення алгоритму.*

Доведення. Дійсно, при $k = 1$ умови (18) стають тривіальними: $n = n$ та $a = a$ відповідно. ⑭ Припустимо, що рівності (18) виконано для якогось кроку $i < k$. Доведемо їх для наступного кроку $i+1$. Перш за все запишемо правила, за якими змінюються члени послідовностей на наступному кроці:

$$u'_{i+1} = u_i, \quad v_{i+1} = v'_i - q_i v_i, \quad u_{i+1} = u'_i - u_i q_i,$$
$$v'_{i+1} = v_i, \quad s_{i+1} = t_i, \quad t_{i+1} = r_i.$$

Тому за припущенням індукції

$$u'_{i+1} a + v'_{i+1} n = u_i a + v_i n = t_i.$$

За правилом перетворення $t_i = s_{i+1}$, тому $u'_{i+1} a + v'_{i+1} n = s_{i+1}$, що й доводить першу рівність у (18) для кроку $i + 1$.

Крім того,

$$\begin{aligned} u_{i+1} a + v_{i+1} n &= (u'_i - u_i q_i) a + (v'_i - q_i v_i) n \\ &= u'_i a + v'_i n - q_i (u_i a + v_i n) \\ &= s_i - q_i t_i. \end{aligned}$$

Згідно алгоритму $r_i = s_i - q_i t_i$, а за правилом перетворення $t_{i+1} = r_i$, звідки $u_{i+1}a + v_{i+1}n = t_{i+1}$, тобто і другу рівність у (18) виконано для кроку $i+1$. $\square$

Теорема 4. *Нехай для певного k виконано умову* (17), *тобто алгоритм* 3 *закінчується на кроці k. Тоді*

$$u_k a + v_k n = (n, a).$$

Таким чином, якщо a та n є взаємно простими, то

$$u_k a + v_k n = 1.$$

Доведення. З другої умови в (18) випливає, що $u_k a + v_k n = t_k$. Оскільки t_k — це остача від ділення на попередньому кроці, то $t_k = (n, a)$ на підставі теореми 1. $\square$

4. КОНТРОЛЬНІ ПИТАННЯ

1. Перевірити, що $n = ka + r$ в алгоритмі 1. (стор. 89).

2. Чому на певному кроці алгоритму 1 число v_k стане меншим за n? (стор. 89).

3. Впевнитись, що на k-ому кроці алгоритм 2 обчислює формулу (2) (стор. 91).

4. Чому остачі в алгоритмі 2 зменшуються на кожному кроці? (стор. 91).

5. Чому у доведенні леми 1 стверджується, що r повинно ділитися на k? (стор. 91).

6. Пояснити, чому (j, r) ділиться на (i, j) у доведенні леми 1? (стор. 91).

7. Чому у доведенні теореми 1 стверджується, що $(a, n) = r_k$? (стор. 92).

8. Чому у формулюванні теореми 2 число y_0 є цілим? (стор. 93).

9. Пояснити, чому рівність $x = c + \lambda n$ виконано для деякого $\lambda \in \mathbf{Z}$ у доведенні теореми 2? (стор. 94).

10. Чому $y = y_0 - a\lambda$ у доведенні теореми 2? (стор. 94).

11. Як знайти c, якщо знати тільки один з розв'язків рівняння (4)? (стор. 94).

12. Перевірити рівність $16^{-1} \pmod{75} = 61$. (стор. 95).

13. Впевнитись, що алгоритм 3 є цілком ідентичним до алгоритму 2, якщо не обчислювати послідовності (16). (стор. 99).

14. Перевірити, що умови (18) стають тривіальними при $k = 1$, а саме $n = n$ та $a = a$. (стор. 100).

5. З А Д А Ч І

Задача 1. *Використовуючи алгоритм Евкліда (алгоритм 2), знайти найбільший спільний дільник (a, b) чисел a та b:*

a) $a = 4076$ *та* $b = 1024$; b) $a = 4076$ *та* $b = 1706$;
c) $a = 1769$ *та* $b = 2378$; d) $a = 1331$ *та* $b = 5005$.

Задача 2. *За допомогою алгоритму Евкліда (алгоритм 2) знайти найбільший спільний дільник чисел*

a) 1024 *та* 1000; b) 2024 *та* 1024;
c) 5040 *та* 7700; d) 3777 *та* 5565.

Задача 3. *За допомогою алгоритму Евкліда знайти*

(a) $(252, 198)$; (b) $(34, 55)$; (c) $(20785, 44350)$.

Задача 4. *За допомогою алгоритму Евкліда (алгоритм 2) знайти*

(a) $(45, 75)$; (b) $(102, 222)$; (c) $(666, 1414)$.

Задача 5. *За допомогою алгоритму Евкліда* (*алгоритм* 2)*знайти найбільший спільний дільник чисел*

a) 2076 *та* 1076; b) 2076 *та* 1776;
c) 1976 *та* 1776; d) 3076 *та* 1776.

Задача 6. *Довести, що теорему* 3 *можна використовувати навіть у випадку* $(a, n) \neq 1$. *Які зміни необхідно внести у формулювання теореми, якщо* $(a, n) \neq 1$?

Задача 7. *Використовуючи обчислення, зроблені при розв'язанні задачі* 1, *та задачу* 6 *записати* $(4076, 1024)$ *у вигляді лінійної комбінації* 4076 *та* 1024. *Цю ж задачу розв'язати для пар чисел* (b)–(d) *з задачі* 1.

Задача 8. *Записати* (a, b) *у вигляді лінійної комбінації* a *та* b *для чисел з задачі* 2.

Задача 9. *Записати* (a, b) *у вигляді лінійної комбінації* a *та* b *для чисел з задачі* 3.

Задача 10. *Записати* (a, b) *у вигляді лінійної комбінації* a *та* b *для чисел з задачі* 4.

Задача 11. *Записати* (a, b) *у вигляді лінійної комбінації* a *та* b *для чисел з задачі* 5.

Задача 12. *Використовуючи розширений алгоритм Евкліда* (*алгоритм* 3), *записати* (a, b) *у вигляді лінійної комбінації* a *та* b *для чисел з задачі* 2.

Задача 13. *Використовуючи розширений алгоритм Евкліда* (*алгоритм* 3), *записати* (a, b) *у вигляді лінійної комбінації* a *та* b *для чисел з задачі* 5.

Задача 14. *Нехай* $(a, n) = d$. *Довести, що* $(a/d, n/d) = 1$.

Задача 15. *Нехай* a, b, c — *три натуральні числа. Довести, що* $(ac, bc) = c(a, b)$.

Задача 16. *Спростувати наступне твердження: якщо* $(a,b) = 1 = (b,c)$, *то* $(a,c) = 1$.

Задача 17. *Спростувати наступне твердження: якщо* $(a,b) = 2 = (b,c)$, *то* $(a,c) = 2$.

Задача 18. *Нехай* $p_1, \ldots, p_n$ *— різні прості числа,* $a = p_1^{\alpha_1} \ldots p_n^{\alpha_n}$, $b = p_1^{\beta_1} \ldots p_n^{\beta_n}$. *Довести, що* $(a,b) = p_1^{\min\{\alpha_1,\beta_1\}} \ldots p_n^{\min\{\alpha_n,\beta_n\}}$.

Задача 19. *Найменшим спільним кратним двох натуральних чисел* a *та* b *називається найменше натуральне число, яке ділиться і на* a, *і на* b. *Це число позначається* $[a,b]$. *Довести, що*

a) *якщо* p *— просте число,* $a = p^\alpha$, $b = p^\beta$, *то* $[a,b] = p^{\max\{\alpha,\beta\}}$;
b) *якщо* p_1, p_2 *— два різних простих числа,* $a = p_1^{\alpha_1} p_2^{\alpha_2}$, $b = p_1^{\beta_1} p_2^{\beta_2}$, *то* $[a,b] = p_1^{\max\{\alpha_1,\beta_1\}} p_2^{\max\{\alpha_2,\beta_2\}}$;
c) *якщо* $p_1, \ldots, p_n$ *— різні прості числа,* $a = p_1^{\alpha_1} \ldots p_n^{\alpha_n}$, $b = p_1^{\beta_1} \ldots p_n^{\beta_n}$, *то* $[a,b] = p_1^{\max\{\alpha_1,\beta_1\}} \ldots p_n^{\max\{\alpha_n,\beta_n\}}$.

Задача 20. *Знайти* $[a,b]$ *для всіх пар чисел* a *та* b *з задачі* 1.

Задача 21. *Знайти* $[a,b]$ *для всіх пар чисел* a *та* b *з задачі* 2.

Задача 22. *Знайти* $[a,b]$ *для всіх пар чисел* a *та* b *з задачі* 3.

Задача 23. *Знайти* $[a,b]$ *для всіх пар чисел* a *та* b *з задачі* 4.

Задача 24. *Знайти* $[a,b]$ *для всіх пар чисел* a *та* b *з задачі* 5.

Задача 25. *Довести, що* $[a,b] \cdot (a,b) = ab$.

Задача 26. *Довести, що* $(a,b) \mid [a,b]$.

Задача 27. *Довести, що* $[ca,cb] = c[a,b]$.

Задача 28. *Чи є вірними наступні твердження?*

a) *Найменше спільне кратне двох простих чисел дорівнює їхньому добутку.*
b) *Найменше спільне кратне двох послідовних натуральних чисел дорівнює їхньому добутку.*
c) *Найменше спільне кратне двох різних простих чисел дорівнює їхньому добутку.*

d) *Якщо* $(a, b) = 1$, *то* $[a, b] = ab$.
e) *Якщо* $p \nmid a$, *то* $[p, a] = pa$.

Задача 29. *Чи є вірними наступні твердження?*

a) *Якщо* $[a, b] = 1$, *то* $a = 1 = b$.
b) *Якщо* $[a, b] = b$, *то* $a = 1$.
c) *Якщо* $[a, b] = b$, *то* $a \mid b$.
d) *Якщо* $[a, b] = ab$, *то* $a = b$.
e) *Якщо* $[a, b] = ab$ *and* $[b, c] = bc$, *то* $[a, c] = ac$.

Задача 30. *Розглянемо прямокутник розміру* 23×13, *який позначимо* P_1 (*див. рис.* 1). *Найбільший квадрат* K_1, *який можна в нього вписати, має розмір* 13×13. *Найбільший квадрат* K_2, *який можна вписати в* $P_2 = P_1 \setminus K_1$, *має розмір* 10×10. *В* $P_3 = P_2 \setminus K_2$ *можна вписати три квадрати розміру* 3×3. *Після цього залишаються три квадрати розміру* 1×1 (*див. рис.* 2).

Рис. 1. *Прямокутник* P_1

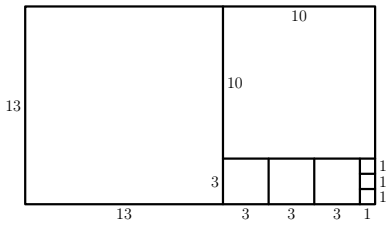


Рис. 2. *Вписані квадрати*

Запишемо тепер дії алгоритму Евкліда для знаходження $(23, 13)$:

$$\begin{aligned} 23 &= 1 \cdot 13 + 10 \\ 13 &= 1 \cdot 10 + 3 \\ 10 &= 3 \cdot 3 + 1 \\ 3 &= 3 \cdot 1. \end{aligned} \tag{19}$$

a) *Чи бачите ви зв'язок між обчисленнями в алгоритмі Евкліда та заповненням прямокутника квадратами?*
b) *Чи є цей зв'язок універсальним?*

Задача 31. *Два гравці починають гру, маючи пару додатних чисел. По черзі вони роблять кроки наступного типу. Гравець може спочатку переставити числа у порядку зростання, а потім замінити нову пару* $\langle x, y\rangle$, $x \geq y$, *на будь-яку іншу вигляду* $\langle x - ty, y\rangle$, *де* t — *таке натуральне число, що* $x - ty \geq 0$. *Виграє той, хто першим отримає пару з нульовою координатою. Доведіть, що якщо гра починається з парою* $\langle a, b\rangle$, *то вона закінчується парою* $\langle 0, (a, b)\rangle$.

Задача 32. *Нехай* $a \in \mathbf{N}$. *Розглянемо всі такі числа* n, *що алгоритм Евкліда закінчується за* n *кроків при обчисленні* (a, b) *для деякого* $b < a$ (*тобто,* $(a, b) = r_{n-1}$). *Найбільше з таких* n *назвемо висотою числа* a *і позначимо* $h(a)$.

a) *Довести, що* $h(a) = 1$ *тоді і тільки тоді, коли* $a = 2$;
b) *Підрахувати* $h(a)$ *для* $a \leq 8$.

6. БІОГРАФІЇ

Евклід, *грец.* $Ενκλειδης$ (близько 365–близько 300 до Р. Х.), старогрецький математик і визнаний основоположник математики.

Евклід

Наукова діяльність Евкліда проходила в Александрійській бібліотеці — суспільній інституції, що являла собою бібліотечний, науковий, навчальний, інформаційно-аналітичний, і культурологічний комплекс.*

Основна праця Евкліда "*Начала*" (латинізована назва "*Елементи*") включає в себе 13 книжок, у яких міститься систематизований виклад геометрії, а також деяких питань теорії чисел.

Книги з такою ж назвою, в яких послідовно викладалися всі основні факти геометрії і теоретичної арифметики, складалися раніше Гіппократом Хіосським, Леонтом і Февдієм. Проте "*Начала*" Евкліда витіснили всі ці твори з ужитку і протягом більш ніж двох тисячоліть

---

* Місто Александрія знаходиться зараз у Єгипті. Александрійська бібліотека заснована, як вважається, Птолемеєм I на початку третього століття до Р. Х. Значення цієї величезної бібліотеки важко переоцінити для елінського світу: у ній зберігалися сотні тисяч папірусних сувій, які використовувались вченими для розвитку науки.

залишалися базовим підручником геометрії. Створюючи свій підручник, Евклід включив в нього багато з того, що було створене його попередниками, обробивши цей матеріал і звівши його воєдино.

У рукописах, що дійшли до нас, до тринадцяти книг Евкліда додані ще дві: XIV книга належить александрійцу Гипсиклу (біля 200 р. до Р. Х.), а XV книгу створено під час життя Ісідора Мілетського, будівельника храму св. Софії в Константинополі (початок VI ст. Р. Х.).

Коментарі до "*Начал*" в античності складали Герон, Порфирій, Папп, Прокл, Симплікій. Зберігся коментар Прокла до I книги, а також коментар Паппа до X книги (у арабському перекладі).

У створенні і розвитку науки нового часу "*Начала*" зіграли важливу ідейну роль; вони залишаються і донині зразком математичного строгості.

Алгоритм знаходження найбільшого спільного дільника двох чисел (алгоритм 2) в "*Началах*" описано двічи, спочатку у книзі VII (для знаходження найбільшого спільного дільника двох натуральних чисел), а потім у книзі X (для знаходження найбільшої загальної міри двох однорідних величин). В обох випадках Евклід надав геометричний опис алгоритму.

Цей алгоритм не було відкрито Евклидом, оскільки згадка про нього є вже в "*Топіках*" Аристотеля. Давньогрецькі математики називали цей алгоритм $\alpha\nu\theta\nu\phi\alpha\iota\rho\varepsilon\sigma\iota\zeta$, тобто "взаємне віднімання".

Про життя Евкліда мало що відомо, крім того, що він жив і викладав в Александрії. Тим не менш, існує багато фольклорних цитат, приписуваних Евкліду. Наприклад, він нібито був учителем правителя Птолемея I, який царював з 306 р. до Р. Х. Якось Птолемей запитав у Евкліда, чи є простіший спосіб вивчити геометрію. Евклід нібито відповів, що у геометрії не існує царської дороги.**

** Про це написав Прокл у коментарях до книги I Евклідівських "*Начал*". Вираз "царська дорога" став крилатим ще в античні часи; так називали найбільш швидкий, легкий й розумний спосіб досягнути своєї мети. Вираз з'явився після того, як Геродот у своїй "*Історії*" із захопленням описав спосіб доставки пошти у V сторіччі до Р. Х. під час правління персидського царя Дарія, який побудував для цього спеціальну дорогу.

Ламе, *Габриель* (1795–1870), французький математик, механік, фізик та інженер. Вніс вагомий вклад в розвиток математичної фізики та теорії пружності.

Габриель Ламе

Ламе вважається провідним французьким математиком свого часу. Про це писали багато хто, зокрема Гаусс, який не був людиною, яка так просто поширювала схвальні відгуки про інших. Дивно, але за межами Франції йому давали більш високі оцінки, ніж усередині країни. Можливо французам, здавалося, що його дослідження є занадто прикладними для математика і водночас занадто теоретичними для інженера.

Одним з найбільших його внесків в математику є використання криволінійних координат, але відомими є також *параметри* (у теорії пружності) та *функції* (у рівняннях математичної фізики) Ламе.

Ламе намагався слідувати новим ідеям Коші про строгість математичних доведень. Відомою є критична стаття Ламе про стиль викладання та непослідовне доведення теореми Тейлора в університеті Санкт-Петербурга, де Ламе провів певний час.

Глава 5

ШИФР ХІЛЛА

Мультиплікативні шифри не забезпечують належну стійкість при криптоатаках. Більш стійкими є так звані *блочні* шифри, один з яких запропонував американський математик Лестер Хілл у 1929 році. Блочний шифр відрізняється від мультиплікативного тим, що букви повідомлення спочатку об'єднуються у групи, а потім шифруються блоки (а не окремі букви, як у мультиплікативному шифрі).

Алгоритм 1. Шифр Хілла для блоків довжини 2

Крок 1. Повідомлення розбити на блоки довжиною 2;

в останню групу при необхідності додати символ ␣;

Крок 2. Букви `X` та `Y` в кожному блоці замінити на

номери $\mathcal{P}_{\mathtt{X}}$, $\mathcal{P}_{\mathtt{Y}}$ їхніх позицій в алфавіті;

Крок 3. Застосувати шифр Хілла з параметрами a, b, c та d:

$$\begin{aligned} \mathcal{C}_{\mathtt{X}} &\equiv a\mathcal{P}_{\mathtt{X}} + b\mathcal{P}_{\mathtt{Y}} \pmod{33}, \\ \mathcal{C}_{\mathtt{Y}} &\equiv c\mathcal{P}_{\mathtt{X}} + d\mathcal{P}_{\mathtt{Y}} \pmod{33}; \end{aligned}$$

Крок 4. Числа $\mathcal{C}_{\mathtt{X}}$, $\mathcal{C}_{\mathtt{Y}}$ в кожному блоці замінити на букви.

Розмір блоків для шифру Хілла може бути іншим, але обов'язково меншим за 33. ①

Приклад 1. За допомогою шифра Хілла

$$\begin{aligned} \mathcal{C}_{\mathtt{X}_1} &\equiv 5\mathcal{P}_{\mathtt{X}_1} + 13\mathcal{P}_{\mathtt{X}_2} \pmod{33}, \\ \mathcal{C}_{\mathtt{X}_2} &\equiv 3\mathcal{P}_{\mathtt{X}_1} + 19\mathcal{P}_{\mathtt{X}_2} \pmod{33} \end{aligned}$$

зашифрувати повідомлення

ХІЛЛ АВТОР ШИФРА

Крок 1. Розбиваємо текст на блоки:

ХІ ЛЛ АВ ТО РШ ИФ РА

Крок 2. Кожну букву замінюємо на номер її позиції в алфавіті:

ХІ	ЛЛ	АВ	ТО	РШ	ИФ	РА
2612	1616	0103	2319	2129	1125	2101

Крок 3. До кожного блока застосовуємо шифр Хілла. Покажемо процес перетворення для першого блока:

$$\begin{aligned} \mathcal{C}_{\mathtt{X}} &\equiv (5 \cdot 26 + 13 \cdot 12) \pmod{33} = 286 \pmod{33} = 22, \\ \mathcal{C}_{\mathtt{I}} &\equiv (3 \cdot 26 + 19 \cdot 12) \pmod{33} = 306 \pmod{33} = 9. \end{aligned}$$

Результат перетворення для усього повідомлення:

$\mathcal{P}_{\mathtt{X}}\mathcal{P}_{\mathtt{Y}}$	2612	1616	0103	2319	2129	1125	2101
$\mathcal{C}_{\mathtt{X}}\mathcal{C}_{\mathtt{Y}}$	2209	2422	1127	3201	2020	1713	1916

Крок 4. Переводимо блоки $\mathcal{C}_{\mathtt{X}}\mathcal{C}_{\mathtt{Y}}$ у буквенний формат.

2209	2422	1127	3201	2020	1713	1916
СЖ	УС	ИЦ	ЮА	ПП	МЇ	ОЛ

Зашифроване повідомлення має вигляд

(1) СЖУСИЦЮАППМЇОЛ

1. Дешифрування шифру Хілла

Для шифрів Хілла зручно використовувати матричну форму запису:

$$\begin{bmatrix} \mathcal{C}_{\mathtt{X}} \\ \mathcal{C}_{\mathtt{Y}} \end{bmatrix} \equiv \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \mathcal{P}_{\mathtt{X}} \\ \mathcal{P}_{\mathtt{Y}} \end{bmatrix} \pmod{33}.$$

Розглянемо звичайне рівняння (без операції mod 33) з загальним вільним членом $(u, v)'$ та невідомими x та y:

$$\begin{bmatrix} u \\ v \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \quad \text{або} \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} u \\ v \end{bmatrix}.$$

У лінійній алгебрі це матричне рівняння називають системою двох рівнянь з двома невідомими. Якщо матриця системи $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ має обернену, то

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} \begin{bmatrix} u \\ v \end{bmatrix}.$$

Тому можна сподіватись, що при деяких умовах на параметри a, b, c та d, шифр Хілла можна дешифрувати за допомогою такої ж формули, але за mod 33:

$$\begin{bmatrix} \mathcal{P}_{\mathtt{X}} \\ \mathcal{P}_{\mathtt{Y}} \end{bmatrix} \equiv \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} \begin{bmatrix} \mathcal{C}_{\mathtt{X}} \\ \mathcal{C}_{\mathtt{Y}} \end{bmatrix} \pmod{33}. \tag{2}$$

Ми встановимо цю рівність за допомогою загальної теорії систем лінійних конгруенцій.

2. Системи лінійних конгруенцій

2.1. Одне рівняння. *Лінійним рівнянням за модулем* m відносно невідомого x ми називаємо

$$ax \equiv b \pmod{m}, \tag{3}$$

де a, b та m задані цілі числа. Зауважимо, що якщо x є розв'язком лінійного рівняння (3), то $x \pm m$ також є розв'язком. ② Крім того, якщо $(a, m) = 1$, то існує $a^{-1} \pmod{m}$ (теорема 3.1) й тому $x = a^{-1}b \pmod{m}$. Це означає, що лінійне рівняння (3) має розв'язок при будь-якому b, якщо $(a, m) = 1$. У подальшому нам знадобиться наступний більш загальний результат.

Теорема 1. *Рівняння* (3) *має єдиний розв'язок* $0 \le x < m$ *для довільного* b *тоді і тільки тоді, коли* $(a, m) = 1$.

Доведення. Припустимо спочатку, що $(a, m) = 1$. Як ми показали вище, в цьому випадку рівняння (3) має розв'язок $x = a^{-1}b \pmod{m}$ при будь-якому b. Якби при цьому існував ще один розв'язок, то серед чисел $ka \pmod{m}$, $0 \le k < m$, існували б два однакових. ③ З іншого боку, наслідок 3.1 стверджує, що всі вони є різними, якщо $(a, m) = 1$. Отримане протиріччя доводить єдиність розв'язку.

Доведемо тепер другу частину теореми. Припустимо, що рівняння (3) має єдиний розв'язок для будь-якого b. Це означає, що всі числа $ka \pmod{m}$, $0 \le k < m$, є різними. ④ В цьому випадку наслідок 3.1 стверджує, що $a^{-1} \pmod{m}$ існує. Тепер з теореми 3.1 випливає, що $(a, m) = 1$. □

2.2. Система двох рівнянь. Системою 2×2 лінійних конгруенцій ми називаємо

$$\begin{aligned} ax + by &\equiv e \pmod{m}, \\ cx + dy &\equiv f \pmod{m}. \end{aligned} \tag{4}$$

Розв'язком цієї системи ми називаємо будь-яку пару цілих чисел x та y, яка задовольняє цю систему.

Теорема 2. *Система* (4) *має єдиний розв'язок за модулем* m *тоді і тільки тоді, коли* $(\Delta, m) = 1$, *де* $\Delta = ad - bc \pmod{m}$. *Нагадаємо, що число* $ad - bc$ *називається визначником матриці системи* (4).

Доведення. Припустимо, що лінійна система (4) має розв'язок $0 \le x_0 < m$ та $0 \le y_0 < m$. Домножимо першу конгруенцію на d, а другу — на b: ⑤

$$\begin{aligned} adx + bdy &\equiv de \pmod{m}, \\ bcx + bdy &\equiv bf \pmod{m}. \end{aligned}$$

Віднявши другу конгруенцію від першої, отримаємо ⑥

$$(ad - bc)x \equiv (de - bf) \pmod{m}.$$

Згідно до теореми 1 це рівняння має єдиний розв'язок $0 \le x_0 < m$ тоді і тільки тоді, коли $(ad - bc, m) = 1$. Аналогічним чином ⑦ можемо з (4) отримати рівняння

$$(bc - ad)y \equiv (ce - af) \pmod{m}. \tag{5}$$

Це рівняння також має єдиний розв'язок тоді і тільки тоді, коли $(\Delta, m) = 1$. ⑧ □

Теорема 2 дає критерій існування розв'язку, але не дає формули для нього. Ці формули містяться у наступному результаті.

Теорема 3. *Якщо система* (4) *має єдиний розв'язок* $0 \le x_0 < m$ *та* $0 \le y_0 < m$, *то*

$$\begin{aligned} x_0 &\equiv \Delta^{-1}(ed - bf) \pmod{m}, \\ y_0 &\equiv \Delta^{-1}(af - ce) \pmod{m}, \end{aligned} \tag{6}$$

де $\Delta = ad - bc$, *а* Δ^{-1} — *обернене число до* Δ *за модулем* m.

Доведення. Оскільки система (4) має єдиний розв'язок, то $(\Delta, m) = 1$ за теоремою 2 й тому $\Delta^{-1} \pmod{m}$ існує. Маємо

$$\begin{aligned} ax_0 + by_0 &= \big(a\Delta^{-1}(ed - bf) + b\Delta^{-1}(af - ce)\big) \pmod{m} \\ &= (ad - bc)\Delta^{-1}e \pmod{m} = e \pmod{m}, \end{aligned}$$

оскільки $\Delta\Delta^{-1} \equiv 1 \pmod{m}$. Це означає, що пара x_0 та y_0 задовольняє перше рівняння системи (4). Таким же чином доводимо, що ця пара задовольняє і друге рівняння. ⑨ Це означає, що пара є x_0 та y_0 є розв'язком системи (4). □

3. Дешифрування шифру Хілла: закінчення

Теорема 4. *Нехай* $(\Delta, 33) = 1$, *де* $\Delta = ad - bc$; *тут* a, b, c *та* d — *параметри шифру Хілла. Тоді дешифрування повідомлень, зашифрованих методом Хілла, здійснюється за формулами*

$$\begin{aligned} \mathcal{P}_{\mathtt{X}} &= \Delta^{-1} \cdot \det \begin{bmatrix} \mathcal{C}_{\mathtt{X}} & b \\ \mathcal{C}_{\mathtt{Y}} & d \end{bmatrix} \pmod{33}, \\ \mathcal{P}_{\mathtt{Y}} &= \Delta^{-1} \cdot \det \begin{bmatrix} a & \mathcal{C}_{\mathtt{X}} \\ c & \mathcal{C}_{\mathtt{Y}} \end{bmatrix} \pmod{33}. \end{aligned} \tag{7}$$

Доведення. Ці формули є наслідками формул (6). ⑩ □

Приклад 2. Дешифруємо повідомлення (1), вважаючи, що воно було зашифровано шифром Хілла з параметрами $a = 5$, $b = 13$, $c = 3$ та $d = 19$.

Перед дешифруванням повідомлення (1) ми розбиваємо текст на блоки довжиною 2:

СЖ УС ИЦ ЮА ПП МЇ ОЛ

Переведемо букви у числовий формат:

СЖ	УС	ИЦ	ЮА	ПП	МЇ	ОЛ
2209	2422	1127	3201	2020	1713	1916

Далі обчислюємо $\Delta = 5{\cdot}19 - 13{\cdot}3 \pmod{33} = 23$. З таблиці 4 у главі 3 знаходимо $23 = \Delta^{-1} \pmod{33}$. Тому

$$\mathcal{P}_{\text{Х}} = 23 \cdot \det \begin{bmatrix} \mathcal{C}_{\text{Х}} & 13 \\ \mathcal{C}_{\text{Ү}} & 19 \end{bmatrix} \pmod{33},$$

$$\mathcal{P}_{\text{Ү}} = 23 \cdot \det \begin{bmatrix} 5 & \mathcal{C}_{\text{Х}} \\ 3 & \mathcal{C}_{\text{Ү}} \end{bmatrix} \pmod{33}.$$

Процес дешифрування продемонструємо для першого блока:

$$\mathcal{P}_{\text{С}} = 23 \cdot \det \begin{bmatrix} 22 & 13 \\ 9 & 19 \end{bmatrix} \pmod{33} = 6923 \pmod{33} = 26,$$

$$\mathcal{P}_{\text{Ж}} = 23 \cdot \det \begin{bmatrix} 5 & 22 \\ 3 & 9 \end{bmatrix} \pmod{33} = -21 \pmod{33} = 12.$$

Результат дешифрування для всього повідомлення представлено нижче:

$\mathcal{C}_{\text{Х}}\mathcal{C}_{\text{Ү}}$	2209	2422	1127	3201	2020	1713	1916
$\mathcal{P}_{\text{Х}}\mathcal{P}_{\text{Ү}}$	2612	1616	0103	2319	2129	1125	2101

Останнім кроком переводимо блоки $\mathcal{P}_{\mathtt{X}}\mathcal{P}_{\mathtt{Y}}$ у буквенний формат:

2612	1616	0103	2319	2129	1125	2101
XI	ЛЛ	АВ	ТО	РШ	ИФ	РА

Нижче наведено алгоритм дешифрування повідомлення, яке було зашифровано за допомогою шифра Хілла для блоків розміру 2.

Алгоритм 2. Дешифрування шифру Хілла з параметрами

Крок 1. Шифроване повідомлення розбити на блоки довжиною 2;

Крок 2. Букви в кожному блоці замінити на їхній числовий код;

Крок 3. Обчислити $\Delta = ad - bc \pmod{33}$;

Крок 4. Знайти $\Delta^{-1} \pmod{33}$;

Крок 5. Дешифрування кожного блоку здійснити за формулою (7).

3.1. Блоки іншого розміру. Шифр Хілла можна використовувати й для інших розмірів блоків. Ми обрали $n = 2$ тільки для спрощення пояснень. Шифрування та дешифрування для блоків довільного розміру $2 < n \leq 33$ здійснюються за правилами, аналогічними до випадку блоків розміру 2. Якщо блоки мають розмір n, то для шифрування використовується $n \times n$ матриця A, для якої $(\det(A), 33) = 1$. Позначимо через $\mathcal{P}_{\mathtt{1}} \ldots, \mathcal{P}_{\mathtt{n}}$ числові коди букв у блоці, а через $\mathcal{C}_{\mathtt{1}}, \ldots, \mathcal{C}_{\mathtt{n}}$ — їхні шифри. Тоді шифрування за Хіллом

здійснюється так

$$\begin{bmatrix} \mathcal{C}_1 \\ \dots \\ \mathcal{C}_n \end{bmatrix} \equiv A \cdot \begin{bmatrix} \mathcal{P}_1 \\ \dots \\ \mathcal{P}_n \end{bmatrix} \pmod{33}.$$

Дешифрування здійснюється за правилом

$$\begin{bmatrix} \mathcal{P}_1 \\ \dots \\ \mathcal{P}_n \end{bmatrix} \equiv A^{-1} \cdot \begin{bmatrix} \mathcal{C}_1 \\ \dots \\ \mathcal{C}_n \end{bmatrix} \pmod{33}.$$

Обернена матриця обчислюється з використанням операцій модульної арифметики.

Зауваження 1. Модуль у шифрі Хілла також може відрізнятись від 33. Для блоків розміру 2 необхідні теоретичні відомості містяться у теоремах 2 та 3.

4. Криптоаналіз шифру Хілла

Оскільки шифр Хілла є блочним, його складніше дешифрувати, ніж мультплікативний шифр. Криптоаналіз, тим не менше, можливий і для шифру Хілла з блоками розміру n, якщо знати частоти, з якими в текстах українською мовою зустрічаються різні комбінації з n букв. Якщо, наприклад, $n = 2$, то існує $33 \cdot 33 = 1089$ "слів", які складаються з двох букв. Аналізуючи частоти у шифрованому повідомленні, можна висунути гіпотезу про матрицю A, яка використана при шифруванні. Після цього можна обчислити обернену матрицю A^{-1} й дешифрувати повідомлення. Якщо ж n стає більшим, цей підхід стає неефективним.

5. Системи лінійних рівнянь за модулем

Системи лінійних конгруенцій вживались ще у стародавньому Китаї, Індії та Греції. Їх використовували астрономи для складання календарів.

Наступна задача зустрічається у китайському рукописі, який археологи відносять до періоду з V до III сторіччя до нашої ери:

> **Старовинна китайська задача.** *Знайти число, яке дає остачу 1 при діленні на 3, остачу 2 при діленні на 5 та остачу 3 при діленні на 7.*

Таким чином задача полягає у знаходженні цілого числа x, для якого

$$(8)\quad x \equiv 1 \pmod 3, \quad x \equiv 2 \pmod 5, \quad x \equiv 3 \pmod 7.$$

Перша конгруенція означає, що $x = 3t_1 + 1$ для деякого цілого числа t_1. Підставивши цей вираз у другу конгруенцію, отримуємо $3t_1 \equiv 1 \pmod 5$ або $t_1 \equiv 2 \pmod 5$, ⑪ тобто $t_1 = 5t_2 + 2$ для деякого цілого t_2. Тому $x = 3t_1 + 1 = 3(5t_2 + 2) + 1 = 15t_2 + 7$. Якщо підставити це у третю конгруенцію, то отримаємо $15t_2 + 7 \equiv 3 \pmod 7$ або $t_2 \equiv 3 \pmod 7$. ⑫ Таким чином, $t_2 = 7s + 3$ для деякого цілого числа s. Звідси випливає, що $x = 105s + 52$ для деякого цілого s. ⑬ Можна показати, що $105s + 52$ є розв'язком задачі при будь-якому цілому s, тобто задача має нескінчену кількість розв'язків. ⑭ Найменшим невід'ємним розв'язком є 52.

Зважаючи на значний внесок китайських математиків у розвиток теорії рівнянь за модулем, наступний результат називають *китайською теоремою про остачі*.

Теорема 5 (*китайська теорема про остачі*)**.** *Нехай $k \geq 1$ є натуральним числом. Нехай $m_1, \ldots, m_k$ є натуральними числами, які є попарно простими (не мають спільних дільників). Тоді система лінійних конгруенцій*

$$x \equiv a_i \pmod{m_i}, \qquad 1 \leq i \leq k, \tag{9}$$

має єдиний розв'язок за модулем $m_1 m_2 \ldots m_k$ для будь-яких натуральних $a_1, \ldots, a_k$.

Доведення. Доведення складається з двох кроків. Спочатку ми побудуємо розв'язок, а потім доведемо, що він є єдиним за модулем $m_1 m_2 \ldots m_k$.

Нехай $M = m_1 \ldots m_k$ та $M_i = M/m_i$, $1 \leq i \leq k$. Оскільки модулі конгруенцій є взаємно простими, то $(M_i, m_i) = 1$ для кожного i. ⑮ Крім того, $M_i \equiv 0 \pmod{m_j}$ якими б не були $i \neq j$. ⑯

Побудова розв'язку. Оскільки $(M_i, m_i) = 1$, то конгруенція $M_i y \equiv 1 \pmod{m_i}$ має єдиний розв'язок y_i, $0 \leq y_i < m_i$. ⑰ Зауважимо, що фактично $y_i = M_i^{-1} \pmod{m_i}$. Покладемо тепер

$$x = a_1 M_1 y_1 + \cdots + a_k M_k y_k.$$

Тоді для будь-якого $1 \leq j \leq k$

$$\begin{aligned} x &= \sum_{i \neq j} a_i M_i y_i + a_j M_j y_j = \sum_{i \neq j} a_i \cdot 0 \cdot y_i + a_j \cdot 1 \pmod{m_j} \\ &= a_j \pmod{m_j}, \end{aligned}$$

тобто x задовольняє кожну з конгруенцій (іншими словами, x є розв'язком системи).

Доведення єдиності за модулем M. Нехай x_0 та x_1 два розв'язки системи. Покажемо, що $x_0 \equiv x_1 \pmod{M}$.

Оскільки $x_0 \equiv a_j \pmod{m_j}$ та $x_1 \equiv a_j \pmod{m_j}$ для $1 \le j \le k$, то $x_1 - x_0 \equiv 0 \pmod{m_j}$. Це означає, що $x_1 - x_0$ ділиться на m_j при будь-якому j. Звідси ми робимо висновок, що $x_1 - x_0$ ділиться на НСК $(m_1, \ldots, m_k)$ найменше спільне кратне чисел $m_1, m_2, \ldots, m_k$.

Але найменшим спільним кратним чисел $m_1, m_2, \ldots, m_k$ є M. ⑱ Таким чином, $x_1 - x_0$ ділиться на M, тобто $x_1 - x_0 \equiv 0 \pmod{M}$ або $x_1 \equiv x_0 \pmod{M}$.

Це й означає, що довільні два розв'язки системи є конгруентними за модулем M. Іншими словами, розв'язок є єдиним за модулем M. □

Зауваження 2. Результат теореми 5 можна виразити іншими словами, а саме, якщо $m_1, \ldots, m_k$ є взаємно простими числами, $M = m_1 \ldots m_k$, а x_0, $0 \le x_0 < M$, — це розв'язок системи (9), то кожне з чисел $x_0 + Ms$, $s \in \mathbf{Z}$, також є розв'язком цієї системи. При цьому, інших розв'язків системи (9) не існує.

У найпростішому випадку $k = 1$ це твердження є іншим способом описати властивість $x \equiv a \pmod{m}$.

Приклад 3. Покажемо як методом теореми 5 можна розв'язати старовинну китайську задачу, яку наведено на стор. 119.

Як ми показали вище, ця задача зводиться до системи (8). Оскільки модулі конгруенцій $m_1 = 3$, $m_2 = 5$ та $m_3 = 7$ є взаємно простими числами, то за теоремою 5 система (8) має єдиний розв'язок за модулем $M = 3 \cdot 5 \cdot 7 = 105$. Обчислимо M_1, M_2, M_3, y_1, y_2 та y_3 за правилом, наведеним

у доведенні теореми 5. Маємо

$$M_1 = \frac{M}{m_1} = \frac{3 \cdot 5 \cdot 7}{3} = 35,$$
$$M_2 = \frac{M}{m_2} = \frac{3 \cdot 5 \cdot 7}{5} = 21,$$
$$M_3 = \frac{M}{m_3} = \frac{3 \cdot 5 \cdot 7}{7} = 15.$$

Рівняння $M_1 y_1 \equiv 1 \pmod{m_1}$, тобто $35y_1 \equiv 1 \pmod 3$, має розв'язок $y_1 \equiv 2 \pmod 3$. Аналогічно, з другої умови $M_2 y_2 \equiv 1 \pmod{m_2}$ випливає

$$21y_2 \equiv 1 \pmod 5, \qquad y_2 \equiv 1 \pmod 5.$$

Нарешті, з умови $M_3 y_3 \equiv 1 \pmod{m_3}$ отримуємо

$$15y_3 \equiv 1 \pmod 7, \qquad y_3 \equiv 1 \pmod 7.$$

За китайською теоремою про остачі розв'язком системи (8) є

$$\begin{aligned} x &= \sum_{i=1}^{3} a_i M_i y_i \pmod M \\ &= 1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 \pmod{105} \\ &= 52 \pmod{105}. \end{aligned}$$

Таким чином 52 — це єдиний розв'язок системи (8) за модулем 105, а загальним розв'язком є $x = 52 + 105s$, $s \in \mathbf{Z}$.

6. Шифр Плейфера

Шифр Плейфера для українського алфавиту використовує матрицю шифрування та ключову фразу. Розміри матриці шифрування та ключова фраза є параметрами шифру (вони обираються заздалегідь). Для визначеності ми використовуємо нижче матрицю шифрування 4×8.

Оберемо Ш И Ф Р П Л Е Й Ф Е Р А у якості ключової фрази. Вибір фрази не є критичним для процедури шифрування. З ключової фрази викреслимо букви, що повторюються: Ш И Ф Р П Л Е Й ~~Ф~~ ~~Е~~ ~~Р~~ А.

Тепер ототожнімо Ґ з Г ⑲ та викреслімо з алфавіту букви, що залишились в ключовій фразі:

~~А~~	Б	В	Г/Ґ	Д	~~Е~~	Є	Ж	З	~~И~~	І	Ї	~~Й~~	К	~~Л~~	М
Н	О	~~П~~	~~Р~~	С	Т	У	~~Ф~~	Х	Ц	Ч	~~Ш~~	Щ	Ь	Ю	Я

Записуємо букви, що залишились у ключовій фразі та алфавіті, до матриці шифрування:

Ш	**И**	**Ф**	**Р**	**П**	**Л**	**Е**	**Й**
А	Б	В	Г	Д	Є	Ж	З
І	Ї	К	М	Н	О	С	Т
У	Х	Ц	Ч	Щ	Ь	Ю	Я

Перед шифруванням необхідно розбити повідомлення на групи по дві букви. Припустимо, що необхідно переслати повідомленням ДУЖЕ СКЛАДНИЙ ШИФР. Після групування отримаємо: ДУ ЖЕ СК ЛА ДН ИЙ ШИ ФР. Тепер шифруємо кожну пару окремо. При цьому розрізняємо такі випадки.

Випадок 1. Обидві букви у парі знаходяться в одному рядку матриці шифрування. Наприклад, при шифруванні

пари ШИ ці букви розташовано у першому рядку матриці шифрування, причому у тому ж порядку. З іншого боку, пару СК розташовано у третьому рядку, але у зворотньому порядку. Нижче наведено відповідні фрагменти матриці шифрування:

Ш	И	Ф	Р	⋆	⋆	⋆	⋆	‖	⋆	⋆	⋆	⋆	⋆	⋆	⋆	⋆
⋆	⋆	⋆	⋆	⋆	⋆	⋆	⋆	‖	⋆	⋆	⋆	⋆	⋆	⋆	⋆	⋆
⋆	⋆	⋆	⋆	⋆	⋆	⋆	⋆	‖	⋆	⋆	К	М	⋆	⋆	С	Т
⋆	⋆	⋆	⋆	⋆	⋆	⋆	⋆	‖	⋆	⋆	⋆	⋆	⋆	⋆	⋆	⋆

У будь-якому випадку зсуваємо їх на одну позицію вправо у відповідному рядку й отримуємо ИФ або ТМ.

Випадок 2. Обидві букви пари розташовано в одному стовпчику матриці шифрування. Наприклад, пару ДН розташовано п'ятому стовпчику, причому у тому ж порядку. З іншого боку, пару ЖЕ розташовано у сьомому стовпчику, але у зворотньому порядку:

⋆	⋆	⋆	⋆	⋆	⋆	⋆	⋆	‖	⋆	⋆	⋆	⋆	⋆	⋆	Е	⋆
⋆	⋆	⋆	⋆	Д	⋆	⋆	⋆	‖	⋆	⋆	⋆	⋆	⋆	⋆	Ж	⋆
⋆	⋆	⋆	⋆	Н	⋆	⋆	⋆	‖	⋆	⋆	⋆	⋆	⋆	⋆	С	⋆
⋆	⋆	⋆	⋆	Щ	⋆	⋆	⋆	‖	⋆	⋆	⋆	⋆	⋆	⋆	⋆	⋆

У будь-якому випадку зсуваємо їх на одну позицію вниз й отримуємо НЩ або СЖ.

Випадок 3. Букви пари розташовано в різних стовпчиках і рядках матриці шифрування. Наприклад, так буде у випадку пари ДУ:

⋆	⋆	⋆	⋆	⋆	⋆	⋆	⋆
А	Б	В	Г	Д	⋆	⋆	⋆
І	Ї	К	М	Н	⋆	⋆	⋆
У	Х	Ц	Ч	Щ	⋆	⋆	⋆

В цьому випадку кожну з букв пари замінюємо буквою з того ж рядка, але іншого стовпчика. Шифром пари ДУ є пара АЩ.

Таким чином, все повідомлення буде зашифровано наступним чином:

ДУ	ЖЕ	СК	ЛА	ДН	ИЙ	ШИ	ФР
3	2	1	3	2	1	1	1
АЩ	СЖ	ТМ	ШЄ	НЩ	ФШ	ИФ	РП

Середній рядок у цій таблиці вказує на той з випадків, описаних вище, який треба застосувати для шифрування відповідної діграми.

Останньою дією переводимо букви у їхній числовий еквівалент:

1 30	22 9	23 17	29 8	18 30	25 29	11 25	21 20
АЩ	СЖ	ТМ	ШЄ	НЩ	ФШ	ИФ	РП

Зауваження 3. В описаній процедурі ми обрали 4×8 матрицю шифрування. Це вимагало від нас ототожніти найбільш схожі букви Ґ з Г. Якщо обрати 3×11 матрицю шифрування, то ототожнювати ці букви не потрібно. Для тієї ж ключової фрази 3×11 матриця шифрування має вигляд:

Ш	**И**	**Ф**	**Р**	**П**	**Л**	**Е**	**Й**	**А**	Б	В
Г	Ґ	Д	Є	Ж	З	І	Ї	К	М	Н
О	С	Т	У	Х	Ц	Ч	Щ	Ь	Ю	Я

Фразу буде зашифровано наступним чином:

ДУ	ЖЕ	СК	ЛА	ДН	ИЙ	ШИ	ФР
3	3	3	1	1	1	1	1
ЄТ	ІП	ЬҐ	ЕБ	ЄГ	ФА	ИФ	РП

Зверніть увагу на особливість шифрування пари ДН: оскільки буква Н є останньою у своєму рядку, то зсув вправо для неї здійснюється за циклом у тому ж рядку: Н→Г.

7. КОНТРОЛЬНІ ПИТАННЯ

1. Чому розмір блоків для шифру Хілла має бути меншим за 33? (стор. 110).

2. Довести, що якщо x є розв'язком лінійного рівняння (3), то $x \pm m$ також є його розв'язком. (стор. 112).

3. Довести, що якщо рівняння (3) має ще один розв'язок, крім $x = a^{-1}b \pmod m$, то серед чисел $ka \pmod m$, $0 \le k < m$, існують два однакових. (стор. 113).

4. Поясніть чому всі числа $ka \pmod m$, $0 \le k < m$, є різними, якщо рівняння (3) має єдиний розв'язок для будь-якого b. (стор. 113).

5. Чому конгруенції можна множити на константу? (стор. 114).

6. Чому конгруенції можна віднімати одну від іншої? (стор. 114).

7. Як з (4) отримати (5)? (стор. 114).

8. Впевнитись, що рівняння (5) також має єдиний розв'язок тоді і тільки тоді, коли $(\Delta, m) = 1$. (стор. 114).

9. Довести, що пара x_0, y_0 у доведенні теореми 3 задовольняє і друге рівняння системи (4). (стор. 115).

10. Перевірити, що (7) є наслідком (6). (стор. 115).

11. Чому з $3t_1 \equiv 1 \pmod 5$ випливає $t_1 \equiv 2 \pmod 5$? (стор. 119).

12. Чому з $15t_2 + 7 \equiv 3 \pmod 7$ випливає $t_2 \equiv 3 \pmod 7$? (стор. 119).

13. Перевірити, що $x = 105s + 52$ для деякого цілого s у розв'язанні старовинної китайської задачі на стор. 119. (стор. 119).

14. Впевнитись у тому, що старовинна китайська задача має нескінчену кількість розв'язків. (стор. 119).

15. Якщо модулі конгруенцій є взаємно простими, то $(M_i, m_i) = 1$ для кожного i у доведенні теореми 5. Чому? (стор. 120).

16. Показати, що $M_i \equiv 0 \pmod{m_j}$ у доведенні теореми 5 якими б не були $i \ne j$. (стор. 120).

17. Згадайте, чому конгруенція $M_i y \equiv 1 \pmod{m_i}$ у доведенні теореми 5 має єдиний розв'язок y_i? (стор. 120).

18. Довести, що найменшим спільним кратним чисел $m_1, \ldots, m_k$ є $M = [m_1, \ldots, m_k,]$, якщо $m_1, \ldots, m_k$ є взаємно простими числами? (стор. 121).

19. Навіщо ототожнювати Γ̓ з Γ у шифрі Плейфера? (стор. 123).

8. З А Д А Ч І

Задача 1. *За допомогою шифру Хілла з матрицею* $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ *зашифрувати фразу*

(a) ДУМИ МОЇ, ДУМИ МОЇ.
(b) НЕ КИДАЙТЕ ХОЧ ВИ МЕНЕ.

Задача 2. *Дешифрувати фразу, яку зашифровано методом Хілла з матрицею* $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$:

(a) ФПСЧШҐЧШЖВ
(b) ШІЗЬЩҐЕХЖСЧШЖВ

Задача 3. *Чи підходить матриця* $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ *для шифрування за Хіллом текстів англійською мовою?*

Задача 4. *Чи підходить матриця* $\begin{bmatrix} 9 & 2 \\ 17 & 5 \end{bmatrix}$ *для шифрування за Хіллом текстів українською мовою?*

Задача 5. *Для матриці* A *розміру* 2×2, *елементами якої є натуральні числа* a_{ij}, $1 \le i, j \le 2$, *побудуємо матрицю* A', *яка складається з елементів* $a_{ij} \pmod n$, *де* $n > 1$ — *довільне натуральне число.*

(a) *Довести, що* $\det(A) \pmod n = \det(A') \pmod n$.
(b) *Довести аналогічне твердження для матриць розміру* $k \times k$.

Задача 6. *Довести, що шифр Хілла з матрицею* A *розміру* 2×2 *є рівносильним шифру Хілла з матрицею* A', *означеної у задачі* 5. *Чи є ця властивість вірною для довільного розміру* $k \times k$?

Задача 7. *Шифром підстановки називається наступне правило перетворення букв алфавіту:* $\mathcal{C}_{\mathtt{X}} = \sigma(\mathcal{P}_{\mathtt{X}})$ *для будь-якої букви* X, *де* $\sigma(\cdot)$ — *це задана перестановка символів алфавіту.*

(a) *Підрахувати кількість шифрів підстановки для українського алфавіту.*

(b) *Чи є шифр Цезаря шифром підстановки?*

(c) *Ототожнімо букви* Ґ *та* Г, *щоб в алфавіті залишилось 32 символи. До кожної з 8 послідовних груп, які складаються з чотирьох букв, застосуємо підстановку:* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$. *Зашифрувати текст* ХЕЛЛОУЇН.

(d) *Записати формулу перетворення* $\mathcal{P}_{\mathtt{X}}$ *в* $\mathcal{C}_{\mathtt{X}}$ *для шифру з задачі* (c).

Задача 8. *Скільки існує матриць* 2×2, *якщо їхні елементи приймають тільки значення* 0 *або* 1? *Скільки серед них матриць, які мають обернені за* mod 2?

Задача 9. *Розглянемо множину матриць* 2×2, *елементи яких* a_{ij}, $1 \le i, j \le 2$, *приймають тільки значення* 0, 1 *або* 2. *Позначимо* $\Delta = \det(A)$ *та розглянемо дві підмножини матриць:*

$$M_1 = \{A : \ a_{11} \neq 0, \ a_{22} = 0, \ \Delta \pmod 3 \neq 0\},$$
$$M_2 = \{A : \ a_{11} \neq 0, \ a_{22} \neq 0, \ \Delta \pmod 3 = 0\}.$$

Довести, що в кожній з цих двох множин міститься 8 матриць.

Задача 10. *Розглянемо множину матриць* 2×2, *елементи яких* a_{ij}, $1 \le i, j \le 2$, *приймають тільки значення* 0, 1 *або* 2. *Розглянемо підмножину матриць*

$$M_3 = \{A : \ a_{11} \neq 0, \ a_{22} \neq 0\}.$$

Скільки існує матриць у цій підмножині? Використовуючи задачу 9, *довести, що існує рівно 36 матриць, які мають обернену за* mod 3 *та* $a_{11} \neq 0$.

Задача 11. *Розглянемо множину матриць* 2×2, *елементи яких* a_{ij}, $1 \le i, j \le 2$, *приймають тільки значення* 0, 1 *або* 2. *Розглянемо підмножину матриць*

$$M_5 = \{A : \ a_{11} = 0, \ \det(A) \pmod 3 \neq 0\}.$$

(a) *Довести, що* $\mathrm{card}(M_5) = 12$.

(b) *Використовуючи задачі* 9 *та* 10, *довести, що існує рівно 48 матриць, для яких* $\det(A) \pmod 3 \neq 0$.

Задача 12. *Число* $(abc)_{10}$ *має остачу 5 при діленні на 12. Якщо це число помножити на 2, то отримаємо число, яке має остачу 4 при діленні на 35. Знайти* a, b, c.

Задача 13. *Знайдіть всі натуральні числа між 200 та 500, які при діленні на 4, 5 та 7 дають остачі 3, 4 та 5, відповідно.*

Задача 14. *Знайдіть всі натуральні числа, які при діленні на 2, 3, 4, 5, 6, 7 дають остачі 0, 1, 2, 3, 4, 5, відповідно.*

Задача 15. *За допомогою китайської теореми про остачі знайти розв'язок системи конгруенцій*

$$\begin{cases} x \equiv 5 \pmod{7}, \\ x \equiv 3 \pmod{11}, \\ x \equiv 10 \pmod{13}. \end{cases}$$

Задача 16. *За допомогою китайської теореми про остачі знайти розв'язок системи конгруенцій*

$$\begin{cases} x \equiv 1 \pmod{15}, \\ x \equiv 3 \pmod{17}, \\ x \equiv 10 \pmod{24}, \\ x \equiv 4 \pmod{19}. \end{cases}$$

Чи існує розв'язок цієї системи, якщо замість 19 в останній конгруенції обрати 8 у якості модуля?

Задача 17. *Китайську теорему про остачі використовують для виконання арифметичних операцій з великими числами. Нехай, наприклад,* $m_1 = 2^{23} - 1$, $m_2 = 2^{29} - 1$, $m_3 = 2^{33} - 1$, $m_4 = 2^{34} - 1$, $m_5 = 2^{35} - 1$. *Можна перевірити, що всі ці числа є простими. Покладемо* $M = m_1 m_2 m_3 m_4 m_5$.

(a) *Чому кожне натуральне число* $x \leq M$ *можна єдиним чином представити п'ятіркою натуральних чисел* $(a_1, \ldots, a_5)$, *де* $a_i = x \pmod{m_i}$?

(b) *Скільки десяткових цифр можуть мати такі числа* x?

(c) *Як, використовуючи остачі від ділення на* $m_1, \ldots, m_5$, *можна здійснювати операції додавання та множення чисел* $x \leq M$ *та* $y \leq M$?

(d) *Якими мають бути* x *та* y, *щоб операції додавання та множення за допомогою остач від ділення на* $m_1, \ldots, m_5$, *давали коректний результат*?

Задача 18. *Можна обчислити, що* $2^{26} = 67,108,864$ *та* $2^{27} = 134,217,728$. *Калькулятор* `Casio fx 330A` *може робити точні обчислення лише для натуральних чисел, які не перевищують* $99,999,999$. *Оскільки* $2^{31} > 99,999,999$, *то при обчисленні калькулятор дає приблизну відповідь* $2^{31} \approx 2.1474836 \cdot 10^9$. *Знайдіть спосіб обчислити точно* 2^{31} *за допомогою лише* `Casio fx 330A` *та китайської теореми про остачі.*

Задача 19. *Довести, що дві конгруенції* $x \equiv a \pmod{n}$ *та* $x \equiv b \pmod{m}$ *мають спільний розв'язок тоді і тільки тоді, коли* $a - b$ *ділиться на* (n, m); *якщо розв'язок існує, то він є єдиним за модулем* $[n, m]$.

Задача 20. *Знайти всі значення* a, *при яких наступна система має хоча б один розв'язок*

$$\begin{cases} 2x \equiv a \pmod{4}, \\ 3x \equiv 4 \pmod{10}. \end{cases}$$

Задача 21. *Знайти хоча б одне* $m > 6$, *при якому наступна система не має жодного розв'язку*:

$$\begin{cases} x \equiv 3 \pmod{6}, \\ x \equiv 7 \pmod{m}. \end{cases}$$

Задача 22. *Довести, що наступні системи не мають розв'язків*:

(a) $\begin{cases} x \equiv 2 \pmod{4}, \\ x \equiv 3 \pmod{6}; \end{cases}$ (b) $\begin{cases} x \equiv 3 \pmod{4}, \\ x \equiv 4 \pmod{5}, \\ x \equiv 4 \pmod{6}. \end{cases}$

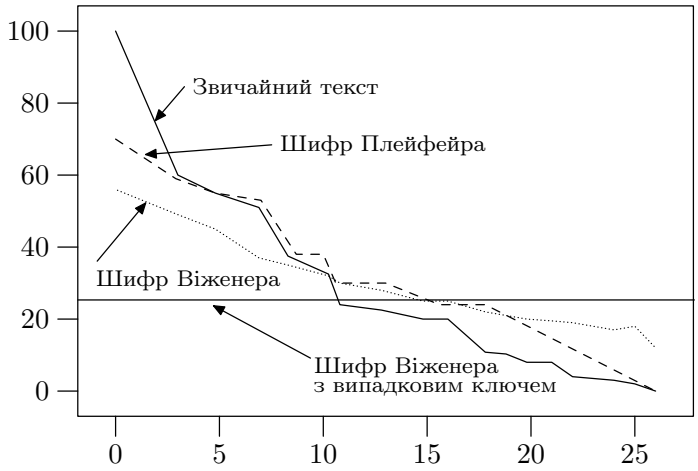
Задача 23. *Довести, що якщо* $x \equiv a \pmod{n}$, *то виконується одна з двох конгруенцій* $x \equiv a \pmod{2n}$ *або* $x + n \equiv a \pmod{2n}$. *Чи можуть ці дві конгруенції справджуватись одночасно?*

Задача 24. *Нехай* a *та* $n > 1$ — *натуральні числа. Покладемо* $a_1 = a \pmod{n}$ *та* $c = a^{-1} \pmod{n}$, $c_1 = a_1^{-1} \pmod{n}$. *Довести, що* $c = c_1$.

Задача 25. *Знайти ціле число, яке при діленні на*

(a) *2, 3, 6, 12 дає остачі 1, 2, 5, 5* (`Ю Хін, пом. 717 р.`);
(b) *3, 4, 5, 6 дає остачі 2, 3, 4, 5* (`Бхаскара, нар. 1114 р.`);
(c) *10, 13, 17 дає остачі 3, 11, 15* (`Регіомонтан (1436-1476)`).

Задача 26. *Наступний малюнок створено на основі аналізу статті в англійській енциклопедії Brittanica про криптологію (стаття складається з більше ніж 70,000 літер).*



Для кожної букви латинського алфавіту було підраховано її відносну частоту у тексті відносно букви "e" (найбільш уживаної букви в англійській мові), тобто обчислено відношення кількості появ цієї букви до кількості появ букви "e". Зрозуміло, що відносна частота букви "e" дорівнює 100%. Виявилось також, що відносна частота,

наприклад, букви "t" дорівнює приблизно 76%. Частоти на малюнку розташовано у порядку спадання. На малюнку показано графіки відносних частот після шифрування статті про криптографію за допомогою шифрів Плейфера та Віженера, а також за допомогою шифру Віженера з випадковим ключем.

(a) *Поясніть, як відносні частоти появ букв у тексті можна використовувати для дешифрування повідомлень? (Способи дешифрування, основані на відносних частотах, називають частотним аналізом.)*

(b) *За допомогою малюнка поясніть, чому шифр Віженера вважається найбільш стійким до дешифрування за допомогою частотного аналізу?*

(c) *Проаналізуйте стійкість інших шифрів, представлених на малюнку.*

Задача 27. *При застосуванні шифра Плейфера в англійській мові використовують таблицю* 5×5, *а букви* `I` *та* `J` *ототожнюють. Якщо кількість букв у повідомленні є непарною, то в кінці додають букву* `X`.

(a) *Чому в англійській мові обрано таблицю* 5×5, *а в українській —* 4×8?

(b) *Для чого ототожнюють букви* `I` *та* `J`? *Чому саме їх*?

(c) *Навіщо в кінці повідомлення додають букву* `X`, *якщо кількість букв у повідомленні є непарною*?

Задача 28. *У романі англійської письменниці Дороті Сейерз "Have His Carcase" шифр Плейфера грає визначальну роль. Повідомлення* `WE ARE DISCOVERED` *в тому романі було зашифровано за допомогою шифра Плейфера з використанням ключового слова* `MONARCHY` *та матриці шифрування*

M	**O**	**N**	**A**	**R**
C	**H**	**Y**	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Зашифрувати повідомлення з роману Д. Сейерз.

Задача 29. *За допомогою тієї ж матриці шифрування, що і в задачі* 28, *дешифрувати закінчення повідомлення*: `XBUF HNZMLIXE`.

Задача 30. *Запишіть наступні числа у вигляді звичайних та десяткових дробів*:

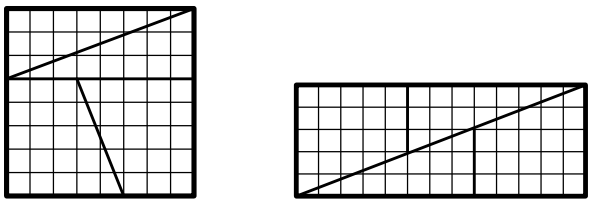
(a) $0,\underset{\text{period}}{(12)}+0,\underset{\text{period}}{(122)}$; **(b)** $0,\underset{\text{period}}{(3)}\cdot 0,\underset{\text{period}}{(4)}$; **(c)** $0,\underset{\text{period}}{(9)}-0,\underset{\text{period}}{(85)}$.

Тут за допомогою $0,\underset{\text{period}}{(xyz)}$ *позначено нескінчений десятковий дріб з періодом* xyz, *тобто* $0,xyzxyzxyz\ldots$.

Задача 31. (`старовинна французька задача`) *Жінка несла на базар кошик яєць. Перехожий ненавмисно штовхнув її, корзина впала і яйця розбилися. Винуватець, бажаючи відшкодувати втрату, запитав, скільки яєць було в кошику. "Точно не знаю, — відповіла жінка, — але пам'ятаю, що коли я виймала з кошика по* 2, *по* 3, *по* 4, *по* 5, *по* 6 *яєць, в кошику завжди залишалося одне яйце, а коли виймала по* 7, *в кошику нічого не залишалося ". Яке найменше число яєць могло бути в кошику?*

Задача 32. (`задача Брахмагупти, VII ст.`) *Якщо виймати яйця з кошику по 2, 3, 4, 5 або 6 за раз, то залишаються 1, 2, 3, 4 або 5 яєць відповідно. Якщо ж виймати по 7, то в кошику нічого не залишиться. Яке найменше число яєць могло бути в кошику?*

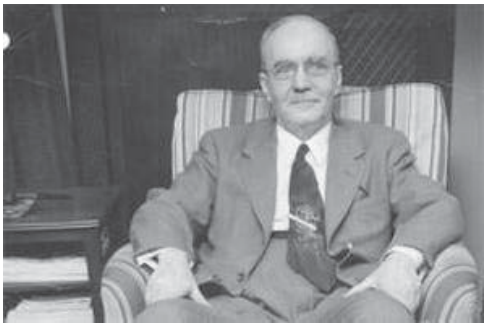
Задача 33. *Нижче наведено геометричне "доведення" рівності* $64 = 65$. *Шахівницю* 8×8 *розрізають на чотири частини, як показано на лівому малюнку, а потім з них складають іншу фігуру, зображену на правому малюнку*:



Як розташувати ті ж чотири частини шахівниці так, щоб "довести" рівність $64 = 63$?

9. БІОГРАФІЇ

Хілл, *Лестер* (1891–1961), американський математик та вчений у галузі шифрування, цікавився застосуваннями математики до теорії інформації та зв'язку.



Лестер Хілл

Він запропонував методи виявлення помилок у телеграфному коді. Має значні внески у розвиток криптографії та теорії кодування. За результати у цих науках відзначений урядом США під час другої світової війни.

У 1929 році він розробив шифри Хілла, які тепер відносять до класу полиграмних шифрів підстановки. Особливістю шифра Хілла було інтенсивне використання методів лінійної алгебри. Процес шифрування та дешифрування методом Хілла розмірності 6 було реалізовано за допомогою механічного пристрою, який здійснював множення матриць 6×6 за допомогою системи шестерінок та приводів. Розташування шестерінок змінювати було неможливо, що означало один і той же ключ для всіх повідомлень. З метою підвищити криптостійкість рекомендувалось послідовно трічи пропускати текст через машину Хілла. Така комбінація була дуже надійною для 1929 року, проте машина попитом не користувалась.

Зараз вважається, що шифр Хілла є вразливим, тобто нестійким до криптоатак.

Плейфер, *Ліон* (1818–1898), шотландський вчений та політик. Його ім'ям названо систему шифрування, застосування якої в англійській армії він домігся, хоча автором є інший англійський вчений *Чарльз Уітстен* (1802–1875).

Ліон Плейфер

Чарльз Уітстен

Простота і надійність цього шифру зробили його надзвичайно популярним в англійській армії. Британці користувались цим шифром під час англо-бурської війни, а пізніше і під час першої світової війни. Навіть під час другої світової війни цей шифр був резервним в американській армії на випадок несподіваних подій. Відомо, що лейтенант Джон Ф. Кеннеді (пізніше став президентом США) у 1943 році використав цей метод шифрування, щоб відправити аварійне повідомлення після того, як його човен був потоплений японськими військовими кораблями поблизу Соломонових островів.

Шифр Плейфера має значні переваги над іншими одноалфавітними шифрами через ускладнену ідентифікацію діграм у разі його застосування. Певний час його навіть вважали незламним. Проте, сучасні криптографи встановили, що цей шифр не є надійним, оскільки він все ж таки зберігає багато структурних особливостей природних текстів. Як правило, кількох сотень символів у повідомленні вистачає, щоб його дешифрувати.

Глава 6

ЛІНІЙНІ ШИФРИ

Як шифр Цезаря, так і мультиплікативний шифр не є стійкими до криптоатак, але їхня комбінація є більш надійною. Як ми бачили у §3.5, глава 3, розширення алфавіту може приводити до підвищення стійкості шифру. Особливо це стає помітним при групуванні символів повідомлення, яке необхідно зашифрувати. Після розширення алфавіт може складатися з довільної кількості букв, тому для загальності аналіза ми розглядаємо алфавіт $\mathscr{A}$, який складається з n букв. Таким чином можна вважати, що *алфавіт* — це сукупність n довільних *символів*.

Ми називаємо *лінійним шифром* наступне перетворення алфавіту $\mathscr{A}$

$$\mathcal{C}_{\mathtt{X}} \equiv a\mathcal{P}_{\mathtt{X}} + b \pmod{n}, \qquad X \in \mathscr{A}, \tag{1}$$

яке визначається параметрами a, b, та n і яке позначається $L_{a,b,n}$. У випадку $n = 33$ ми замість $L_{a,b,33}$ пишемо $L_{a,b}$. Лінійні шифри називають також *афінними*.

Тут a та b два параметри лінійного шифру. Дію $L_{a,b}$ шифра можна описати словами наступним чином: шифр $\mathcal{C}_{\mathtt{X}}$ кожної букви $\mathtt{X}$ дорівнює зсунутому на b добутку її позиції $\mathcal{P}_{\mathtt{X}}$ в алфавіті $\mathscr{A}$ на a та обчисленому за модулем n.

Зауваження 1. Лінійний шифр $L_{a,b}$ при $a = 1$ перетворюється в шифр Цезаря C_b, а при $b = 0$ — в мультиплікативний шифр M_a.

Приклад 1. Нижче показано процедуру перетворення повідомлення УРА за допомогою $L_{2,5}$ шифру:

УРА $\longrightarrow$ 24 21 1	перетворення букв у числа
$\longrightarrow$ 48 42 2	множення на 2
$\longrightarrow$ 53 47 7	зсув на 5
$\longrightarrow$ 20 14 7	обчислення mod 33
$\longrightarrow$ П Й Е	перетворення чисел у букви

Закодованим повідомленням є ПЙЕ.

1. Дешифрування лінійного шифру

Як і для мультиплікативних шифрів, параметри a та n повинні бути взаємно простими для того, щоб $L_{a,b}$ шифр був взаємно однозначним. ① Ми знаємо (див. §3.1, глава 3), що для дешифрування мультиплікативного шифру використовується число обернене до a за модулем n, причому $a^{-1} \pmod n$ існує, якщо $(a,n)=1$. Тому в такому випадку конгруенцію (1) можна перетворити наступним чином

$$\mathcal{P}_{\mathtt{X}} \equiv a^{-1}\mathcal{C}_{\mathtt{X}} - a^{-1}b \pmod n. \tag{2}$$

② Таким чином, дешифрування $L_{a,b}$ шифру здійснюється за допомогою лінійного шифру з параметрами $a^{-1} \pmod n$ та $-b\cdot a^{-1} \pmod n$. Щоб привести цю формулу до вигляду (1), другий параметр у рівності (2) можна записати у вигляді $n - a^{-1}b \pmod n$. ③ Таким чином,

$$\begin{gathered}\mathcal{P}_{\mathtt{X}} = u\mathcal{C}_{\mathtt{X}} + v \pmod n,\\ u = a^{-1} \pmod n,\\ v = n - a^{-1}b \pmod n.\end{gathered} \tag{3}$$

Приклад 2. Нижче показано процедуру дешифрування повідомлення ПЙЕ, закодованого за допомогою $L_{2,5}$ шифру. Нагадаємо, що $2^{-1} \pmod{33} = 17$, тому дешифрування здійснюється за правилом:

$$\mathcal{P}_{\mathtt{X}} \equiv 17\mathcal{C}_{\mathtt{X}} - 17 \cdot 5 \pmod{33}.$$

Оскільки $14 = 33 - 17 \cdot 5 \pmod{33}$, то

$$\mathcal{P}_{\mathtt{X}} \equiv 17\mathcal{C}_{\mathtt{X}} + 14 \pmod{33}.$$

Тому

ПЙЕ	$\longrightarrow$	20	14	7	перетворення букв у числа
	$\longrightarrow$	340	238	119	множення на 17
	$\longrightarrow$	354	252	133	зсув на 14
	$\longrightarrow$	24	21	1	обчислення mod 33
	$\longrightarrow$	У	Р	А	перетворення чисел у букви

Таким чином, закодовано було повідомлення УРА.

2. Скільки існує лінійних шифрів?

Існує 33 шифрів Цезаря та 20 однозначних мультиплікативних шифрів для українського алфавіту (див. §3.2, глава 3). ④ Тому загалом існує $33 \cdot 20 = 660$ лінійних шифрів. ⑤ Один з них, а саме $L_{1,0}$, є тотожним перетворенням, тому існує 659 нетривіальних лінійних шифрів. Чи нема серед них однакових? Однаковими ми вважаємо такі два шифри, для яких коди довільної букви є однаковими. Якщо ж коди хоча б однієї букви є різними, то ми вважаємо, що шифри є різними.

Теорема 1. *Нехай* $1 \le a_1, a_2 < n$ *та* $0 \le b_1, b_2 < n$. *Тоді, якщо для будь-якого* $0 \le m < n$

$$a_1 m + b_1 \equiv a_2 m + b_2 \pmod{n}, \tag{4}$$

то $a_1 = a_2$ *та* $b_1 = b_2$.

Таким чином, теорема 1 стверджує, що всі 659 лінійних шифрів є різними.

Доведення теореми 1. При умовах теореми, накладених на b_1 та b_2, з конгруенції (4) при $m = 0$ випливає, що $b_1 = b_2$. ⑥ Знову скористаємось конгруенцією (4), але тепер при $m = 1$, й отримаємо $a_1 = a_2$. ⑦ □

2.1. Випадок загального n**.** Скільки існує лінійних шифрів для алфавіту, який складається з n букв? Зрозуміло, що для такого алфавіту існує n шифрів Цезаря, але скільки існує однозначних мультиплікативних шифрів? Ми знаємо, що у випадку $n = 33$ таких шифрів рівно 20. А як обчислити їхню кількість у загальному випадку?

Означення 1. *Функцією Ойлера* $\phi(n)$ для аргументу n називається кількість натуральних чисел, менших за n та взаємно простих з n.

Таким чином, відповідь на поставлене питання визначається функцією Ойлера: існує $\phi(n)$ мультиплікативних шифрів й $n\phi(n)$ лінійних шифрів для алфавіту, який складається з n букв.

Приклад 3. Нагадаємо, що латинський алфавіт складається з 26 букв. Скільки існує лінійних шифрів для латинського алфавіту? Відповідь вже відома: існує $26 \cdot \phi(26)$

лінійних шифрів. Але чому дорівнює $\phi(26)$? Безпосередньо можна обчислити, що $\phi(26) = 12$, оскільки 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25 є взаємно простими з 26. ⑧ Тому існує 312 лінійних шифрів для латинського алфавіту.

Чи можна запропонувати алгоритм обчислення значення функції Ойлера для довільного аргумента?

3. Функція Ойлера

Зрозуміло, що $\phi(n) \leq n - 1$. ⑨ Ця оцінка є точною, оскільки $\phi(n) = n - 1$, якщо n є простим числом. ⑩

Властивість 1. *Якщо p є довільним простим числом, то $\phi(p) = p - 1$.*

Значення функції Ойлера нескладно отримати й для степеня простого числа.

Властивість 2. *Нехай p є простим числом, а $k \geq 1$. Тоді*

$$\phi\left(p^k\right) = p^k - p^{k-1}. \tag{5}$$

Доведення властивості 2. Тільки числа вигляду $p{\cdot}j$, $j \in \mathbf{N}$, не є взаємно простими з p^k. ⑪ Таких чисел, менших за p^k, існує p^{k-1}. ⑫ Звідси і випливає необхідне твердження. □

Властивість 3. *Нехай p та q є різними простими числами. Тоді*

$$\phi(pq) = (p-1)(q-1). \tag{6}$$

Доведення властивості 3. Серед чисел, що не перевищують pq, тільки ті числа не є взаємно простими з pq, які діляться або на p, або на q. ⑬ Ці дві множини мають одне спільне число pq. Тому $\phi(pq) = pq - p - q + 1$. ⑭ □

Приклад 4. На підставі формули (6) ⑮

$$\phi(33) = \phi(3 \cdot 11) = (3-1)(11-1) = 20,$$
$$\phi(26) = \phi(2 \cdot 13) = (2-1)(13-1) = 12.$$

Властивість 4. *Нехай p та q є різними простими числами, а $i, j \geq 1$. Тоді*

$$\phi\left(p^i q^j\right) = (p^i - p^{i-1})(q^j - q^{j-1}). \tag{7}$$

Доведення властивості 3. Рівно $p^{i-1}q^j$ чисел, менших за $p^i q^j$, діляться на p. ⑯ Аналогічно, рівно $p^i q^{j-1}$ чисел, що не перевищують $p^i q^j$, діляться на q, й рівно $p^{i-1}q^{j-1}$ чисел, що не перевищують $p^i q^j$, діляться на pq. Тому $\phi\left(p^i q^j\right) = p^i q^j - p^{i-1}q^j - p^i q^{j-1} + p^{i-1}q^{j-1}$. ⑰ Ця рівність є еквівалентною до рівності (7). □

Зауважимо, що властивість 3 можна записати у вигляді

$$\phi\left(p^i q^j\right) = \phi\left(p^i\right)\phi\left(q^j\right). \tag{8}$$ ⑱

3.1. Формула включення/виключення. Доведення всіх властивостей функції Ойлера, розглянутих вище, використовує одну просту, але важливу, ідею. Її можна представити наступним чином: якщо певна множина містить рівно N елементів, з яких

- рівно N_1 елементів задовольняють обмеженню V_1,
- рівно N_2 елементів задовольняють обмеженню V_2,
- рівно N_{12} елементів задовольняють обом обмеженням V_1 та V_2,

то

$$M = N - N_1 - N_2 + N_{12} \tag{9}$$

де M — це кількість елементів, які не задовольняють жодне з обмежень.

Наприклад, при доведенні властивості 4 множина елементів складається з натуральних чисел, які не перевищують $N = p^i q^j$; обмеження V_1 означає, що число з цієї множини ділиться на p, а V_2 — що ділиться на q. Тоді $N_1 = p^{i-1} q^j$, а $N_2 = p^i q^{j-1}$. В доведенні властивості 4 ми встановили, що кількість чисел, які не діляться на p та на q, дійсно дорівнює (9).

Ідея підрахунку необхідної кількості полягає в тому, що ми виключаємо з множини ті її елементи, які мають властивості V_1 та V_2, а потім включаємо туди ті елементи, які мають обидві властивості. Елементи, які залишились в множині, не мають жодного з обмежень. Через такий спосіб утворення необхідної множини, формула (9) називається *формулою включення/виключення.*

Формула включення/виключення відома й для довільної кількості обмежень, а не тільки для двох, як у випадку (9). Символічно загальну формулу можна записати наступним чином: якщо M — це кількість елементів, які не задовольняють жодному з обмежень $V_1, \ldots, V_k$, то

$$M = N - \underbrace{(N_1 + \ldots)}_{\text{одне обмеження}} + \underbrace{(N_{12} + \ldots)}_{\text{два обмеження}} - \underbrace{(N_{123} + \ldots)}_{\text{три обмеження}} + \cdots + (-1)^k \underbrace{N_{123\ldots k}}_{k \text{ обмежень}}.$$

Тут вираз з назвою “одне обмеження” дорівнює сумі всіх можливих чисел N_α, $1 \le \alpha \le k$, де N_α — це кількість

елементів, які задовольняють обмеженню V_α; вираз з назвою "два обмеження" дорівнює сумі всіх можливих чисел $N_{\alpha\beta}$, $1 \le \alpha < \beta \le k$, де $N_{\alpha\beta}$ — це кількість елементів, які задовольняють обмеженням V_α та V_β; вираз з назвою "три обмеження" дорівнює сумі всіх можливих чисел $N_{\alpha\beta\gamma}$, $1 \le \alpha < \beta < \gamma \le k$, де $N_{\alpha\beta\gamma}$ — це кількість елементів, які задовольняють обмеженням V_α, V_β та V_γ; ... . Нарешті, вираз з назвою "k обмежень" дорівнює одному числу $N_{123\ldots k}$ — кількості елементів, які задовольняють всі k обмежень.

3.2. Загальна формула для функції Ойлера. Саме варіант формули включення/виключення з довільною кількістю обмежень використовується при доведенні формули для функції Ойлера у найбільш загальному вигляді.

Властивість 5. *Нехай $p_1, \ldots, p_k$ — різні прості числа, а $i_1, \ldots, i_k \ge 1$. Тоді*

$$\phi\left(p_1^{i_1} \ldots p_k^{i_k}\right) = p_1^{i_1} \ldots p_k^{i_k} \left(1 - \frac{1}{p_1}\right) \ldots \left(1 - \frac{1}{p_k}\right). \tag{10}$$

Зауважимо, що при $k = 2$ властивість 5 є рівносильною (7). ⑲

Доведення властивості 5. Позначимо $m = p_1^{i_1} \ldots p_k^{i_k}$. Для будь-якого $1 \le j \le k$ існує рівно m/p_j чисел, які не перевищують m та діляться на p_j. Аналогічно, для будь-якої пари різних $j_1 \le k$ та $j_2 \le k$ існує рівно $m/p_{j_1}p_{j_2}$ чисел, які не перевищують m та діляться на $p_{j_1}p_{j_2}$.

Якщо $l \le k$, то для будь-яких $j_1 \le k, \ldots, j_l \le k$ існує рівно $m/p_{j_1} \ldots p_{j_l}$ чисел, які не перевищують m та діляться на $p_{j_1} \ldots p_{j_l}$. Згідно до правила включення-виключення, серед

чисел, що не перевищують m, існує рівно

$$\sum_{j=1}^{k}\frac{m}{p_j}-\sum_{j_1\neq j_2}\frac{m}{p_{j_1}p_{j_2}}+\sum_{j_1,j_2,j_3\ \text{різні}}\frac{m}{p_{j_1}p_{j_2}p_{j_3}}-\cdots+(-1)^k\frac{m}{p_1\ldots p_k} \tag{11}$$

таких чисел, які діляться на хоча б одне з $p_1,\ldots,p_k$. Індукцією за k нескладно довести, ⑳ що цей вираз дорівнює

$$m\left(1-\left(1-\frac{1}{p_1}\right)\ldots\left(1-\frac{1}{p_k}\right)\right). \tag{12}$$

Звідси випливає, що чисел, менших за m, та взаємно простих з m існує рівно

$$m\left(1-\frac{1}{p_1}\right)\ldots\left(1-\frac{1}{p_k}\right),$$

що є еквівалентним (10). □

Властивість 6. *Нехай m та n є взаємно простими, тобто $(m,n)=1$. Тоді*

$$\phi(mn)=\phi(m)\,\phi(n). \tag{13}$$

Зауваження 2. Рівність (13) не є вірною для довільних m та n. Наприклад, при $m=n=p$, де p — просте число, маємо за властивістю 1

$$\phi\left(p^2\right)=p^2-p\neq(p-1)(p-1)=\phi(p)\,\phi(p).$$

Доведення властивості 6. Нехай $m = p_1^{i_1} \dots p_k^{i_k}$ та $n = q_1^{j_1} \dots q_k^{j_l}$ — це канонічні розклади чисел m та n в добуток простих дільників. Оскільки m та n є взаємно простими, то серед $p_1, \dots, p_k, q_1, \dots, q_l$ немає однакових чисел. ㉑ Тому з властивості (10) випливає, що

$$\begin{aligned}\phi\left(p_1^{i_1} \dots p_k^{i_k} q_1^{j_1} \dots q_k^{j_l}\right) &= p_1^{i_1} \dots p_k^{i_k} q_1^{j_1} \dots q_k^{j_l} \\ &\quad \times \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right) \\ &\quad \times \left(1 - \frac{1}{q_1}\right) \dots \left(1 - \frac{1}{q_l}\right) \\ &= \phi\left(p_1^{i_1} \dots p_k^{i_k}\right) \phi\left(q_1^{j_1} \dots q_k^{j_l}\right). \qquad \square\end{aligned}$$

Означення 2. Функція f, для якої $f(mn) = f(m)f(n)$ при $(m, n) = 1$, називається *мультиплікативною.*

Згідно до властивості 6 функція Ойлера є мультаплікативною.

4. Теорема Ойлера

Ми розглянемо один з результатів Ойлера про функцію $\phi(\cdot)$, який має багаточисельні застосування у криптографії.

Теорема 2 (*Л. Ойлер*). *Якщо* $(a, m) = 1$, *то*

$$a^{\phi(m)} \equiv 1 \pmod{m}. \tag{14}$$

Доведення. Нехай $x_1, \dots, x_{\phi(m)}$ — різні натуральні числа, що не перевищують m та є взаємно простими з m. Розглянемо всі можливі добутки вигляду $x_i a$ для i від 1 до

$\phi(m)$. Оскільки a є взаємно простим з m та x_i є взаємно простим з m, то й $x_i a$ також є взаємно простим з m, тобто $x_i a \equiv x_j \pmod{m}$ для деякого $1 \leq j \leq \phi(m)$.

Зауважимо, що всі залишки від ділення чисел $x_i a$, $1 \leq i \leq \phi(m)$, на m є різними. Дійсно, якщо це не так, то існують такі $i_1 \neq i_2$, що $1 \leq i_1, i_2 \leq \phi(m)$ та

$$x_{i_1} a \equiv x_{i_2} a \pmod{m}$$

або

$$(x_{i_1} - x_{i_2})a \equiv 0 \pmod{m}.$$

Оскільки a є взаємно простим з m, то остання рівність є рівносильною тому, що

$$x_{i_1} - x_{i_2} \equiv 0 \pmod{m}$$

або

$$x_{i_1} \equiv x_{i_2} \pmod{m} \quad \Longleftrightarrow \quad x_{i_1} = x_{i_2}.$$

Це протирічить припущенню про те, що числа $x_1, \ldots, x_{\phi(m)}$ є різними натуральними числами. Тому всі числа x_j у конгруенціях $x_i a \equiv x_j \pmod{m}$, $i = 1, 2, \ldots, \phi(m)$, є різними.

Перемножимо тепер всі конгруенції $x_i a \equiv x_j \pmod{m}$. Отримуємо

$$x_1 \ldots x_{\phi(m)} a^{\phi(m)} \equiv x_1 \ldots x_{\phi(m)} \pmod{m}$$

або

$$x_1 \ldots x_{\phi(m)}(a^{\phi(m)} - 1) \equiv 0 \pmod{m}.$$

Оскільки число $x_1 \ldots x_{\phi(m)}$ є взаємно простим з m, то остання конгруенція є равносильною тому, що

$$a^{\phi(m)} - 1 \equiv 0 \pmod{m}$$

або $a^{\phi(m)} \equiv 1 \pmod{m}$. $\square$

4.1. Обчислення оберненого за модулем. Теорему Ойлера можна використати для обчислення оберненого числа $a^{-1} \pmod{n}$, якщо $(a, n) = 1$. Дійсно з (14) випливає, що $a^{\phi(n)-1} \cdot a \equiv 1 \pmod{n}$, тобто

$$a^{-1} = a^{\phi(n)-1} \pmod{n}. \tag{15}$$

Таким чином за допомогою функції Ойлера можна обчислювати числа, обернені за модулем.

Приклад 5. На підставі прикладу 4 маємо $\phi(33) = 20$. Тому (всі рівності у наступному рядку треба розуміти за модулем 33)

$$2^{-1} = 2^{19} = 2^{10} \cdot 2^9 = 1024 \cdot 512 = 1 \cdot 17 \equiv 17 \pmod{33}.$$

4.2. Мала теорема Ферма. Ще одним важливим для криптографії результатом є наступний наслідок теореми 2.

Теорема 3 (*мала теорема Ферма*)**.** *Якщо p є простим числом, то*

$$a^{p-1} \equiv 1 \pmod{p} \tag{16}$$

для будь-якого a, яке не ділиться на p.

Теорема 3 випливає з (14) та (5). ㉒

5. Таблиця перших значень функції Ойлера

Нижче наведено значення функції Ойлера $\phi(n)$ для $n = 1, 2, \ldots, 99$.

Таблиця 1. Таблиця значень функції $\phi(n)$

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0+		1	1	2	2	4	2	6	4	6
10+	4	10	4	12	6	8	8	16	6	18
20+	8	12	10	22	8	20	12	18	12	28
30+	8	30	16	20	16	24	12	36	18	24
40+	16	40	12	42	20	24	22	46	16	42
50+	20	32	24	52	18	40	24	36	28	58
60+	16	60	30	36	32	48	20	66	32	44
70+	24	70	24	72	36	40	36	60	24	78
80+	32	54	40	82	24	64	42	56	40	88
90+	24	72	44	60	46	72	32	96	42	60

Цю таблицю можна використати для для обчислення значень $\phi(n)$ для багатьох інших n, якщо використати властивість мультиплікативності. Наприклад,

$$\phi(100) = \phi(25 \cdot 4) = \phi(25) \cdot \phi(4) = 20 \cdot 4 = 80.$$

6. Контрольні питання

1. Пояснити чому параметри a та n повинні бути взаємно простими для того, щоб шифр $L_{a,b}$ був взаємно однозначним? (стор. 137).

2. Довести, що дешифрування $L_{a,b}$ шифру дійсно здійснюється за формулою (2). (стор. 137).

3. Чому другий параметр у формулі (2) можна записати у вигляді $n - b \cdot a^{-1} \pmod{n}$? (стор. 137).

4. Пояснити чому існує 33 шифрів Цезаря та 20 однозначних мультиплікативних шифрів для українського алфавіту? (стор. 138).

5. Чому існує 660 лінійних шифрів для українського алфавіту? (стор. 138).

6. Впевнитись, що за умов теореми, накладених на b_1, b_2, з конгруенції (4) при $m = 0$ випливає, що $b_1 = b_2$. (стор. 139).

7. Перевірити, що з конгруенції (4) при $m = 1$ випливає $a_1 = a_2$. (стор. 139).

8. Перевірити, що серед чисел, що не перевищують 26, тільки 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25 є взаємно простими з 26. (стор. 139).

9. Пояснити чому $\phi(n) \leq n - 1$? (стор. 140).

10. Чому $\phi(n) = n - 1$, якщо n є простим числом? (стор. 140).

11. Довести, що тільки числа вигляду $p \cdot j$, $j \in \mathbf{N}$, не є взаємно простими з p^k. (стор. 140).

12. Чому існує рівно p^{k-1} чисел, які є меншими за p^k та які мають спільний дільник з p, більший за 1? (стор. 140).

13. Впевнитись, що серед чисел, що не перевищують pq, тільки ті числа не є взаємно простими з pq, які діляться або на p, або на q. (стор. 140).

14. Перевірити, що $\phi(pq) = pq - p - q + 1$. (стор. 140).

15. Чому в прикладі 4 обрано числа 33 та 26? (стор. 140).

16. Довести, що рівно $p^{i-1}q^j$ чисел, менших за p^iq^j, діляться на p. (стор. 141).

17. Довести методом включення–виключення, що $\phi\left(p^iq^j\right) = p^iq^j - p^{i-1}q^j - p^iq^{j-1} + p^{i-1}q^{j-1}$. (стор. 141).

18. Чому властивість 3 можна записати у вигляді (8)? (стор. 141).

19. Перевірити, що властивість 5 при $k = 2$ є рівносильною (8). (стор. 143).

20. Роз'язати задачу 5. (стор. 144).

21. Показати, що якщо $m = p_1^{i_1} \dots p_k^{i_k}$ та $n = q_1^{j_1} \dots q_k^{j_l}$ є взаємно простими, то серед $p_1, \dots, p_k, q_1, \dots, q_l$ немає однакових чисел. (стор. 144).

22. Довести, що теорема 3 випливає з (14) та (5). (стор. 147).

7. З А Д А Ч І

Задача 1. *За допомогою лінійного шифра з параметрами* $a = 23$, $b = 7$ *зашифрувати повідомлення* `СЕКРЕТ`. *Чи можна вживати параметр* $a = 21$ *для* $L_{a,b}$ *шифру*?

Задача 2. *За допомогою лінійного шифра з параметрами* $a = 23$, $b = 7$ *зашифрувати повідомлення* SECRET, *використовуючи латинський алфавіт. Чи можна вживати параметр* $a = 21$ *для* $L_{a,b}$ *шифру?*

Задача 3. *Результатом застосування лінійного шифра з параметрами* $a = 23$, $b = 7$ *отримано фразу* ЄЩХБФШАЕ. *Знайти текст, який було зашифровано.*

Задача 4. *Результатом застосування лінійного шифра з параметрами* $a = 23$, $b = 7$ *до фрази англійською отримано* TJBYREJ. *Знайти текст, який було зашифровано.*

Задача 5. *Довести, що* (12) *випливає з* (11).

Задача 6. *Проаналізувати таблицю* 1 *й висловити гіпотезу стосовно парності функції* $\phi(n)$. *Довести цю гіпотезу.*

Задача 7. *Показати, що* $\phi(5186) = \phi(5187) = \phi(5188)$.

Задача 8. *Показати, що для кожного натурального* n *виконується властивість*

$$\phi(2n) = \begin{cases} \phi(n), & \text{якщо } n \text{ непарне,} \\ 2\phi(n), & \text{якщо } n \text{ парне.} \end{cases}$$

Задача 9. *Знайти остачу від ділення* 7^{1020} *на* 15.

Задача 10. *Знайти остачу від ділення* 79^{1776} *на* 24.

Задача 11. *Визначити останню цифру числа* 17^{6666}.

Задача 12. *Розв'язати рівняння* $\phi(x) = x/3$.

Задача 13. *Розв'язати рівняння* $\phi(2x) = \phi(3x)$.

Задача 14. *Розв'язати рівняння* $\phi(x) = 2$.

Задача 15. *Довести, що* $\phi\left(n^2\right) = n\phi(n)$.

Задача 16. *Нехай* $m \mid n$. *Довести, що* $\phi(mn) = m\phi(n)$.

Задача 17. *Нехай* $d=(m,n)$. *Довести, що*

$$\phi(mn)=\phi(m)\,\phi(n)\,\frac{d}{\phi(d)}.$$

Задача 18. *Нехай* $d=(m,n)$, *а* $K=[m,n]$. *Довести, що*

$$\phi(m)\,\phi(n)=K\phi(d).$$

Задача 19. *Для* $n=7,10,12,17$ *підрахувати*

$$\sum_{d|n}\phi(d). \tag{17}$$

На основі обчислень висунути гіпотезу стосовно значення цієї суми у загальному випадку.

Задача 20. *Довести, що сума* (17) *дорівнює* n *для будь-якого* n. *Цей результат отримав Ф. Гаус.*

Задача 21. *Для* $n=7,10,12,17$ *підрахувати*

$$\sum_{d|n}(-1)^{n/d}\phi(d). \tag{18}$$

На основі обчислень висунути гіпотезу стосовно значення цієї суми у загальному випадку.

Задача 22. *Позначимо через* T_n *суму* (18). *Довести, що*

$$T_n=\begin{cases}-n, & n \text{ є непарним},\\ 0, & n \text{ є парним}.\end{cases}$$

Задача 23. *Нехай* p *є простим числом.*

(a) *Знайти* $\phi(1)+\phi(p)$.

(b) *Нехай* $\alpha>1$ *є натуральним числом. Знайти суму*

$$\phi(1)+\phi(p)+\cdots+\phi(p^{\alpha}).$$

Задача 24. *Нехай* $(a,b)=1$. *Розглянемо таблицю*

$$\begin{array}{ccccc} 1 & 2 & 3 & \dots & b \\ b+1 & b+2 & b+3 & \dots & 2b \\ \vdots & \vdots & \vdots & \dots & \vdots \\ (a-1)b+1 & (a-1)b+2 & (a-1)b+3 & \dots & ab. \end{array}$$

У яких стовпчиках цієї таблиці знаходяться числа, які є взаємно простими з числом b? *Скільки у кожному з цих стовпчиків чисел, які є взаємно простими з* a? *Доведіть мультиплікативність функції Ойлера на підставі відповідей на попередні два питання.*

Задача 25. *Відомо, що* $(m,n)>1$. *Яке з чисел є більшим:* $\phi(mn)$ *чи* $\phi(m)\,\phi(n)$?

Задача 26. *Коло розділено* n *точками на* n *рівних частин. Скільки існує різних замкнених ламаних з* n *рівних ланцюгів з вершинами у цих точках*?

Задача 27. *Чи існує степінь трійки, яка закінчується на 0001?*

Задача 28. *З використанням функції* $\phi(n)$ *знайти правило, за яким утворено початок послідовності* $1,2,2,4,4,4,6,8,6,\dots$.

Задача 29. *Скільки існує правильних нескоротних дробів зі знаменником 150*?

Задача 30. *Знайти кількість натуральних чисел* n, *які не перевищують* 615 *та мають властивість* $(n,615)=15$.

Задача 31. *Чи існує границя* $\phi(n)/n$ *при* $n\to\infty$? *Довести, що*

$$\liminf_{n\to\infty}\frac{\phi(n)}{n}=0, \qquad \limsup_{n\to\infty}\frac{\phi(n)}{n}=1.$$

Задача 32. *Нехай* $0<\delta<1$. *Довести, що*

$$\lim_{n\to\infty}\frac{\phi(n)}{n^{1-\delta}}=\infty.$$

Задача 33. *Нехай f — мультиплікативна функція. Довести, що якщо*

$$\lim_{p^m \to \infty} f(p^m) = 0$$

(тут p — просте число), то $f(n) \to 0$ при $n \to \infty$.

8. БІОГРАФІЇ

Ойлер, *Леонард* (1707–1783), швейцарський математик, вважається найвидатнішим математиком 18-го століття, а, можливо, навіть усіх часів. Вплив Ойлера на математику описує висловлювання "*Читайте Ойлера, читайте Ойлера, він є вчителем усіх нас*", яке приписується Пьєру Лапласу (також великому математику з Франції).

Леонард Ойлер

Першу наукову роботу Ойлер написав у віці 19 років. Ця робота не отримала премії на конкурсі Паризької академії в 1727 році, але, в інші роки й за інші роботи, його було нагороджено нею 72 рази. Загалом ним опубліковано більше 700 книг та статей. Половину свого творчого життя (у 1727–1741 та 1766–1783 роках) провів у Російській імперії, а іншу половину (у 1741–1766 роках) — у Прусії. Повне зібрання трудів Ойлера публікується з 1911 року Швейцарською академією наук: до цього часу вийшло 76 томів, загальна кількість має скласти 85 томів.

Досягнення Ойлера добре відомі в математичному аналізі, де він довів до досконалості використання степеневих рядів, наприклад

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}.$$

Саме число e носить ім'я Ойлера. У комплексному аналізу відомою є формула Ойлера: $e^{ix} = \cos(x) + i\sin(x)$, з якої випливає тотожність

Ойлера: $e^{i\pi}+1=0$. Останню називають "*найчудовішою математичною формулою*". Загально відомою є інша математична константа γ, яку називають константою Ойлера–Маскероні:

$$\gamma=\lim_{n\to\infty}\left[\sum_{k=1}^{n}\frac{1}{k}-\ln(n)\right].$$

Ойлер також довів формулу $V-E+F=2$, що пов'язує число вершин, ребер і граней опуклого багатогранника, а отже, і планарних графів (для планарних графів $V-E+F=1$). Цю формулу він отримав при розв'язанні задачі про сім мостів у м. Кенігсберг.

Леонард Ойлер зробив значний внесок у розвиток механіки, де його ім'я носять *рівняння* руху ідеальної рідини, та *кути*, якими описується обертання твердого тіла. Основні рівняння лагранжевої механіки часто називають рівняннями Ойлера–Лагранжа.

П. Л. Чебишов (див. [Чебишов], стор. 383) писав: "*Ойлером було покладено початок всіх досліджень, які тепер складають загальну теорію чисел*". Багато ранніх робіт Ойлера з теорії чисел базувалось на роботах П'єра Ферма (див. [Ферма], стор. 30). Ойлер опрацював деякі ідеї Ферма, і спростував деякі з його припущень. Він спростував гіпотезу Ферма про те, що всі числа виду $F_n=2^{2^n}+1$ є простими; виявилося, що F_5 ділиться на 641. Дав одне з розв'язань задачі про чотири куби.* Довів, що число Мерсенна $2^{31}-1=2,147,483,647$ є простим; протягом майже ста років (до 1867 року) воно залишалося найбільшим відомим простим числом.

Ойлер створив основу теорії порівнянь і квадратичних лишків, вказавши для останніх критерій існування. Ойлер ввів поняття первісного кореня і висунув гіпотезу, що для будь-якого простого числа p існує первісний корінь за модулем p; довести це він не зумів, пізніше теорему довели Лежандр (див. [Лежандр], стор. 381) і Гаусс (див. [Гаусс], стор. 345). Велике значення в теорії мала інша гіпотеза Ойлера про квадратичний закон взаємності також доведена пізніше Гауссом. Ойлер довів Велику теорему Ферма для $n=3$ і $n=4$, створив повну теорію неперервних дробів, досліджував різні класи діофантових рівнянь.

---

*Полягає у розвязанні рівняння $x^3+y^3+z^3=w^3$ у натуральних числах.

Глава 7

КРИПТОАНАЛІЗ ЛІНІЙНИХ ШИФРІВ

Згідно до формули (6.2), якщо було застосовано лінійний $L_{a,b,n}$ шифр, то дешифрування довільної букви $\mathtt{X}$ з алфавіту, який складається з n букв, відбувається за формулою

$$\mathcal{P}_{\mathtt{X}} \equiv a^{-1}\mathcal{C}_{\mathtt{X}} - a^{-1}b \pmod{n}, \tag{1}$$

де $a^{-1} \pmod{n}$ — це число обернене до a за модулем n.

Метод грубої силу (повного перебору) для знаходження параметрів a та b не є таким ефективним для лінійних шифрів, як у випадку мультиплікативних шифрів. Тому алгебраїчний метод (який для мультиплікативних $M_{a,n}$ шифрів ми розглянули в §3.3, глава 3) становить ще більший інтерес у випадку лінійних $L_{a,b,n}$ шифрів.

1. Алгебраїчний метод для $L_{a,b}$ шифрів

Як і у випадку мультиплікативних шифрів, дешифрування алгебраїчним методом починається з висунення гіпотези про відповідність однієї з букв (або кількох букв) певному коду.

1.1. Як розв'язувати лінійні рівняння у модульній арифметиці. Спочатку ми розглянемо спосіб дешифрування $L_{a,b}$ шифру при наявності лише однієї умови.

Приклад 1. Повідомлення закодовано за допомогою $L_{a,b}$ шифру. Знайти a та b, якщо відомо, що $\mathcal{C}_{\mathtt{B}} = \mathcal{P}_{\mathtt{T}}$.

З таблиці 2.4 знаходимо, що $\mathcal{P}_{\mathtt{B}} = 3$ та $\mathcal{P}_{\mathtt{T}} = 23$. Позначивши $c = a^{-1} \pmod{n}$, маємо

$$\mathcal{P}_{\mathtt{B}} \equiv c\mathcal{P}_{\mathtt{T}} - cb \pmod{33} \quad \text{або} \quad 3 \equiv 23c - bc \pmod{33}.$$

Розв'яжемо цю конгруенцію відносно b: ①

$$b \equiv 23 - 3a \pmod{33}.$$

Нагадаємо, що для однозначного дешифрування необхідно, щоб $(a, 33) = 1$. Звідси випливає, що $(c, 33) = 1$. ② Надаючи c всіх можливих значень, отримуємо наступну таблицю розв'язків останньої конгруенції:

a	1	2	4	5	7	8	10	13	14	16	17	19
$23-3a$	20	17	11	8	2	−1	−7	−16	−19	−25	−28	−34
b	20	17	11	8	2	32	26	17	14	8	5	32

a	20	23	25	26	28	29	31	32
$23-3a$	−37	−46	−52	−55	−61	−64	−70	−76
b	29	20	14	11	5	2	29	23

Таким чином, умову $\mathcal{C}_{\mathtt{B}} = \mathcal{P}_{\mathtt{T}}$ задовольняють 20 пар a, b. ③

Яким же чином можна використати отриманий в прикладі 1 результат для дешифрування повідомлення?

Приклад 2. Відомо, що слово ТБЙЇ було зашифровано за допомогою $L_{a,b}$ шифру, причому $\mathcal{C}_{\mathtt{B}} = \mathcal{P}_{\mathtt{T}}$. Дешифрувати це повідомлення.

У першому та другому рядках таблиці, наведеної нижче, вказано кілька пар a та b, при яких $L_{a,b}$ шифр має властивість $\mathcal{C}_{\mathtt{B}} = \mathcal{P}_{\mathtt{T}}$ (всі пари з такою властивістю знайдено у

прикладі 1). Оскільки для дешифрування необхідно знати $c = a^{-1} \pmod{33}$, $d = cb \pmod{33}$ та $e = 33 - d$; ці числа також наведено у третьому та четвертому рядках таблиці.

a	1	2	4	5	7	8	10	13	14
b	20	17	11	8	2	32	26	17	14
c	1	17	25	20	19	29	10	28	26
d	20	25	11	28	5	4	26	14	1
e	13	8	22	5	28	29	7	19	32

④ Тепер дешифрування здійснюється згідно до формули (1) для кожної пари чисел a та b, при яких $L_{a,b}$ шифр має властивість $\mathcal{C}_{\texttt{В}} = \mathcal{P}_{\texttt{Т}}$. Нижче показано результат дешифрування для перших чотирьох пар.

шифр	$L_{1,13}$	$L_{17,8}$	$L_{25,22}$	$L_{20,5}$
оригінал/цифра	3 15 27 26	3 9 15 31	3 6 9 17	3 12 21 1
оригінал/буква	В К Ц Х	В Ж К Ь	В Д Ж М	В І Р А

⑤ Першою парою, для якої отримано зрозумілий результат, виявилась $a = 5$ та $b = 8$. Тому ВІРА є одним з кандидатів на правильну відповідь. Можна впевнитись, що дешифроване слово не є українським для жодної з інших пар параметрів a та b, тому ВІРА є єдиною відповіддю на поставлене питання.

1.2. Як розв'язувати системи лінійних рівнянь у модульній арифметиці. Причиною, за якою відповідь на питання у прикладі 1 є неоднозначним, пояснюється тим, що кожен $L_{a,b}$ шифр має два параметри, а умова для дешифрування була тільки одна. Якщо умов дві — то дешифрування стає простішим.

Приклад 3. Знайти a та b, при яких $L_{a,b}$ шифр має такі властивості: $\mathcal{C}_{\texttt{У}} = \mathcal{P}_{\texttt{П}}$ та $\mathcal{C}_{\texttt{Е}} = \mathcal{P}_{\texttt{К}}$.

Оскільки $\mathcal{P}_{\text{У}} = 24$ та $\mathcal{P}_{\text{П}} = 20$, то

$$24a + b \equiv 20 \pmod{33}. \tag{2}$$

Аналогічно, $\mathcal{P}_{\text{Е}} = 7$ та $\mathcal{P}_{\text{К}} = 15$ й тому

$$7a + b \equiv 15 \pmod{33}. \tag{3}$$

Параметр a нескладно знайти, віднімаючи від першої конгруенції другу: ⑥

$$17a \equiv 5 \pmod{33} \quad \text{або} \quad a \equiv 10 \pmod{33}, \tag{4}$$

оскільки $2 = 17^{-1} \pmod{33}$. Таким чином, $a = 10$.

Тепер, підставляючи знайдене значення a в одну з двох конгруенцій системи (ми обираємо другу), знаходимо параметр b:

$$b \equiv -55 \pmod{33} \quad \text{або} \quad b \equiv 11 \pmod{33}. \tag{5}$$ ⑦

Таким чином, зазначені властивості має тільки $L_{10,11}$ шифр.

Яким чином можна знаходити розумні гіпотези, які допомагають при дешифруванні $L_{a,b}$ шифрів? Здається, що обрати правильну гіпотезу серед чисельних інших кандидатів можна тільки випадково. Тим не менше, існують певні підходи, які підказують як правильно обирати початкову гіпотезу. Один з ефективних способів (і не тільки для $L_{a,b}$ шифрів) називається *частотним аналізом*.

2. Частотний аналіз

Існує багато досліджень, метою яких є встановлення частот, з якими букви зустрічаються у текстах. Різні дослідження дають різні частоти букв українського алфавіту: вони залежать від специфічного авторського стилю та змісту або жанру твору (в технічних текстах частоти можуть відрізнятися від відповідних частот в літературних текстах на 10%). В таблиці 1 наведено результат одного з досліджень стосовно частот букв українського алфавіту.

Таблиця 1. Частоти букв українського алфавіту

А	Б	В	Г	Ґ	Д	Е	Є	Ж	З	И
0,064	0,015	0,053	0,015	0,000	0,031	0,048	0,005	0,008	0,023	0,064
І	Ї	Й	К	Л	М	Н	О	П	Р	С
0,052	0,011	0,010	0,039	0,032	0,034	0,068	0,100	0,029	0,050	0,043
Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ю	Я
0,052	0,032	0,004	0,013	0,012	0,012	0,006	0,004	0,018	0,009	0,021

Справжня частота букви Ґ в українських текстах становить $0,00006$. Дані у наведеній таблиці не враховують частоту пробілів між словами (символ $\sqcup$), яка насправді дорівнює 17%, що перевищує частоту будь-якої букви.

Найбільш уживані букви та їхні частоти наведено в таблиці 2. Як видно з цієї таблиці, 60% символів у текстах, написаних українською мовою, є однією з букв О, Н, А, И, В, І, Т, Р, Е, С.

Таблиця 2. 10 найбільш уживаних букв

О	Н	А	И	В	І	Т	Р	Е	С
0,100	0,068	0,064	0,064	0,053	0,052	0,052	0,050	0,048	0,043

Наведені таблиці зручно використовувати для дешифрування лінійних шифрів.

Приклад 4. Повідомлення

ЛЇ ЬМФЬ ШР ТРБРСНИШЩ
МЩОЩ ОН МРУҐКЕ
ЦЩФЩЧ ЦШЩТЬ ЄҐФРЇРУР
ОН СЇФНЖОЕ МҐКЕИ

було зашифровано за допомогою лінійного шифру. Знайти оригінал повідомлення.

Щоб висунути обґрунтовану ґіпотезу стосовно відповідності букв їхнім кодам, підрахуємо кількість появ у цьому повідомленні кожної з десяти найбільш уживаних букв з таблиці 2:

(6)

Р	Щ	О	Н	Ф	У	Е	Ш	С	Ц
7	6	4	4	4	3	3	3	2	2

Повідомлення складається з 61 символа, а букви, для яких підраховано частоти, входять в повідомлення 36 разів, тобто 59%, що добре узгоджується з таблицями 1 та 2.

Частіше за інших у тексті зустрічається буква Р, тому доцільно зробити припущення, що $\mathcal{C}_{\mathtt{О}} = \mathcal{P}_{\mathtt{Р}}$, тобто

$$a\mathcal{P}_{\mathtt{О}} + b \equiv \mathcal{P}_{\mathtt{Р}} \pmod{33} \quad \text{або} \quad 19a + b \equiv 21 \pmod{33}.$$

Ми знаємо, що розв'язання значно спрощується, якщо зробити друге припущення. Оскільки частота букв, вказана в таблиці 2, є майже однаковою, то друге припущення не є таким очевидним, як перше. Ми зробимо друге припущення згодом, а зараз переведемо повідомлення у числовий формат:

16-13 31-17-25-31 29-21 23-21-2-21-22-18-11-29-30
17-30-19-30 19-18 17-21-24-5-15-7
27-30-25-30-28 27-29-30-23-31 8-5-25-21-13-21-24-21
19-18 22-13-25-18-9-19-7 17-5-15-7-11

Для кращого сприйняття тексту ми до кожного числа додаємо справа символ "-".

Зробимо тепер друге припущення згідно таблиці частот: другою за частотою в таблиці (6) є буква Щ, тому з огляду на таблицю 2 робимо припущення $\mathcal{C}_{\text{Н}} = \mathcal{P}_{\text{Щ}}$. Оскільки $\mathcal{P}_{\text{Н}} = 18$ та $\mathcal{P}_{\text{Щ}} = 30$, то

$$18a + b \equiv 30 \pmod{33}.$$

Як і у прикладі 3, звідси випливає, що

$$a \equiv -9 \pmod{33} \quad \text{або} \quad a = 24.$$

Оскільки $(24, 33) \neq 1$, то цей шифр треба відкинути.

Ми можемо зробити інше припущення стосовно другої букви. Найчастіше за інші букви після Щ в повідомленні зустрічається О. Зробимо припущення про те, що $\mathcal{C}_{\text{Н}} = \mathcal{P}_{\text{О}}$. Оскільки $\mathcal{P}_{\text{О}} = 19$, то

$$18a + b \equiv 19 \pmod{33}. \tag{7}$$

Тоді $a = 2$. ⑧ Тому $b = 16$. ⑨

Обчислимо $a^{-1} \pmod{33} = 17$, $a^{-1}b = 272$ та застосуємо $L_{17,-272}$ шифр, ⑩ який є еквівалентним $L_{17,25}$ шифру. ⑪ Отримуємо

33-15 24-17-21-24 23-19 20-19-26-19-3-1-14-23-7

17-7-18-7 18-1 17-19-4-11-16-12

22-7-21-7-6 22-23-7-20-24 29-11-21-19-15-19-4-19

18-1 3-15-21-1-13-18-12 17-11-16-12-14

або

ЯК УМРУ ТО ПОХОВАЙТЕ
МЕНЕ НА МОГИЛІ
СЕРЕД СТЕПУ ШИРОКОГО
НА ВКРАЇНІ МИЛІЙ

Тарас Шевченко, "*Заповіт*"

3. Надійність лінійних шифрів

Ми підрахували кількість різних лінійних шифрів в розділі 6.2: виявилось, що таких шифрів існує 627. У цих підрахунках ми виходили з того, що алфавіт складається з 33 букв. Як ми бачили в §3.5, глава 3, алфавіт можна розширити, включивши інші символи клавіатури. Іншим (і більш ефективним) способом розширити алфавіт є групування символів у вихідному тексті (див. §3.5.2, глава 3). Таким чином, можна вважати, що лінійні шифри залежать від трьох параметрів: множника a, зсуву b та модуля для конгруенцій n. Ми позначаємо такі шифри через $L_{a,b,n}$.

Приклад 5. Відомо, що повідомлення було закодовано за допомогою $L_{a,b,31}$ шифра. Чи легко знайти a та b, щоб дешифрувати повідомлення?

Оцінимо спочатку кількість таких шифрів. Оскільки 31 є простим числом, існує 30 взаємно простих з n чисел a. Параметр b задовольняє умові $b \leq 31$ й тому існує 930 різних $L_{a,b,31}$ шифрів, що на 50% більше, ніж шифрів для звичайного українського алфавіту.

На сучасному комп'ютері знадобиться приблизно 1 хвилина для того, щоб перевірити всі 31 параметрів зсуву для фіксованого мультиплікативного параметру. Тому в середньому необхідно 15 хвилин для того, щоб зламати $L_{a,b,n}$ шифр при відомому n. ⑫

3.1. Принцип Керкхоффса. В усіх прикладах, які ми розглядали вище, припускалось, що відомим є принцип шифрування: приклад 5 починається словами "*Відомо, що шифрування здійснено за допомогою лінійного шифру*". Проте при дешифруванні цей факт не може бути відомим й здається, що надійність кодів від цього тільки виграє.

Проте криптологи дотримуються принципу Керкхоффса, згідно з яким стійкість криптографічного алгоритму не має залежати від принципу шифрування, але має залежати тільки від ключів. Іншими словами, при оцінці надійності шифрування необхідно вважати, що супротивник знає все про систему шифрування, крім ключів. Ключем для лінійного шифра є трійка (a, b, n).

3.2. Принцип складності обчислень. Може здатися, що згідно до принципу Керкхоффса жоден з шифрів не є надійним (стійким), оскільки вважається відомим принцип шифрування і єдине, що залишається — це перебрати усі

можливі варіанти. Це дійсно так, якщо існує лише обмежена кількість ключів. Але якщо ключів настільки багато, що метод грубої сили може дати результат тільки через кілька днів чи навіть років, то можливо відповідний шифр можна вважати досить стійким.

Нагадаємо (див. розділ 6.3), що $\phi(n)$ — це кількість чисел $a \leq n$, для яких $(a, n) = 1$ (взаємно простих з n). Тоді кількість різних лінійних кодів для алфавіту $\mathscr{A}_n$ дорівнює

$$n\phi(n). \tag{8}$$

До речі, одним з цих кодів є тотожній, тобто такий, що $\mathcal{C}_X = \mathcal{P}_X$, $X \in \mathscr{A}_n$.

3.3. Лист Джона Неша. Ідея використання складності обчислень у задачах криптографії вперше була висловлена Джоном Нешем в 1955 році у листі до Агенства національної безпеки США, який було розсекречено лише в 2012 році.

У своєму листі Неш пропонував оцінювати безпеку криптосистем базуючись на обчислювальній складності, тобто саме на тому принципі, який через 20 років потому ліг в основу сучасної криптографії.

В 1955 році Неш не був настільки відомим, як тепер,* тому здається, що керівництво АНБ не звернуло особливої уваги на його лист, можливо через молодий вік кореспондента, а можливо через особливості його особистості. Неш писав:

> "*Моя загальна гіпотеза виглядає наступним чином: майже для всіх досить складних типів шифрування ... середня складність обчислення ключа зростає експоненціально з довжиною ключа.*"

*В 1994 році Джон Неш отримав Нобелевську премію; історію його життя висвітлено у знаменитому художньому фільмі "Ігри розуму".

Вираз "експоненціально зростає" можна розуміти, наприклад, таким чином: при зміні ключа, який складається з n параметрів, на ключ з $n+1$ параметром, складність обчислень цих параметрів зростає удвічі. Д. Неш розумів значення своєї гіпотези:

> "*Важливість цієї загальної гіпотези, якщо припустити її істинність, очевидна. Вона означає, що цілком ймовірним стає створення шифрів, які фактично неможливо зламати. Зі зростанням складності шифру змагання між командами шифрувальників та дешифрувальників, стане надбанням історії.*"

3.4. Найбільш загадковий рукопис. На противагу принципу Керкхоффса існують підходи, основані на збереженні в секреті самого способу шифрування. Один з відомих прикладів — це єгипетська ієрогліфічна система, яку змогли зрозуміти лише в XIX сторіччі. Іншим є загадка Тайлера, яку опублікував в 1841 р. Е. По (див. [По], стор. 35). Лише в 2016 р. молодий програміст Джил Броза з Канади зміг відновити оригінальний текст Тайлера. Проте не всі загадки, які дійшли до людства з стародавніх часів, нам вдалося розгадати.

В бібліотеці Єльського університету (США) зберігається манускрипт, який називають "*найбільш загадковим текстом*", відомим людству. Цей текст, який складається з 240 пергаментних сторінок і містить приблизно 170000 символів, створений невідомим автором. Засобами радіовуглецевого аналізу в 2011 році встановлено, що манускріпт було створено у період з 1404 по 1438. За призвіщем букініста, який на початку XX сторіччя відкрив людству цей зразок криптографічної майстерності, манускріпт називають *руко-*

писом Войнича. Саме цю книгу протягом XX століття називали "*святим Граалем криптографії*".

За характером ілюстрацій, вміщених в рукопис, можна віднести його до ботаніки або фармацевтики. З таким же успіхом можна вважати його текстом з астрономії або космології. Статистичний аналіз тексту виявив, що його структура є характерною для для природних мов. Проте принцип шифрування досі невідомий і тому ми до цього часу не знаємо зміст цього тексту.

Безліч теорій було висунуто з приводу мови, яка використана у манускрипті. Фактично лише гіпотеза про україномовне походження рукопису дозволяє отримати реальні прочитання фрагментів рукопису. Проте й ця гіпотеза багатьма спеціалістами вважається необґрунтованою.

Гіпотеза про україномовне походження рукопису належить Джону Стойко, який в 1978 році запропонував дешифрацію 9 його сторінок. Необхідно відзначити, що дану версію прочитання не можна вважати єдиним текстом, оскільки сторінки були узяті в різнобій. Навіть в Україні, як серед фахівців, так і читачів, дешифрування Стойко й, одночасно і сам підхід, запропонований ним, розглядається багатьма украй критично, аж до позначень "маячня". З іншого боку, у 2010 р. з'явилося декілька нових версій прочитання окремих сторінок рукопису Войнича, в яких саме підхід Стойко брався за основу методу реконструкції тексту.

3.5. Час, потрібний для зламу лінійного шифру. Ми розглянемо лише кілька ілюстративних прикладів оцінки часу, потрібного для зламу лінійних шифрів методом грубої сили.

Приклад 6. Відомо, що повідомлення було зашифровано

за допомогою лінійного $L_{a,b,231}$ шифру. В найгіршому випадку, скільки шифрів треба перебрати, що дешифрувати повідомлення?

В найгіршому випадку знадобиться перевірка $231 \cdot \phi(231)$ шифрів (див. (8)). Оскільки $231 = 3 \cdot 7 \cdot 11$, то

$$\phi(231) = 3{\cdot}7{\cdot}11{\cdot}\left(1-\frac{1}{3}\right){\cdot}\left(1-\frac{1}{7}\right){\cdot}\left(1-\frac{1}{11}\right) = 2{\cdot}6{\cdot}10 = 120.$$

(див. властивість 6.5). Таким чином, у найгіршому випадку знадобиться перевірка $231 \cdot 120 = 27,720$ шифрів.

Приклад 7. Супротивник перехопив повідомлення, яке було закодовано за допомогою $L_{a,b,221}$ шифру. Без комп'ютера вдається перевірити 7 шифрів за 5 хвилин. Скільки необхідно часу, щоб дешифрувати повідомлення без комп'ютера?

У найгіршому випадку необхідно перевірити всі шифри, число яких $221 \cdot \phi(221)$ (див. (8)). Оскільки $221 = 13 \cdot 17$, то існує $221 \cdot 12 \cdot 16 = 42,432$ шифрів. ⑬ Таким чином, в найгіршому випадку знадобиться

$$\frac{42432}{7} \cdot 5 \approx 30,308$$

хвилин, щоб дешифрувати повідомлення. Зауважимо, що це відповідає більше, ніж 21 добі неперервних обчислень.

Приклад 8. Розвідка перехопила повідомлення, яке було зашифровано за допомогою лінійного $L_{a,b,440}$ шифра. Досвід свідчить, що спеціалізована комп'ютерна програма здатна перевірити за 2 хвилини всі лінійні шифри при фіксованому параметрі a та різних параметрах b. Через який

час можна очікувати, що перехоплене повідомлення буде розшифровано?

Загалом існує $440 \cdot \phi(440)$ шифрів (див. (8)). Оскільки $440 = 2^3 \cdot 5 \cdot 11$, то $\phi(440) = \left(2^3 - 2^2\right) \cdot 4 \cdot 10 = 160$. Це означає, що комп'ютер здатен обробити всі варіанти за $2 \cdot 160 = 320$ хвилин, що дорівнює 5 годин та 20 хвилин. Саме за такий час повідомлення буде дешифровано напевно.

4. Ще раз про знаходження оберненого за модулем

Критично важливим для дешифрування лінійних шифрів є вміння знаходити обернене число за модулем. Правило для знаходження оберненого за модулем наведено в теоремі 4.3, яка фактично є наслідком розширеного алгоритма Евкліда (див. алгоритм 4.3).

Для знаходження числа, оберненого за модулем, необхідні не тільки остачі $\{r_i\}$, які обчислюються у звичайному алгоритмі Евкліда (див. алгоритм 4.2), але й дільники $\{q_i\}$, які визначаються формулою (4.2). Умовою закінчення алгоритмів Евкліда є рівність (4.3). Основною для знаходження оберненого у модульній арифметиці є формула (4.12) (нагадаємо, що члени послідовності $\{u_i\}$ обчислюються у зворотному порядку, тобто числа u_2 та u_1 обчислюються останніми).

Для ілюстрації розглянемо дуже простий приклад з малими числами a та n.

Приклад 9. Для знаходження $(20, 7)$ алгоритм Евклі-

да 4.2 обчислює $r_i \equiv r_{i-2} \pmod{r_{i-1}}$:

i	-1	0	1	2	3
r_i	20	7	6	1	0

Розширений алгоритм Евкліда 4.3 додатково знаходить q_i за формулою $r_{i-2} = r_{i-1}q_i + r_i$:

i	-1	0	1	2	3
r_i	20	7	6	1	0
q_i			2	1	6

Згідно з теоремою 4.3 тепер необхідно заповнити другий рядок таблиці (4.11). Числа $\{u_i\}$ обчислюються за формулою (4.13). В нашому випадку обчислення є такими:

$$\begin{pmatrix} - & - & q_2 & q_1 \\ 0 & 1 & - & - \end{pmatrix} = \begin{pmatrix} - & - & 1 & 2 \\ 0 & 1 & - & - \end{pmatrix} \longrightarrow \begin{pmatrix} - & - & 1 & 2 \\ 0 & 1 & 1 & 3 \end{pmatrix}$$

Тому $20 \cdot 1 - 7 \cdot 3 = -1$, звідки $3 = 7^{-1} \pmod{20}$. ⑭

5. КОНТРОЛЬНІ ПИТАННЯ

1. У прикладі 1 отримати конгруенцію $b \equiv 23 - 3a \pmod{33}$. (стор. 157).

2. Пояснити, чому $(c, 33) = 1$ у прикладі 1? (стор. 157).

3. Поясніть, чому саме 20 пар у прикладі 1 задовольняють умову $\mathcal{C}_{\mathtt{B}} = \mathcal{P}_{\mathtt{T}}$. (стор. 157).

4. Перевірити обчислення у першій таблиці прикладу 2. (стор. 158).

5. Перевірити обчислення у другій таблиці прикладу 2. (стор. 158).

6. Чому конгруенції можна віднімати? (стор. 159).

7. Перевірити, що (5) можна отримати, якщо підставити a, знайдене в (4), у конгруенцію (2). (стор. 159).

8. Перевірити, що $a = 2$ в (7). (стор. 162).

9. Чому $b = 16$ в (7)? (стор. 162).

10. Чому саме $L_{17,-272}$ шифр застосовано у прикладі 4? (стор. 162).

11. Чому шифри $L_{17,-272}$ та $L_{17,25}$ є еквіалентними? (стор. 162).

12. Поясніть чому необхідно 15 хвилин для того, щоб зламати $L_{a,b,n}$ шифр при відомому n? (стор. 164).

13. Як у прикладі 7 було підраховано, що існує 42,432 шифрів? (стор. 168).

14. Чому з $20 \cdot 1 - 7 \cdot 3 = -1$ випливає, що $3 = 7^{-1} \pmod{20}$? (стор. 170).

6. З А Д А Ч І

Задача 1. *Довести, що якщо*

a) *відомий параметр a лінійного шифру $L_{a,b}$, то його дешифрація еквівалентна дешифрації шифру Цезаря*;

b) *відомий параметр b лінійного шифру $L_{a,b}$, то його дешифрація еквівалентна дешифрації мультиплікативного шифру.*

Задача 2. *Ви отримали повідомлення*

ІАУЛЬО ЗЯЛЯРЇ ЄУРОБФ ЯЩЯРЇІ АУЛЬОЗ ЯЛЯРЇЯ РЇБФЯЩ

яке було зашифровано лінійним шифром з параметром $a = 17$. Дешифрувати це повідомлення.

Задача 3. *Припустимо, що вам стало відомим місце, на якому в тексті, зашифрованому лінійним шифром $L_{a,b}$, стоїть код комбінації* АБ. *Як без обчислень визначити параметри a та b?*

Задача 4. *Припустимо, що вам випадково стало відомим, яким буквам в повідомленні відповідає комбінація* АБ *у тексті, отриманому застосуванням лінійного шифру. Як без обчислень визначити параметри лінійного шифру?*

Задача 5. *Повідомлення* ФЕРМА *зашифровано лінійним шифром. Зашифрованим текстом є* ИҐЧІЙ. *Визначити параметри шифру.*

Задача 6. *Повідомлення* ЕВКЛІД *зашифровано лінійним шифром. Зашифрованим текстом є* ЗТМСБҐ. *Визначити параметри шифру.*

Задача 7. *Повідомлення* ОЙЛЕР *зашифровано лінійним шифром. Зашифрованим текстом є* РИКЩФ. *Визначити параметри шифру.*

Задача 8. *Повідомлення* ГАУСС *зашифровано лінійним шифром. Зашифрованим текстом є* ЬЗДФФ. *Визначити параметри шифру.*

Задача 9. *За допомогою частотного аналізу дешифрувати повідомлення українською мовою*

БЩЬФХИЙЬ КЦГХИІДИ ТМИАНДЧЮ УЗСХГХДФ ЗСХКТЦИБ
ТЗЛЗБЗВД ГУЧМИАНЩ ІГХИЕГУЗ ЙЗБЗЛЗШЇ ГСХЗХДЗЛ
ЗГДГЬКЕЩ ЕГМИАНЗІ ГДЗЛЗХЧЦ СХЩ

яке було зашифровано мультиплікативним шифром $M_{a,33}$.

Задача 10. *У повідомленні, зашифрованому шифром* $L_{a,b}$, *найбільш уживаними буквами є* А *та* Ц. *Знайти параметри* a *та* b.

Задача 11. *Повідомлення можна спочатку зашифрувати лінійним шифром* L_{a_1,b_1}, *а потім отриманий результат зашифрувати лінійним шифром* L_{a_2,b_2}. *В результаті повідомлення буде зашифровано так званим продакт шифром. Знайти продакт шифр для комбінації* $L_{5,3}$ *та* $L_{17,3}$.

Задача 12. *Відомим в історії криптографії є випадок, який трапився під час II світової війни. Кожного дня радист німецької армії в пустелі Сахара надсилав в Берлін одне і те ж повідомлення* НІЧОГО НЕ ТРАПИЛОСЬ (*кожного дня зашифроване за допомогою нового ключа*). *Оскільки текст самого повідомлення був відомий англійським криптографам, вони кожного дня обчислювали ключ і за його допомогою дешифровували інші, часом важливі повідомлення від німецької армії в Сахарі.*

Припустимо, що ви знаєте, що текст НІЧОГО НЕ ТРАПИЛОСЬ *відповідає повідомленню* ДЦХЄИЄДМЛІҐЗФБЄЙЮ, *зашифрованому* $L_{a,b}$ *шифром з невідомими параметрами* a *та* b. *Знайти параметри цього шифру та дешифрувати інше повідомлення*: ДҐЙНЗЄЖЙЮГЦЬ.

Задача 13. *Доведіть, що для будь-яких цілих чисел a та b, $b > 0$, існують цілі числа q та r, $-b/2 < r \leq b/2$, для яких $a = bq + r$. Цей спосіб представлення одного числа через інше є іншим способом ділення з остачею.*

Задача 14. *Довести, що $a \pmod n = b \pmod n$ тоді і тільки тоді, коли $b - a$ ділиться на n.*

Задача 15. *Нехай $(a, b) = 1$. Довести, що*

a) $(a + b, a - b) = 1$ *або* 2;
b) $(2a + b, a + 2b) = 1$ *або* 3;
c) $(a + b, a^2 + b^2) = 1$ *або* 2;
d) $(a + b, a^2 + -ab + b^2) = 1$ *або* 3.

Задача 16. *Нехай a та b є ненулевими цілими числами. Довести, що наступні три умови є еквівалентними*:

a) $a \mid b$;
b) $(a, b) = |a|$;
c) $[a, b] = |b|$.

Задача 17. *Нехай a, b та $m > 0$ — цілі числа. Довести, що якщо*

a) $a \equiv b \pmod m$, *то* $a \pmod m = b \pmod n$;
b) $a \pmod m = b \pmod n$, *то* $a \equiv b \pmod m$.

Задача 18. *Знайти контрприклад до твердження*: *якщо $m > 2$ є цілим, то*

a) $(a + b) \pmod m = a \pmod m + b \pmod m$ *для будь-яких цілих чисел a та b*;
b) $ab \pmod m = (a \pmod m) \cdot (b \pmod m)$ *для будь-яких цілих чисел a та b.*

Задача 19. *В турнірі приймають участь $N = 2m$ команд. Кожна команда має грати з іншою лише один раз. У кожному раунді повинні грати всі команди. Як можна скласти графік для такого турніру*?

Один з методів складання графіка турніру, який ми зараз опишемо, базується на властивостях конгруенцій: *команда і грає з*

командою j в раунді k, якщо $(i+j) \equiv k \pmod{N-1}$. Це правило не стосується команди N, яка грає з командою i, для якої $2i \equiv k \pmod{N-1}$.

a) *Показати, що у кожному раунді k існує тільки одна команда i, для якої $2i \equiv k \pmod{N-1}$.*
b) *Показати, що для кожної команди i в кожному раунді k існує тільки одна команда j, для якої $(i+j) \equiv k \pmod{N-1}$.*
c) *Показати, що кожна команда грає з іншою тільки один раз протягом турніру.*

Задача 20. *Прочитайте уважно умови задачі* 19.

a) *Як скласти графік турніру, у якому приймають участь непарна кількість команд?*
b) *Складіть графік турніру для п'яти команд.*

Задача 21. *Нехай $\sigma(n)$, $n > 1$, — це сума всіх дільників натурального числа включно з* 1 *та n. Покладемо також $\sigma(1) = 1$. Довести, що якщо p є простим числом, то*

a) $\sigma(p) = p + 1$;
b) $\sigma(p^k) = (p^{k+1} - 1)/(p-1)$ *для* $k \geq 1$;
c) $\sigma(pq) = \sigma(p)\sigma(q)$ *для простого числа* $q > 1$;
d) $\sigma(p^k q^l) = \sigma(p^k)\sigma(q^l)$, *якщо* $q > 1$ *є простим числом, а* $k, l \geq 1$.

Задача 22. *Довести, що функція $\sigma(n)$, означена у задачі* 21, *є мультиплікативною, тобто*

$$\sigma(mn) = \sigma(m)\sigma(n),$$

якщо $(m, n) = 1$.

Задача 23. *Число n називається досконалим, якщо сума його дільників (без n) дорівнює цьому числу, тобто якщо $\sigma(n) - n = n$ або $\sigma(n) = 2n$ (означення функції $\sigma(n)$ див. в задачі* 21). *Довести теорему Евкліда: якщо $2^k - 1$ є простим числом, то $2^{k-1}(2^k - 1)$ є досконалим числом.*

Задача 24. *Нехай n є досконалим числом (означення досконалого числа див. в задачі 23). Довести, що*

$$\sum_{d|n} \frac{1}{d} = 2.$$

Задача 25. *Число n називається k-досконалим, якщо $\sigma(n) = kn$ (означення функції $\sigma(n)$ див. в задачі 21). Доведіть, що жодне з чисел $2^k 3^l$ не є досконалим.*

Задача 26. *Число n називається супердосконалим, якщо $\sigma(\sigma(n)) = 2n$ (означення функції $\sigma(n)$ див. в задачі 21). Доведіть, що число $n = 2^k$ є супердосконалим, якщо $2^{k+1} - 1$ є простим.*

Задача 27. *Нехай m — просте число; a та b — натуральні числа, $(a, m) = 1$. Для розв'язання рівняння*

$$ax \equiv b \pmod{m} \tag{9}$$

можна використати метод, який базується на наступних діях.

a) *Покажіть, що якщо x є розв'язком рівняння (9), то x також є розв'язком рівняння*

$$a_1 x \equiv -b[m/a] \pmod{m}$$

для $a_1 \equiv m \pmod{a}$. Нова конгруенція є такого ж типу, як і початкова, але з меншим коефіцієнтом у лівій частині.

b) *Повторюючи процедуру з* a), *отримуємо послідовність коефіцієнтів $a = a_0 > a_1 > a_1 > \dots$. Показати, що знайдеться n, при якому $a_n = 1$, тобто на цьому кроці рівняння має вигляд $x \equiv B \pmod{m}$.*

c) *Застосувати метод, описаний в* b), *для розв'язання рівняння $6x \equiv 7 \pmod{23}$.*

Задача 28. *Астроном знає, що період обертання супутника навколо Землі є кратним 1 годині і є меншим 1 дня. Астроном помітив, що супутник здійснює 11 обертань за час, який починається у момент, коли годинник показує 0 годин і закінчується, коли годинник показує 17 годин. Яким є період обертання супутника навколо Землі?*

Задача 29. *В таблиці, наведеній нижче, записано кількість днів у кожному з місяців високосного року, починаючи з грудня*:

i	XII	I	II	III	IV	V	VI	VII	$VIII$	IX	X	XI
D_i	31	31	29	31	30	31	30	31	31	30	31	30
d_i	3	3	1	3	2	3	2	3	3	2	3	2

У третьому рядку обчислено значення $d_i \equiv D_i \pmod 7$, *де* D_i — *це кількість днів у місяці* i, $1 \le i \le 12$. *Кожному дню тижня припишемо такі числа:*

день	понеділок	вівторок	середа	четвер	п'ятниця	субота	неділя
w	1	2	3	4	5	6	0

Відомо, що 29.12.2015 припав на вівторок, для якого $w = 2$. *Тому 29.01.2016 припаде на* $(w + d_I) \pmod 7 = 5$, *тобто на п'ятницю.*

a) *Знайти правило, аналогічне тому, що було наведено вище для 29.01.2016, за яким можна визначати день тижня для кожної дати протягом 2016 року якщо знати на які дні тижня припадають дні довільного місяця.*
b) *Визначити скільки разів число 13 припаде на п'ятницю в 2016 році.*

Задача 30. *Прочитайте уважно текст задачі* 29. *Знайдіть правило, аналогічне тому, що було наведено у задачі* 29 *для 29.01.2016, за яким можна визначати день тижня для кожної дати протягом*

a) *невисокосного року*;
b) *будь-якого року, як завгодно далекого від 2015.*

Задача 31. *Історія математики зберігає багато задач про конгруенції, які вважались складними у свій час. Розв'яжіть три наступні задачі-головоломки.*

a) (*задача Махавіракарайя, 850 р.*) *Є* 7 *окремих бананів та* 63 *зв'язок по однаковій кількості бананів у кожній. Всі банани розділили порівну між* 23 *гостями. Скільки бананів було у кожній зв'язці?*

b) (*задача Йен Кунга, 1372 р.*) *Є кілька монет. Їх можна розкласти порівну у* 78 *стовпчиках. Якщо ж їх розкласти у* 77 *стовпчиках так, щоб кожен містив однакову кількість, то ще залишиться* 27 *монет. Скільки є монет?*

c) (*задача Ойлера, 1770 р.*) *Розбити число* 100 *на два доданки так, щоб один з них ділився на* 7, *а інший на* 11.

7. БІОГРАФІЇ

Керкхоффс, *Огюст* (1835–1903), нідерландський криптограф, лінгвист, історик, математик. Автор фундаментальної праці "*Військова криптографія*" ("*La Cryptographie Militaire*"), у якій він сформулював загальні вимоги до криптосистем. Одним з висновків цієї праці є висновок про те, що тільки криптоаналіз є єдино вірним способом оцінити надійність шифрів.

Своє знайомство з криптографією почав з вивчення телеграфних військових шифрів. Він особливо підкреслював, що на відміну від листування старого часу, телеграф значно збільшив обсяги інформації, якою обмінюються кореспонденти, що породжує принципово нові вимоги до шифрів.

"*Військова криптографія*" вперше була опублікована двома частинами в журнальному варіанті в січні і лютому 1883 року, а пізніше в тому ж році була перевидана у вигляді окремої брошури. Незважаючи на безсумнівну фундаментальність, праця була невеликою за обсягом — всього 64 сторінки. Запропоновані ним рішення нових криптографічних проблем були розумними і добре обґрунтованими. Керкхоффс сформулював шість загальних вимог до криптостійкості систем:

(1) система повинна бути фізично незламною;
(2) потрапляння системи в руки ворога не повинно завдавати проблем її автору;
(3) зберігання та передача ключа повинні здійснюватись без паперових записів; кореспонденти повинні мати можливість міняти ключ за своїм розсудом;
(4) система повинна бути придатною для передачі повідомлень телеграфом;
(5) система повинна легко адаптуватись при зміні місця; для роботи з нею не вимагається участь кількох осіб одночасно;
(6) нарешті, система повинна бути простою у використанні й не вимагати значного розумового напруження або дотримання

великої кількості правил.

Неш, *Джон* (1928–2015), американський математик, який працював у галузі теорії ігор та диференціальної геометрії.

Лауреат Нобелівської премії з економіки 1994 року (разом з Райнхардом Зелтеном та Джоном Харсані), а також Абелівської премії 2015 року (разом з Луїсом Ніренбергом). Найбільших досягнень Неш здобув у теорії ігор, яка вразила його уяву ще у віці 20 років. Неш зумів створити основи наукового методу, що зіграв величезну роль у розвитку світової економіки. У 1949 році 21-річний учений написав дисертацію у галузі теорії ігор, а через сорок п'ять років він отримав за цю роботу Нобелівську премію з економіки. У рішенні Нобелівського комітету записано, що Неш отримує нагороду "*за фундаментальний аналіз рівноваги в теорії некооперативних ігор*".

1998 року професор журналістики Колумбійського університету Сильвія Назар опублікувала біографічну книгу "*A Beautiful Mind*". У книзі вона змалювала багатогранне життя Джона Неша, описала проблеми впливу його тяжкої хвороби на світ особистих і професійних стосунків. 2001 року, за мотивами книги "*A Beautiful Mind*", історію Джона Неша покладено в основу голлівудського фільму "*Ігри розуму*", який пізніше отримав 4 премії Оскар.

Джон Неш загинув 23 травня 2015 р. разом зі своєю дружиною при поверненні з Норвегії із церемонії нагородження Абелівською премією. Трагедія сталася у штаті Нью-Джерсі: при перелаштуванні з лівої до правої смуги водій таксі втратив керування машиною і зіткнувся з огорожею та ще одним авто. Поліція встановила, що подружжя не було пристебнуте ременями безпеки, через це смерть настала практично миттєво.

Глава 8

ЕКСПОНЕНЦІАЛЬНІ ШИФРИ

В 1978 році американські математики С. Поліґ та М. Хеллман розглянули новий математичний шифр, який тепер називається *експоненціальним*. Він діє за правилом

$$\mathcal{C}_{\mathtt{X}} \equiv \mathcal{P}_{\mathtt{X}}^{k} \pmod{n}. \tag{1}$$

Таким чином, експоненціальний шифр залежить від двох параметрів: показника k та модуля n. Його дію словами можна описати наступним чином: цифровий код кожної букви підноситься до степеня k, після чого обчислюється остача від ділення на n. Експоненціальні коди будемо позначати $E_{k,n}$.

1. Особливості експоненціального шифру

Уважний читач може мати сумнів стосовно надійності такого шифру, оскільки завжди $\mathcal{C}_{\mathtt{A}} = \mathcal{P}_{\mathtt{A}}$. ① Це дійсно проблема, але її легко усунути: для цього шифруються не окремі букви повідомлення, а блоки букв (див. §3.5.2, глава 3).

Приклад 1. Якщо блоки утворюються з двох букв, то числовим кодом групи `AO` є $\mathcal{P}_{\mathtt{AO}} = 119$, оскільки $\mathcal{P}_{\mathtt{A}} = 1$ та $\mathcal{P}_{\mathtt{O}} = 19$. Таким чином, шифр групи `AO`, обчисленим за допомогою $E_{2,1000}$ шифру, є

$$\mathcal{C}_{\mathtt{AO}} \equiv 119^2 \pmod{1000} = 14,161 \pmod{1000} = 161.$$

Існує ще одна проблема, пов'язана з неоднозначністю такого представлення блоків у числовому вигляді: той самий код 119 має група ИЖ, оскільки $\mathcal{P}_{\text{И}} = 11$ та $\mathcal{P}_{\text{Ж}} = 9$. Але і цю проблему легко усунути, домовившись, що цифровими кодами букв $\text{А}, \text{Б}, \ldots, \text{Ж}$ є $\texttt{01}, \texttt{02}, \ldots, \texttt{09}$. Тоді $\mathcal{P}_{\text{АО}} = 0119 = 119$, а $\mathcal{P}_{\text{ИЖ}} = 1109$.

Приклад 2. До речі, за допомогою шифру $E_{2,1000}$ група ИЖ шифрується в

$$\mathcal{C}_{\text{ИЖ}} \equiv 1109^2 \pmod{1000} = 1,229,881 \pmod{1000} = 881.$$

Зауваження 1. Ще одним способом впорядкувати букви в алфавіті є лексикографічний порядок (див. зауваження 3.6).

1.1. Яким має бути n. Модуль шифра (1) має бути достатньо великим. Щоб пояснити це, розглянемо шифр $E_{k,701}$ для блоків з двох букв. Тоді група ПЄ має числовий код $\mathcal{P}_{\text{ПЄ}} = 2008$. Але

$$2008 \equiv 1307 \equiv 606 \pmod{701}, \qquad (2)$$

звідки випливає, що при шифруванні повідомлень комбінації 2709, 2008, 1307, 606 дають однаковий результат. ③ Таким чином $\mathcal{C}_{\text{ЦЖ}} = \mathcal{C}_{\text{ПЄ}} = \mathcal{C}_{\text{ЇЕ}} = \mathcal{C}_{\text{ДД}}$.

Щоб уникнути такої неоднозначності при шифруванні українських текстів, модуль n повинно бути більшим за 3333. ④

1.2. Експоненціальний шифр не є підстановкою. Експоненціальний шифр вигляду (1) є *підстановкою*. Це означає, що кожна буква має свій фіксований код і завжди шифрується саме в цей код. Наприклад, буква Г за допомогою

$E_{3,33}$ шифру завжди перетворюється в

$$\mathcal{C}_{\text{Г}} = 4^3 \pmod{33} = 31.$$

Для кожного підстановочного шифру можна скласти таблицю відповідності $\mathcal{P}_{\text{Х}} \to \mathcal{C}_{\text{Х}}$, $X \in \mathscr{A}$, й при шифруванні користуватись тільки нею.

Ситуація змінюється при шифруванні блоками. Якщо експоненціальний шифр використовується для блоків, то він перестає бути підстановкою. Наприклад, текст

Ш	И	Р	О	К	О	Г	О
29	11	21	19	15	19	04	19

при групуванні у чотири символи другого рядку перетворюється в послідовність чисел

2911 2119 1519 0419

жодне з яких не повторюється, не зважаючи на те, що буква О тричі входить у початковий текст. Це означає, що у шифрованому тексті буква О буде мати різні значення. Наприклад, при використанні експоненціального шифру $E_{2,3334}$ це повідомлення зашифрується у

(3) 2227 2597 233 2193 ⑤

й буква О у зашифрованному тексті має три різні значення 97, 33 та 93. Тим не менше, у великих текстах повтори можливі, але вибором більшого n вони усуваються.

Зауваження 2. Остання група може мати меншу кількість символів, ніж всі інші. В таких випадках ми дописуємо справа необхідну кількість символів $\sqcup$ й вважаємо,

що $\mathcal{P}_{\sqcup} = \texttt{00}$. Таким чином, якщо групи складаються з двох символів, то текст НІЧ перетворюється в НІЧ$\sqcup$ й має числовий еквівалент 1812 2800, оскільки

$$\mathcal{P}_{\texttt{Н}} = \texttt{18}, \quad \mathcal{P}_{\texttt{І}} = \texttt{12}, \quad \mathcal{P}_{\texttt{Ч}} = \texttt{28}, \quad \mathcal{P}_{\sqcup} = \texttt{00}.$$

2. Властивість конгруенцій, необхідна для експоненціальних шифрів

Теорема 1. *Якщо* $a \equiv b \pmod{n}$, *то* $a^s \equiv b^s \pmod{n}$ *для будь-якого* $s \geq 1$.

Для $s = 2$ теорема 1 випливає з властивості 8 теореми 2.4: $a \cdot a \equiv b \cdot b \pmod{n}$. Щоб довести теорему 1 для довільного $s \geq 2$, можна застосувати метод математичної індукції. Ми ж наведемо інше доведення цього факту.

Доведення. Оскільки

$$a^s - b^s = (a-b)\left(a^{s-1} + a^{s-2}b + \cdots + ab^{s-2} + b^{s-1}\right), \tag{4}$$

⑥ то, якщо $a-b$ ділиться на n, то й $a^s - b^s$ ділиться на n. □

Наведемо приклад, який показує як теорему 1 можна застосувати, щоб полегшити обчислення при користуванны експоненцыальними шифрами.

Приклад 3. Обчислити $137^5 \pmod{140}$.

Оскільки $137 \pmod{140} = -3$, з теореми 1 випливає

$$137^5 \pmod{140} = (-3)^5 \pmod{140} = -243 \pmod{140} = 37.$$

3. Дешифрування експоненціального шифру

Формула обчислення експоненціального шифру (1) підказує, що "дешифрування" відбувається за формулою

$$\mathcal{P}_{\mathtt{X}} \equiv \mathcal{C}_{\mathtt{X}}^{1/k} \pmod{n}.$$

Але як обчислити корінь степеня k за модулем? Щоб отримати коректну відповідь, міркуємо за аналогією з мультиплікативними шифрами. Назвемо число j *показником кореня k-ого степеня* за модулем n, якщо

$$a^{kj} \equiv a \pmod{n} \quad \text{для всіх} \quad a. \tag{5}$$

Якщо j — це показник кореня k-ого степеня за модулем n, то за теоремою 1

$$\mathcal{C}_{\mathtt{X}}^{j} \equiv \left(\mathcal{P}_{\mathtt{X}}^{k}\right)^{j} \pmod{n} = \mathcal{P}_{\mathtt{X}}^{kj} \pmod{n} = \mathcal{P}_{\mathtt{X}} \pmod{n}$$

або

$$\mathcal{P}_{\mathtt{X}} \equiv \mathcal{C}_{\mathtt{X}}^{j} \pmod{n}. \tag{6}$$

Теорема 2. *Дешифрування тексту після застосування експоненціального шифру $E_{k,n}$ здійснюється за допомогою експоненціального шифру $E_{j,n}$, де j — це показник кореня k-ого степеня за модулем n.*

3.1. Обчислення показника кореня. Як же можна обчислити показник кореня k-ого степеня за модулем n? Ми розглянемо два випадки, коли це зробити нескладно. Корисним для цих і інших випадків є наступний результат.

Лема 1. *Нехай n є натуральним числом, а k та j є такими, що*

$$kj \equiv 1 \pmod{\phi(n)}, \tag{7}$$

тобто k та j є оберненими одне до іншого за модулем $\phi(n)$, де $\phi(n)$ — це функція Ойлера (див. §2.1, глава 6). Якщо a — натуральне число, для якого $(a,n) = 1$, то $a^{kj} \equiv a \pmod{n}$.

Доведення. Рівність за модулем (7) є еквівалентною звичайній рівності $kj = t\phi(n) + 1$ для деякого $t \in \mathbf{N}$, звідки $a^{kj} = a^{t\phi(n)+1} = a^{t\phi(n)} \cdot a$. Оскільки $(a,n) = 1$, то з теореми Ойлера (див. теорему 6.2) випливає, що

$$a^{kj} \equiv a^{t\phi(n)} \cdot a \pmod{n} = \left(a^{\phi(n)}\right)^t \cdot a \pmod{n} = a \pmod{n}.$$

⑦ □

3.2. Обчислення показника кореня, коли $n = p$. В цьому випадку існування показника кореня забезпечується наступною лемою.

Лема 2. *Нехай $n = p$ — просте число, а k та j є оберненими одне до іншого за модулем $\phi(p)$, ⑧ тобто виконано умову (7). Тоді*

$$a^{kj} \equiv a \pmod{p} \quad \textit{для всіх} \quad a. \tag{8}$$

Доведення. Конгруенція (8) є вірною на підставі леми 1, якщо $(a,p) = 1$. Якщо ж $(a,p) \neq 1$, то $(a,p) = p$, ⑨, тобто

$a = tp$ для деякого $t \in \mathbf{N}$. Іншими словами, $a \equiv 0 \pmod{p}$. Звідси випливає, що

$$a^{kj} \equiv 0^{kj} \pmod{p} = a \pmod{p}.$$

□

Лема 2 дозволяє знаходити показник кореня k-ого степеня за модулем n, якщо n є простим числом, а k та $\phi(n)$ є взаємно простими числами.

Правило 1. Показник кореня k-ого степеня за модулем $n = p$

Нехай n є простим числом, причому k та $\phi(n)$ є взаємно простими числами. Якщо показник кореня k-ого степеня за модулем n позначити через j, то $j = k^{-1} \pmod{\phi(n)}$.

Дійсно, з умови $(k, \phi(n)) = 1$ випливає, що існує ⑩ обернене число $k^{-1} \pmod{\phi(n)}$, яке ми позначимо через j. Саме воно і є степенем коріня з k за модулем n.

Приклад 4. Нехай $k = 7$, $n = 31$. Знайти показник кореня 7-ого степеня за модулем 31.

Оскільки 31 є простим числом, то $\phi(31) = 30$. Оскільки $(7, 30) = 1$, то $j = 7^{-1} \pmod{30} = 13$ згідно з правилом 1. ⑪ Таким чином, якщо текст зашифровано $E_{7,31}$ шифром, то його дешифрують $E_{13,31}$ шифром.

3.3. Обчислення показника кореня, коли $n = pq$. Ще одним випадком, коли степінь кореня за модулем можна ефективно обчислити, є $n = pq$, де p та q — різні прості числа.

Лема 3. *Нехай $n = pq$, де p та q — різні прості числа. Припустимо, що k та j є оберненими одне до іншого за модулем $\phi(pq)$,* ⑫ *тобто виконано умову* (7). *Тоді*

$$a^{kj} \equiv a \pmod{pq} \quad \textit{для всіх} \quad a. \tag{9}$$

Доведення. Перепишемо умову (7) у вигляді $kj = t\phi(n) + 1$ для деякого $t \in \mathbf{N}$. Оскільки $\phi(\cdot)$ є мультиплікативною функцією, то $\phi(pq) = \phi(p)\,\phi(q)$ й тому $kj = t\phi(p)\,\phi(q) + 1$. Зокрема, $kj \equiv 1 \pmod{\phi(p)}$. З леми 2 тепер випливає

$$a^{kj} \equiv a \pmod{p} \quad \text{для всіх цілих} \quad a. \tag{10}$$

Аналогічно,

$$a^{kj} \equiv a \pmod{q} \quad \text{для всіх цілих} \quad a. \tag{11}$$

⑬ З останніх двох конгруенцій випливає, що

$$a^{kj} \equiv a \pmod{pq} \quad \text{для всіх цілих} \quad a.$$

Дійсно, конгруенції (10) та (11) означають, що $a^{kj} = up + a$ та $a^{kj} = vq + a$ для деяких $u, v \in \mathbf{N}$. ⑭ Віднімаючи від першої рівності другу, отримуємо $up - vq = 0$ або $up = vq$. Це означає, що u ділиться на q, ⑮ звідки $a^{kj} = up + a = wpq + a$ для деякого $w \in \mathbf{N}$, тобто $a^{kj} \equiv a \pmod{pq}$. □

З леми 3 випливає наступне правило знаходження показника кореня k-ого степеня за модулем n, якщо $n = pq$. ⑯

Правило 2. Показник кореня k-ого степеня за модулем $n = pq$

Нехай $n = pq$, де p та q — різні прості числа, причому k та $\phi(n)$ є взаємно простими числами. Показник кореня k-ого степеня модулем n позначимо через j. Тоді $j = k^{-1} \pmod{\phi(pq)}$.

Твердження, наведене наприкінці доведення леми 3, знадобиться нам у подальшому (див. розділ 10.4), тому сформулюємо його окремо. ⑰

Лема 4. *Нехай p та q два різних простих числа. Якщо $c \equiv d \pmod{p}$ та $c \equiv d \pmod{q}$, то $c \equiv d \pmod{pq}$.*

Приклад 5. Нехай $k = 2$, $n = 33$. Знайти показник кореня 27-ого степеня за модулем 33.

Оскільки $33 = 3 \cdot 11$, то $\phi(33) = 20$. ⑱ Оскільки $(27, 20) = 1$, то $j = 27^{-1} \pmod{20} = 3$. ⑲ Таким чином, якщо текст зашифровано $E_{2,33}$ шифром, то його дешифрують $E_{3,33}$ шифром.

3.4. Як створити свій експоненціальний код. Оберемо $n = p$ або $n = pq$, де p та q — два різних простих числа. Оберемо натуральне число k так, щоб $(k, \phi(n)) = 1$. Знайдемо $j \equiv k^{-1} \pmod{\phi(n)}$. Тоді шифрування здійснюємо за формулою (1), а дешифрування — за формулою (6).

Приклад 6. Знайти хоча б одне число k, яке можна використати в експоненціальному шифрі $E_{k,77}$.

Оскільки $n = 77 = 7 \cdot 11$, то $\phi(77) = 60 = 2^2 \cdot 3 \cdot 5$. Тому можна обрати k, яке не ділиться на 2, 3 та 5. Наприклад, $k = 7$ або $k = 11$. Обчислюємо $7^{-1} \equiv 43 \pmod{60}$ та

$11^{-1} \equiv 11 \pmod{60}$. ⑳ Експоненціальними шифрами $E_{7,77}$ та $E_{11,77}$ можна користуватись.

4. Швидке піднесення до степеня

Для обчислення степенів a^k існує ефективний алгоритм, оснований на двійковому представленні числа k.

Для скорочення ми пишемо $k = (b_i \dots b_0)_2$, якщо

$$k = b_i 2^i + \cdots + b_0 2^0. \tag{12}$$

Числа $b_i, \dots, b_0$ називаються *двійковими цифрами* (*бінарними цифрами*) у *двійковому представленні бінарному представленні* числа k.

Алгоритм 1. Швидке піднесення до степеня

Вхідні дані: натуральні числа a, k;

Вихідні дані: $n = a^k$;

знайти двійкове представлення числа $k = (b_i \dots b_0)_2$;

обчислити $a^{2^1}, a^{2^2}, \dots, a^{2^i}$;

покласти $n = 1$;

якщо $b_0 = 1$, то помножити n на a;

якщо $b_1 = 1$, то помножити n на a^2;

. . . . . .

якщо $b_i = 1$, то помножити n на a^{2^i}.

Алгоритм 1 пояснюється представленням (12), згідно з яким ㉑

$$a^k = a^{b_i 2^i} \times \cdots \times a^{b_0 2^0}.$$

Приклад 7. При обчисленні 11^{13} спочатку знаходимо двійкові цифри числа 13: $(13)_{10} = (1101)_2$, тобто $13 = 2^3 + 2^2 + 2^0$. Потім послідовно обчислюємо $11^2 = 121$, $11^4 = 11^2 \cdot 11^2 = 14,641$, $11^8 = 11^4 \cdot 11^4 = 214,358,881$. Тепер

$$\begin{aligned} 11^{13} &= 11^{2^3} \times 11^{2^2} \times 11^{2^1} = 214,358,881 \times 14,641 \times 11 \\ &= 214,358,881 \times 161,051 \\ &= 34,522,712,143,931. \end{aligned}$$

Для чисел, розглянутих у прикладі, оптимізація обчислень не є суттєвою, але для тих чисел, які насправді необхідні в практичній роботі, вона може стати критично важливою.

5. Швидке піднесення до степеня за модулем

Для обчислення остачі $a^k \pmod{n}$ існує ефективний метод, принцип якого ми спочатку пояснюємо на простому числовому прикладі для $a = 7$, $k = 13$ та $n = 10$. Таким чином, ми обчислюємо $7^{13} \pmod{10}$.

Обчислити $7^{13} \pmod{10}$ нескладно й безпосередньо, помітивши, що послідовність остач 7^k при діленні на 10 є періодичною:

k	1	2	3	4	5	6	7	8	9	10	11	12	13
$7^k \pmod{10}$	7	9	3	1	7	9	3	1	7	9	3	1	7

Таким чином, $7 = 7^{13} \pmod{10}$.

Алгоритм, який ми збираємось продемонструвати, є універсальним. На першому його кроці необхідно знайти бінарне представления числа k. В данному випадку,

$$13 = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 \quad \text{або} \quad (13)_{10} = (1101)_2.$$

За допомогою цього представлення, будуємо послідовність обчислень, на кожному кроці якої виконується одна з двох наступних операцій:

1) $\uparrow$ (піднести до квадрату й обчислити $\bmod\ n$) або
2) $\uparrow\times$ (піднести до квадрату, помножити на a й обчислити $\bmod\ n$).

Послідовність операцій визначається наступним чином:

> якщо чергова двійкова цифра у двійковому запису числа n дорівнює 0, то застосовується операція ($\uparrow$), в іншому випадку — операція ($\uparrow\times$).

Аргументом кожної операції є результат обчислення попередньої; для першої операції аргументом є 1. Результат останньої операції дорівнює необхідній остачі. Алгоритм обчислення у загальному випадку представлено нижче. ㉒

Алгоритм 2. Піднесення до степеня за модулем

Вхідні дані: натуральні числа a, k, n;

Вихідні дані: $a^k \pmod n$;

знайти двійкове представлення числа $k = (b_i b_{i-1} \dots b_0)_2$;

якщо $b_i = 0$, то $x_1 = 1^2 \pmod n$; інакше $x_1 = 1^2 \times a \pmod n$;

якщо $b_{i-1} = 0$, то $x_2 = x_1^2 \pmod n$; інакше $x_2 = x_1^2 \times a \pmod n$;

. . . . . .

якщо $b_0 = 0$, то $x_{i+1} = x_i^2 \pmod n$; інакше $x_{i+1} = x_i^2 \times a \pmod n$;

покласти $a^k \pmod n = x_{i+1}$.

Оскільки $(13)_{10} = (1101)_2$, то при обчисленні остачі від ділення 7^{13} на 10, послідовність операцій є такою:

$$\uparrow\times \qquad \uparrow\times \qquad \uparrow \qquad \uparrow\times$$

Тому алгоритм 2 здійснює такі обчислення:

1. $x_1 = (1^2 \times a) \pmod{n}$;
2. $x_2 = (x_1^2 \times a) \pmod{n}$;
3. $x_3 = x_2^2 \pmod{n}$;
4. $x_4 = (x_3^2 \times a) \pmod{n}$.

Якщо підставити числові значення, то отримаємо

1. $x_1 = 1^2 \times 7 \pmod{10} = 7$;
2. $x_2 = 7^2 \times 7 \pmod{10} = 343 \pmod{10} = 3$;
3. $x_3 = 3^2 \pmod{10} = 9$;
4. $x_4 = 9^2 \times 7 \pmod{10} = 567 \pmod{10} = 7$.

5.1. Бінарне представлення. Оскільки для швидкого обчислення a^k та $a^k \pmod{n}$ необхідним є знаходження двійкового запису числа, ми зупинимось на процедурах переводу чисел з десятичної системи у двійкову.

Розглянемо два найпростіших способа отримання бінарного представлення десяткового числа. Принцип роботи кожного з них розглянемо на прикладі десяткового числа $x = 15$.

5.1.1. Почати обчислення з першої цифри. Позначимо $x_0 = x$. Спочатку знаходимо найбільший степінь m_0 двійки, для якого $2^{m_0} \le x_0$. Зрозуміло, що у нашому прикладі $m_0 = 3$, оскільки $2^3 \le 15 < 2^4$. Тепер повторимо цю ж процедуру, але для числа $x_1 \stackrel{\text{def}}{=} x_0 - 2^{m_0} = 15 - 2^3 = 7$. Отримуємо число $m_1 = 2$, оскільки $2^2 \le 7 < 2^3$. Тепер обчислюємо $x_2 = x_1 - 2^{m_1} = 7 - 2^2 = 3$. Далі діємо за тим же принципом: знаходимо $m_2 = 1$, оскільки $2^1 \le 3 < 2^2$. Після цього обчислюємо $x_3 = x_2 - 2^{m_2} = 2 - 2^1 = 1$ й знаходимо $m_3 = 0$, оскільки $2^0 \le 1 < 2^2$. Нарешті обчислюємо $x_4 \stackrel{\text{def}}{=} x_3 - 2^{m_3} = 0$. У загальному випадку алгоритм закінчує

роботу, коли чергове x стає рівним 0.

Для числа 15 алгоритм зупиняється після обчислення x_4.

Двійкове представлення числа 15 складається з m_0+1 позицій: позиції нумеруються зліва направо, починаючи з 0. В позиціях m_0, m_1, m_2, ... двійкового представлення записуємо одиниці, в інших позиціях — нулі. ㉓

У нашому прикладі необхідні $m_0 + 1 = 4$ позиції для двійкового запису десяткового числа 15, причому в позиціях $m_0 = 3$, $m_1 = 2$, $m_2 = 1$, $m_3 = 0$ необхідно записатти двійкові одиниці. Таким чином, $(15)_{10} = (1111)_2$.

Алгоритм у загальному випадку має такий вигляд.

Алгоритм 3. Двійкове представлення (починаємо ліворуч)

Вхідні дані: натуральне число k;

Вихідні дані: двійкове представлення $k = (b_i \dots b_0)_2$;

знайти m_0: $2^{m_0} \le k < 2^{m_0+1}$ та покласти $x_1 = k - 2^{m_0}$, $i = 1$;

якщо $x_1 = 0$, то виконати процедуру **WriteExpansion**. `STOP`.

якщо ж $x_1 > 0$, то знайти m_1: $2^{m_1} \le x_1 < 2^{m_1+1}$ та

покласти $x_2 = x_1 - 2^{m_1}$, $i = 2$;

якщо $x_2 = 0$, то виконати процедуру **WriteExpansion**. `STOP`.

якщо ж $x_2 > 0$, то знайти m_2: $2^{m_2} \le x_2 < 2^{m_2+1}$ та

покласти $x_3 = x_2 - 2^{m_2}$, $i = 3$;

. . . . . .

Процедура **WriteExpansion**

покласти $b_{m_0} = 1$, $b_{m_1} = 1$, ... , $b_{m_i} = 1$

та $b_j = 0$ для всіх інших $0 \le j \le m_0$.

У представленому алгоритмі переводу числа з десяткової

системи у двійкову для зручності використовується проста процедура **WriteExpansion**, яка за результатами обчислень показників $m_0, m_1, \ldots$ записує двійкове представлення числа k, а саме в позиціях двійкового представлення з номерами $m_0, m_1, \ldots$ вона записує одиниці, а в інших позиціях — нулі. У розглянутому вище прикладі з $k = 15$ ця процедура записала б чотири одиниці й жодного нуля.

Особливістю алгоритму 3, представленого нижче, є необхідність обчислювати степені двійки. Ці обчислення виконуються швидко за рекурсивною формулою $2^k = 2^{k-1} \cdot 2$.

5.1.2. Почати обчислення з останньої цифри. Існує ще один алгоритм переведення чисел з десяткової системи у двійкову. Його особливість у тому, що двійкові цифри обчислюються починаючи з молодших розрядів. Перевага цього алгоритму ㉔ у тому, що він не потребує попереднього обчислення ступенів двійки. Недоліком алгоритму 4 є те, що він використовує операцію ділення на двійку, яка виконується доволі "повільно".

Як і вище, дію цього алгоритму продемонструємо спочатку на прикладі запису числа 15 у двійковій системі.

Оскільки число $x_0 = 15$ є непарним, то $b_0 = 1$ (інакше треба покласти $b_0 = 0$). Нехай $x_1 \stackrel{\text{def}}{=} (x_0 - b_0)/2$, тобто $x_1 = 7$. Число $x_1 = 7$ є непарним, тому покладемо $b_1 = 1$ (якщо x_1 є парним, ми покладемо $b_1 = 0$). Продовжуємо аналогічно: $x_2 \stackrel{\text{def}}{=} (x_1 - b_1)/2 = 3$, $b_2 = 1$, $x_3 \stackrel{\text{def}}{=} (x_2 - b_2)/2 = 1$, $b_3 = 1$, $x_4 \stackrel{\text{def}}{=} (x_3 - b_3)/2 = 0$. Алгоритм закінчується, коли чергове x стає рівним 0. У нашому прикладі алгоритм закінчується обчисленням x_4, тому необхідні 4 позиції для того, щоб записати двійкове представлення числа 15: $(15)_{10} = (b_3 b_2 b_1 b_0)_2 = (1111)_2$.

Алгоритм 4. Двійкове представлення (починаємо праворуч)

Вхідні дані: натуральне число k

Вихідні дані: двійкове представлення $k = (b_0 b_1 \dots b_i)_2$;

позначимо $x_0 = k$;

якщо x_0 є непарним числом, то $b_0 = 1$; інакше $b_0 = 0$;

покладемо $x_1 = \dfrac{x_0 - b_0}{2}$; якщо $x_1 = 0$, то `STOP`.

якщо x_1 є непарним числом, то $b_1 = 1$; інакше $b_1 = 0$;

покладемо $x_2 = \dfrac{x_1 - b_1}{2}$; якщо $x_2 = 0$, то `STOP`.

якщо x_2 є непарним числом, то $b_2 = 1$; інакше $b_2 = 0$;

покладемо $x_3 = \dfrac{x_2 - b_2}{2}$; якщо $x_3 = 0$, то `STOP`.

. . . . . .

6. КОНТРОЛЬНІ ПИТАННЯ

1. Чому $\mathcal{C}_{\mathtt{A}} = \mathcal{P}_{\mathtt{A}}$ для будь-якого експоненціального шифру $E_{k,n}$? (стор. 180).

2. Перевірити конгруенції (2). (стор. 181).

3. Пояснити чому комбінації 2709, 2008, 1307, 606 дають однаковий результат при використанні шифру $E_{k,701}$? (стор. 181).

4. Чому модуль мультиплікативного шифру $E_{k,n}$ повинен перевищувати 3333? (стор. 181).

5. Перевірити обчислення в (3). (стор. 182).

6. Довести формулу (4). (стор. 183).

7. Чому $\left(a^{\phi(n)}\right)^t \cdot a \pmod{n} = a \pmod{n}$? (стор. 185).

8. Чому дорівнює $\phi(p)$? (стор. 185).

9. Чому $(a, p) = p$, якщо $(a, p) \neq 1$? (стор. 185).

10. У якому результаті стверджується, що $k^{-1} \pmod{\phi(n)}$ існує, якщо k та $\phi(n)$ є взаємно простими? (стор. 186).

11. Перевірити, що $7 \pmod{30} = 13$. (стор. 186).
12. Згадайте, чому дорівнює $\phi(pq)$? (стор. 186).
13. Доведіть конгруенцію (11). (стор. 187).
14. Пояснити рівності $a^{kj} = up + a$ та $a^{kj} = vq + a$, які використано у доведенні леми 3. (стор. 187).
15. У доведенні леми 3 стверджується, що $q \mid u$, якщо $up = vq$. Чому це є вірним? (стор. 187).
16. Пояснити правило 2. (стор. 187).
17. Перевірити, чи дійсно ми вже довели лему 4? (стор. 188).
18. Підрахувати $\phi(33)$. (стор. 188).
19. Перевірити рівність $27^{-1} \pmod{20} = 3$. (стор. 188).
20. Чому $7^{-1} \equiv 43 \pmod{60}$ та $11^{-1} \equiv 11 \pmod{60}$? (стор. 188).
21. Чому алгоритм 1 випливає з представлееня (12)? (стор. 189).
22. Чому алгоритм 2 завжди дає $a^k \pmod{n}$? (стор. 191).
23. Пояснити, чому алгоритм 3 є правильним у загальному випадку? (стор. 193).
24. Пояснити, чому алгоритм 4 є правильним у загальному випадку? (стор. 194).

7. З А Д А Ч І

Задача 1. *Знайти два різні натуральні числа* $a < 29$ *та* $b < 29$, *для яких* $a^2 \equiv b^2 \pmod{29}$. *Пояснити, чому не варто використовувати шифр* $E_{2,29}$?

Задача 2. *Перевірити, що* $9^k \equiv 0 \pmod{27}$ *для будь-якого* $k \geq 2$. *Чому мультиплікативний шифр з модулем* $n = 27$ *не варто використовувати*?

Задача 3. *Оскільки* $391 = 17 \times 23$, *то*

$$\phi(391) = \phi(17)\,\phi(23) = 16 \cdot 22 = 352.$$

Пояснити, що означає рівність $\phi(391) = 352$ *з точки зору*

a) *теорії чисел,*
b) *мультплікативних шифрів,*
c) *експоненціальних шифрів.*

Задача 4. *Обчислити*

a) $31^{11} \pmod{59}$;
b) $11^{41} \pmod{521}$;
c) $19^{107} \pmod{1249}$.

Задача 5. *Використовуючи конгруенцію* $29 \equiv -2 \pmod{31}$, *обчислити*

a) $29^2 \pmod{31}$; b) $29^5 \pmod{31}$.

Задача 6. *Скільки операцій множення необхідно зробити, щоб обчислити*

a) a^{47}? b) a^{147}?

Задача 7. *Записати* $(2015)_{10}$ *у двійковій системі числення за допомогою*

a) *алгоритму* 3; b) *алгоритму* 4.

Задача 8. *Записати* $(988)_{10}$ *у двійковій системі числення за допомогою*

a) *алгоритму* 3; b) *алгоритму* 4.

Задача 9. *Записати позиції букв тексту* `КІНО` *у десятковій та двійковій системах числення.*

Задача 10. *Записати позиції букв тексту* `ШИФР` *у десятковій та двійковій системах числення.*

Задача 11. *Використовуючи алгоритм* 2, *зашифрувати текст* `КІНО` *за допомогою експоненціального шифру з параметрами* $k = 2015$ *та* $n = 1000$.

Задача 12. *Використовуючи алгоритм* 2, *зашифрувати текст* `ШИФР` *за допомогою експоненціального шифру з параметрами* $k = 988$ *та* $n = 51$.

Задача 13. *Знайти* j, *при якому* $a^{7j} \equiv a \pmod{34}$.

Задача 14. *Знайти j, при якому $a^{7j} \equiv a \pmod{523}$. Зважте на те, що 523 є простим числом.*

Задача 15. *За допомогою експоненціального шифру $E_{7,34}$ отримано зашифрований текст* ЇАС. *Дешифрувати його (використати обчислення, зроблені у задачі* 13).

Задача 16. *За допомогою експоненціального шифру $E_{7,523}$ отримано зашифрований текст* 131 95 1. *Дешифрувати його (використати обчислення, зроблені у задачі* 14).

Задача 17. *Нехай $p \equiv 2 \pmod 3$, де p — просте число. Показати, що $(3, \phi(p)) = 1$. Це означає, що $k = 3$ можна обрати для експоненціального шифру за модулем p. Показати, що показник степеня для дешифрації такого шифру дорівнює $j = \frac{2p-1}{3}$.*

Задача 18. *Нехай $p \equiv 2 \pmod 3$ та $q \equiv 2 \pmod 3$, де p та q — прості числа. Покладемо $n = pq$. Показати, що $(3, \phi(n)) = 1$. Це означає, що $k = 3$ можна обрати для експоненціального шифру за модулем n. Знайти показник степеня для дешифрації такого шифру.*

Задача 19. *Нехай $n = p_1p_2p_3$, де p_1, p_2, p_3 — три різних простих числа. Нехай k та j є взаємно оберненими за модулем $\phi(n)$. Довести, що $a^{kj} \equiv a \pmod{\phi(n)}$ для всіх цілих a.*

Задача 20. *Використовуючи задачу* 19, *визначити показник j кореня з k за модулем $\phi(n)$, якщо $k = 7$, $n = p_1p_2p_3$, $p_1 = 11$, $p_2 = 13$, $p_3 = 19$.*

Задача 21. *Нехай a та m — натуральні числа, причому $(a, m) = 1$. Довести, що послідовність $r_i = a^i \pmod m$, $i \geq 0$, є періодичною.*

Задача 22. *Згідно до задачі* 21, *послідовність $r_i = a^i \pmod m$, $i \geq 0$, є періодичною, якщо $(a, m) = 1$. Найменший період цієї послідовності назвемо порядком числа a за модулем m і позначатимемо $\mathrm{ord}_m(a)$. Нехай натуральне число u є таким, що $a^u \equiv 1 \pmod m$. Довести, що $\mathrm{ord}_m(a) \mid u$.*

Задача 23. *Позначення* $\mathrm{ord}_m(a)$ *для натуральних чисел* a *та* m *пояснено у задачі* 22. *Довести, що якщо* $(a,m)=1$, *то* $\mathrm{ord}_m(a) \mid \phi(m)$.

Задача 24. *Довести, що якщо* $ab \equiv 1 \pmod{m}$, *то* $\mathrm{ord}_m(a) = \mathrm{ord}_m(b)$.

Задача 25. *Позначимо* $e = \mathrm{ord}_m(a)$. *Нехай* k *— натуральне число. Довести, що*

$$\mathrm{ord}_m(a^k) = \frac{e}{(e,k)}.$$

Задача 26. *Натуральне число* α *називається примітивним коренем для модуля* m, *якщо* $(\alpha,m)=1$ *та* $\mathrm{ord}_m(\alpha) = \phi(m)$. *Перевірити, що*

a) 3 *та* 5 *є примітивними коренями для модуля* 7;
b) 2 *є примітивними коренями для модуля* 9.

Довести, що не існує жодного примітивного кореня для модуля 12.

Задача 27. *Нехай* $\mathrm{ord}_m(a) = e$. *Довести, що* $a^i \equiv a^j \pmod{m}$ *тоді і тільки тоді, коли* $i \equiv j \pmod{e}$.

Задача 28. *Нехай* α *— це примітивний корінь для модуля* m (*ми також кажемо, що* m *має примітивний корінь* α). *Позначимо*

$$r_k = \alpha^k \pmod{m}, \qquad 1 \le k \le \phi(m).$$

Довести, що $r_1, \ldots, r_{\phi(m)}$ *— це перестановка чисел, які не перевищують* m *та є взаємно простими з ним.*

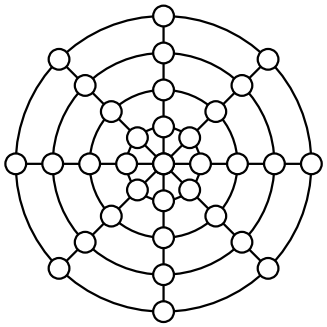
Задача 29. *Довести, що якщо число* m *має примітивний корінь, то воно має* $\phi(\phi(m))$ *примітивних коренів. Зокрема, якщо* m *є простим числом, то воно має* $\phi(m-1)$ *примітивних коренів.*

Задача 30. *Довести, що якщо просте число* $p > 3$ *має примітивний корінь, то воно має парну кількість примітивних коренів.*

Задача 31. *Нехай натуральне число* m *є таким, що* $(a,m)=1$ *та* $\mathrm{ord}_m(a) = m-1$. *Довести, що* m *є простим числом.*

Задача 32. *Довести, що* 2 *не є примітивним коренем для жодного з чисел Ферма* $F_n = 2^{2^n} + 1$, $n \geq 2$.

Задача 33. *На малюнку, наведеному нижче, розташувати числа* $1, 2, \ldots, 33$ *в маленьких колах так, щоб суми чисел на усіх більших колах та на діаметрах були б однаковими.*

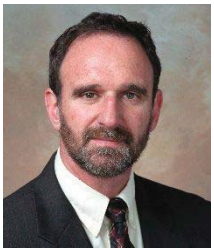


Цю задачу запропонував китайський математик Янг Ху у книзі "Розвиток стародавніх математичних методів для з'ясування дивних властивостей чисел", виданій у 1275 році. Він розглядав задачі про магічні квадрати, а наведений рисунок був однією з ілюстрацій до його відкриттів. Хоча, звичайно, коло зовсім не квадрат, але магія чисел з зазначеними властивостями присутня!

8. БІОГРАФІЇ

Поліґ, *Стефен* (нар. 1953 р.), американський інженер-електрик, працює в Масачусетському технологічному інституті. В середині 70-х років XX сторіччя був аспірантом Мартіна Хеллмана в Стенфордському університеті. Саме тоді він брав участь у розробці експоненціального шифру. Отримані ним формули використовуються також і для обчислення дискретних логарифмів.

В 1978 році разом з М. Хеллманом (див. [Хеллман], стор. 201) отримав патент "*Метод для експоненціального шифрування*".



Хеллман, *Мартін* (нар. 2.10.1945), американський криптограф. Здобув популярність головним чином завдяки розробці першої асиметричної криптосистеми у співавторстві з Уітфілдом Діффі і Ральфом Меркле у 1976 році. Проте його спільна робота з С. Поліґом стосовно експоненціальних шифрів також добре відома спеціалістам. В 1978 році разом з У. Діффі (див. [Діффі], стор. 263) нагороджений премією за найкращу статтю. У тому ж році разом з С. Поліґом (див. [Поліг], стор. 201) отримав патент "*Метод для експоненціального шифрування*". В 2015 році отримав премію Тьюрінга. Останнім часом активно працює над аналізом ризиків ядерної загрози.

Глава 9

КРИПТОАНАЛІЗ ЕКСПОНЕНЦІАЛЬНИХ ШИФРІВ

Дешифрування повідомлення, до якого застосовано експоненціальний шифр, є складною обчислювальною задачею, хоча з точки зору теорії для цього не існує жодних перешкод. Ми розглянемо це питання на прикладах, з яких стане зрозумілим це твердження.

1. Дешифрування у випадку коли степінь та модуль відомі

Розглянемо приклад дешифрування повідомлення, закодованного за допомогою експоненціального шифру з відомими показником та модулем.

Приклад 1. Дешифрувати повідомлення

(1) `4149 3569 4142 2290 1930 4679`

яке було зашифровано за допомогою $E_{k,n}$ шифру з показником $k = 1649$ та модулем $n = 5251$.

Перш за все розкладемо модуль на множники: $5251 = 59 \cdot 89$. Зауважимо, що 59 та 89 є простими числами. Тому з властивості 3 функції Ойлера (див. главу 6) випливає, що $\phi(5251) = 58 \cdot 88 = 5104$.

Згідно до формули (8.6), дешифрування здійснюється наступним чином

$$\mathcal{P}_{\mathtt{X}} \equiv \mathcal{C}_{\mathtt{X}}^{j} \pmod{5251},$$

де j — це показник кореня k-ого степеня за модулем n. Згідно правилу 2, наведеному у главі 8, $j = 1649^{-1} \pmod{5104}$.

Обернене число за модулем знаходимо за допомогою узагальненого алгоритму Евкліда (див. алгоритм 3 у главі 4):

$$5104 = 1649 \cdot 3 + 157,$$
$$1649 = 157 \cdot 10 + 79,$$
$$157 = 79 \cdot 1 + 78,$$
$$78 = 78 \cdot 1 + 0.$$

Тому таблиця (4.11) має вигляд

		1	1	10	3
0	1	1	2	21	65

Утворюємо лінійну комбінацію

$$1649 \cdot 65 - 5104 \cdot 21 = 1,$$

звідки отримуємо $65 = 1649^{-1} \pmod{5104}$.

Тепер для окремих груп повідомлення (1) обчислюємо остачі від ділення степенів на модуль:

$$4149^{65} \pmod{5251} = 322,$$
$$3569^{65} \pmod{5251} = 702,$$
$$4142^{65} \pmod{5251} = 2406,$$
$$2290^{65} \pmod{5251} = 706,$$
$$1930^{65} \pmod{5251} = 1902,$$
$$4679^{65} \pmod{5251} = 2107.$$

Всі обчислені остачі перевищують 33, тому природно зробити припущення, що спочатку текст було розбито на групи і потім шифрувались групи. Оскільки $33^2 < k < 33^3$ ①, то робимо висновок, що групи складались з двох букв. ②

Тепер переводимо розшифрований цифровий формат в групи з двох букв:

0322	0702	2406	0706	1902	2107
ВС	ЕБ	УД	ЕД	ОБ	РЕ

Нарешті нескладно здогадатись, що зашифровано було наступний текст

(2) ВСЕ БУДЕ ДОБРЕ

Зауваження 1. Зверніть увагу, що число 322 відповідає саме групі ВС, а не ЮБ. ③

Приклад 2. На останньому кроці дешифрування у прикладі 1 було розв'язано "шараду" для отримання тексту (2). Якби при групуванні між словами використовувались символи ␣ (які мають код 00), то цей крок був би непотрібний. Не пояснюючи деталей, покажемо процеси шифрування та дешифрування у цьому випадку. Шифрування здійснюється за формулою

$$\mathcal{C}_{\mathtt{XY}} = (\mathcal{P}_{\mathtt{XY}})^{1649} \pmod{5251}.$$

В наступній таблиці наведено результати шифрування.

Процес шифрування

групи	ВС	Е␣	БУ	ДЕ	␣Д	ОБ	РЕ
$\mathcal{P}_{\mathtt{XY}}$	0322	0700	0224	0607	0006	1902	2107
$\mathcal{C}_{\mathtt{XY}}$	4149	1501	3033	3699	1092	1930	4679

Перша та остання групи у новому тексті такі ж, як і у тексті з прикладу 1, тому їхні шифри також однакові.

Як і у прикладі 1, дешифрування повідомлення з пробілами між словами здійснюється за формулою

$$\mathcal{P}_{\mathtt{XY}} = (\mathcal{C}_{\mathtt{XY}})^{65} \pmod{5251}.$$

В наступній таблиці наведено результати дешифрування.

Процес дешифрування

$\mathcal{C}_{\mathtt{XY}}$	4149	1501	3033	3699	1092	1930	4679
$\mathcal{P}_{\mathtt{XY}}$	322	7	224	67	6	192	217
з нулями	0322	0700	0224	0607	0006	1902	2107
групи	ВС	Е␣	БУ	ДЕ	␣Д	ОБ	РЕ

Зверніть увагу на особливість кодування символа ␣ у різних блоках:

$$\mathtt{E␣} \to 0700, \qquad \mathtt{␣Д} \to 0006.$$

Це пояснюється тим, що у першому випадку група Е␣=0700 закінчується символом ␣, а у другому — група ␣Д=0006, з нього починається.

2. Дешифрування у випадку коли показник або модуль невідомі

Дешифрування повідомлення, до якого застосовано експоненціальний шифр з невідомими показником та модулем, майже неможлива без удачі. Розглянемо наступний приклад.

Приклад 3. Дешифрувати повідомлення

```
496 343 0 663 1 94 664 161 664
```

яке було зашифровано за допомогою $E_{k,n}$ шифру.

Аналіз почнемо з аналізу послідовності чисел у шифрованому тексті. Оскільки максимальним числом є `664`, то робимо висновок, що модуль n не є меншим за 665. ④ Числа $665 = 5 \cdot 7 \cdot 19$ та $666 = 2 \cdot 3^2 \cdot 37$ не є простими, а їхній канонічний розклад не має вигляду pq для різних простих чисел p та q. ⑤ Цю властивість має наступне число $667 = 23 \cdot 29$. ⑥ Приймаємо гіпотезу про те, що $n = 667$, хоча не виключено, що ця гіпотеза є помилковою. ⑦

Щоб дешифрувати повідомлення `Аліси`, необхідно перевірити всі степені $k \leq n$, які є взаємно простими з $\phi(n)$ ⑧. Оскільки $\phi(667) = 616$, то таких чисел існує рівно $\phi(616) = \phi\left(2^3 \cdot 7 \cdot 11\right) = 240$. ⑨

Процес дешифрування почнемо з $k = 3$. Знаходимо ⑩

$$3^{-1} \pmod{667} = 411,$$

тому пробне дешифрування здійснюємо за правилом

$$\mathcal{P}_{\mathtt{X}} = (\mathcal{C}_{\mathtt{X}})^{411} \pmod{667}.$$

Результатом дешифрування є ⑪

```
НЕ␣ПАЛИТИ
```

Зауваження 2. Нам пощастило при аналізі шифртексту в прикладі 3, оскільки там зустрілось число 664 й ми зробили

правильне припущення $n = 667$. Крім того, нам не знадобилось перевіряти усі 240 варіантів для показника шифру, оскільки ми вгадали, що $k = 3$. ⑫ Якби припущення $n = 667$ виявилось хибним, то перевірка усіх 240 варіантів для k була б марною, а її результатом стало б те, що всі обчислення необхідно було б повторити, але тепер для $n = 669$. ⑬ Без комп'ютера ці обчислення потребують надто багато часу. Але чи завжди комп'ютер розв'яже задачу?

Приклад 4. Дешифрувати повідомлення

7940 6667 6104 6334 6657 2266 256 6667 1 6460 3662
7815 2147 2401 6334 6667 2266 3757 6657 2266

яке було зашифровано за допомогою $E_{k,n}$ шифру з модулем $n = 8537$.

На перший погляд задача здається простішою, ніж у прикладі 3, оскільки тепер ми знаємо модуль n. Для того, щоб дешифрувати повідомлення, необхідно

(i) знайти всі числа k, взаємно прості з $\phi(n)$;
(ii) для кожного з них визначити j, обернене число за модулем $\phi(n)$;
(iii) для кожного k здійснити пробне $E_{j,n}$ дешифрування.

Перше питання, яке постає при реалізації цієї програми, стосується факторизації числа $n = 8537$. Чи є воно простим? Якщо ні, то які дільники воно має? За допомогою комп'ютера можна встановити, що число $n = 8537$ є простим, тому у найгіршому випадку необхідно перевірити 8536 показників. ⑭

Тепер починаймо перевіряти показники крок за кроком, починаючи з $k = 2$. А чи існує кращий метод? ⑮

Приклад 5. Дешифрувати повідомлення

```
5330549  5278727  9659311  866598  3106889  676181  2027066
```

яке було зашифровано за допомогою $E_{k,n}$ шифру з показником $k = 3$ та модулем $n = 15,002,557$.

Задача є схожею до прикладу 1. Число n має факторизацію $15,002,557 = 2447 \cdot 6131$, ⑯ тому $\phi(n) = 14,993,980$. ⑰ Можна також знайти, що $3^{-1} \pmod{14993980} = 9,995,987$. ⑱ Тепер для дешифрування необхідно для кожного слова в шифрованому повідомленні виконати операцію

$$\mathcal{P}_{\mathtt{X}} = {\mathcal{C}_{\mathtt{X}}}^{9,995,987} \pmod{15,002,557}. \qquad (3)$$ ⑲

Наприклад, для першого слова `5330549` необхідно виконати операцію

$$\mathcal{P}_{\mathtt{X}} = 5,330,549^{9,995,987} \pmod{15,002,557}.$$

Це означає, що число, яке перевищує 5 мільйонів, треба піднести до степеня, який майже дорівнює 10 мільйонам, а потім знайти остачу від ділення на число, яке перевищує 15 мільйонів. Сучасні алгоритми та комп'ютери дозволяють це зробити майже миттєво. Ситуація змінюється докорінно, якщо k є невідомим: цю операцію треба виконати для кожної групи в шифрованому тексті й повторити це для всіх k. Як довго треба чекати результату дешифрування, якщо невідомими є показник k та модуль n?

3. Надійність експоненціальних шифрів

Уявімо, наприклад, що модулем експоненційного шифру $E_{k,n}$ є $n = 944,871,836,856,449,473$. Для дешифрування необхідно обчислити $\phi(944,871,836,856,449,473)$. Як ми знаємо, значення функції Ойлера для аргументу n легко обчислити, якщо знати його канонічне представлення у вигляді добутку простих дільників. ⑳ Ми обмежуємось модулями одного з двох видів: $n = p$ або $n = pq$. Навіть при цьому обмеженні факторизацію

$$944,871,836,856,449,473 = 961,748,941 \times 982,451,653$$

знайти нелегко, оскільки кожен з цих двох простих дільників ㉑ майже дорівнює мільярду. Варто все ж таки відзначити, що знаходження зазначеної факторизації зараз не є проблемою для комп'ютера. З іншого боку, існують настільки великі числа, факторизувати які не під силу навіть найпотужнішим сучасним комп'ютерам, об'єднаним у мережу для здійснення параллельних обчислень.

Приклад 6. Число

310 7418240490 0437213507 5003588856 7930037346 0228427275
4572016194 8823206440 5180815045 5634682967 1723286782
4379162728 3803341547 1073108501 9195485290 0733772482
2783525742 3864540146 9173660247 7652346609

складається з 193 десяткових цифр. Оскільки його двійковий розклад містить 640 двійкових цифр, то воно називається RSA-640 (скорочення RSA стане зрозумілим у главі 10).

8 листопада 2005 року спеціалісти німецького федерального агенства з питань інформаційних технологій змогли

факторизувати RSA-640. Виявилось, що воно розкладається у добуток двох простих (дуже великих) множників

1634733 6458092538 4844313388 3865090859 8417836700 3309231218
1110852389 3331001045 0815121211 8167511579

×

1900871 2816648221 1312685157 3935413975 4718967899 6851549366
6638539088 0271038021 0449895719 1261465571

Факторизація числа RSA-640 відбулася через 2 роки з початку досліджень, причому задача була всісвітньо відомою й багато колективів намагались її розв'язати. Це означає, що задача факторизації числа RSA-640 є дуже складною з точку зору часу комп'ютерних обчислень, які необхідні для її розв'язання.

Для криптології це означає, що до 8 листопада 2005 року будь-яке повідомлення, зашифроване експоненціальним шифром з модулем RSA-640, було неможливо прочитати непосвяченій стороні, навіть якщо їй було відомо, що шифрування здійснювалось саме для модуля RSA-640! ㉒

Такою ж відомою зараз є задача про факторизацію чисел RSA-704, RSA-768, RSA-896, RSA-1024, RSA-1536 та RSA-2048. За факторизацію кожного з них пропонується грошова премія: вона становить $200,000 у випадку RSA-2048.

Зауваження 3. Варто також додати, що після успішної факторизації числа n (після знаходження двох його дільників p та q) задача не закінчується, оскільки необхідно перевірити, що кожен з дільників є простим числом. Для великих чисел і ця задача є складною з точки зору обчислень Більш детально ми розглянемо її у главі 12. Зараз лише зауважимо, що задача перевірки чисел на простоту в

сучасних умовах розв'язується у нетрадиційний спосіб: відповідь на питання про простоту великих чисел отримується лише з певною ймовірністю.

У главі 10 ми розглянемо один з класичних методів факторизації чисел вигляду $n = pq$, який називається алгоритмом Ферма. Метод Ферма є ефективним, якщо дільники числа n є достатньо близькими до $\sqrt{n}$.

3.1. Метод факторизації Крайчика. Узагальнення методу Ферма було знайдено М. Крайчиком у 1926 році. Замість пар (x, y), які мають властивість $x^2 - y^2 = n$ і на якій базується метод Ферма, він запропонував шукати пари, які задовольняють більш загальне співвідношення $x^2 \equiv y^2 \pmod{n}$. В 1981 з'явився алгоритм наступного покоління, який розробив Д. Диксон з використанням ідей Крайчика.

Спочатку ми познайомимось з методом Крайчика на конкретному прикладі, а потім розглянемо загальний випадок.

Приклад 7. Покажемо як факторизувати число $n = 18601$ методом Крайчика. Будемо використовувати поліном другого степеня $Q(x) = x^2 - n$. Покладемо $x_0 = [\sqrt{n}]$ ($x_0 = 136$ у випадку $n = 18601$). ㉓ Позначимо $x_k = x_0 + k$ для $k \geq 1$ й обчислимо числа $Q_k = Q(x_k)$ для перших п'яти k:

k	1	2	3	4	5
x_k	137	138	139	140	141
Q_k	$168 = 2^3 \cdot 3 \cdot 7$	443	$720 = 2^4 \cdot 3^2 \cdot 5$	$999 = 3^3 \cdot 37$	$1280 = 2^8 \cdot 5$

㉔ Зауважимо, що $Q_3 Q_5 = 2^{12} \cdot 3^2 \cdot 5^2 = 960^2$, тобто $Q_3 Q_5$ є повним квадратом. За означенням чисел Q_k цю властивість

можна записати таким чином:

$$(139^2 - n)(141^2 - n) = 960^2, \quad \text{або}$$
$$(139^2 - n)(141^2 - n) \equiv 960^2 \pmod{n}, \quad \text{або}$$
$$139^2 \cdot 141^2 \equiv 960^2 \pmod{n},$$

тобто ми знайшли розв'язок конгруенції $x^2 \equiv y^2 \pmod{n}$ для $y = 960$. ㉕ Цим розв'язком є $x \equiv 139 \cdot 141 \pmod{n}$, тобто $x = 998$. ㉖ Тепер підрахуємо найбільші спільні дільники: ㉗

$$(n, x + y) = (18601, 960 + 998) = 979,$$
$$(n, y - x) = (18601, 998 - 960) = 19.$$

Нескладно перевірити, що $18601 = 979 \cdot 19$.

Зауваження 4. Числа $Q_k = Q(x_k)$ є достатньо малими у порівнянні з n, якщо k є відносно малим. ㉘ Саме ця властивість пояснює наш вибір $x_k = x_0 + k$, хоча в алгоритмі Крайчика можна використати будь-яку іншу послідовність натуральних чисел $\{x_k\}$.

Найбільшим недоліком алгоритму Крайчика є те, що він використовує метод спроб та помилок. Для реалізації на комп'ютері такий метод зазвичай не є ефективним, тому у сучасних комп'ютерних програмах метод Крайчика не є популярним.

У загальному випадку алгоритм Крайчика знаходження дільників натурального числа можна описати наступним чином.

Алгоритм 1. Алгоритм факторизації Крайчика

Вхідні дані: складене натуральне число n;

Вихідні дані: дільники $n_1 \mid n$ та $n_2 \mid n$;

обчислити $x_0 = \lceil \sqrt{n} \rceil$; покласти $m = 1$;

`Вибір нового` m:

збільшити m на одиницю;

для $x_k = x_0 + k$, $k = 1, 2, \ldots, m$, обчислити $Q_k = x_k^2 - n$;

`Вибір підмножини індексів`:

обрати новий набір індексів $i_1, \ldots, i_s \subseteq \{1, \ldots, m\}$;

якщо добуток $Q_{i_1} \ldots Q_{i_s} \stackrel{\text{def}}{=} y^2$ є повним квадратом та

$(x \pm y, n) \neq 1$, де $x \stackrel{\text{def}}{=} x_{i_1} \ldots x_{i_s}$, то

$n_1 \stackrel{\text{def}}{=} (x - y, n)$ та $n_2 \stackrel{\text{def}}{=} (x + y, n)$ є дільниками n; `STOP`.

інакше повернутись до `Вибору підмножини індексів`;

Зауваження: якщо на кроці `Вибір підмножини індексів`

всі підмножини індексів $i_1, \ldots, i_s \subseteq \{1, \ldots, m\}$

вже перевірено, але повний квадрат не знайдено,

то перейти до кроку `Вибір нового` m.

Доведення алгоритму Крайчика. Якщо для певного набору індексів $i_1, \ldots, i_s$ число $Q_{i_1} \ldots Q_{i_s} \stackrel{\text{def}}{=} y^2$ є повним квадратом, то знайдено розв'язок $x = x_{i_1} \ldots x_{i_s}$ конгруенції

$$x^2 \equiv y^2 \pmod{n}, \tag{4}$$

оскільки $(x_{i_1}^2 - n) \ldots (x_{i_s}^2 - n) \equiv y^2 \pmod{n}$ за означенням послідовності $\{Q_i\}$. ㉙ Тому з (4) випливає, що $n \mid (x^2 - y^2)$. Якщо $(n, x \pm y) = 1$, то $n = n_1 n_2$. Інакше знайдеться натуральне число n_3, для якого $n = n_1 n_2 n_3$. ㉚ $\square$

Зауваження 5. Якщо $n = pq$, а p та q є простими числами, то алгоритм Крайчика знаходить саме p та q (в цьому випадку $n_3 = 1$). Якщо в результаті виконання алгоритму Крайчика виявиться, що $n_1 n_2 < n$, тобто $n = n_1 n_2 n_3$ й $n_3 > 1$, то алгоритм можна повторити, щоб знайти факторизацію числа n_3.

4. Односторонні функції

Перевірка правильності факторизації RSA-640 є рутинною задачею. Навіть без комп'ютера це можна зробити методом множення у стовпчик. ㉛ З іншого боку, обернена операція — факторизація числа — є складною.

Означення 1. Функція, значення якої обчислити доволі легко для будь-яких аргументів, називається *односторонньою*, якщо відновити аргументи за значенням функції дуже складно.

Як ми бачили вище, прикладом односторонньої функції є множення двох простих чисел.

4.1. Односторонні функції з секретом. Це такі односторонні функції, які мають додаткову властивість: якщо відома певна додаткова інформація, то обчислення аргументу за значенням функції стає простою задачею.

Однією з таких функцій є

$$f(x) = x^2 \pmod{n}, \quad \text{якщо} \quad n = pq,$$

де p та q є простими числами. Вона називається *функцією Рабіна*. Додатковою інформацією, яка робить обчислення x за значенням $f(x)$ простими, є знання p та q. Справедливим

є також і обернене твердження: задача факторизації числа n стає простою, якщо вміти обчислювати x за $f(x)$.

Іншу односторонню функцію з секретом ми будемо детально розглядати в главі 10.

4.2. Дискретний логарифм. Ще однією односторонньою функцією є *дискретний логарифм* за модулем n та базою a, який позначається $\mathrm{dlog}_{a,n}(h)$ для аргументу h. Дискретний логарифм є розв'язком задачі

$$a^{\mathrm{dlog}_{a,n}(h)} \equiv h \pmod{n}, \qquad h \in \{0,1,2,\ldots,n-1\}. \tag{5}$$

Означення 2. Нехай a та n натуральні числа. Дискретним логарифмом цілого числа $x \in \{0,1,2,\ldots,n-1\}$ за модулем n та базою a називається таке ціле число $\mathrm{dlog}_{a,n}(h) \in \{0,1,2,\ldots,n-1\}$, для якого виконано рівність (5).

Назва пояснюється аналогією зі звичайним логарифмом за базою a, який позначається $\log_a(h)$ і є розв'язком задачі:

$$a^{\log_a(h)} = h, \qquad h > 0.$$

Ми фактично вже зустрічались з дискретними логарифмами, а саме ми назвали число j показником кореня k-ого степеня за модулем n, якщо

$$a^{kj} \equiv a \pmod{n} \quad \text{для всіх} \quad a$$

(див. формулу (8.5)). З використанням позначення для дискретного логарифма, попередню рівність можна записати наступним чином

$$1 + \mathrm{dlog}_{a,n}(1) = k \cdot j \pmod{n}. \tag{6}$$

㉜

Зауваження 6. Дискретний логарифм існує не при всіх комбінаціях a та n. Наприклад, якщо a та n є взаємно простими, то $\mathrm{dlog}_{a,n}(0)$ не існує. ㉝ Більше того, $\mathrm{dlog}_{a,n}(0)$ існує тільки тоді, коли одне з чисел a або n ділиться на інше. ㉞

Приклад 8. Обчислимо дискретний логарифм 6 за основою 31 та з базою 3, тобто обчислимо $\mathrm{dlog}_{3,31}(6)$.

Оскільки $3^0 \not\equiv 6 \pmod{31}$, то $\mathrm{dlog}_{3,31}(6) \neq 0$. ㉟ Аналогічно, $\mathrm{dlog}_{3,31}(6) \neq 1$. Продовжуючи ці обчислення для $x = 2, 3, \ldots$, тільки при $x = 25$ отримаємо $3^x \equiv 6 \pmod{31}$, тобто $\mathrm{dlog}_{3,31}(6) = 25$.

4.3. Захист пароля. Для ідентифікації часто використовують паролі або PIN (Personal Identification Number). Паролі зазвичай передаються хост-комп'ютеру через захищені лінії зв'язку; комп'ютер порівнює пароль з тими, що зберігаються в його списку.

Такі системи ідентифікації мають вразливі сторони, однією з яких є потенційна можливість отримати несанкціонований доступ до списку паролів. Цей недолік можна усунути за допомогою метода з використанням односторонньої функції. Цей метод передбачає, що зберігаються не самі паролі, а лише значення односторонньої функції, аргументами якої є паролі.

Наприклад, якщо паролем є число x, то комп'ютер може зберігати $H(x) = a^x \pmod{n}$, де a та n фіксовані великі числа. Всякий раз, коли ви повідомляєте свій пароль x, обчислюється значення $H(x)$, яке порівнюється з записами у базі даних. Якщо $H(x)$ знайдено у базі даних, ви пройшли етап ідентифікації.

Якщо зловмисник отримує несанкціонований доступ до бази даних, він не може обчислити ваш пароль, оскільки це еквівалентно обчисленню дискретного логарифма, що, як ми знаємо, є складною операцією. Отже, ваш пароль захищений від несанкціонованого доступу до списку паролів.

4.4. Алгоритм Шенкса. Більш ефективним для знаходження дискретного логарифма, ніж простий перебір, є алгоритм Шенкса. Нижче ми наводимо спрощений алгоритм Шенкса, який напевно дає результат, якщо n є простим числом, а a є примітивним коренем за модулем n. Існує модифікація цього алгоритму для загального випадку, але ми її не розглядаємо.

Означення 3. Нехай n є натуральним числом. Натуральне число a називається *примітивним* або *первісним коренем* за модулем n, якщо

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

та

$$a^l \not\equiv 1 \pmod{n} \quad \text{для будь-якого} \quad 1 \le l < \phi(n).$$

Зауважимо, що примітивні корені існують не для всіх n, а тільки для $n = 2, 4, p^\alpha, 2p^\alpha$. Існування примітивного кореня для простих n довів К. Гаусс, але він сам писав, що цим поняттям користувався ще Л. Ойлер. Оскільки n є простим числом в алгоритмі, наведеному нижче, то примітивний корень за модулем n існує.

Через $\lceil x \rceil$ ми позначаємо найменше натуральне число, яке не є меншим за x.

Алгоритм 2. Алгоритм Шенкса

Вхідні дані: цілі числа a, n, h;
Вихідні дані: $\operatorname{dlog}_{a,n}(h)$;
обчислити $m = \lceil \sqrt{n} \rceil$ й $c \equiv a^{-m} \pmod{n}$;
обчислити $a^r \pmod{n}$, $r = 0, 1, \ldots, m-1$;
почати цикл з $q = 0$;
`Спроба знайти дискретний логарифм`:
якщо $hc^q \pmod{n} = a^r \pmod{n}$ для якогось r,
то $\operatorname{dlog}_{a,n}(h) = mq + r$ `STOP`.
Якщо ж $hc^q \pmod{n} \neq a^r \pmod{n}$ для будь-якого r,
то збільшити q на одиницю
та повторити `Спробу знайти дискретний логарифм`.

Доведення алгоритму Шенкса. Позначимо $m = \lceil x \rceil$, $x = \operatorname{dlog}_{a,n}(h)$. Поділимо x на m з остачею: $x = mq + r$ для деяких $q \geq 0$ та $0 \leq r < m$. Тому

$$h \equiv a^x = (a^m)^q \cdot a^r \pmod{n},$$

звідки $h\,(a^{-m})^q \equiv a^r \pmod{n}$. ㊱ Саме ці числа q та r знаходить алгоритм Шенкса, а за ними обчислює $\operatorname{dlog}_{a,n}(h)$. ㊲ □

Приклад 9. Обчислимо $\operatorname{dlog}_{3,31}(6)$ за алгоритмом Шенкса. Перш за все впевнімось, що $a = 3$ є примітивним коренем за модулем $n = 31$. Оскільки $\phi(31) = 30$, то для цього

необхідно здійснити наступні обчислення:

l	1	2	3	4	5	6	7	8	9	10
$3^l \pmod{31}$	3	9	27	19	26	16	17	20	29	25
l	11	12	13	14	15	16	17	18	19	20
$3^l \pmod{31}$	13	8	24	10	30	28	22	4	12	5
l	21	22	23	24	25	26	27	28	29	30
$3^l \pmod{31}$	15	14	11	2	6	18	23	7	21	1

㊳ Оскільки $3^l \equiv 1 \pmod{31}$ в множині $\{1, 2, \ldots, \phi(31)\}$ тільки для $l = 30$, то $a = 3$ дійсно є примітивним коренем за модулем $n = 31$. Тепер $m = \lceil \sqrt{n} \rceil = 6$ й $2 \equiv 3^{-6} \pmod{31}$, оскільки $2 \cdot 3^6 = 1458 = 47 \cdot 31 + 1$. ㊴ Далі обчислюємо $a^r \pmod{n}$, $r = 0, 1, \ldots, m-1$:

(7)

r	0	1	2	3	4	5
$3^r \pmod{31}$	1	3	9	27	19	26

㊵

Нарешті обчислюємо $6 \cdot 2^q \pmod{31}$:

q	0	1	2	3	4
$6 \cdot 2^q \pmod{31}$	6	12	24	17	3

㊶

Для кожного $q \geq 0$ шукаємо число $6 \cdot 2^q \pmod{31}$ в таблиці (7). Тільки для $q = 4$ ми отримали співпадіння числа $6 \cdot 2^q \pmod{31}$ з одним з елементів попередньої таблиці, а саме $6 \cdot 2^4 \pmod{31} = 3^1 \pmod{31}$. Таким чином, $\operatorname{dlog}_{3,31}(6) = mq + r$, тобто $\operatorname{dlog}_{3,31}(6) = 25$. ㊷

5. КОНТРОЛЬНІ ПИТАННЯ

1. Перевірити, що $33^2 < k < 33^3$. (стор. 203).

2. Чому у прикладі 1 зроблено висновок про те, що групи складались з двох букв? (стор. 203).

3. Чому у прикладі 1 згадується саме група ЮБ? (стор. 204).

4. Чому у прикладі 3 ми вважаємо, що $n > 664$? (стор. 205).

5. Розкласти на множники числа 665 та 666. (стор. 205).

6. Перевірити, що $667 = 23 \cdot 29$. (стор. 205).

7. Пояснити чому у прикладі 3 ми вважаємо, що $n = pq$ для деяких простих чисел p та q? (стор. 205).

8. Чому для дешифрування у прикладі 3 необхідно перевірити всі степені $k \leq n$, які є взаємно простими з $\phi(n)$? (стор. 206).

9. Пояснити чому $\phi(616) = 240$? (стор. 206).

10. Для обчислення $3^{-1} \pmod{667} = 411$ використати розширений алгоритм Евкліда. (стор. 206).

11. Зробити необхідні обчислення для дешифрування у прикладі 3. (стор. 206).

12. Чому у зауваженні 2 сказано, що потрібно перевіряти саме 240 варіантів для показника шифру? (стор. 206).

13. Чому у зауваженні 2 сказано, що наступним кандидатом для модуля шифру є саме число 669? (стор. 206).

14. Чому у прикладі 4 сказано, що для експоненціального шифру $E_{k,8537}$ необхідно перевірити саме 8536 показників? (стор. 207).

15. Спробуйте у прикладі 4 застосувати частотний аналіз для дешифрації повідомлення. (стор. 207).

16. Перевірити факторизацію $15,002,557 = 2447 \cdot 6131$. Чи є 2447 та 6131 простими числами? (стор. 208).

17. Чому $\phi(15,002,557) = 14,993,980$? (стор. 208).

18. Довести, що $3^{-1} \pmod{14993980} = 9,995,987$? (стор. 208).

19. Чому операцію (3) треба застосувати у прикладі 5? (стор. 208).

20. Пригадайте як обчислюється значення функції Ойлера, якщо відомим є канонічний розклад у добуток простих дільників аргументу функції? (стор. 208).

21. Чому 961,748,941 та 982,451,653 є простими числами? (стор. 209).

22. Пояснити докладніше, чому у прикладі 6 стверджується, що до 8 листопада 2005 року будь-яке повідомлення, зашифроване експо-

ненціальним шифром з модулем RSA-640, було неможливо прочитати непосвяченій стороні, навіть якщо їй було відомо, що шифрування здійснювалось саме для модуля RSA-640? (стор. 210).

23. Обчислити x_0 у прикладі 7. (стор. 211).

24. Перевірити обчислення та факторизацію чисел Q_k у прикладі 7. (стор. 211).

25. Пояснити конгруенцію $x^2 \equiv y^2 \pmod{n}$, яку використано у прикладі 7. (стор. 212).

26. Розв'язати конгруенцію $x \equiv 139 \cdot 141 \pmod{n}$ у прикладі 7. (стор. 212).

27. Підрахувати найбільші спільні дільники $(n, 998 + 960) = 979$ та $(n, 998 - 960) = 19$ у прикладі 7. (стор. 212).

28. Поясніть, що у зауваженні 4 означає фраза "числа $Q_k = Q(x_k)$ є достатньо малими у порівнянні з n, якщо k є відносно малим"? (стор. 212).

29. Перевірити, що $x = x_{i_1} \ldots x_{i_s}$ дійсно є розв'язком конгруенції (4). (стор. 213).

30. Чому у доведенні алгоритму Крайчика стверджується, що знайдеться натуральне число n_3, для якого $n = n_1 n_2 n_3$, якщо $(n, x+y) \neq 1$ або $(n, x-y) \neq 1$? (стор. 213).

31. Напишіть програму для комп'ютера множення великих чисел та перевірте правильність факторизації числа RSA-640. (стор. 214).

32. Перевірити рівність (6). (стор. 215).

33. Чому $\operatorname{dlog}_{a,n}(0)$ не існує, якщо a та n є взаємно простими? (стор. 215).

34. Довести, що $\operatorname{dlog}_{a,n}(0)$ існує тільки тоді, коли одне з чисел a або n ділиться на інше. (стор. 215).

35. Чому $\operatorname{dlog}_{3,31}(6) \neq 0$? (стор. 216).

36. Чому $h\left(a^{-m}\right)^q \equiv a^r \pmod{n}$ у доведенні алгоритма Шенкса? (стор. 218).

37. Чому алгоритм Шенкса працює коректно у випадку простого n? (стор. 218).

38. Перевірити обчислення $3^l \pmod{31}$ у прикладі 9. (стор. 219).

39. Обчислити $2 \equiv 3^{-6} \pmod{31}$. (стор. 219).

40. Перевірити обчислення $3^r \pmod{31}$ у прикладі 9. (стор. 219).

41. Перевірити обчислення $6 \cdot 2^q \pmod{31}$, $1 \leq l \leq 30$ у прикладі 9. (стор. 219).

42. Перевірити безпосередньо, що $\mathrm{dlog}_{3,31}(6) = 25$. (стор. 219).

6. З А Д А Ч І

Задача 1. *Дешифрувати текст*

27 23 31 8 1 6

зашифрований $E_{3,37}$ *шифром.*

Задача 2. *Дешифрувати текст*

23 7 31 15 10 31 1 23

зашифрований $E_{3,41}$ *шифром.*

Задача 3. *Доведіть, що шифрація та дешифрація згідно* $E_{11,31}$ *шифру здійснюються однаковим алгоритмом.*

Задача 4. *Нехай* $n = pq$, *де* p *та* q *є простими числами. Доведіть, що константу* j *для дешифрації* $E_{k,n}$ *шифру можно визначити за формулою*

$$kj \equiv 1 \pmod{m},$$

де $m = [p-1, q-1]$ *— найменше спільне кратне чисел* $p-1$ *та* $q-1$.

Задача 5. *Повідомлення зашифровано за допомогою експоненціального шифру з модулем* $n = 491$. *Скільки степенів* k *необхідно перевірити для дешифрації повідомлення, якщо використовується метод грубої сили?*

Задача 6. *Скільки чисел* k *можна використовувати для експоненціального шифру* $E_{k,437}$? *Напишіть формулу для кількості можливих чисел* k, *які можна використовувати для експоненціального шифру* $E_{k,n}$.

Задача 7. *Нехай* $n = pq$. *Припустимо, що* $x > \sqrt{n}$ *є таким натуральним числом, що* $y^2 \stackrel{\text{def}}{=} x^2 - n$ *є повним квадратом.*

a) *Доведіть, що* $p = x + y$, $q = x - y$.
b) *Чи варто користуватись експоненціальним шифром* $E_{k,n}$ *з* $n = 97343$?
c) *Яку рекомендацію необхідно надати розробнику експоненціального шифру?*

Задача 8. *При виборі модуля $n = pq$ для експоненціального шифра $E_{k,n}$ необхідно мати на увазі наступну обставину. Якщо $p-1$ та $q-1$ мають великий спільний дільник, то $(p-1, q-1)$ є достатньо малим числом у порівнянні з $\phi(n)$.*

a) *Пояснити, чому в цьому випадку найменше спільне кратне $u \stackrel{\text{def}}{=} [p-1, q-1]$ є малим числом у порівнянні з $\phi(n)$?*
b) *Довести, що для дешифрації можна обрати $j \equiv k \pmod{u}$.*
c) *Пояснити, чому знаходження j методом перебору є відносно простою задачею, якщо $(p-1, q-1)$ є достатньо малим числом у порівнянні з $\phi(n)$?*
d) *Яку рекомендацію необхідно надати розробнику експоненціального шифру?*

Задача 9. *Розглянемо критичний випадок задачі 8, коли $p-1$ ділиться на $q-1$, тобто $(q-1) \mid (p-1)$.*

a) *Довести, що в цьому випадку $j \equiv k^{-1} \pmod{p-1}$.*
b) *Обчислити j, якщо $n = 11041$.*

Задача 10. *Припустимо, що $n \geq 2$, а канонічний розклад $\phi(n)$ містить тільки малі прості числа. Тоді число j можна знайти методом грубої сили.*

a) *Нехай, наприклад, $\phi(n) = 2^{\alpha_2} \cdot 3^{\alpha_3} \cdot 5^{\alpha_5}$. Оцінити зверху кількість спроб для знаходження j методом грубої сили.*
b) *Яку рекомендацію необхідно надати розробнику експоненціального шифру?*

Задача 11. *Якщо обидва числа q та $2q+1$ є простими, то q називається числом Софі Жермейн. Досі невідомо чи є послідовність чисел Софі Жермейн скінченою, але використання таких чисел у криптографії дозволяє уникнути багатьох проблем.*

a) *Показати, що проблеми, згаданої у задачах 9 та 10, можна позбутись, якщо $p = 2q+1$.*
b) *Довести, що 2, 3, 5, 11, 23, 29, 41, 53, 83, 89 є числами Софі Жермейн.*

Задача 12. *Нехай n_1, n_2, n_3 є попарно простими числами, а m є натуральним числом. Позначимо $m_i \equiv m^3 \pmod{n_i}$, $i = 1, 2, 3$.*

a) *Пояснити як китайська теорема про остачі допомагає обчислити $M \equiv m^3 \pmod{n_1 n_2 n_3}$.*
b) *Як дешифрувати повідомлення m, якщо знати M?*
c) *Яку рекомендацію необхідно надати розробнику експоненціального шифру?*

Задача 13. *Припустимо, що один і той же текст надіслано трьом різним особам, які отримали повідомлення m_1, m_2 та m_3. Припустимо, що текст було зашифровано за допомогою експоненціальних шифрів E_{3,n_1}, E_{3,n_2} та E_{3,n_3}.*

a) *Уважно прочитайте умови задачі* 12.
b) *Нехай $n_1 = 517$, $n_2 = 697$, $n_3 = 667$, $m_1 = 131$, $m_2 = 614$, $m_3 = 127$. Відновити повідомлення.*

Задача 14. *Повідомлення m зашифровано експоненціальними шифрами $E_{3,493}$ та $E_{5,493}$. Зашифрованими повідомленнями є* 293 *та* 421 *відповідно. Знайти m.*

Задача 15. *Одне і те ж повідомлення m зашифровано шифрами $E_{k_1,n}$ та $E_{k_2,n}$, причому $(k_1, k_2) = 1$. Тоді повідомлення m можна відновити за зашифрованим текстом $c_1 \equiv m^{k_1} \pmod{n}$ або $c_2 \equiv m^{k_2} \pmod{n}$. Як?*

Задача 16. *Нехай $n = 1591$.* `Аліса` *використовує експоненціальний шифр $E_{k,n}$ з найменшим можливим k. Вона отримала повідомлення $c = 1292$. Як дешифрувати це повідомлення за допомогою китайської теореми про остачі (теорема* 5.5)?

Задача 17. *За допомогою експоненціального шифра $E_{k,n}$ шифрується повідомлення $m \in \{0, 1, \ldots, n-1\}$. Зашифрованим повідомленням є $c \equiv m^k \pmod{n}$. Доведіть, що існує i, для якого*

$$m^{k^i} \equiv m \pmod{n}.$$

Доведіть, що для такого i виконується

$$c^{k^{i-1}} \equiv m \pmod{n}.$$

Чи зменшує така властивість небезпечність експоненціального шифра $E_{k,n}$?

Задача 18. *Припустимо, що* $(p-1) \mid (k-1)$ *та* $(q-1) \mid (k-1)$. *Довести, що*

a) *будь-яке повідомлення* m *шифрується в* m *за допомогою експоненціального шифру* $E_{k,n}$;
b) *пояснити, чому вибір* $k = \phi(n)/2 + 1$ *є особливо поганим для експоненціального шифру, хоча він задовольняє вимогам стосовно величини параметра* k?

Задача 19. *Для кожного експоненціального шифру існують тексти, які не змінюються при шифруванні. Таких текстів є принаймні чотири.*

Нехай m *— це розв'язок системи лінійних конгруенцій*:

$$m \equiv a \pmod{p}, \qquad m \equiv b \pmod{q}, \tag{8}$$

де $a, b \in \{+1, -1\}$.

a) *Чому система* (8) *має розв'язок*?
b) *Пригадати, чому параметр* k *експоненціального шифру* $E_{k,n}$ *є непарним числом*?
c) *Довести, що* $m \equiv m^k \pmod{pq}$, *де* m *— це розв'язок системи* (8).
d) *Знайти чотири тексти, які не змінюються при шифруванні* $E_{7,55}$ *шифром.*

Задача 20. *Нехай* c *— це повідомлення* m, *яке було зашифровано за допомогою* $E_{k,n}$ *шифру. Припустимо, що* r *— це випадкове число. Нарешті, припустимо, що повідомлення* $cr^k \pmod{n}$ *вдається дешифрувати. Як відновити* m?

Задача 21. *За допомогою метода Крайчика факторизувати число* 12499.

Задача 22. *За допомогою метода Крайчика факторизувати число* 20437.

Задача 23. *За допомогою метода Шенкса знайти дискретний логарифм числа* $h = 15$ *за модулем* $p = 29$ *та базою* $a = 2$.

Задача 24. *За допомогою метода Шенкса знайти дискретний логарифм числа* $h = 20$ *за модулем* $p = 47$ *та базою* $a = 5$.

Задача 25. *Дешифрацію повідомлень в рамках мультиплікативних шифрів можна прискорити майже вдвічи, якщо використати китайську теорему про остачі.*

Нехай $n = pq$, *де* p *та* q *є простими числами. Нехай* k — *це показник для шифрації, а* j — *показник для дешифрації у випадку експоненціального шифру* $E_{k,n}$. *Нехай* $c \equiv m^k \pmod{n}$. *Для дешифрації цього повідомлення обчислимо*

$$c_p \equiv c^{j \pmod{p-1}} \pmod{p}, \qquad c_q \equiv c^{j \pmod{q-1}} \pmod{q}.$$

Після цього знаходимо $\lambda \in \{0, 1, \ldots, n-1\}$, *яке задовольняє наступну конгруенцію:*

$$\lambda \equiv c_p \pmod{p}, \qquad \lambda \equiv c_q \pmod{q}.$$

a) *Чому існує розв'язок цієї конгруенції?*
b) *Довести, що* $\lambda = m$. *Як обчислити* λ?
c) *Припустимо, що відомі числа* x *та* y, *для яких* $xp + yq = 1$. *Як у цьому випадку знайти* λ?
d) *Як знайти* x *та* y?

Задача 26. *Повідомлення* m *зашифровано експоненціальним шифром* $E_{3,253}$, *результатом є* $c = 119$.

a) *Факторизувати* n.
b) *Знайти показник дешифрації* j.
c) *Обчислити* m *за допомогою* j.
d) *Обчислити* m *методом, описаним у задачі* 25.

Задача 27. *Ще одним надійним криптометодом є метод Рабіна. Щоб ним користуватись, необхідно обрати такі два великих простих числа* p *та* q, *що* $p \equiv 3 \pmod{4}$, $q \equiv 3 \pmod{4}$. *Тоді повідомлення* m *шифрується за правилом*

$$c \equiv m^2 \pmod{n},$$

де $n = pq$.

Для дешифрації повідомлення обчислюються числа

$$m_p \equiv c^{(p+1)/4} \pmod{p}, \qquad m_q \equiv c^{(q+1)/4} \pmod{q}.$$

Обгрунтування процедури дешифрації основано на китайській теоремі про остачі й нагадує метод, описаний в задачі 25: спочатку знаходимо x *та* y*, для яких* $xp + yq = 1$*; потім обчислюємо*

$$r \equiv (xpm_q + yqm_p) \pmod{n}, \qquad r \equiv (xpm_q - yqm_p) \pmod{n}.$$

Тоді одне з чисел $\pm r$, $\pm s$ *дорівнює* m.

a) *Чому такі прості числа* p *та* q *можна знайти?*
b) *Чому* $\pm m_p$ *є квадратним коренем з* c *за модулем* p*, а* $\pm m_q$ *є квадратним коренем з* c *за модулем* q*?*
c) *Чому розв'язок рівняння* $xp + yq = 1$ *існує? Як його знайти?*
d) *Чому кожне з чотирьох чисел* $\pm r$, $\pm s$ *є квадратним коренем з* c *за модулем* m*?*

Задача 28. *Криптосистема Рабіна (див. задачу* 27*) використовується з* $p = 11$ *та* $q = 23$*, тобто з* $n = 253$*. Повідомлення* m *шифрується в* $c \equiv m^2 \pmod{n}$*, тобто* $c = 170$*. Обчислити* m.

Задача 29. `Аліса` *грає з* `Бобом` *в "очко"* через Інтернет. Для цього вони спільно обрали дуже велике просте число* p *й різні (секретні) показники* k_A *та* k_B*, щоб використовувати приватні експоненціальні шифри* $E_{k_A,p}$ *та* $E_{k_B,p}$*. Крім того, вони узгодили нумерацію карт в колоді.*

Кожен раунд починається з того, що `Аліса` *перетасовує колоду карт (переставляє карти у випадковому порядку) й шифрує їх своїм шифром. Раунд продовжується наступним чином:*

i) `Аліса` *надсилає* `Бобу` *послідовність зашифрованих номерів;*
ii) `Боб` *обирає одне з чисел і повідомляє його* `Алісі`*; вона дешифрує це число і знає свою карту у цьому раунді;*

*Англійською мовою "*blackjack*"

iii) Боб *обирає інше число з послідовності, шифрує його своїм шифром, результат надсилає* Аліcі; *вона застосовує до отриманого числа свою операцію дешифрації і цей результат повертає* Бобу;

iv) Боб *застосовує до отриманого числа свою операцію дешифрації і дізнається, якою є його карта у цьому раунді.*

Дві карти, обрані у цьому раунді, вилучаються з колоди і у наступних не використовуються. Ця процедура повторюється допоки Боб *не зупиняє гру.*

a) *Чи не дізнається* Боб *про карту* Аліси *на кроці* ii)?
b) *Чи не дізнається* Аліса *про карту* Боба *на кроці* iii)?
c) *Чи правильно* Боб *визначає свою карту на кроці* iv)?
d) *Як після гри впевнитись, що гравці не мухлювали?*

Задача 30. Аліса *надіслала* Бобу *повідомлення*:

```
21 27 49 19 45 42 27 49 25 19 29 21 27 7  27
43 25 30 33 20 32 21 45 30 25 14 42 45 19 27
```

зашифроване експоненціальним шифром $E_{7,53}$. Єва *не вміє використати параметри шифру для дешифрації, але їй здається, що повідомлення містить фрагмент* НІКОЛИ НЕ ПОГОДИТЬСЯ.

a) *Як їй впевнитись у своїй гіпотезі?*
b) *Чи зможе вона дешифрувати повідомлення?*

Глава 10

КРИПТОСИСТЕМИ З ВІДКРИТИМ КЛЮЧЕМ

Існують два типи криптографії: та, що дозволяє тобі мати секрети від твоєї молодшої сестри, і та, що дозволяє мати секрети від твого уряду.

Б. Шнайер, криптограф

Слідуючи традиції та загальноприйнятій практиці, надалі сторони, які приймають участь у шифрованому листуванні, називаються `Алісою` та `Бобом`.

Для приватного листування між `Алісою` та `Бобом` вистачає простих шифрів, які ми вивчали у попередніх главах. Для збереження інформації в секреті `Аліса` та `Боб` можуть домовитись про, наприклад, використання експоненціального $E_{k,n}$ шифру з фіксованими параметрами k та n, які є невідомими для інших осіб. Щоб підтримувати секретність, ці значення необхідно змінювати час від часу. Конфеденційність є найменшою в той момент, коли `Аліса` та `Боб` обмінюються цими параметрами.

Уявімо тепер, що `Аліса` має листуватись з багатьма іншими особами (`Алісою` може, наприклад, бути великий банк). В такому випадку цілком слушною стратегією для `Аліси` є надати кожному зі своїх кореспондентів унікальні параметри k та n. Але в цьому випадку їй необхідно мати список цих параметрів, щоб не переплутати їх при листуванні з кореспондентами. Наявність такого списку підвищує ризик втрати конфеденційності, оскільки список можна вкрасти

або прочитати його з комп'ютера, якщо він зберігається у файлі.

Таким чином, найбільш уразливими етапами секретного листування є обмін ключами та збереження ключів у тайні.

1. Головоломки Меркла

Припустимо, що `Аліса` і `Боб` хотіли б приховати від інших зміст свого листування. Щоб запобігти втраті конфеденційності під час обміну ключами, `Боб` надсилає до `Аліси` *велику* кількість головоломок, кожну з яких вона в змозі розв'язати за помірний час. Ці головоломки можуть бути зашифрованими повідомленнями з невідомими ключами. `Аліса` обирає *випадковим* чином одну з них і розв'язує її (методом грубої сили). Тепер `Аліса` та `Боб` можуть спілкуватись, оскільки обидва знають ключ. Жоден зловмисник не може прочитати їхні повідомлення, оскільки не знає яку з головоломок обрала `Аліса`. Щоб отримати код, зловмисник має розв'язати *всі* головоломки, але для цього потрібно набагато більше часу, ніж витратила `Аліса`. Через певний час `Боб` та `Аліса` можуть повторити процедуру вибору ключа й не хвилюватись, що зловмисник має доступ до їхнього листування.

Описаний підхід до вибору ключів запропонував (саме в такій формі) в 1974 році Роберт Меркл; його метод було опубліковано 4 роки потому.

2. Метод В. Діффі та М. Хеллмана

В 1976 році Вітфілд Діффі та Мартін Хеллман опублікували роботу, у якій запропонували революційний спосіб об-

міну ключами по несекретним каналам, який вони назвали *методом відкритих ключів*. Кожен з користувачів криптосистеми, яку описали Діффі та Хеллман, має два ключі: *приватний* та *відкритий*.

Приватний ключ тримається в секреті й ніколи никому не повідомляється. Жодних захисних дій стосовно збереження секретності відкритого ключа не здійснюється; вважається, що він є відомим всім, в тому числі й зловмисникам.

Якщо `Аліса` хоче надіслати `Бобу` повідомлення, вона використовує його відкритий ключ. Для того, щоб прочитати повідомлення, `Боб` використовує свій приватний ключ. Хоча ці ключі й пов'язані один з іншим, не існує можливості дізнатися про приватний ключ за допомогою відкритого. Тому третя сторона не зможе прочитати листи від `Аліси` до `Боба`.

Зауваження 1. Всі шифри, які вивчались у попередніх главах, мали лише один, секретний, ключ, а кожне зашифроване повідомлення можна було розшифрувати з використанням певного параметра, який однозначно обчислювався за допомогою секретного ключа.

Наприклад, число a є ключем для мультиплікативного шифру $M_{a,33}$, яке використовують для шифрування повідомлень за формулою (3.1). Для дешифрування повідомлення (див. формулу (3.7)) необхідно знання оберненого за модулем числа $a^{-1} \pmod{33}$, яке однозначно обчислюється за секретним ключем a.

Зверніть увагу на наступну обставину. Оскільки відкритий ключ у системі Діффі–Хеллмана є загально відомим, будь-хто, не тільки `Аліса`, може надіслати `Бобу` шифроване повідомлення.

Така ж ситуація спостерігається у кожному з парадних багатоповерхівок: будь-хто може залишити листа Бобу, вкинувши лист у його поштову скриньку. З іншого боку, тільки Боб може дістати листа зі скриньки, оскільки тільки Боб має ключ від неї. У даному випадку, ключ від поштової скриньки грає роль приватного ключа в системі Діффі–Хеллмана, а отвір в поштовій скриньки — роль відкритого ключа.

Чи можна аналогічну ситуацію змоделювати в криптографії? Іншими словами, чи можна практично реалізувати ідею Діффі–Хеллмана?

3. Шифр RSA

Після виходу з друку статті Діффі та Хеллмана, їхніми ідеями зацікавились Рональд Рівест та Аді Шамір з Масачусетського технологічного інституту. Обговорюючи ідею Діффі–Хеллмана, вони знайшли спосіб її практичної реалізації. Свої розробки вони показали своєму колезі Леонарду Еделману, який водночас знайшов помилку у їхніх міркуваннях. Наступна спроба Рівеста та Шаміра також мала вади, на які вказав той же Еделман. Ця історія повторювалась 42 рази й лише на 43-ій спробі Еделман визнав, що помилки не існує.

В 1978 році вийшла спільна стаття трьох співавторів, Рівеста, Шаміра та Еделмана з описом методу, який зараз називається *шифром RSA*, що є абревіатурою за першими буквами їхніх прізвищ, написаних англійською мовою. Шифр RSA не тільки став першим прикладом системи з відкритими ключами, але й зберігає популярність донині.

3.1. Що таке шифр RSA. RSA — це експоненціальний шифр з модулем, який дорівнює добутку двох простих

чисел, тобто $n = pq$. Саме такі шифри ми вивчали у главах 8 та 9. З 1978 року числа, які дорівнюють добутку двох простих, називають *RSA числами*.

Є одна принципова властивість RSA шифру, яка вирізняє його серед інших шифрів $E_{k,n}$, а саме:

Правило 1. Властивість RSA шифру

не тільки модуль $n = pq$ шифру RSA має бути дуже великим, але й його прості дільники p та q мають бути дуже великими.

Кожен $E_{k,n}$ є шифром з приватним ключем (k, n): це зовсім просто зрозуміти, якщо n є простим числом або $n = pq$. Дійсно, в цих випадках дешифрування здійснюється за допомогою показника кореня $k^{-1} \pmod{\phi(n)}$ (див. правила 1 та 2 в главі 8).

Оскільки всі параметри експоненціального шифру необхідно тримати у секреті, то виникає цілком слушне питання: чи може в такому разі $E_{k,n}$ бути ще й шифром з відкритим ключем?

Знаходження оберненого числа за модулем є відносно швидкою операцією. У прикладі 9.1 ми показали процес дешифрування для RSA з $k = 1649$ та $n = 5251$. Оскільки n не є надто великим, його факторизація є простою: $5251 = 59 \cdot 89$. Подальші обчислення у прикладі 9.1 також були досить простими.

Схожу задачу ми розв'язували у прикладі 9.5. В цьому випадку $k = 3$, а $n = 15,002,557$. Ми вказали без обчислень, що $15,002,557 = 2447 \cdot 6131$. Перевірка цієї рівності

є простою задачею, ① але як встановити цю факторизацію, якщо її не знати зазделегідь?

В розділі 9.3 ми відзначили, що факторизація великих чисел є складною операцією. Саме ця обставина дозволяє застосовувати RSA у якості шифра з відкритим ключем.

3.2. Відкритий та приватний ключі для RSA. Для дешифрування повідомлення, закодованого за допомогою $E_{k,n}$ шифру, необхідно обчислити обернене за модулем число

$$j = k^{-1} \pmod{\phi(n)}$$

(див. формулу (8.6)).

Для RSA шифру $\phi(n) = (p-1)(q-1)$ ②, тобто знання p та q дає змогу обчислити $\phi(n)$, а потім й обернене число $k^{-1} \pmod{\phi(n)}$. Якщо p та q є дуже великими числами, то знання їхнього добутку pq не дозволяє швидко знайти дільники p та q (згадайте історію про число RSA-640 в прикладі 9.6). Ми повернемося до питання складності факторизації нижче у §3.3.

Термінологія у випадку RSA шифру трохи змінюється: числа k та j у випадку шифру RSA називають *відкритою експонентою* та *приватною експонентою* (або *відкритим ключем* та *приватним ключем*). Як зрозуміло з назв, k є відомим числом, а j — секретним. Тим не менше, для їхнього добутку справджується ключова властивість

$$a^{kj} \equiv a \pmod{n} \qquad \text{для всіх } a. \qquad (1)$$

③

Немає жодної потреби вимагати, щоб k було дуже великим числом, ④ тому часто обирають $k = 3$ (це полегшує шифрування повідомлень).

Правило 2. Відкритий та приватний ключі для RSA

Таким чином, відкритим ключем RSA шифру є пара чисел k та n, а приватним — число j. Можна також вважати, що приватним шифром є пара чисел p та q, причому $n = pq$. ⑤

Наскільки складно знайти дільники числа? Якщо, наприклад, дільники числа n приблизно однакові, а для їх пошуку використовується метод послідовного перебору, то для знаходження найменшого з дільників знадобиться час, пропорційний $\sqrt{n}$. Якщо n має величину порядку 10^{400} (в сучасній криптографії використовуються ще більші числа), то $\sqrt{n}$ має порядок 10^{200}. Навіть якщо припустити, що суперкомп'ютер за одну секунду перевіряє 100 мільярдів потенційних дільників (насправді, можливості сучасних комп'ютерів набагато скромніші), то для розв'язання задачі факторизації числа n йому знадобиться приблизно 10^{189} секунд або більше, ніж 10^{180} років.

3.3. Надійність RSA. З попереднього обговорення випливає, що для безпеки RSA-криптосистеми важливо правильно вибрати прості числа p і q. Якщо вони малі, то система легко зламується методом простого перебору. Проте бездумно обирати великі p і q також не варто: навіть якщо p і q величезні, але різниця $|p-q|$ мала, їхній добуток $n = pq$ досить легко розкладається на множники (див. задачу 12).

Поняття складності операції можна інтуїтивно зрозуміти на такому прикладі. Припустимо, що однієї секунди вистачить, що прочитати вголос всі цифри від 0 до 9. Оскільки чисел від 0 до 99 в 10 разів більше, то необхідно 10 секунд,

щоб їх прочитати вголос. У загальному випадку, додавання однієї додаткової цифри до десяткового представлення числа збільщує час читання в 10 разів.

Подивіться на наступну таблицю, з якої стає зрозумілим як швидко зростає час, необхідний для здійснення операції читання вголос при додаванні додаткової цифри:

додаткові цифри	час (у секундах)	час в інших одиницях
1	10	
2	100	≈ 1.5 хвил.
3	$1,000$	15 хвил.
4	$10,000$	2.5 год.
5	$100,000$	1 день
6	$1,000,000$	10 днів
7	$10,000,000$	100 днів
8	$100,000,000$	≈ 3 роки
9	$1,000,000,000$	30 років
10	$10,000,000,000$	300 років

Таким чином, додавши лише 10 додаткових цифр, ми кардинально змінили необхідний час для виконання операції від 1 секунди до 300 років!

3.4. Початок історії RSA. Робота Рівеста, Шаміра, Еделмана з'явилась у 1978 році, але увага до шифру RSA виникла роком раніше. В 1977 році популяризатор науки Мартін Гарднер у своїй постійній рубриці "*Математичні ігри*" (тоді вважалось, що це ігри!) у журналі *Scientific American* опублікував загадкове і надто велике навіть для математиків число

$$\begin{aligned}\text{RSA-129} = {} & 1143816257\ 5788886766\ 9235779976\ 1466120102\ 1829672124 \\ & 2362562561\ 8429357069\ 3524573389\ 7830597123\ 5639587050 \\ & 5898907514\ 7599290026\ 879543541\end{aligned}$$

та зашифрований за його допомогою текст

9686	9613	7546	2206
1477	1409	2225	4355
8829	0575	9991	1245
7431	9874	6951	2093
0816	2982	2514	5708
3569	3147	6622	8839
8962	8013	3919	9055
1829	9451	5781	5154

за дешифрування якого пропонувалась премія в \$100.

Гарднеру цю головоломку запропонували автори шифру RSA. Рон Рівест, один з авторів RSA, оцінив час, потрібний для дешифрування: він вважав, що дешифрування стане можливою не раніше, ніж через $40 \cdot 10^{15}$ років. Зауважте, що 10^9 — це мільярд, а 10^{15} — в мільйон разів більше число, ніж мільярд! Це означало, що фактично він не сподівався на те, що число RSA-129 взагалі можна факторизувати.

Головоломку було дешифровано через 17 років, коли група з 600 ентузіастів та їхні 1600 комп'ютерів змогли факторизувати RSA-129 за 8 місяців неперервної роботи. Це стало можливим завдяки новому потужному методу *квадратичного решета*, розробленому Карлом Померанцем в 1981 році. Координація обчислень здійснювалась через Інтернет. Факторизацію RSA-129 було опубліковано в 1994 році

$$\begin{aligned}\text{RSA-129} = {} & 3490529510\ 8476509491\ 4784961990\ 3898133417\ 7646384933 \\ & 8784399082\ 0577 \\ & \times 3276913299\ 3266709549\ 9619881908\ 3446141317\ 76429679 \\ & 929425397\ 98288533.\end{aligned}$$

разом з дешифрованою фразою

```
The magic words are squeamish ossifrage
```

яка не мала особливого смислу: Рівест пояснював, що слова, які формують фразу, було обрано випадковим чином.

Отримані за розв'язанні цієї задачі 100 доларів США були пожертвувані Фонду вільного програмного забезпечення (Free Software Foundation) — некомерційній організації, заснованій Р. Сталлменом у жовтні 1985 року для підтримки руху вільного програмного забезпечення і, особливо, проекту GNU.

3.5. Припущення щодо RSA. Віра в метод RSA базується на трьох припущеннях.

Правило 3. Три припущення щодо RSA

1. Найшвидшим способом дешифрування повідомлення є використання приватного ключа.
2. Найшвидшим способом знаходження приватного ключа є обчислення $k^{-1} \pmod{\phi(n)}$.
3. Найшвидшим способом обчислення функції Ойлера $\phi(n)$ є факторизація числа n.

Найменш обгрунтованим здається перше припущення. Існує принаймні два аргументи на користь його доцільності. Перше полягає у тому, що метод грубої сили базується на послідовному переборі всіх чисел i з метою досягти врешті решт значення $k^{-1} \pmod{\phi(n)}$. Для кожного чергового числа i необхідно здійснити спробу дешифрування повідомлення m, тобто обчислити $x \equiv y^i \pmod{n}$, де y — це шифр повідомлення m, тобто $y \equiv m^k \pmod{n}$. Якщо спроба виявиться безуспішною, то перейти до наступного i. Цей спосіб потребує не менше обчислень, ніж факторизація

числа n.

Другий аргумент на користь першого припущення, полягає у тому, що якщо оригінальний текст написано іншою мовою, то простий перебір може так і не дати потрібного результату, оскільки результатом дешифрування при кожному i буде незнайомий текст.

3.6. Інший спосіб запису RSA. При використанні методу RSA `Аліса` спочатку виконує алгоритм 1.

Алгоритм 1. RSA: вибір параметрів

1. Обрати два великих простих числа $p \neq q$.
2. Обчислити $n = pq$ та $\phi(n) = (p-1)(q-1)$.
3. Обрати $1 < k < \phi(n)$ так, щоб $(k, \phi(n)) = 1$.
4. Знайти j, для якого $kj \equiv 1 \pmod{\phi(n)}$.
5. Опублікувати n та k.

Знаючи відкритий ключ (k, n), `Боб` шифрує своє повідомлення згідно алгоритму 2.

Алгоритм 2. RSA: шифрування

Вхідні дані: Відкритий ключ (k, n) та повідомлення $m < \min\{p, q\}$;
Вихідні дані: зашифроване повідомлення $y \equiv m^k \pmod{n}$.

`Аліса` дешифрує повідомлення `Боба` згідно алгоритму 3.

Алгоритм 3. RSA: дешифрування

Вхідні дані: Відкритий ключ (k, n), приватна експонента j та зашифроване повідомлення y;
Вихідні дані: справжнє повідомлення $m \equiv y^j \pmod{n}$.

Зауваження 2. Бачимо, що алгоритм RSA дозволяє шифрувати тексти, числовий еквівалент яких не перевищує найменше з p та q, тобто $\min\{p, q\}$. Це означає, що оригінальний текст попередньо необхідно розбити на групи, числовий еквівалент кожної з яких не перевищує $\min\{p, q\} - 1$.

4. Доведення алгоритму RSA

Нагадаємо, що $m < \min\{p, q\}$. Нехай $y = m^k \pmod{n}$. Ми знайдемо $y^j \pmod{n}$. За означенням $y = sn + m^k$ для деякого цілого числа s. Тому

$$\begin{aligned} y^j \pmod{n} &= \left(m^k + sn\right)^j \pmod{n} = m^{kj} \pmod{n} \\ &= m^{t(p-1)(q-1)+1} \pmod{n} \end{aligned}$$

для деякого невід'ємного цілого числа t. Остання рівність справджується в силу $kj \equiv 1 \pmod{\phi(n)}$. Таким чином

$$y^j \pmod{n} = m \cdot m^{t(p-1)(q-1)} \pmod{n}. \tag{2}$$

Оскільки $m < p$, то m не ділиться на p. Тому й $m^{t(q-1)}$ не ділиться на p, тобто p та $m^{t(q-1)}$ є взаємно простими. Тепер з малої теореми Ферма (теорема 6.3) випливає

$$\left(m^{t(q-1)}\right)^{p-1} \equiv 1 \pmod{p}$$

й тому

$$m \equiv m \cdot m^{t(p-1)(q-1)} \pmod{p}.$$

Аналогічно доводимо, що

$$\left(m^{t(p-1)}\right)^{q-1} \equiv 1 \pmod{q},$$

оскільки $m^{t(p-1)}$ не ділиться на q, звідки

$$m \cdot m^{t(p-1)(q-1)} \equiv m \pmod{q}.$$

За лемою 8.4,

$$m \cdot m^{t(p-1)(q-1)} \equiv m \pmod{pq}. \tag{3}$$

Згадавши, що $n = pq$, з (2) та (3) отримуємо

$$y^j \equiv m \pmod{n}.$$

□

Приклад 1. Розглянемо просту (та нереалістичну) RSA систему шифрування. `Аліса` згідно до алгоритму 1 обирає два простих числа $p = 3$, $q = 5$ й обчислює $n = 15$, $\phi(n) = 8$. Далі вона обирає $k = 3$ й знаходить j, для якого $kj \equiv 1 \pmod{\phi(n)}$, тобто $j = 3$. Нарешті `Аліса` публікує k та n.

`Боб` згідно алгоритму 2 шифрує дуже коротке повідомлення "`Б`", тобто $m = \mathcal{P}_{\texttt{Б}} = 2$:

$$y \equiv m^k \pmod{n} \equiv 2^3 \pmod{15} = 8.$$

Отримавши повідомлення `Аліса` дешифрує його за допомогою алгоритму 3:

$$x \equiv y^j \pmod{n} \equiv 8^3 \pmod{15} = 512 \pmod{15} = 2.$$

Таким чином, `Аліса` отримала повідомлення "`Б`".

5. Атаки на RSA

Атаками на криптографічні шифри називають методи дешифрування, які не базуються на знанні секретних ключей.

При використанні методу RSA необхідно враховувати багато додаткових рекомендацій, які ускладнюють дешифрування повідомлень третіми особами. Наприклад, якщо `Аліса` часто вживає у тексті слово "`Я`", то це підказує третій особі шлях до атаки на такий текст. Цього недоліку можна позбутися, якщо до кожного слова у повідомленні додавати випадковий символ: це приховає слово "`Я`", а для `Боба` не створить значних незручностей.

5.1. Факторизація n якщо відоме $\phi(n)$. Секретність листування за допомогою методу RSA основана на складності факторизації модуля $n = pq$. Таким чином, дільники p та q необхідно тримати у секреті, щоб запобігти вдалій атаці на криптосистему. Але, щоб дешифрувати повідомлення, третій стороні необхідно набагато менше інформації, ніж знання дільників. Наприклад p та q визначити нескладно, якщо відомим є значення $\phi(n)$. Дійсно,

$$\phi(n) = (p-1)(q-1) = pq - (p+q) + 1, \qquad \text{звідки}$$

$$p + q = n - \phi(n) + 1. \tag{4}$$

Оскільки $n = pq$, то у цьому випадку відомими є коефіцієнти поліному другого степеня

$$f(x) = x^2 - (p+q)x + pq$$

і тому його корені знайти нескладно. Зауважимо, що його коренями є числа p та q, оскільки $f(x) = (x-p)(x-q)$.

5.2. Факторизація n, якщо $|p-q|$ є малим. Оберемо p дуже великим простим числом, а q — наступним простим числом. Здається, що криптосистема RSA на базі модуля $n = pq$ є надійною, оскільки n є великим. Проте, якщо $|p-q|$ є невеликим числом, то існує простий алгоритм факторизації n, який носить ім'я Ферма.

Алгоритм 4. Алгоритм Ферма

Вхідні дані: непарне число n;

Вихідні дані: цілі числа x та y, для яких $n = (x-y)(x+y)$, або інформація, що n просте.

`Крок 1.` Покладемо $x = [\sqrt{n}]$;
якщо $x^2 = n$, то $y = 0$; `STOP.`
якщо ж $x^2 \neq n$, то збільшити x на одиницю;

`Крок 2.` якщо $x = (n+1)/2$, то n є простим; `STOP.`
якщо ж $x < (n+1)/2$, то обчислити $y = \sqrt{x^2 - n}$;

`Крок 3.` якщо y ціле, то $n = (x-y)(x+y)$; `STOP.`
якщо ж y неціле, то збільшити x на одиницю;
перейти до `Кроку 2`;

В задачі 12 читачу пропонується довести, що алгоритм 4 є правильним, тобто він завжди знаходить факторизацію числа n. Час роботи цього алгоритму є незнчним, якщо $|p-q|$ є малим числом.

Тому при практичному використанні методу RSA необхідно дотримуватись вимоги, щоб $|p-q|$ було достатньо великим числом. Більш складний метод Крайчика для факторизації натуральних чисел розглянуто в §3.1, глава 9.

Приклад 2. Для факторизації числа $n = 17947$ методом Ферма спочатку обчислюємо $x = [\sqrt{n}] = 133$. Оскільки $x^2 \neq n$, збільшуємо x на одиницю й обчислюємо $y = \sqrt{x^2 - n} = \sqrt{134^2 - n} = \sqrt{17956 - 17947} = 3$. Оскільки y є цілим числом, то $n = (x - y)(x + y) = 131 \times 137$.

6. Задача про рюкзак в криптографії

Наступна комбінаторна *задача про рюкзак* має застосування у криптографії. Нехай об'єм рюкзака дорівнює V. Чи можна його щільно запакувати деякими предметами, які мають об'єми $a_1, \ldots, a_n$? Іншими словами, чи має задача

$$V = a_1x_1 + a_2x_2 + \cdots + a_na_n \tag{5}$$

розв'язок $x_1, \ldots, x_n$, де $x_i = 0$ або $x_i = 1$ для кожного $i = 1, 2, \ldots, n$? В залежності від V та $a_1, \ldots, a_n$ задача про рюкзак може не мати розв'язків або мати декілька розв'язків.

Вважається, що задача про рюкзак є "складною" з точки зору необхідної кількості обчислень, навіть якщо для її розв'язання використовуються комп'ютери.

6.1. Задача про рюкзак для суперзростаючих послідовностей. Існує простий алгоритм знаходження розв'язку задачі про рюкзак (5), якщо послідовність $a_1, \ldots, a_n$ є *суперзростаючою*, тобто такою, що

$$a_i > a_1 + \cdots + a_{i-1} \quad \text{для} \quad 2 < i \leq n.$$

Припустимо, що V дійсно дорівнює сумі деяких чисел a_i, індекси яких утворюють певну підмножину в $\{1, 2, \ldots, n\}$, тобто $V \leq a_1 + \cdots + a_n$.

Для пошуку розв'язку задачі (5), застосуємо такі міркування. Якщо $V \geq a_n$, то обов'язково $x_n = 1$, оскільки $a_1 + \cdots + a_{n-1} < a_n \leq V$, тобто в цьому випадку не існує розв'язку з $x_n = 0$. Якщо ж $V < a_n$, то обов'язково $x_n = 0$. ⑥ Визначивши таким чином коефіцієнт x_n, зводимо початкову задачу до іншої задачі про рюкзак

$$V - a_n x_n = a_1 x_1 + a_2 x_2 + \cdots + a_{n-1} x_{n-1}.$$

До цієї задачі застосовуємо аналогічні міркування й через кілька кроків визначимо усі $x_n, x_{n-1}, \ldots, x_1$. Не завжди знайдена послідовність $x_n, x_{n-1}, \ldots, x_1$ є розв'язком задачі (5), але в цьому випадку розв'язків немає взагалі.

Приклад 3. Нехай $n = 3$ та $a_1 = 1$, $a_2 = 2$, $a_3 = 5$. Ця послідовність є суперзростаючою. Нижче наведено всі випадки та розв'язання для $V \leq 1 + 2 + 5$:

V	$a_1x_1 + a_2x_2 + a_3x_3$	(x_1, x_2, x_3)
1	$1 + 0 + 0$	$(1, 0, 0)$
2	$0 + 2 + 0$	$(0, 1, 0)$
3	$1 + 2 + 0$	$(1, 1, 0)$
4		немає розв'язку
5	$0 + 0 + 5$	$(0, 0, 1)$
6	$1 + 0 + 5$	$(1, 0, 1)$
7	$0 + 2 + 5$	$(0, 1, 1)$
8	$1 + 2 + 5$	$(1, 1, 1)$

Повчальним є випадок $V = 4$. Покажемо до чого приводить процедура описана вище: оскільки $V < a_3$, то $x_3 = 0$; оскільки $V - a_3x_3 \geq a_2$, то $x_2 = 1$; оскільки $V - a_3x_3 - a_2x_2 \geq a_1$, то $x_1 = 1$ і на цьому процедура завершується. Оскільки $V \neq a_1x_1 + a_2x_2 + a_3x_3$ для знайдених x_1, x_2, x_3, то задача розв'язків не має взагалі.

6.2. Криптосистема, основана на задачі про рюкзак. В 1978 році Р. Меркл та М. Хеллман запропонували наступну криптографічну систему, основану на задачі про рюкзак. Щоб описати ідею Меркля–Хеллмана, наведемо двійковий код букв українського алфавіту.

Таблиця 1. Двійковий код букв українського алфавіту

А	1	000001	І	12	001100	Т	23	010111
Б	2	000010	Ї	13	001101	У	24	011000
В	3	000011	Й	14	001110	Ф	25	011001
Г	4	000100	К	15	001111	Х	26	011010
Ґ	5	000101	Л	16	010000	Ц	27	011011
Д	6	000110	М	17	010001	Ч	28	011100
Е	7	000111	Н	18	010010	Ш	29	011101
Є	8	001000	О	19	010011	Щ	30	011110
Ж	9	001001	П	20	010100	Ь	31	011111
З	10	001010	Р	21	010101	Ю	32	100000
И	11	001011	С	22	010110	Я	33	100001

`Аліса` запроваджує свою систему шифрування, обираючи спочатку деяку суперзростаючу послідовність $a_1, a_2, \ldots, a_n$, модуль $m > 2a_n$ та множник a, $0 < a < m$, для якого $(a, m) = 1$. При такому виборі параметрів a та m рівняння $ax \equiv 1 \pmod{m}$ має єдиний розв'язок (теорема 5.1). Позначимо його через c. Спочатку `Аліса` обчислює

$$b_i \equiv aa_i \pmod{m}, \qquad 1 \le i \le n.$$

Зрозуміло, що $0 < b_i < m$, $1 \le i \le m$. Послідовність

$b_1, \ldots, b_n$, отримана після перетворення чисел $a_1, \ldots, a_n$, як правило, не є суперзростаючою.

Послідовність $a_1, \ldots, a_n$ та числа a та m є приватним ключем Аліси, тоді як послідовність $b_1, \ldots, b_n$ є її відкритим ключем. Кожен, хто бажає надіслати повідомлення Алісі, використовує $b_1, \ldots, b_n$ у якості ключа для шифрування.

Якщо Боб бажає надіслати повідомлення Алісі, то першою його дією є переведення позицій букв у двійкове представлення, використовуючи таблицю 1.

Отриману послідовність Боб розбиває на блоки по n бінарних цифр. Останній блок при необхідності доповнюється одиницями. Тепер кожен блок $x_1, \ldots, x_n$ шифрується за допомогою відкритого ключа Аліси $b_1, \ldots, b_n$:

$$S = b_1x_1 + b_2x_2 + \cdots + b_nx_n.$$

Саме S є шифром блока $x_1, \ldots, x_n$, а послідовність чисел S, які відповідають різним блокам, є шифром повідомлення.

Зрозуміло, що дешифрування блока є рівносильною розв'язанню задачі про рюкзак для послідовності $b_1, \ldots, b_n$, яка не є суперзростаючою. На перший погляд, Аліса змушена розв'язувати саме цю складну задачу, не маючи переваги перед іншими, хоча саме вона започаткувала цю систему. Насправді ж Аліса має перевагу перед іншими, оскільки володіє приватною послідовністю $a_1, \ldots, a_n$. Нехай $c = a^{-1} \pmod m$. Аліса обчислює

$$\begin{aligned} S' &\equiv cS \pmod m \equiv cb_1x_1 + cb_2x_2 + \cdots + cb_nx_n \pmod m \\ &\equiv caa_1x_1 + caa_2x_2 + \cdots + caa_nx_n \pmod m. \end{aligned}$$

Оскільки $ca \equiv 1 \pmod m$, то

$$S' \equiv a_1x_1 + a_2x_2 + \cdots + a_nx_n \pmod m.$$

Тепер знайти $x_1, \ldots, x_n$ нескладно, оскільки послідовність $a_1, \ldots, a_n$ є суперзростаючою (див. §6.1).

7. Метод Ель-Гамаля

У 1985 році Тахер Ель-Гамаль запропонував метод шифрування, оснований на одному з варіантів *задачі про дискретні логарифми.* Ця задача полягає у знаходженні показника $0 < x < \phi(n)$, для якого $r^x \equiv y \pmod{n}$ для заданих r, y та n. ⑦ Показник x називається *дискретним логарифмом* числа y для основи r по модулю n (див. §4.2, глава 9). Щоб зрозуміти ідею Ель-Гамаля, пригадаємо кілька властивостей *примітивного кореня* (див. також означення 9.3).

7.1. Примітивний корінь числа. Число a називається *примітивним коренем* (див. означення 9.3) для $n > 1$, якщо

(i) $(a, n) = 1$;
(ii) $a^k \not\equiv 1 \pmod{n}$ для будь-якого $0 < k < \phi(n)$.

Зауважимо, що $a^{\phi(n)} \equiv 1 \pmod{n}$ за теоремою Ойлера (теорема 6.2).

Приклад 4. Щоб довести, що 3 є примітивним коренем для 7, зауважимо, що $\phi(7) = 6$ та

k	1	2	3	4	5	6
3^k	3	9	27	81	243	729
$3^k \pmod 7$	3	2	6	4	5	1

Можна довести, що примітивний корінь існує для будь-якого простого числа. ⑧ Примітивні корені існують також і для деяких непростих чисел, хоча і не для всіх. Існування примітивного кореня для натурального числа є скоріше

виключенням. Наприклад, число mn не має примітивного кореня, якщо $m > 2$, $n > 2$ та $(m, n) = 1$. ⑨ Більше того, тільки числа 2, 4, p^k та $2p^k$ мають примітивні корені, де p — просте число, а k — натуральне. ⑩

Нижче наведено таблицю примітивних коренів χ_p для перших простих чисел p:

Таблиця 2
Примітивні корені χ_p для перших простих чисел p

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71
χ_p	1	2	2	3	2	2	3	2	5	2	3	2	6	3	5	2	2	2	2	7

В наведеній таблиці можна побачити багато парадоксальних рис примітивних коренів. Наприклад, з таблиці 2 видно, що $\chi_p \le 7$ для $p \le 71$. Насправді ця властивість зберігається для всіх $p \le 181$. Подальші обчислення для перших сотень простих чисел p не показують зростання послідовності χ_p, хоча й можна довести, що

$$\limsup_{p\to\infty} \chi_p = \infty. \qquad (6)$$ ⑪

Таблиця 2 свідчить також про те, що $\chi_p = 2$ для більше, ніж половини $p \le 71$. Обчислення для більших p тільки підтверджують цю властивість, хоча математики не в змозі довести, що існує нескінченна кількість простих чисел p, для яких $\chi_p = 2$.

При вивченні криптографічних систем корисним є наступне твердження про примітивні корені.

Теорема 1. *Нехай a — це примітивний корінь для натурального числа $n > 1$. Тоді*

а) $a^k \not\equiv 0 \pmod{n}$ *для будь-якого* $k \in \mathbf{N}$;

b) $a^{k_1} \not\equiv a^{k_2} \pmod{n}$ *для будь-яких різних натуральних чисел* k_1 *та* k_2, $0 < k_1 < k_2 \leq \phi(n)$;

c) $a^u \equiv a^v \pmod{n}$ *тоді і тільки тоді, коли*

$$u \equiv v \pmod{\phi(n)}.$$

Доведення. Якщо припустити, що $a^k \equiv 0 \pmod{n}$ для деякого $k \in \mathbf{N}$, то обов'язково $(a, n) > 1$. ⑫ Тому конгруенція $a^m \equiv 1 \pmod{n}$ неможлива для жодного $m \in \mathbf{N}$, тобто a не є примітивним коренем для n. ⑬ Отримане протиріччя доводить твердження a).

Тепер припустимо, що $a^{k_1} \equiv a^{k_2} \pmod{n}$ для деяких $0 < k_1 < k_2 \leq \phi(n)$. Тоді $a^{k_2} - a^{k_1} = a^{k_1}\left(a^{k_2-k_1} - 1\right)$ ділиться на n. Перший множник a^{k_1} не ділиться на n згідно з твердженням a). Тому $a^{k_2-k_1} \equiv 1 \pmod{n}$, причому $0 < k_2 - k_1 < \phi(n)$. Це протирічить тому, що a є примітивним коренем для n, і доводить твердження b).

Для доведення твердження c) нехай $u = \lambda_1\phi(n) + \mu_1$ для деякого $\lambda_1 \in \mathbf{N}$ та $0 \leq \mu_1 < \phi(n)$, а також $v = \lambda_2\phi(n) + \mu_2$ для деякого $\lambda_2 \in \mathbf{N}$ та $0 \leq \mu_2 < \phi(n)$. Якщо $\mu_1 = \mu_2$, тобто $u \equiv v \pmod{\phi(n)}$, то $a^u \equiv a^v \pmod{n}$, оскільки

$$(7) \qquad a^u = \left(a^{\phi(n)}\right)^{\lambda_1} \cdot a^{\mu_1}, \qquad a^v = \left(a^{\phi(n)}\right)^{\lambda_2} \cdot a^{\mu_2}. \qquad ⑭$$

З іншого боку, якщо $a^u \equiv a^v \pmod{n}$ для деяких натуральних чисел u та v, то з (7) випливає, що $\mu_1 = \mu_2$ на підставі твердження b). ⑮ Тому $u \equiv v \pmod{\phi(n)}$ і твердження c) доведено. □

7.2. Криптосистема Ель-Гамаля. Між системами RSA та Ель-Гамаля є багато спільного. Як і RSA, криптосистема Ель-Гамаля використовує приватні та відкриті ключі: вони необхідні для кожного користувача цієї системи. Як і в RSA, кожен користувач шифрує свої повідомлення за допомогою відкритих ключів, а дешифрує за допомогою приватних ключів.

Як і в RSA, дешифрування є надто складною обчислювальною задачею для сторони, яка не володіє приватними ключами. З іншого боку, сторона, яка знає приватний ключ, дешифрує повідомлення за лічені секунди з використанням комп'ютерів. Нарешті, користувачі обох систем не обмінюються приватними ключами, що повністю виключає можливість перехоплення ключів під час передачі.

7.2.1. Як працює криптосистема Ель-Гамаля. Припустимо, що `Аліса` вирішила розробити свою систему Ель-Гамаля для секретного листування з друзями. Щоб заснувати свою криптосистему, `Аліса` спочатку обирає параметри (p, r, a), як описано у наступному алгоритмі.

Алгоритм 5. Метод Ель-Гамаля: вибір параметрів

1. Обрати просте число p.
2. Обчислити примітивний корінь r для p.
3. Випадковим чином вибрати k, $2 \leq k \leq p-2$.
4. Обчислити $a \equiv r^k \pmod{p}$.

Зауважимо, що задачу обчислення примітивного кореня необхідно розв'язувати лише один раз у момент, коли обираються параметри криптосистеми. Крім цього, у більшості випадків $r = \chi_p$ є доволі малим числом. Серед перших

19,863 простих чисел (останнім серед них є 223,051) нерівність $\chi_p < 6$ виконується для 80% простих чисел p; рівність $\chi_p = 2$ має місце для 7429 простих чисел, що становить 37%, а $\chi_p = 3$ спостерігається для 4515 простих чисел або 23%.

Відкритим ключем `Аліси` є трійка (p, r, a). Число k є її приватним ключем.

`Боб` переводить своє повідомлення у цифровий формат й використовує відкритий ключ `Аліси`, щоб надіслати їй повідомлення, використовуючи наступний алгоритм. Алгоритм розділяє повідомлення на блоки й шифрує їх окремо. Шифром кожного блоку є пара натуральних чисел. При шифруванні використовується додатковий параметр j, який ускладнює можливі атаки на шифр.

Алгоритм 6. Метод Ель-Гамаля: шифрування

Вхідні дані: Відкритий ключ `Аліси` (p, r, a);
повідомлення M у цифровому форматі.

Вихідні дані: Зашифроване повідомлення.

Кроки алгоритму.

1. Розбити послідовність десяткових цифр M на блоки $B < p$.
2. Випадковим чином обрати натуральне число j, $2 \le j \le p-2$.
3. Для кожного блоку B обчислити $C_1 \equiv r^j \pmod{p}$ та
$$C_2 \equiv Ba^j \pmod{p}.$$
4. Шифром повідомлення є послідовність пар (C_1, C_2).

Зауважимо, що число j може змінюватись з кожним наступним блоком. Це надасть ще більшої стійкості методу шифрування Ель-Гамаля. Відмітимо, що `Аліса` не знає яке

число j обрав Боб для кожного блоку. Виявляється, що це їй не потрібно.

Позначимо чере m кількість пар (C_1, C_2), отриманих при шифруванні за допомогою алгоритму 6.

Алгоритм 7. Метод Ель-Гамаля: дешифрування

Вхідні дані: Відкритий ключ (p, r, a) та приватний ключ k; зашифроване повідомлення $(C_{1,i}, C_{2,i})$, $1 \le i \le m$.

Вихідні дані: Дешифроване повідомлення.

1. Для кожної пари (C_1, C_2) обчислити $T \equiv C_2 C_1^{p-k-1} \pmod{p}$.
2. Дешифрованим повідомленням є послідовність чисел T_i.

Отримавши повідомлення від Боба, яке складається з m пар $(C_{1,i}, C_{2,i})$, $1 \le i \le m$, Аліса використовує свій приватний ключ k й дешифрує кожний блок за допомогою алгоритму 7.

Щоб впевнитись, що Аліса правильно дешифрує повідомлення Боба, зауважимо, що $a \equiv r^k \pmod{p}$ й тому для кожного фрагменту (C_1, C_2) зашифрованого тексту

$$\begin{aligned} T &\equiv C_2 C_1^{p-k-1} \pmod{p} \equiv (Ba^j) \cdot (r^j)^{p-k-1} \pmod{p} \\ &\equiv B(r^k)^j \cdot r^{j(p-1)-jk} \pmod{p} \\ &\equiv B(r^{p-1})^j \pmod{p} \equiv B \pmod{p}. \end{aligned}$$

Остання конгруенція є справедливою на підставі малої теореми Ферма (теорема 6.3). ⑯

Приклад 5. Припустимо, що відкритим ключем Аліси є трійка $(p, r, a) = (43, 3, 22)$, а приватним — число $k =$

15. Згідно до алгоритму 5 вибору параметрів шифру Ель-Гамаля, маємо $a \equiv r^k \pmod{p}$, тобто $22 \equiv 3^{15} \pmod{43}$. ⑰

Припустимо далі, що Боб хоче надіслати повідомлення "НОВИЙ". Перш за все він переводить його у цифровий формат: НОВИЙ=1819031114. Наступним кроком Боб розбиває повідомлення на блоки з двох символів:

НОВИЙ=18 19 03 11 14.

Тепер він обирає $j = 23$. Для спрощення ми вважаємо, що це число є однаковим для всіх блоків. Згідно алгоритму 6 Боб обчислює

$$C_1 \equiv r^j \pmod{p} = 3^{23} \pmod{43} = 34,$$
$$a^j \pmod{p} = 22^{23} \pmod{43} = 32.$$

Після цього він знаходить $Ba^j \pmod{p}$ для кожного двосимвольного блоку B. Наприклад, для першого блоку його обчислення є такими

$$C_2 = 18 \cdot 32 \equiv 17 \pmod{43}.$$

Таким чином, шифром першого блоку є пара $(34, 17)$. Для інших блоків обчислення цілком аналогічні.

Отримавши повідомлення від Боба, Аліса дешифрує його, виконуючи дії алгоритму 7:

$$C_1^{p-k-1} \pmod{p} = 34^{43-15-1} \pmod{43} = 34^{27} \pmod{43}$$
$$= 39. \quad ⑱$$

Подальші обчислення для відтворення першого символу є такими:

$$T = C_2 C_1^{p-k-1} \pmod{p} = 17 \cdot 39 \pmod{43}$$
$$= 663 \pmod{43} = 18. \qquad ⑲$$

`Аліса` правильно дешифрувала перший символ повідомлення `Боба`. Всі інші символи відтворюються аналогічно.

Зауваження 3. Криптосистеми Ель-Гамаля працюють повільніше у порівнянні з RSA. Тому їх використовують лише у так званих *гібридних системах* для шифрування ключів RSA, які є набагато меншими у порівнянні з самим повідомленням. Тому час шифрування ключів не грає вирішальнох ролі.

8. КОНТРОЛЬНІ ПИТАННЯ

1. Перевірте, що $15,002,557 = 2447 \cdot 6131$. (стор. 233).

2. Пригадайте, чому $\phi(n) = (p-1)(q-1)$ у випадку $n = pq$? (стор. 234).

3. Пригадайте, чому властивість (1) є вірною? (стор. 234).

4. Пояснити, чому не обов'язково вимагати, щоб в методі RSA k було дуже великим числом? (стор. 234).

5. Чи дійсно знання j є еквівалентним до знання (p, q) в методі RSA? (стор. 234).

6. Чому $x_n = 0$, якщо $V < a_n$ в задачі про рюкзак? (стор. 244).

7. Навіщо використовується обмеження $0 < x < \phi(n)$ у задачі про дискретний алгоритм? (стор. 248).

8. Спробуйте довести, що примітивний корінь існує для будь-якого простого числа. (стор. 248).

9. Спробуйте довести, що число mn не має примітивного кореня, якщо $m > 2$, $n > 2$ та $(m, n) = 1$. (стор. 248).

10. Спробуйте довести, що тільки числа 2, 4, p^k та $2p^k$ мають примітивні корені, де p — просте число, а k — натуральне. (стор. 248).

11. Спробуйте довести властивість (6) (стор. 249).
12. Пояснити, чому $(a,n) > 1$, якщо $a^k \equiv 0 \pmod{n}$ для деякого $k \in \mathbf{N}$? (стор. 250).
13. Пояснити, чому число a не може бути примітивним коренем для n, якщо $a^k \equiv 0 \pmod{n}$? (стор. 250).
14. Чому из $u \equiv v \pmod{\phi(n)}$ випливає, що $a^u \equiv a^v \pmod{n}$, де a — це примітивний корінь для n? (стор. 250).
15. Чому з рівності (7) та конгруенції $a^u \equiv a^v \pmod{n}$ випливає, що $u \equiv v \pmod{\phi(n)}$? (стор. 250).
16. Перевірити застосування малої теореми Ферма у поясненні алгоритму 7. (стор. 253).
17. Перевірити, що $22 \equiv 3^{15} \pmod{43}$. (стор. 253).
18. Впевнитись, що $34^{27} \pmod{43} = 39$. (стор. 254).
19. Впевнитись, що $17 \cdot 39 \pmod{43} = 18$. (стор. 254).

9. З А Д А Ч І

Задача 1. *Використовуючи відкритий ключ* $(n,k) = (2773, 21)$ *криптосистеми RSA зашифрувати повідомлення*

М О В Ч А Н Н Я Ц Е З О Л О Т О

Задача 2. *Використовуючи відкритий ключ* $(n,k) = (2773, 21)$ *криптосистеми RSA дешифрувати повідомлення*

2454 2500 2278 1008 2278 1600 588
2454 588 2055 588 764 2055 2278

Задача 3. *Нехай* $n = pq$, *де* p *та* q — *прості числа*, $p > q$. *Виразити* p *та* q *через* n *та* $\phi(n)$.

Задача 4. *Відомо, що в криптосистемі RSA* $n = pq = 274279$ *та* $\phi(n) = 272376$. *Знайти* p *та* q.

Задача 5. *Припустимо, що відкритим ключем криптосистеми RSA є* $n = 3233$, $k = 37$. *Обчислити приватний ключ.*

Задача 6. *За допомогою RSA алгоритму з відкритим ключем* $(n, k) = (1643, 223)$ *отримано шифроване повідомлення*

1171 79 812 1188 1502 1171 79 812 1 586

Дешифрувати це повідомлення.

Задача 7. *Припустимо, що криптоаналітик аналізує повідомлення* M*, яке було зашифровано за допомогою методу RSA. Виявилось, що* M *не є взаємно простим з* $n = pq$*, де* p *та* q *є простими числами. Показати, що в цьому випадку факторизація* n *є простою задачею.*

Задача 8. *Припустимо, що* Боб *обрав* n*,* $n = pq$*, для своєї RSA криптосистеми, де* p *та* q *два великих простих числа, та два показника* k_1 *та* k_2*. Сподіваючись краще захистити своє листування, він просить* Алісу *шифрувати повідомлення, які вона йому надсилає, спочатку RSA шифром з ключем* (n, k_1)*, а потім ще раз з ключем* (n, k_2)*. Чи додає такий спосіб шифрування більшої безпеки у листуванні між* Алісою *та* Бобом*?*

Задача 9. *Припустимо, що у своїх RSA криптосистемах* Аліса *та* Боб *використовують спільний модуль* n*, але різні показники* k_1 *та* k_2*. Припустимо, що* Аліса *надсилає* Бобу *повідомлення* M*, зашифроване його відкритим ключем* (n, k_2)*, а* Боб *надсилає* Алісі *те ж саме повідомлення* M*, але зашифроване відкритим ключем* Аліси (n, k_1)*. Покажіть, что в цьому випадку відновлення* M *є доволі простою задачею.*

Задача 10. *Припустимо, що система RSA використовується для шифрації повідомлень* M_1 *та* M_2*, а також їхнього добутку* $M = M_1 M_2$*. Показати, що шифр для* M *дорівнює добутку шифрів для* M_1 *та* M_2 *за модулем* n*.*

Задача 11. *Нехай* $n = 1,342,127$*. Позначимо через* x *найменше з цілих чисел, для яких* $x^2 - n \geq 0$*. Оскільки* $x = 1159$*, то* $\sqrt{x^2 - n}$ *не є цілим, тому збільшимо* x *на одиницю й продовжимо цей процес доти, поки число* $\sqrt{x^2 - n}$ *не стане цілим або не досягнемо межі* $x = (n + 1)/2$*. Обчислення наведено у наступній таблиці*:

x	1159	1160	1161	1162	1163	1164
$\sqrt{x^2 - n}$	33, 97	58, 93	76, 11	90, 09	102, 18	113

Зрозуміло, що $1,342,127 = (1164+113)(1164-113)$.

a) *Перевірити всі наведені обчислення.*
b) *Здійснити аналогічну процедуру для* $n = 5609$ *та* $n = 5751$.

Задача 12. *Довести, що алгоритм 4 є правильним, тобто*

a) *якщо* n *є складеним, то існує таке натуральне число* x, $\sqrt{n} \le x < (n+1)/2$, *для якого* $\sqrt{x^2-n}$ *є натуральним числом*;
b) *якщо* n *є простим, то* $\sqrt{x^2-n}$ *не є натуральним числом для будь-якого* $x < (n+1)/2$.

Задача 13. *Зазначимо, що у загальному випадку кожне натуральне число* n *можна представити у вигляді* $n = ab$ *для* $1 < a < b < n$ *кількома різними способами. Яке ж з таких представлень знаходить алгоритм* 4?

Задача 14. *Довести, що алгоритм 4 ніколи не закінчиться, якщо* $n = 2k$ *для непарного числа* k.

Задача 15. *Розглянемо такий цифровий алфавіт на базі латинського:*

A=00	K=10	U=20	1=30	
B=01	L=11	V=21	2=31	
C=02	M=12	W=22	3=32	
D=03	N=13	X=23	4=33	
E=04	O=14	Y=24	5=34	
F=05	P=15	Z=25	6=35	
G=06	Q=16	,=26	7=36	
H=07	R=17	.=27	8=37	
I=08	S=18	?=28	9=38	
J=09	T=19	0=29	!=39	$\sqcup$ = 99

a) *Записати фразу* `NO WAY` *у цьому цифровому алфавіті.*
b) *Оберемо* $k = 47$, $p = 29$, $q = 53$. *Чи можна користуватись таким шифром* $\mathrm{RSA}_{k,n}$?

c) *Позначимо цифровий запис фрази з a) через M. Десяткові цифри в M об'єднаємо у групи по три. Зашифрувати кожну з груп за допомогою шифра* $\mathrm{RSA}_{k,n}$, *де числа k, p та q визначені в b).*

d) *Визначити експоненту j для дешифрації шифру* $\mathrm{RSA}_{47,29\cdot53}$. *Дешифрувати повідомлення, яке отримано в c). Перевести його у звичайний формат.*

Задача 16. *Довести, що задача про рюкзак*

a) $22 = 3x_1 + 7x_2 + 9x_3 + 11x_4 + 20x_5$ *не має розв'язків*;
b) $27 = 3x_1 + 7x_2 + 9x_3 + 11x_4 + 20x_5$ *має декілька розв'язків.*

Задача 17. *Нехай $a_i = 2^i$ для всіх $0 \le i \le n$, а $V < 2^{n+1}$. Довести, що задача про рюкзак має єдиний розв'язок.*

Задача 18. *Знайти розв'язок наступної задачі про рюкзак*

$$28 = 3x_1 + 5x_2 + 11x_3 + 20x_4 + 41x_5.$$

Задача 19. *Впевнитись, що алгоритм у* §6.1 *дійсно знаходить розв'язок початкової задачі, причому цей розв'язок є єдиним.*

Задача 20. *Перевірити, що послідовності $a_1, \ldots, a_n$ в задачах* 17 *та* 18 *є суперзростаючими.*

Задача 21. a) *Використовуючи суперзростаючу послідовність $a_1 = 1$, $a_2 = 2$, $a_3 = 4$, модуль $m = 9$ та множник $a = 4$, обчислити послідовність b_1, b_2, b_3.*

b) *Перевести в бінарну систему повідомлення* ПРИВІТ.
c) *Зашифрувати повідомлення* ПРИВІТ, *використовуючи криптосистему, основану на задачі про рюкзак та відкритий ключ b_1, b_2, b_3, обчислений у* a).
d) *Перевірити алгоритм дешифрації на результаті, отриманому в c).*

Задача 22. Аліса *створює свою криптосистему, обираючи суперзростаючу послідовність* $a_1 = 3$, $a_2 = 5$, $a_3 = 11$, $a_4 = 20$, $a_5 = 41$, *а також модуль* $m = 85$ *та множник* $a = 44$.

a) *Обчислити відкритий ключ* b_1, b_2, b_3, b_4, b_5 *криптосистеми* Аліси.

b) *Знайти* c, *для якого* $44c \equiv 1 \pmod{85}$.

Боб *хоче передати* Алісі *повідомлення* ДОПОМОЖИ.

c) *Використовуючи цифровий алфавіт*

А 000000	**Б** 000001	**В** 000010	**Г** 000011	**Ґ** 000100
Д 000101	**Е** 000110	**Є** 000111	**Ж** 001000	**З** 001001
И 001010	**І** 001011	**Ї** 001100	**Й** 001101	**К** 001110
Л 001111	**М** 010000	**Н** 010001	**О** 010010	**П** 010011
Р 010100	**С** 010101	**Т** 010110	**У** 010111	**Ф** 011000
Х 011001	**Ц** 011010	**Ч** 011011	**Ш** 011100	**Щ** 011101
Ь 011110	**Ю** 011111	**Я** 100000		

перевести це повідомлення у бінарний формат.

d) *Зашифрувати повідомлення* Боба *за допомогою відкритого ключа.*

Щоб дешифрувати повідомлення Боба, Аліса *спочатку обчислює код повідомлення* Боба *для її суперзростаючої послідовності, а потім розв'язує задачу про рюкзак для кожного блока.*

e) *Зашифрувати повідомлення* Боба *для приватного ключа* Аліси.

f) *Дешифрувати повідомлення* Боба.

Задача 23. *Знайти всі розв'язки задачі про рюкзак*

$$21 = 2x_1 + 3x_2 + 5x_3 + 7x_4 + 9x_5 + 11x_6.$$

Задача 24. *Які з послідовностей, наведених нижче, є суперзростаючими*:

a) 3, 13, 20, 37, 81.

b) 5, 13, 25, 42, 90.

c) 7, 27, 47, 97, 197, 397.

Задача 25. *Знайти єдиний розв'язок кожної з наступних задач про рюкзак з суперзростаючою послідовністю*:

a) $118 = 4x_1 + 5x_2 + 10x_3 + 20x_4 + 41x_5 + 99x_6$.
b) $51 = 3x_1 + 5x_2 + 9x_3 + 18x_4 + 37x_5$.
c) $54 = x_1 + 2x_2 + 5x_3 + 9x_4 + 18x_5 + 40x_6$.

Задача 26. *Нехай послідовність додатних цілих чисел* $a_1, a_2, \ldots, a_n$ *має властивість* $a_{i+1} > 2a_i$ *для всіх* $i = 1, 2, \ldots, n-1$. *Довести, що ця послідовність є суперзростаючою.*

Задача 27. *Відкритим ключем рюкзачної криптосистеми є* 49, 32, 30, 43. *Якщо приватний модуль дорівнює* $m = 50$, *а множник —* $a = 33$, *то якою є приватна суперзростаюча послідовність*?

Задача 28. *Приватним ключем рюкзачної криптосистеми* `Аліси` *є суперзростаюча послідовність* 2, 3, 7, 13, 27, *модуль* $m = 60$ *та множник* $a = 11$. *Знайти відкритий ключ цієї криптосистеми.*

Задача 29. `Аліса` *використовує у своїй рюкзачній криптосистемі відкритий ключ* $\{b_1, b_2, b_3, b_4, b_5\} = \{5, 15, 25, 55, 29\}$, *модуль* $m = 73$ *та множник* $a = 5$. *Зашифрувати повідомлення* `УРА` *в рюкзачній криптосистемі* `Аліси`.

Задача 30. `Аліса` *використовує у своїй рюкзачній криптосистемі суперзростаючу послідовність* 1, 3, 5, 11, 35, *модуль* $m = 73$ *та множник* $a = 5$. `Боб` *надіслав* `Алісі` *повідомлення*

`44 84 55 104`.

Що написав `Боб`?

Задача 31. *Закінчити обчислення для інших блоків у прикладі 5.*

Задача 32. *Криптосистема Ель-Гамаля має приватний ключ* $k = 30$ *та відкритий ключ* $(p, r, a) = (71, 7, 32)$. *Дешифрувати повідомлення*

(49,24) (49,62) (49,46) (49,32) (49,51) (49,2)
(49,49) (49,62) (49,30) (49,40) (49,5) (49,67).

Задача 33. *Криптосистема Ель-Гамаля має приватний ключ* $k = 17$ *та відкритий ключ* $(p, r, a) = (37, 2, 18)$. `Боб` *надсилає повідомлення* "`ЧАС ЦЕ ГРОШІ`", *використовуючи в циклі* $j = 13$, $j = 15$ *та* $j = 11$.

a) *Яким є зашифроване повідомлення* `Боба`?

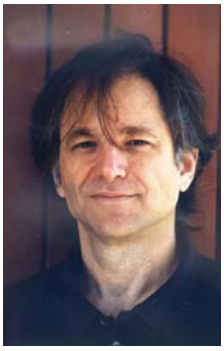
b) *Як* `Аліса` *відтворює це повідомлення*?

10. БІОГРАФІЇ

Діффі, *Еітфілд* (нар. 5.06.1944), американський криптограф, один з найвідоміших спеціалістів, що заслужив світову популярність за концепцію криптографії з відкритим ключем. Його інтерес до криптографії з'явився у віці 10 років, коли батько (професор, викладав іспанську історію та культуру) приніс додому книги з криптографії. У 1965 році Діффі отримав ступінь бакалавра в Массачусетському технологічному інституті. В 1974 році Діффі познайомився з Мартіном Хеллманом, професором факультету електротехніки Стенфордського університету (див. [Хеллман], стор. 201). У спільній роботі, яку було опубліковано в 1976 році, вони розглянули революційно новий метод, якій пізніше стали називати системою обміну ключами Діффі–Хеллмана.

В Стенфордському університеті
М. Хеллман (у центрі) та В. Діффі (праворуч)

Діффі вважається одним з перших *шіфропанків* — людей, які вважають що приватна інформація є недоторканною і повинна бути захищена за допомогою криптографії. Він є затятим противником спроб уряду обмежити використання криптографії в персональних цілях і багато разів виступав у сенаті США, захищаючи свою позицію.



Еделман, *Леонард* (нар. 31.12.1945), американський учений-теоретик у галузі комп'ютерних наук. Він відомий як співавтор системи шифрування RSA і принципів ДНК-обчислень. Отримав ступінь бакалавра з математики у 1968 році в університеті Берклі. Леонард Еделман, разом з Рональдом Рівестом (див. [Рівест], стор. 266) та Аді Шаміром (див. [Шамір], стор. 268), отримав премію Тьюринга 2002 року (яку часто називають Нобелівською премією у галузі комп'ютерних наук) за внесок у винахід криптосистеми RSA.

Л. Еделман відомий своїм терміном *комп'ютерний вірус*. Він вважає, що комп'ютерні віруси відкривають багато можливостей в технологіях майбутнього і що користь, отримана від них, потенційно може переважити негативні сторони їх використання.

В останні роки він розробляє застосування ДНК у якості обчислювальної системи.

> *Найголовніше в ДНК-обчисленнях є те, що вони показують, що молекули ДНК можуть зробити таке, що зазвичай вважається можливим лише для комп'ютерів. Це означає, що комп'ютерна наука і біологія тісно пов'язані. Кожну живу істоту можна розглядати, як обчислювальну систему, і інколи живі істоти можна зрозуміти краще, якщо дивитись на них їх, як на комп'ютери.*
>
> Л. Еделман

В результаті робіт Еделмана у галузі молекулярної біології було створено математичну модель імунної недостатності, викликаної вірусом СНІД. Це дало розуміння того, як вірус працює, а також відкрило різні напрями досліджень для пошуку шляхів лікування. Л. Еделман та Д. Вофсі описали результати перевірки однієї з гіпотез про розвиток синдрому набутого імунного дефіциту.

Проте Л. Еделман найбільше пишається своєю роботою (спільною з К. Померанцем (див. [Померанц], стор. 266) та Р. Румлі) про новий метод перевірки чисел на простоту (опубліковано в 1983 році). Цей

метод дозволяє перевірити простоту числа n за час $O\left((\ln n)^{c \ln\ln\ln n}\right)$, c — деяка універсальна константа.

Ель-Гамаль, *Тахер* (нар. 18.08.1955), єгипетський криптограф, створив численні технології та стандарти для безпечного використання даних та цифрових підписів. Він є автором криптосистеми, основаній на задачі про дискретний логарифм. Його система цифрового підпису використана при розробці широко відомого алгоритму DSA (*Digital Signature Algorithm*), який пізніше став стандартом DSS (*Digital Signature Standard*) в США. Ель-Гамаль не зміг запатентувати свій алгоритм, оскільки був іноземним випускником Стенфордського університету. Згідно закону він повинен був залишатися студентом до моменту видачі патенту. Ель-Гамаль вирішив опублікувати свої дослідження, які стали надбанням громадськості. Завдяки такому кроку його ім'я стало відомим в усьому світі.

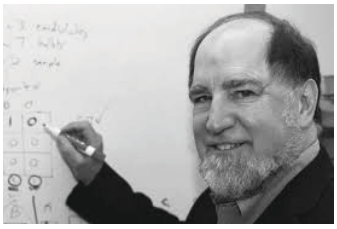
Він приймав участь у розробці платіжного протоколу SET для кредитних карток, а також ряду платіжних систем для Інтернету. Його називають "батьком SSL" — протоколу безпечного з'єднання в Інтернеті. Керівником його магістерської дисертації в Стенфордському університеті був М. Хеллман (див. [Хеллман], стор. 201).

Меркл, *Ральф* (нар. 2.02.1952), американський криптограф, відомий своїми роботами у галузі криптографічних систем з відкритими ключами (протокол Діффі–Хеллмана–Меркла) і хешування (так звана структура Меркла–Дамгарда). В 1974 році отримав в університеті Берклі ступінь бакалавра у галузі інформатики. Починаючи з 1975 року, Меркл цікавився методами захисту ліній передачі даних. Використовуючи ідею змішування випадкових чисел, він намагався розв'язати проблему обміну відкритими ключами.

Після зустрічі з М. Хеллманом (див. [Хеллман], стор. 201), Меркл продовжив аспірантуру в Стенфордському університеті. За допомогою Хеллмана і Діффі (див. [Діффі], стор. 263) у 1976 році він зміг досягти успіху у розробці теорії цифрового підпису.

В останні роки Меркл намагається довести реальність ідеї *кріоніки* (наука про збереження в стані глибокого охолодження людей і тварин в надії на те, що в майбутньому їх вдасться оживити і при необхідності — вилікувати). Є директором *Alcor*'а — некомерційної організації, яка займається *кріонікою*.

Померанц, *Карл* (нар. у 1944 р.), американський математик та криптограф, фахівець з теорії чисел. Ступінь магістра отримав в Гарвардському университеті. У кандидатській дисертації довів, що кожне досконале число має принаймні 7 простих дільників. Він є автором одного з найбільш важливих алгоритмів факторизації цілих чисел — методу квадратичного решета, за допомогою якого в 1994 році вдалося зламати RSA–129. Він є одним з авторів алгоритму Еделмана–Померанца–Румлі для перевірки чисел на простоту (див. [Едельман], стор. 263). Він є автором понад 200 публікацій, у тому числі основоположної книги "*Прості числа: Криптографічні та обчислювальні аспекти*" (разом з Р. Крендаллом).



Рівест, *Роналд* (нар. 7.05.1947), американський спеціаліст з криптографії. Має ступінь бакалавра з математики від Єльського університету (1969 рік) та вчений ступінь доктора філософії з комп'ютерних наук від Стенфордського університету (1974 рік). Він є одним з авторів криптографічного алгоритму RSA разом з Аді Шаміром (див. [Шамір], стор. 268) і Леонардом Еделманом (див. [Еделман], стор. 263). Ідея алгоритму осінила його в ніч на свято єврейської Пасхи, у якій брала участь

вся трійця алгоритму RSA. Але ця ідея визріла після довгих спільних досліджень протягом року.

Автори RSA
зліва направо: А. Шамір, Р. Рівест, Л. Еделман

Спільно з Еделманом і Шаміром, Рівест заснував компанію для випуску RSA-чіпів. Еделман був президентом компанії, Рівест — головою правління, а Шамір — скарбником. В 1983 році компанію придбала корпорація "*Security dynamics*".

Рівест є автором таки алгоритмів симетричного шифрування як RC2, RC4, RC5; він також брав участь в розробці RC6. Шифри RC1 та RC3 виявились вразливими. Взагалі, літери *RC* означають *Rivest Cipher* (шифр Рівеста).

У 2006 році Рівест разом з У. Смітом опублікував ідею системи голосування "*ThreeBallot*", яка дозволяє виборцю упевнитися у тому, що його голос врахований на виборах при збереженні повної конфіденційності. Цікаво, що ця система жодним чином не використовує криптографію. Більше того, ця система не використовує компьютери; для її функціонування потрібні лише технологічно прості пристрої для голосування. Голосування є таємним, але перевіряється самим виборцем. Рівест опублікував систему як суспільне надбання, під девізом "*Наша демократія є надто важливою для нас*".

Сталлмен, *Річард* (нар. 16.03.1953), засновник руху вільного програмного забезпечення, а також проекту GNU, Фонду вільних програм та Ліги за свободу програмування. Автор концепції, втіленої у ліцензії GNU General Public License (GNU GPL) для комп'ютерних програм. Столмен радить не користуватися мобільними телефонами, тому, що вважає, що можливість визначення місцезнаходження телефону може створити різні проблеми для абонента.

Шамір, *Аді* (нар. 6.07.1952), відомий ізраїльський криптоаналітик, вчений у галузі теорії обчислювальних систем, професор прикладної математики в інституті Вейцмана, лауреат премії Тьюринга за "... *унікальний внесок у збільшення практичної цінності систем шифрування* ... ". Спільно з Роналдом Рівестом (див. [Рівест], стор. 266) і Леонардом Еделманом (див. [Еделман], стор. 263) розробив знамениту криптосхему з відкритим ключем RSA. А. Шамір отримав ступінь бакалавра від Тель-Авівського університету (1973), магістра (1975) і доктора філософії з інформатики (1977) від інституту Вейцмана. Крім RSA, Аді Шамір відомий розробкою (1979) схеми "розподіленого" секрету, математичного методу для розподілу деякого "секрету" серед кількох "учасників" з можливістю подальшої його реконструкції. У 1986 році він брав участь у розробці протоколу аутентифікації, названого згодом протоколом Фейга–Фіата–Шаміра. Шамір разом зі своїм учнем Е. Біхамом розробив диференціальний криптоаналіз, метод атаки на блочні шифри.

Глава 11

ЦИФРОВИЙ ПІДПИС

В методі RSA відкритий ключ є відомим кожному. Тому кожен, хто знає відкритий ключ Боба, може надіслати йому шифроване повідомлення. Іноді така можливість створює проблему.

Припустимо, що Боб отримав зашифрованого листа, з якого можна зрозуміти, що він від Аліси. Використовуючи свій приватний ключ, Боб дешифрував це повідомлення:

(1) ЗУСТРІЧАЄМОСЬ О ВОСЬМІЙ АЛІСА

Чи може Боб *бути впевненим, що саме* Аліса *написала цього листа?*

Відповіддю на це питання є "ні", й це є серйозною проблемою, без розв'язання якої метод RSA є нікчемним.

З проблемою *аутентифікації* люди зустрічались протягом усієї своєї історії. Вона розв'язувалась різними засобами від особистих печаток до підпису. У сучасному світі для аутентифікації використовують сканування сітківки ока та відбитки пальців, але ці способи не підходять при електронному листуванні, оскільки потребують фізичного, а не електронного, підтвердження. Чи існує спосіб аутентифікації електронних листів?

Над проблемою аутентифікації задумувались й автори RSA і саме вони вказали на спосіб її розв'язання в рамках свого методу.

1. Метод RSA для цифрового підпису

Коли Аліса шифрує повідомлення для Боба, вона використовує його відкритий ключ. Щоб підписати своє повідомлення, Аліса використовує свій приватний ключ. Наприклад, якщо Аліса має

відкритий показник	відкритий модуль	приватний показник
k_A	n_A	j_A

то кожний символ $\mathcal{S}_{\mathtt{X}}$ свого підпису вона шифрує у символ цифрового підпису $\mathcal{H}_{\mathtt{X}}$ за допомогою формули

$$\mathcal{H}_{\mathtt{X}} \equiv (\mathcal{S}_{\mathtt{X}})^{j_A} \pmod{n_A}. \tag{2}$$

Так зашифрувати свій підпис може тільки Аліса, оскільки тільки вона знає свій приватний ключ. Проте кожен, включно з Бобом, може прочитати її підпис, використовуючи відкритий ключ Аліси:

$$\begin{aligned}(\mathcal{H}_{\mathtt{X}})^{k_A} &= \left((\mathcal{S}_{\mathtt{X}})^{j_A}\right)^{k_A} \pmod{n_A} = (\mathcal{S}_{\mathtt{X}})^{k_A j_A} \pmod{n_A} \\ &\overset{/1/}{=} \mathcal{S}_{\mathtt{X}} \pmod{n_A}. \qquad ①\end{aligned} \tag{3}$$

Приклад 1. Розглянемо детально формування повідомлення з цифровим підписом. Для цього використовуємо такі "іграшкові" ключі:

ім'я	відкритий показник	модуль	приватний показник
Аліса	3	85	43
Боб	3	187	107

Аліса надсилає повідомлення (1) й супроводжує його таким підписом

ЦЕ Я АЛІСА

В таблиці нижче показано процес шифрування першого слова у повідомленні Аліси: перший рядок містить символи повідомлення, другий рядок — їхній цифровий еквівалент (позицію букви в алфавіті), а третій — коди, отримані за допомогою відкритого ключа Боба. Елементи третього рядка таблиці обчислено за правилом $\mathcal{C}_{\text{Х}} \equiv (\mathcal{P}_{\text{Х}})^3 \pmod{187}$:

(4)

	Х	З	У	С	Т	Р	І	Ч	А	Є	М	О	С	Ь
$\mathcal{P}_{\text{Х}}$	10	24	22	23	21	12	28	1	8	17	19	22	31
$\mathcal{C}_{\text{Х}}$	65	173	176	12	98	45	73	1	138	51	127	176	58

У наступній таблиці показано процес шифрування підпису Аліси: перший рядок містить символи підпису, другий рядок — їхній цифровий еквівалент (позицію букви в алфавіті), а третій — коди, отримані за допомогою приватного ключа Аліси. Обчислення для цифрового підпису Аліса здійснює за правилом: $\mathcal{S}_{\text{Х}} \equiv (\mathcal{P}_{\text{Х}})^{43} \pmod{85}$:

Х	Ц	Е	Я	А	Л	І	С	А
$\mathcal{P}_{\text{Х}}$	27	7	33	1	16	12	22	1
$\mathcal{S}_{\text{Х}}$	3	48	67	1	16	23	28	1

Таким чином Аліса надсилає таке повідомлення Бобу:

(5)

```
 65  173  176  12  98  45  73   1  138  51  127  176  58
127   27  127 176  58  51  45 126    1 169   45  176   1
 3  48  67  1  16  23  28  1
```

Перша частина цього повідомлення складається з двох рядків й містить шифр усієї фрази (1). Друга частина, яка

складається з одного (останнього) рядка, містить цифровий підпис.

Приклад 2. Коли Боб отримує листа, він починає дешифрування: основну частину повідомлення за допомогою свого приватного ключа, а підпис — за допомогою відкритого ключа Аліси.

Таблиця нижче показує результат дешифрування листа (5), який отримав Боб: індекс 1 у першому та другому рядках таблиці означає, що символи відносяться до першого рядка у листі, а індекс 2 — що символи відносяться до другого рядка. Символом $\mathcal{P}_{\mathtt{X}}$ ми позначаємо номер позиції букви X в алфавіті (цифровий формат букви X). Дешифрування Боб здійснює за правилом $\mathcal{P}_{\mathtt{X}} \equiv (\mathcal{C}_{\mathtt{X}})^{107} \pmod{187}$:

$\mathcal{C}_{\mathtt{X}_1}$	65	173	176	12	98	45	73	1	138	51	127	176	58
$\mathcal{P}_{\mathtt{X}_1}$	10	24	22	23	21	12	28	1	8	17	19	22	31
$\mathcal{C}_{\mathtt{X}_2}$	127	27	127	176	58	51	45	126	1	169	45	176	1
$\mathcal{P}_{\mathtt{X}_2}$	19	3	19	22	31	17	12	14	1	16	12	22	1

Оскільки у таблиці (4) вже наведено буквенний еквівалент першого рядка, то перетворення у буквенний формат здійснимо тільки для другого рядка:

$\mathcal{P}_{\mathtt{X}_2}$	19	3	19	22	31	17	12	14	1	16	12	22	1
$\mathtt{X}_2$	О	В	О	С	Ь	М	І	Й	А	Л	І	С	А

Щоб дешифрувати цифровий підпис, Боб використовує відкритий ключ Аліси; нижче показано результат його обчислень за правилом $\mathcal{P}_{\mathtt{X}} \equiv (\mathcal{S}_{\mathtt{X}})^3 \pmod{85}$:

$\mathcal{S}_{\mathtt{X}}$	3	48	67	1	16	23	28	1
$\mathcal{P}_{\mathtt{X}}$	27	7	33	1	16	12	22	1
X	Ц	Е	Я	А	Л	І	С	А

Тільки тепер Боб може бути вневненим, що лист йому надіслала саме Аліса.

2. Дайджест

Метод RSA розв'язує багато проблем, пов'язаних з секретністю ключів та інформації, яку необхідно передати від однієї сторони до іншої. По-перше, при використанні RSA немає питання про надійність процесу обміну ключами, оскільки цей етап взагалі відсутній в RSA: будь-хто може надіслати шифрованого листа Бобу, оскільки кожен знає відкритий ключ Боба, але жодна третя сторона не може прочитати цього листа допоки приватний ключ Боба тримається в секреті.

Більше того, ніхто не може підробити підпис Аліси у її листі до Боба, оскільки ніхто, крім неї, не знає її приватного ключа. Чи це дійсно так?

Припустимо, що Боб отримав наступний лист від Аліси разом з її цифровим підписом (ми наводимо листування у природному (буквенному) вигляді, оскільки нашою метою є пояснити проблему та шлях її подолання):

повідомлення: ВІДДАЙ ЕВІ ГРОШІ ЩО ТИ ВИНЕН МЕНІ
підпис: ЦЕ Я АЛІСА

Ми задаємо те ж питання, що й на початку цієї глави:

> *Чи може* Боб *бути впевненим, що саме* Аліса *написала цього листа?*

Його сумніви можуть бути пов'язані з тим, що Аліса перед цим листувалась з Євою. В одному з листів до Еви Аліса

використала такий же цифровий підпис:

(6)
повідомлення: ТИ ВЖЕ ПІДГОТУВАЛАСЬ ДО ІСПИТУ
підпис: ЦЕ Я АЛІСА

Тому Ева могла повторити цей підпис у листі до Боба, яке наведено вище. Таким чином, ніхто не може підробити цифровий підпис Аліси, але не виключено, що хтось має його копію і може її використати.

Щоб уникнути цієї проблеми, необхідно прив'язати цифровий підпис до змісту самого повідомлення: тоді підпис кожного разу є іншим і визначається самим повідомленням. Чи можна це зробити? Так, це можливо. Наприклад, підписом може служити саме повідомлення. Якщо k_B — це відкрита експонента Боба, а j_A — це приватна експонента Аліси, то Аліса своє повідомлення шифрує так:

лист шифрується з k_B: ВІДДАЙ ЕВІ ГРОШІ ЩО ТИ ВИНЕН МЕНІ
підпис шифрується з j_A: ВІДДАЙ ЕВІ ГРОШІ ЩО ТИ ВИНЕН МЕНІ

Зрозуміло, що такий спосіб не є економним. Загальноприйнятим підходом є використання *дайджеста*, тобто повторення повідомлення у скороченному (але все ж таки репрезентативному) вигляді. Наприклад, дайджестом у нашому прикладі може бути "слово", складене з кожного третього символа повідомлення (включно з пробілами між словами). Аліса включає дайджест ("слово" з підкреслених букв у першому рядку) у свій підпис:

лист шифрується з k_B: ВІДДАЙ␣ЕВІ␣ГРОШІ␣ЩО␣ТИ␣ВИНЕН␣МЕНІ
підпис шифрується з j_A: ДЙВГШЩТВМІ АЛІСА

Тепер сумнівів у Боба стосовно аутентичності не залишилось, оскільки своє повідомлення (6) до Еви Аліса підписала зовсім іншим чином:

повідомлення: ТИ␣ВЖЕ␣ПІДГОТУВАЛАСЬ␣ДО␣ІСПИТУ
підпис: ␣ЕІОВА␣␣ПУ АЛІСА

Таким чином, копія цього підпису у листі до Боба означала б, що цей лист надсилала не Аліса.

2.1. Хеш функції. Формування дайджесту, розглянутого вище, можна описати математично.

Приклад 3. Розглянемо подальшу процедуру на прикладі повідомлення МИР, дайджестом якого є "слово" Р. Для отримання дайджесту, спочатку переведемо кожну букву у її числовий формат:

$$\text{М} \to 17, \qquad \text{И} \to 11, \qquad \text{Р} \to 21.$$

Потім утворимо число, записавши числові еквіваленти один за іншим:

$$m = 171121.$$

Тоді

$$m - \left[\frac{m}{100}\right] \cdot 100 = 21 = \mathcal{D}_{\text{Р}}$$

є числовим кодом букви Р, яка входить в дайджест. ②

Дайджести для повідомлень можна утворювати різними способами, а не тільки тим, що ми використовували досі. У подальшому будемо вважати, що повідомлення записано у числовому вигляді, як пояснено вище. Таким чином, кожному повідомленню ми співставляємо певне число m.

В наступному означенні ми не формалізуємо вирази "*обчислити легко*", "*обчислити важко*", "*може трапитись дуже рідко*". У загальному випадку дати пояснення цим виразом складно, але для конкретних прикладів вони стають цілком зрозумілими.

Означення 1. Відображення $H : \mathbf{N} \to \mathbf{N}$ ми називаємо *хеш-функцією*, якщо

1. для заданого m значення $H(m)$ обчислити легко;
2. для заданого $H(m)$ значення m обчислити складно;
3. рівність $H(m_1) = H(m_2)$ для $m_1 \neq m_2$ може трапитись дуже рідко.

Зауваження 1. Перші дві умови означення 1 свідчать, що H є односторонньою функцією (див. означення 9.1). Третя умова означає, що можна бути майже впевненим у тому, що значення хеш-функції $H(m)$ "майже" визначає саме число m. Зверніть увагу, що третя умова означає, що все повідомлення можна "майже" замінити одним єдиним числом $H(m)$. Оскільки повідомлення однозначно описується числом m, то важливим є те, що $H(m)$ є значно меншим за m.

Фактично функції H з такими властивостями нам знайомі. Таким, наприклад, є дискретний логарифм. Відмінністю хеш-функцій від просто односторонніх є третя умова, яка означає, що H^{-1} не обов'язково є однозначною функцією.

Зауваження 2. Якщо H^{-1} є однозначною функцією, то рівність $H(m_1) = H(m_2)$ взагалі неможлива для $m_1 \neq m_2$. ③

Зауваження 3. Дайджест, який ми використали у прикладі 3, також є функцією від числового еквівалента повідомлення. Позначимо її через H. Ясно, що умова 1 означення 1 справджується для неї. Можна також погодитись, що й умова 2 є вірною, умова ж 3 мабуть не є вірною для такої хеш-функції H.

В подальшому ми кажемо, про *колізію*, якщо рівність $H(m_1) = H(m_2)$ виконується для певної пари $m_1 \neq m_2$.

Зауваження 4. Колізії можуть виникати й для добре відомих функцій, наприклад $H(x) = H(-x)$ для $H(x) = x^2$.

Правило 1. Хеш-функції для цифрового підпису

Для цифрового підпису необхідно використовувати хеш-функції; при виборі H необхідно досягти компромісу між величиною значень $H(m)$ (їх необхідно робити якомого меншими) та частотою виникнення колізій (їхню кількість необхідно зменшити; для цього необхідно розширити область значень для H; значення $H(m)$ можуть при цьому зростати).

3. Сліпий цифровий підпис

Розглянемо ще один аспект цифрового підпису та застосування ідеї RSA. Автором підходу, розглянутого нижче, є американський криптолог Девід Чаум.

Припустимо, що `Аліса` бажає, щоб

(w_1) `Боб` поставив свій підпис під її повідомленням.

Додатковою її умовою є

(w_2) `Боб` не зможе прочитати саме повідомлення, навіть якщо він залишить собі його копію.

Такі ситуації є доволі розповсюдженими у стосунках між бізнес партнерами, коли один з них робить пропозицію іншому й бажає, щоб цей факт було засвідчено нотаріусом (важливими є також дата та час, коли ця пропозиція зроблена). Умовою обох партнерів є те, що нотаріус не бачить суми, яку один з них пропонує іншому. Таким чином, нотаріус засвідчує документ "всліпу", що й пояснює назву такого підпису.

Чи можна задовольнити ці дві вимоги `Аліси`?

Приклад 4. Розглянемо уявну модель нашої ситуації, для якої поставлену задачу можна розв'язати. Уявімо, що в конверті знаходиться документ і копіювальний лист. Якщо нотаріус ставить підпис на конверті, то він через копірку відбивається на документі. Відкривши конверт, дістаємо підписаний нотаріусом документ, причому його зміст нотаріусу невідомий.

Чи можна описати модель з приклада 4 у математичних термінах? Перш за все зауважимо, що якщо `Боб` (нотаріус) має відкритий ключ $\langle n_B, k_B\rangle$ (модуль та експоненту), то фактично вимоги `Аліси` полягають у тому, щоб `Боб` поставив цифровий підпис з використанням n_B та k_B. Тоді, у разі потреби, кожен зможе пересвідчитись, що саме `Боб` завізував повідомлення. ④

3.1. Вимоги до схеми сліпого підпису. Будь-яка схема безпечного сліпого підпису повинна мати наступні три

властивості, які відповідають вимогам Аліси.

1) *Нульове розголошення.* Ця властивість означає, що Аліса отримує підпис Боба на своєму повідомленні, не розкриваючи його змісту.
2) *Неможливість пов'язати підпис та повідомлення.* Навіть якщо Аліса опублікує підпис Боба, який підписав її повідомлення всліпу, Боб не зможе прочитати повідомлення.
3) *Абсолютна впевненість.* Ця властивість означає, що тільки Боб може поставити такий електронний підпис, тобто Аліса зможе довести згодом, що саме він підписав її повідомлення.

Алгоритм 1. Сліпий цифровий підпис

1. Аліса переводить своє повідомлення у числовий формат m;
2. Аліса обирає $0 < \ell < n$, для якого $(\ell, n) = 1$;
3. Аліса знаходить $i = \ell^{-1} \pmod{n}$;
4. Аліса маскує своє повідомлення $\mathtt{mask}(m) \stackrel{\text{def}}{=} t = m\ell^k \pmod{n}$;
5. Боб підписує замасковане повідомлення за допомогою свого приватного ключа, тобто Боб обчислює $\mathtt{sign}(\mathtt{mask}(m)) \stackrel{\text{def}}{=} y = t^j \pmod{n}$;
6. Аліса демаскує повідомлення з підписом, тобто обчислює $z = yi \pmod{n}$.

Перша реалізація сліпих підписів, представлена в алгоритмі 1, була здійснена Чаумом за допомогою криптосистеми RSA. Вона задовольняє зазначеним вище трьом вимогам.

В цій схемі $\langle n, k\rangle$ — це відкритий ключ Боба, а j — його приватний ключ. Алгоритм 1 спирається на дві процедури mask$(\cdot)$ та sign$(\cdot)$. Перша з них є процедурою маскування повідомлення Аліси, друга — процедурою цифрового підпису Боба.

3.2. Доведення алгоритму 1. Щоб зрозуміти алгоритм 1, перш за все встановимо чому дорівнює число z, обчислене на шостому кроці:

$$
\begin{aligned}
z &= yi \pmod n = t^j i \pmod n = \left(m\ell^k\right)^j i \pmod n \\
&\overset{/2/}{=} m^j \ell^{kj} i \pmod n = m^j \ell i \pmod n \qquad ⑤ \\
&\overset{/3/}{=} m^j \pmod n . \qquad ⑥
\end{aligned} \tag{7}
$$

Таким чином, z — це повідомлення Аліси, зашифроване приватним ключем Боба. Це доводить, що тільки Боб міг завізувати документ m, оскільки ніхто інший не знає j і тому не може отримати y.

Аліса зберігає z і у будь-який момент може довести, що саме Боб завізував документ. ⑦

Боб не може прочитати документ m на кроці 5, оскільки він отримує лише t, з якого не можна відтворити m у легкий спосіб. ⑧

Приклад 5. Аліса робить пропозицію Валерії вартістю 1000 доларів. Аліса бажає, щоб її агент Боб засвідчив її пропозицію, але не бажає, щоб він бачив суму, вказану у пропозиції. Відкритим ключем Боба є $(n, k) = (5561, 235)$.

1. Повідомленням Аліси є $m = 1{,}000$. Вона випадковим чином обирає число $\ell = 91$ й знаходить i, обернене до ℓ

за модулем n, тобто $i = 550$. ⑨ Тепер Аліса маскує свою пропозицію, використовуючи відкритий ключ Боба:

$$t \equiv m\ell^k \pmod{n} = 1,000 \times 91^{235} \pmod{5561} = 1715. \quad ⑩$$

2. Боб підписує всліпу замасковане повідомлення t, використовуючи для цього свій приватний ключ (n, j). Іншими словами, він обчислює

$$y \equiv t^j \pmod{n} = 1715^j \pmod{5561} = 216.$$

Зауважте, що Боб не відкриває свій приватний ключ j під час цієї процедури. ⑪

3. Зрозуміло, що

$$\begin{aligned} y &\equiv t^j \pmod{n} = (m\ell^k)^j \pmod{n} \\ &\overset{/4/}{=} m^j \ell \pmod{n}. \end{aligned} \quad (8) \quad ⑫$$

Тепер Аліса знімає маску, домноживши на обернене до ℓ за модулем n:

$$z \equiv yi \pmod{n} = 216 \times 550 \pmod{5561} = 2019. \quad (9) \quad ⑬$$

4. Валерія може прочитати повідомлення Аліси, якщо використає відкритий ключ Боба й обчислить

$$m \equiv z^k \pmod{n} = 2,019^{235} \pmod{5561} = 1000. \quad (10) \quad ⑭$$

Ніхто, крім Боба (навіть читач цих рядків!), не знає його приватний ключ (n, j). Тому, поки число $n = 5561$ не факторизовано, ніхто не знає j. ⑮

4. Застосування схеми сліпого підпису

4.1. Електронні гроші. Готівкові гроші для багатьох людей мають кілька переваг перед безготівковими, серед яких

i) ними легко розраховуватись,
ii) вони є анонімними у тому розумінні, що ними можна розраховуватись не називаючи себе.

Здається, що електронних конкурентів готівка мати не може, проте сучасні математичні ідеї дозволяють перенести ці властивості готівки на так звані *електронні гроші*.

Розглянемо наступну ілюстративну модель електронних грошей, запропоновану Д. Чаумом. Він запропонував систему електронних платежів під назвою eCash, метою якої було вирішити ряд проблем, пов'язаних з повільністю і слабкою захищеністю платежів за кредитними картками. За задумом Чаума, eCash повинен був оперувати борговими зобов'язаннями у вигляді електронних сертифікатів, які міг випускати тільки банк або інша сертифікована кредитна організація. При необхідності ці зобов'язання можна було обміняти на гроші у емітента.

Ідею Чаума поіснімо на наступному (трохи) спрощеному прикладі. Спрощення стосується лише технічних деталей здійснення операцій, а не суті самих операцій.

Припустимо, що `Аліса` бажає отримати від банку чек вартістю 20 гривень. Вона також бажає, щоби банк не дізнався яким чином і коли вона використає цей чек.

Модель Чаума для електронних грошей

1. Банк видає **Алісі** чистий аркуш паперу; вона обирає випадкове число й записує його на цьому аркуші. Це число будемо називати серійним номером чеку.
2. **Аліса** вкладає цей аркуш разом з копіркою у конверт і звертається до банківського співробітника. Він ставить спеціальну печатку на конверті, яка свідчить, що чек в конверті відповідає саме 20 гривням. Крім цього, співробітник банку переводить 20 гривень з рахунку **Аліси** на спеціальний рахунок, який використовується для електронних розрахунків всіх клієнтів банку (ця операція називається *дебетуванням* рахунку).
3. **Аліса** дістає аркуш з відбитком банківського штампу й розраховується ним у магазині.
4. Продавець надсилає чек до банку. Банк перевіряє чи надсилався раніше чек з таким серійним номером. Якщо чек з таким номером надійшов вперше, то банк переказує 20 гривень з спецрахунку на рахунок продавця (ця операція називається *кредитуванням* рахунку) й вносить номер чеку до списку сплачених чеків.

Оскільки банк не знав серійний номер до надходження чеку до банку, він не знає хто саме скористався таким чеком, тобто анонімність **Аліси** збережено.

Зауваження 5. Припустимо, що разом з **Алісою** аналогічний чек отримав **Боб**. Якщо так трапиться, що вони впишуть однаковий серійний номер у свої чеки, то пізніше один з них не зможе ним розрахуватись. ⑯ Щоб уникнути такої неприємної події, банк може вимагати від клієнтів обирати дуже великі випадкові числа (наприклад, з проміжку від 10^{100} до $10^{101}-1$). В цьому випадку ймовірність співпадіння двох номерів є майже нулевою.

Нижче наведено алгоритм, який реалізує у цифровому

вигляді модель, описану вище.

Алгоритм 2. Електронні гроші

1. `Аліса` обирає серійний номер S й маскуючий коефіцієнт ℓ; кілька перших цифр в S ідентифікують банк, всі решта обираються випадково. `Аліса` обчислює $i \equiv \ell^{-1} \pmod{n}$.
2. `Аліса` маскує серійний номер, обчислюючи $y \equiv S\ell^k \pmod{n}$; значення y вона надсилає до банку.
3. Банк дебетує рахунок `Аліси` на 20 гривень й підписує замаскований серійний номер, обчислюючи $t \equiv y^j \pmod{n}$; це значення банк повертає `Алісі`.
4. `Аліса` знімає своє маскування, обчислюючи $z \equiv ti \pmod{n}$; при купівлі вона повідомляє число z продавцю.
5. Продавець обчислює $S \equiv z^k \pmod{n}$; за першими цифрами S продавець ідентифікує банк й надсилає туди S.
6. Банк перевіряє серійний номер S й кредитує рахунок продавця на 20 гривень.

В алгоритмі 2 ми вважаємо, що (n, k) — це відкритий ключ, а j — це приватний ключ, які банк використовує для чеків вартістю 20 гривень.

Зауважимо, що на кроці 4 описаної процедури `Аліса` фактично обчислює

$$\begin{aligned} z &\equiv ti \pmod{n} = y^j i \pmod{n} = (S\ell^k)^j i \pmod{n} \\ &= S^j \ell^{kj} i \pmod{n} = S^j \ell i \pmod{n} = S^j \pmod{n}, \end{aligned}$$

тобто серійний номер, зашифрований приватним ключем банка. Це обчислення пояснює результат на кроці 5. ⑰

4.2. Таємне голосування. Ідея сліпих цифрових підписів використовується для організації таємного голосування. Опишемо один з підходів, опублікований в 1992 році японськими вченими А. Фудзіока, Т. Окамото та К. Охта. Термінологія, яку ми використовуємо нижче ("маскування", "підпис" тощо), є зрозумілою з алгоритма 1.

Практичні реалізації електронного голосування добре відомі: наприклад, саме так організовано вибори в Естонії. Перша реалізація проекту в Естонії припала на місцеві вибори в жовтні 2005 року. Система витримала реальні випробування і була естонськими чиновниками визнана успішною. Парламентські вибори з використанням системи електронного голосувань також пройшли успішно.

Для здійснення процедури таємного голосівання обираються дві комісії, контрольна (КК) та лічильна (ЛК). Контрольна комісія встановлює особу виборця, але не має доступу до його вибору. Лічильна комісія встановлює результат голосування виборця, але не може ідентифікувати його особу. Наявність двох комісій, а не однієї, підвищує конфіденційність процедури голосування. Кожен з суб'єктів виборчого процесу має свій приватний та відкритий ключ.

При електронному голосуванні результатом є число, яке однозначно визначає уподобання виборця (наприклад, номер свого фаворита у виборчому списку).

Дії кожної з сторін виборчого процесу наведено у таблиці нижче. Для приховування свого уподобання виборець генерує 100 випадкових цифр й утворює велике число, записуючи спочатку 50 перших згенерованих цифр, потім свій вибір, потім останні згенеровані цифри. Це число ми позначаємо через C.

Процедура електронного голосування

	Виборець	Контрольна комісія	Лічильна комісія
1.	Маскує вибір $C \to M$ своїм приват–ним ключем		
2.	Вносить маску M в бюлетень		
3.	Підписує бюлетень відкритим ключем КК		
4.	Надсилає бюлетень в КК		
5.		Перевіряє підпис на бюлетені своїм приват–ним ключем	
6.		Перевіряє чи голосував цей виборець	
7.		Підписує бюлетень приватним ключем ЛК	
8.		Повертає бюлетень виборцю	
9.	Видаляє свій підпис		
10.	Надсилає бюлетень в ЛК		
11.			Перевіряє підпис КК своїм при–ватним ключем
12.			Встановлює M

Після здійснення кроку 12 лічильна комісія ще не в змозі встановити уподобання виборця C. Це стає можливим лише після того, як у заздалегідь узгоджений момент виборець надішле свій ключ до ЛК.

Зауваження 6. Неважко помітити, що КК знає особу виборця, який надсилає бюлетень, але не може встановити його вибір, оскільки в бюлетені записано M, а не C. З іншого боку, ЛК не може встановити особу виборця, оскільки отримує бюлетень з видаленим його підписом. Результат голосування виборця ЛК може отримати лише після того, як він надішле ключ.

Зауваження 7. Підпис виборця на кроці 3 має бути таким, щоб КК була у змозі ідентифікувати його особу. Для цього напередодні виборів КК надає кожному виборцю ідентифікаційний номер, який використовується у підпису виборця.

Зауваження 8. Оскільки виборець отримує від КК підписаний бюлетень, він може змінити свій вибір перед тим, як повідомити ЛК про свій вибір. Цю можливість можна заблокувати, якщо домовитись, що підпис КК включає M.

Зауваження 9. Слабким місцем описаної схеми є відсутність захисту від змови між КК та ЛК, результатом якої стає втрата конфеденційності виборця, оскільки КК має M та знає особу виборця, а ЛК спочатку отримує M, а згодом і C. Об'єднання даних КК та ЛК розкриває таємницю голосування.

5. Цифровий підпис для схеми Ель-Гамаля

Особливістю криптосистеми Ель-Гамаля (розділ 10.7), як

і системи RSA, є наявність ефективної процедури цифрової перевірки (*аутентифікації*) особи кореспондента. Нехай `Аліса` використовує систему Ель-Гамаля з відкритим ключем (p, r, a) та приватним ключем k. Нижче наведено алгоритм 3 цифрового підпису для криптосистеми Ель-Гамаля, який використовує певну хеш функцію H, яка є додатковим (приватним) параметром цієї системи.

Алгоритм 3. Цифровий підпис для системи Ель-Гамаля

Вхідні дані: Відкритий ключ (p, r, a) та приватний ключ k; шифр-повідомлення M.

Вихідні дані: Цифровий підпис: пара чисел c, d.

`Крок 1`. Обрати випадково число $1 \le j \le p-1$, яке має властивість $(j, p-1) = 1$;

`Крок 2`. обчислити $c \equiv r^j \pmod{p}$;

`Крок 3`. обчислити значення хеш функції $B = H(M)$;

`Крок 4`. знайти розв'язок d лінійної конгруенції $jd + kc \equiv B \pmod{p-1}$.

Вважається, що дайджест B повідомлення M не є секретним, але хеш функцію H, для якої $B = H(M)$, треба обирати дуже ретельно, щоб M не можна було відновити за B.

Метод розв'язання конгруенції, що виникає на `Кроці 4` алгоритму 3, описано в розділі 4.2. Розв'язок можна записати у вигляді $d \equiv (B - kc)j^{-1} \pmod{p-1}$.

Пара цілих чисел (c, d) і є цифровим підписом, який додається до повідомлення. Його може створити тільки той,

хто знає приватний ключ k, випадкове ціле число j та саме повідомлення M.

Боб за допомогою відкритого ключа Аліси (p, r, a) перевіряє підпис. Для цього він підраховує два числа

$$V_1 \equiv a^c c^d \pmod{p}, \qquad V_2 \equiv r^B \pmod{p}.$$

Зрозуміло, що $0 \le V_1, V_2 \le p-1$. Цифровий підпис приймається, якщо $V_1 = V_2$. Це випливає з наступних конгруенцій

$$\begin{aligned} V_1 &\equiv a^c c^d \equiv (r^k)^c (r^j)^d \equiv r^{kc+jd} \equiv r^B \\ &\equiv V_2 \pmod{p}, \qquad ⑱ \end{aligned} \tag{11}$$

оскільки $a = r^k \pmod{p}$. Зауважимо, що ця процедура аутентифікації цифрового підпису не вимагає знання приватного ключа k.

Приклад 6. Припустимо, що Аліса використовує криптосистему Ель-Гамаля з відкритим ключем $p = 43$, $r = 3$, ⑲ $a = 22$ та приватним ключем $k = 15$. ⑳ Вона бажає надіслати Бобу повідомлення M з своїм цифровим підписом. Для цього вона спочатку обирає ціле число $0 \le j \le 42$ з $(j, 42) = 1$, наприклад $j = 25$. Перш за все Аліса обчислює

$$c \equiv 3^{25} \equiv 5 \pmod{43}.$$

Якщо значенням хеш функції $H(M)$ є $B = 13$, то вона після цього розв'язує лінійну конгруенцію

$$25d \equiv 13 - 5 \cdot 15 \pmod{42}$$

й отримує $d \equiv 16 \pmod{42}$. ㉑ Пара $(5, 16)$ являє собою цифровий підпис Аліси. Отримавши від Аліси повідомлення, Боб перевіряє підпис, порівнюючи два цілих числа V_1 таV_2:

$$\begin{aligned} V_1 &\equiv 22^5 \cdot 5^{16} \equiv 39 \cdot 40 \equiv 12 \pmod{43}, \\ V_2 &\equiv 3^{13} \equiv 12 \pmod{43}. \end{aligned} \tag{12}$$

㉒

5.1. Невдала хеш функція. Найпростішою хеш функцією є $H(x) = x$. Для передачі цифрового підпису з такою хеш функцією потрібен такий же час, як і для самого повідомлення. Для великих повідомлень це може бути неприйнятним. Але вибір такої хеш функції є невдалим навіть і для малих повідомлень, оскільки надійність системи суттєво знижується при $H(x) = x$.

Припустимо, що Аліса у листуванні з Бобом використовує його систему Ель-Гамаля. Вона завжди використовує саме повідомлення у якості цифрового підпису. В цьому випадку існує спеціальне повідомлення з правильним підписом, яке будь-хто інший може надіслати Бобу, а він не зможе помітити, що повідомлення надійшло не від Аліси.

Твердження 1. *Нехай l_1 та l_2 — довільні цілі числа, $0 \le l_1, l_2 \le p-1$, а l_2^{-1} — це обернене до l_2 за модулем $p-1$. Позначимо*

$$\beta \equiv r^{l_1} a^{l_2} \pmod{p}, \qquad \gamma \equiv -\beta l_2^{-1} \pmod{p-1}.$$

Тоді пара чисел β, γ є правильним підписом для повідомлення

$$M \equiv \gamma l_1 \pmod{p-1}.$$

Доведення. Нагадаємо, що $r^{p-1} \equiv 1 \pmod{p}$. Тому, якщо $u \equiv v \pmod{p-1}$, то $r^{\lambda u} \equiv r^{\lambda v} \pmod{p}$ для будь-якого натурального числа λ. ㉓ Ми тричі використаємо цю властивість у ланцюжку міркувань, записаних нижче. Таким чином, за модулем p

$$V_1 = a^{\beta}\beta^{\gamma} \equiv r^{k\beta}r^{(l_1+kl_2)\gamma} \overset{/5/}{\equiv} r^{k\beta}r^{(l_1+kl_2)(-\beta l_2^{-1})}$$
$$\equiv r^{k\beta}r^{-\beta l_1 l_2^{-1}-\beta k} \overset{/6/}{\equiv} r^{-\beta l_1 l_2^{-1}} \overset{/7/}{\equiv} r^{\gamma l_1} \equiv r^{M} \pmod{p} = V_2.$$

Саме у конгруенціях /5/, /6/ та /7/ ми застосували зазначену вище властивість чисел r та p. ㉔

Таким чином, $V_1 = V_2$ й `Боб` вірить цьому підпису, хоча таке повідомлення з таким правильним підписом могло надійти від будь-якого кореспондента, а не тільки від `Аліси`, оскільки l_1 та l_2 довільні. □

5.2. Атака, якщо j є відомим. Число j, яке випадковим чином обирається в алгоритмі 3, необхідно тримати у суворому секреті. Якщо ж воно стає відомим третій стороні, то приватний ключ k легко відтворюється, оскільки

$$k \equiv (B - jd)c^{-1} \pmod{p-1}.$$

Тут $B = H(M)$ — це дайджест повідомлення M, який використано для цифрового підпису (див. `Крок 4` в алгоритмі 3).

5.3. Атака, якщо j повторюється. Не можна підписувати різні повідомлення, використовуючи одне і те ж число j, інакше є небезпека, що третя сторона зможе його обчислити. Щоб показати це, позначимо через d_1 та d_2 другі частини підписів для повідомлень M_1 та M_2 (перші частини у них однакові завжди і дорівнюють c). Для спрощення

вважатимемо, що $H(x) = x$, тобто $B_1 = M_1$ та $B_2 = M_2$ (див. `Крок 3` в алгоритмі 3). Тоді

$$\begin{aligned} a^c c^{d_1} &\equiv r^{kc+jd_1} \equiv r^{M_1} \pmod{p}, \\ a^c c^{d_2} &\equiv r^{kc+jd_2} \equiv r^{M_2} \pmod{p}. \end{aligned}$$

Згідно з твердженням c) теореми 10.1 ці дві конгруенції еквівалентні двом таким $M_1 \equiv kc + jd_1 \pmod{p-1}$ та $M_2 \equiv kc + jd_2 \pmod{p-1}$, звідки

$$M_2 - M_1 \equiv j(d_2 - d_1) \pmod{p-1}.$$

Якщо позначити через g найбільший спільний дільник чисел $p-1$ та $d_2 - d_1$, тобто $g = (p-1, d_2 - d_1)$, то можемо записати

$$\frac{M_2 - M_1}{g} \equiv \frac{j(d_2 - d_1)}{g} \left(\mathrm{mod}\ \frac{p-1}{g}\right)$$

й тому

$$j \equiv \frac{M_2 - M_1}{g} \left(\frac{d_2 - d_1}{g}\right)^{-1} \left(\mathrm{mod}\ \frac{p-1}{g}\right).$$

Обернене за модулем існує, оскільки $(d_2 - d_1)/g$ та $(p-1)/g$ є взаємно простими. Таким чином, j можна обчислити, якщо його використано у двох різних повідомленнях, саме через цю обставину число j обирається випадково на `Кроці 1` в алгоритмі 3: це допомагає не повторювати його у різних повідомленнях.

6. Розподілення секретів

Дуже стисло розглянемо одне з застосувань криптографії, а саме, спосіб для розподілення секретів. Припустимо, що для функціонування певної системи необхідна вкрай важлива, але надзвичайно чутлива до втрати конфеденційності, інформація. Прикладом подібної інформації може служити код до банківського сейфу: його не можна загубити, але не можна і довірити будь-кому.

Інформацію, якою користується система, не можна втратити у жодному випадку: щоб не допустити втрати інформації її необхідно розповсюдити якомога ширше. Але такий підхід протирічить іншій її властивості про чутливість до втрати кофеденційності, яка означає якомога ширші обмеження щодо розповсюдження.

Одним з підходів до розв'язання зазначеної ділеми є розподілення секрету між кількома учасниками так, щоб кожному дісталась лише його частина. У подальшому будемо говорити про ключ (число) k, який і є тією чутливою інформацією, про яку ми говорили вище. Щоб захистити ключ k як від втрати, так і від несанціонованого доступу, ми будуємо його *тіні* $k_1, \ldots, k_r$, які розподіляються між r різними особами. Тіні буде побудовано так, щоб ключ можна було відновити з будь-якої комбінації $s < r$ тіней, але, щоб знання меншої, ніж s, кількості тіней не дозволяло обчислити ключ. Схема з такими властивостями називається (r, s) *пороговою схемою*.

Виберемо просте число $p > k$ та послідовність попарно взаємно простих чисел $m_1 < m_2 < \cdots < m_r$, кожне з яких не ділиться на p. Ці числа додатково мають властивість

$$m_1 m_2 \ldots m_s > p m_r m_{r-1} \ldots m_{r-s+2}. \tag{13}$$

Формула (13) означає, що добуток найменших s чисел послідовності $\{m_1, m_2, \ldots, m_r\}$ є більшим, ніж добуток p та $s-1$ найбільших чисел. Позначимо $M = m_1 m_2 \ldots m_s$. Тоді з властивості (13) випливає, що M/p є більшим за добуток будь-яких $s-1$ чисел з послідовності $\{m_1, m_2, \ldots, m_r\}$. ㉕

Оберемо випадково натуральне число $0 \leq t < M/p$ й позначимо

$$k_0 = k + tp.$$

Тоді $k \leq k_0 \leq M - 1$. ㉖ Означимо тепер

$$k_j \equiv k_0 \pmod{m_j}, \qquad 1 \leq j \leq r.$$

Оберемо довільну підмножину $\{j_1, \ldots, j_s\} \subseteq \{1, \ldots, r\}$ з s індексів й покажемо, що за допомогою $k_{j_1}, \ldots, k_{j_s}$ можна обчислити відповідне число k_0. Розглянемо наступну систему лінійних конгруенцій

$$x \equiv k_j \pmod{m_j}, \qquad j \in \{j_1, \ldots, j_s\}.$$

Згідно китайській теоремі про остачі (теорема 5.5) ця система має єдиний розв'язок за модулем $M_s = m_{j_1} \ldots m_{j_s}$. Оскільки $0 \leq k_0 < M \leq M_s$, то цим розв'язком є k_0. Тепер обчислюємо $k = k_0 - tp$.

Покажемо тепер, що знання довільної множини $s-1$ тіней $k_{j_1}, \ldots, k_{j_{s-1}}$ недостатньо, щоб визначити k. Розглянемо тепер систему лінійних конгруенцій

$$x \equiv k_j \pmod{m_j}, \qquad j \in \{j_1, \ldots, j_{s-1}\}.$$

Як і у міркуваннях, проведених вище для s тіней, ця система має єдиний розв'язок за модулем $M_{s-1} = m_{j_1} \ldots m_{j_{s-1}}$

(позначимо його через a). Тому $k_0 = a + xM_{s-1}$ для деякого $0 \le x < M/M_{s-1}$. ㉗ Тепер з (13) робимо висновок, що $M/M_{s-1} > p$. Таким чином, натуральне x є меншим за M/M_{s-1} й може бути будь-яким з множини остач при діленні на p. ㉘ Оскільки $(m_j, p) = 1$ для $j \in \{j_1, \ldots, j_{s-1}\}$, то $(M_{s-1}, p) = 1$ й тому $a + xM_{s-1}$ також може бути довільним числом з множини остач при діленні на p. ㉙ Це й означає, що знання будь-яких $s-1$ тіней недостатньо для того, щоб обчислити k_0, оскільки k_0 може бути будь-яким з множини остач при діленні на p.

Зауваження 10. Зауважимо, що між учасниками порогової схеми фактично розподіляється інформація (k_j, m_j), а не просто k_j. Це означає, що j-му учаснику порогової схеми відомими є два числа k_j та m_j.

Зауваження 11. Порогова (r, s) схема дозволяє відновити ключ навіть тоді, коли втрачено $r - s$ тіней. Проте втрата більшої кількості тіней означає втрату ключа. Остання властивість означає також, що зговір будь-яких $s-1$ (або меншої кількості) учасників порогової схеми не дозволяє їм відновити ключ.

Приклад 7. Нехай $k = 16$. Побудуємо $(3, 2)$ порогову схему. Обираємо $p = 17$ та $m_1 = 19$, $m_2 = 21$, $m_3 = 23$. Тоді $M = 399$ й можна взяти $t = 10$. Тому $k_0 = 16 + 10 \cdot 17 = 186$ й $k_1 = 186 \pmod{19} = 15$, $k_2 = 186 \pmod{21} = 18$, $k_3 = 186 \pmod{23} = 2$.

Таким чином, секретна інформація розподіляється частинами (тінями) між учасниками порогової схеми наступним чином:

секрет першого	секрет другого	секрет третього
15, 19	18, 21	2, 23

Найменшим розв'язком будь-якої з систем

$$\underline{j_1=1,\ j_2=2}\quad \begin{cases} x=15 \pmod{19} \\ x=18 \pmod{21} \end{cases} \qquad \underline{j_1=1,\ j_2=3}\quad \begin{cases} x=15 \pmod{19} \\ x=2 \pmod{23} \end{cases} \qquad \underline{j_1=2,\ j_2=3}\quad \begin{cases} x=18 \pmod{21} \\ x=2 \pmod{23} \end{cases}$$

є число $k_0 = 186$:

$$186 = \begin{cases} 9\cdot 19+15 \\ 8\cdot 21+18 \end{cases} \qquad 186 = \begin{cases} 9\cdot 19+15 \\ 8\cdot 23+2 \end{cases} \qquad 186 = \begin{cases} 8\cdot 21+18 \\ 8\cdot 23+2 \end{cases}$$

У кожному з випадків можна відновити ключ:

$$k = 186 - 10\cdot 17 = 16.$$

Таким чином, втрата однієї з тіней не є критичною для відновлення самого ключа. Проте втрата двох або трьох тіней означає втрату ключа. Наприклад, якщо втрачено тіні першого та другого учасника, то конгруенція третього учасника $x = 2 \pmod{23}$ дає розв'язок $x = 2$, якого недостатньо для того, щоб відновити ключ.

7. КОНТРОЛЬНІ ПИТАННЯ

1. Пояснити рівність /1/ у ланцюжку (3). (стор. 270).

2. Аналогічним (до прикладу 3) чином описати процедуру утворення дайджеста для "довгих" повідомлень. (стор. 275).

3. Чому рівність $H(m_1) = H(m_2)$ неможлива для $m_1 \neq m_2$, якщо H^{-1} є однозначною функцією? (стор. 276).

4. Як можна пересвідчитись, що саме Боб завізував повідомлення у прикладі 4? (стор. 278).

5. пояснити рівність /2/ в (7). (стор. 280).

6. пояснити рівність /3/ в (7). (стор. 280).

7. Яким чином Аліса може довести, що саме Боб завізував документ у прикладі §3.2? (стор. 280).

8. Чому Боб не може у легкий спосіб прочитати документ m на кроці 5 у прикладі §3.2? (стор. 280).

9. Перевірити, що $550 \times 91 \equiv 1 \pmod{5561}$. (стор. 280).

10. Довести, що $t \equiv 1715 \pmod{5561}$. (стор. 281).

11. Визначити приватний ключ Боба у прикладі 5. (стор. 281).

12. Пояснити рівність /4/ в (8). (стор. 281).

13. Перевірити рівність $z = 2019$ в (9). (стор. 281).

14. Перевірити обчислення Валерії в (10). (стор. 281).

15. Факторизувати число 5561 й визначити j в останньому рядку прикладу 5. (стор. 281).

16. Припустимо, що Боб отримав такий же електронний чек, як і Аліса. Чому один з них не зможе розрахуватись (див. зауваження 5)? (стор. 283).

17. Перевірити обчислення на кроці 5 в алгоритмі 2. (стор. 284).

18. Пояснити чому з (11) випливає, що $V_1 = V_2$. (стор. 289).

19. Впевнитись, що $r = 3$ є примітивним коренем для $p = 43$. (стор. 289).

20. Довести, що $a = r^k \pmod{p}$ при $a = 22$, $r = 3$, $k = 15$, $p = 43$. (стор. 289).

21. Впевнитись, що $d = 16$ є розв'язком конгруенції $25d \equiv 13 - 5 \cdot 15 \pmod{42}$. (стор. 289).

22. Перевірити всі конгруенції, які використані при обчисленні V_1 та V_2 в (12). (стор. 290).

23. Впевнитись, що $r^{\lambda u} \equiv r^{\lambda v} \pmod{p}$ для будь-якого натурального числа λ, якщо $u \equiv v \pmod{p-1}$, а r є примітивним коренем для p. (стор. 290).

24. Довести конгруенції /5/, /6/ та /7/. (стор. 291).

25. Чому з властивості (13) випливає, що M/p є більшим за добуток будь-яких $s-1$ чисел з послідовності $\{m_1, m_2, \ldots, m_r\}$? (стор. 293).

26. Чому $k \le k_0 \le M - 1$? (стор. 294).

27. Пояснити, чому $k_0 = a + xM_{s-1}$ для деякого $0 \le x < M/M_{s-1}$? (стор. 294).

28. Чому число x у доведенні неможливості відновити ключ з довільної комбінації $s-1$ тіней може бути будь-яким з множини остач при діленні на p? (стор. 294).

29. Чому число $a+xM_{s-1}$ у доведенні неможливості відновити ключ з довільної комбінації $s-1$ тіней може бути будь-яким з множини остач при діленні на p? (стор. 294).

8. З А Д А Ч І

В задачах 1–6, наведених нижче, вважати, що Аліса та Боб використовують RSA систему з відкритими ключами $(k_A, n_A) = (3, 512557)$ та $k_B, n_B) = (3, 565291)$.

Задача 1. *Знайти приватний ключ* Аліси.

Задача 2. *Знайти приватний ключ* Боба.

Задача 3. *Зашифрувати повідомлення* "ПРИВІТ" *від* Аліси *до* Боба *та підписати його* "АЛІСА".

Задача 4. *Повторити обчислення* Боба *при дешифрації повідомлення та підпису, вказаних у задачі* 3.

Задача 5. *Зашифрувати відповідь* "ПРИВІТ" *від* Боба *до* Аліси *та підписати його* "БОБ".

Задача 6. *Повторити обчислення* Аліси *при дешифрації повідомлення та підпису, вказаних у задачі* 5.

У задачах 7–10 вважати, що відкритим ключем Боба є $k_B = 5$, $n_B = 323$.

Задача 7. Аліса *хоче, щоб* Боб *поставив сліпий підпис під її повідомленням. Для цього вона обирає* $\ell = 3$. *Знайти* $\ell^{-1} \pmod{n_B}$.

Задача 8. *Повідомленням* Аліси *є* "CIM". *Обчислити замасковане повідомлення, яке передається* Бобу *на підпис.*

Задача 9. *Яким є замасковане повідомлення з підписом* Боба?

Задача 10. *Яким є повідомлення з підписом* Боба *після демаскування*?

В задачах 11–15 відкритим ключем банка є $k = 3$, $n = 437$. Аліса бажає мати електронну готівку; для цього вона обирає серійний номер $S = 3801$ та маскуючий коефіцієнт $\ell = 5$.

Задача 11. *Зробити початкові обчислення для* Аліси *й знайти* $i \equiv \ell^{-1} \pmod{n}$.

Задача 12. *Замаскувати серійний номер електронної готівки* Аліси.

Задача 13. *Обчислити електронний підпис банка при дебетуванні готівки для* Аліси.

Задача 14. *Зняти маскування* Аліси *на її електронній готівці.*

Задача 15. Аліса *розраховується у супермаркеті, передаючи продавцю демаскований підпис банку. Зробити обчислення за продавця.*

В задачах 16–19 Аліса використовує криптосистему Ель-Гамаля Боба з відкритим ключем $p = 67$, $r = 2$, $a = 2$ і секретним ключем $k = 3$. Тут r — примітивний корінь p (таблиця 10.2), а $a \equiv r^k \pmod{p}$ (алгоритм 10.5).

Задача 16. Аліса *обирає* $j = 7$. *Обчислити для неї* $c \equiv r^j \pmod{p}$.

Задача 17. Аліса *надсилає* Бобу *повідомлення* "УРА". *Вони з* Бобом *домовились у якості цифрового підпису використовувати саме повідомлення, але записане у зворотному порядку, тобто в цьому випадку* "АРУ". *Таким чином, підписом є пара чисел* c *та* d, *де*

$$jd + kc \equiv B \pmod{p-1},$$

а B *— цифрове значення для* "АРУ". *Обчислити для* Аліси *число* d.

Задача 18. *Дешифрувати за* Боба *повідомлення* Аліси.

Задача 19. *Щоб впевнитись у тому, що повідомлення надійшло від* Аліси, Боб *порівнює два числа*

$$V_1 \equiv a^c c^d \pmod{p}, \qquad V_2 \equiv r^B \pmod{p}.$$

Зробити ці обчислення за Боба.

Задача 20. *Припустимо, що в RSA криптосистемі* Боба *модуль* n *є настільки великим, що факторизацію* n *неможливо отримати за прийнятний час.* Аліса *надсилає повідомлення* Бобу, *у якому вона кожну букву шифрує окремо від інших. Чи є такий метод надійним? Відповідь обгрунтувати.*

Задача 21. Аліса *та* Боб *використовують криптосистему Ель-Гамаля з параметрами* $p = 3023$, $r = 5$, $a = 2391$. Аліса *надсилає повідомлення* $m = 121$ *з підписом* $c = 480$, $d = 532$. *Чи довіряє* Боб *такому підпису?*

Задача 22. Аліса *та* Боб *використовують криптосистему Ель-Гамаля з параметрами* $p = 7481$, $r = 6$, $a = 5979$. Аліса *надсилає повідомлення* $m = 487$ *з підписом* $c = 1723$, $d = 7045$. *Чи довіряє* Боб *такому підпису?*

В задачах 23–26 представлено операції спрощенного варіанту шифрування методом DES для блоків з 8 бітів замість блоків з 64 бітів, в оригінальному алгоритмі. Більш сучасний варіант DES називається протоколом AES.

Задача 23. *Першим кроком алгоритму DES є перестановка бітів* $b_1b_2b_3b_4b_5b_6b_7b_8$. *Наприклад, початкову послідовність можна переставити й отримати послідовність* $b'_1b'_2b'_3b'_4b'_5b'_6b'_7b'_8$, *де* $b'_1 = b_4$, $b'_2 = b_3$ *і так далі, що визначається перестановкою*

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 2 & 1 & 8 & 7 & 6 & 5 \end{pmatrix}. \tag{14}$$

У загальному випадку перестановка записується наступним чином

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ i_1 & i_2 & i_3 & i_4 & i_5 & i_6 & i_7 & i_8 \end{pmatrix},$$

де $i_1, i_2, i_3, i_4, i_5, i_6, i_7, i_8$ *— це різні числа з набору* $\{1, 2, 3, 4, 5, 6, 7, 8\}$. *Перестановка діє за правилом* $b'_k = b_{i_k}$ *для кожного* $1 \le k \le 8$.

a) *Перевірити, що якщо застосувати двічі перестановку* (14), *то отримаємо початкову послідовність бітів.*

b) *Перевірити таку ж властивість, як в* a), *для перестановок* $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$ *та* $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 \end{pmatrix}$.

c) *Чи виконується та ж властивість, що і в* a), *для будь-якої перестановки? Навести приклад.*

Задача 24. *Результат дії операції* `XOR` *для двох бінарних чисел* b' *та* b'' *позначається* $b' \oplus b''$ *та означається наступним чином*

$$b' \oplus b'' = \begin{cases} 0, & \text{якщо } b' = b'', \\ 1, & \text{якщо } b' \ne b''. \end{cases}$$

Для блока бітів операція `XOR` *означається поелементно. Припустимо, що* $k_1k_2k_3k_4k_5k_6k_7k_8$ *— це фіксований блок бітів, який називається ключем. Чи існує операція* $\ominus$, *за допомогою якої з*

$$p_1p_2p_3p_4p_5p_6p_7p_8 \stackrel{\text{def}}{=} b_1b_2b_3b_4b_5b_6b_7b_8 \oplus k_1k_2k_3k_4k_5k_6k_7k_8$$

можна обчислити $b_1b_2b_3b_4b_5b_6b_7b_8$, *тобто*

$$p_1p_2p_3p_4p_5p_6p_7p_8 \ominus k_1k_2k_3k_4k_5k_6k_7k_8 = b_1b_2b_3b_4b_5b_6b_7b_8\,?$$

Задача 25. *Зафіксуємо 6 бітів $k_1k_2k_3k_4k_5k_6$. Додамо ще два біта k_7k_8 за правилом*: $k_7 = k_1+k_2+k_3 \pmod 2$, $k_8 = k_5+k_6+k_7 \pmod 2$. *Саме так утворюється ключ для метода DES. Припустимо, що випадково змінено один з бітів $k_1k_2k_3k_4k_5k_6k_7k_8$. Чи можна це розпізнати?*

Задача 26. *Спрощений метод шифрування DES для блоків довжини 8 полягає у виконанні таких кроків*:

(i) *Зробити початкову перестановку бітів блока.*
(ii) *Розділити переставлений блок на дві частини однакового розміру, L та R, кожна по 4 біта.*
(iii) *Розширити R та звузити ключ.*
(iv) *Обчислити $X = f(E(R), P(K))$, де $E(R)$ — це розширена частина R, а $P(K)$ — це підключ для K.*
(v) *Сформувати блок $B = R \cup X$, обчислити $B' = B+L \pmod 2$.*
(vi) *Зробити фінальну перестановку бітів блока B'.*

Кожне з перетворень (i)–(vi) можна представити за допомогою матриць розміру 2×8. В задачі 23 пояснено як це зробити для кроків (i) *та* (vi). *Для кроку* (iii) *матрицями є*

$$\pi_L = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \checkmark & \checkmark & \checkmark & \checkmark & \bullet & \bullet & \bullet & \bullet \end{pmatrix} \qquad \pi_R = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \bullet & \bullet & \bullet & \bullet & \checkmark & \checkmark & \checkmark & \checkmark \end{pmatrix}$$

Кожен з операторів π_L та π_R діє на блок з восьми бітів наступним чином: результатом є блок з чотирьох бітів, в який включаються біти, позначені символом $\checkmark$; біти, позначені $\bullet$, у вихідний блок не включаються.

Розширення блоку R до блоку $E(R)$ з шести бітів відбувається за рахунок включення його ж бітів. Включати ($\checkmark$) чи не включати ($\bullet$) додатковий біт визначається матрицею:

$$\pi_{E(R)} = \begin{pmatrix} 1 & 2 & 3 & 4 & 1 & 2 & 3 & 4 \\ \checkmark & \checkmark & \checkmark & \checkmark & \bullet & \checkmark & \checkmark & \bullet \end{pmatrix}.$$

Звуження ключа до підключа, який складається з шести символів, відбувається відповідно до матриці:

$$\pi_{P(K)} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \checkmark & \bullet & \checkmark & \checkmark & \checkmark & \checkmark & \bullet & \checkmark \end{pmatrix}.$$

Перетворення на кроці (iv) *схематично зображено нижче:*

$$b_1b_2b_3b_4b_5b_6 \longrightarrow \boxed{S} \longrightarrow b'_1b'_2b'_3b'_4$$

S-блок на цій схемі виконує операцію $b_1b_2b_3b_4b_5b_6 \oplus k_1k_2k_3k_4k_5k_6$ *з розширеним* R *та звуженим ключем* K. *Крім цього, S-блок з шести бітів залишає лише чотири згідно до матриці*:

$$\pi_X = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ \checkmark & \checkmark & \bullet & \checkmark & \checkmark & \bullet \end{pmatrix}.$$

a) *Записати матрицю перетворення для кроку* (v).
b) *Використовуючи матрицю* (14) *для початкової та фінальної перестановки, а також матриці* π_L, π_R, $\pi_{E(R)}$, $\pi_{P(K)}$ *та* π_X, *наведені вище, зашифрувати спрощеним методом DES блок* `00000101` *з ключем* `01101100`.

Задача 27. *Припустимо, що ключем є число* $k = 4$. *Оберемо параметрами для* $(3, 2)$ *порогової схеми розподілення секретів, описаної на стор.* 293–296, *наступні* $p = 7$, $m_1 = 11$, $m_2 = 12$, $m_3 = 17$ *та* $t = 14$. *Перевірити, чи задовольняють ці параметри всім вимогам схеми?*

Задача 28. *Визначити тіні ключа за допомогою схеми розподілення секретів з параметрами, розглянутими у задачі* 27.

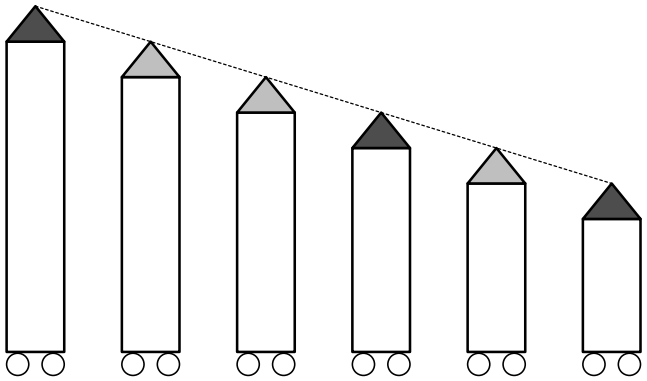
Задача 29. *Обчислити ключ* k *за будь-якою комбінацією з* $s = 2$ *тіней для порогової схеми розподілення секретів, представленої в задачі* 27 (*тіні обчислено в задачі* 28).

Задача 30. *Для визначення рівня розумового розвитку обрано групу з* $n > 1$ *учасників* $L_1, \ldots, L_n$. *Їх розташували у порядку зменшення зросту так, що кожен бачить голови усіх, кого розташовано після нього (іншими словами, голови усіх хто має менший зріст). На рисунку нижче зображено один з можливих варіантів для* $n = 6$.

Перед початком тесту кожному з учасників буде одягнуто капелюшок одного з двох кольорів, білого або чорного. Під час тесту кожен має вгадати колір свого капелюшка, сказавши тільки одне

слово "білий" або "чорний". При цьому кожен наступний чує слова, які сказали його попередники.

Перед початком тесту група збирається для обговорення спільної стратегії під час проведення тесту.



Вважається, що група пройшла тест, якщо буде правильно названо n або принаймні $n-1$ кольорів капелюшків.

a) *Чи існує стратегія, яка допоможе виконати умову тесту?*

b) *Спочатку розгляньте випадок $n = 2$.*

Зауваження. Якщо б дозволялось вимовляти інші слова, крім "білий" або "чорний", то правильною стратегією була б такою: перший називає кількість b_1 чорних капелюшків, які бачить він. Тоді наступний учасник підраховує кількість b_2 чорних капелюшків, які він бачить. Якщо $b_1 = b_2$, то він каже "білий"; в іншому випадку — "чорний". На підставі відповідей першого та другого, третій учасник знає кількість чорних капелюшків, які бачить другий, і тому діє за тією ж схемою. Аналогічно діють і всі решта учасників. Проблема при розв'язанні задачі 30 у загальному випадку полягає у тому, що не дозволяється вимовляти інших слів крім "білий" або "чорний".

9. БІОГРАФІЇ

Чаум, *Девід* (нар. 1955 р.), американський криптограф, автор чисельних криптографічних протоколів, серед яких `ecash` та `DigiCash`. Його робота "*Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms*", опублікована в 1981 році, стала основою для багатьох досліджень та розробок у галузі анонімного обміну даними. Ідею сліпого підпису обгрунтував в роботі 1982 року.

В 1989 році він (разом з Хансом ван Антверпеном) описав протокол так званих *незаперечних підписів*. Особливість процесу верифікації такого цифрового підпису полягає у тому, що верифікацію може здійснити не кожен користувач. Такі підписи ставлять розробники програмного забезпечення, для того, щоб тільки зареєстровані користувачі могли перевірити підпис (що може означати, що тільки після реєстрації/придбання з'являється можливість користуватись даним програмним продуктом).

В 1991 році він (разом з Юджином ван Хейстом) розробив протокол так званих групових підписів, який дозволяє кожному члену групи анонімно підписати повідомлення від імені всієї групи. При цьому керівник групи має право відкликати анонімність будь-кого з підписантів у разі виникнення суперечок.

Чаум є відомим також своїм визначним внеском у розробку безпечних систем голосування. В 2011 році Чаум висловив ідею рандомізованих виборів, основану на випадковому формуванні груп виборців з збереженням анонімності. При цьому результат голосування цієї групи є репрезентативним для популяції, з якої було обрано виборців.

Він є також автором концепції *доведень з нульовим знанням*. Зрозуміти цю концепцію можна на прикладі Ніколи Тарталья, який у 1535 році проголосив, що знає загальну формулу для розв'язків кубічного рівняння $ax^3 + bx^2 + cx + d = 0$. Він ніколи не опублікував цю формулу, хоча беззаперечно довів, що володіє нею, оскільки зміг розв'язати велику кількість кубічних рівнянь, запропонованих йому опонентами.

Глава 12

ПЕРЕВІРКА ЧИСЕЛ НА ПРОСТОТУ

Задача відокремлення простих чисел від складених і розкладання останніх у добуток простих множників є найбільш важливою і корисною в арифметиці.

Карл Гаусс (1801)

Метод RSA, розглянутий у главі 10, використовує дуже великі прості числа. З розвитком математичних методів та зростанням можливостей обчислювальної техніки, криптоаналіз стає можливим для таких чисел, як RSA-129 (див. §3.4, глава 10), або навіть більших. Результатом такого розвитку є зростаюча потреба у знаходженні все більших простих чисел (з метою розробки більш стійких методів шифрування). Відповіддю на використання у криптографії нових великих чисел є подальший розвиток математичних методів та розробка новітніх комп'ютерних технологій.

Цей процес може тривати безкінечно, оскільки множина простих чисел є необмеженою (див. теорему 1.2 або теорему 2.6).

Як же математики знаходять великі прості числа? Один зі способів був запропонований грецьким математиком Ератосфеном ще 22 сторіччя тому (розділ 1.4). Решето Ератосфена є досить ефективним для пошуку помірно великих простих чисел (до 10^9, наприклад), але воно не є достат-

ньо швидким способом у сучасних пошуках нових простих чисел (більших за 10^{100}, наприклад).

Перед тим, як ми перейдемо до розгляду більш ефективних алгоритмів, варто згадати, що в деяких книгах ще зовсім недавно зазначалось, що кількість простих чисел до 10^9 дорівнює 50,847,478. Насправді ж таких чисел 50,847,534. Різниця у 56 чисел не є випадковою друкарською помилкою, оскільки у майже усіх книгах, виданих до XXI сторіччя, вказувалось одне й те ж число. Мабуть автори повторювали один за другим одне і те ж (помилкове) число.

Хто ж першим припустився цієї помилки і чому? Цій помилковій інформації про кількість простих чисел ми "завдячуємо" данському математику Н. Бертельсену, який за допомогою решета Ератосфена в 1893 році нарахував на 56 простих чисел меньше, ніж їх є у дійсності. За іронією долі метою його роботи було виправити недоліки у деяких таблицях простих чисел. Замість цього він припустився помилки, яку можна знайти у багатьох книгах, виданих до 1993 року.

1. Кілька відомих способів перевірки чисел на простоту

Відомі способи перевірки натуральних чисел на простоту можна розділити на два класи:

i) використання формул, які описують прості числа, та
ii) використання критеріїв простоти чисел.

Жоден з цих способів не має практичного значення. Тим не менше, ми наводимо два приклади.

1.1. Формула Міллса. Не існує простої формули для простих чисел, проте існують доволі прості формули, які

задають не всі, але безкінечно багато простих чисел. Однією з них є *формула Міллса*, яку він знайшов у 1947 році. Він довів, що існує таке дійсне число λ, що

$$\left[\lambda^{3^n}\right] \qquad ① \tag{1}$$

є простим числом для будь-якого $n \geq 1$. Хоча результат Міллса має неабияке теоретичне значення, обчислення чисел (1) є складною задачею, оскільки обчислення λ з достатньою точністю є надто складною задачею.

1.2. Критерій Вілсона. В теорії чисел відомі кілька критеріїв простоти, жоден з яких не є достатньо ефективним з обчислювальної точки зору для того, щоб ним користуватись на практиці. Наступний *критерій Вілсона* є відомим ще з XVIII сторіччя. Цікаво, що формулювання критерію належить Е. Валлісу, а доведення — Ж. Лагранжу. Що стосується Дж. Вілсона, то він був учнем Валліса й намагався (безуспішно) довести цей критерій.

Теорема 1. *Натуральне число $n \geq 2$ є простим тоді і тільки тоді, коли*

$$(n-1)! \equiv -1 \pmod{n}. \tag{2}$$

Доведення. Нехай n є простим числом; доведемо, що виконується конгруенція (2). Оскільки будь-яке натуральне число m, $1 \leq m < n$, є взаємно простим з n, то рівняння $mx \equiv 1 \pmod{n}$ має єдиний розв'язок, який позначимо m' (див. теорему 5.1). Якщо $m = m'$, то $m^2 \equiv 1 \pmod{n}$, тобто $(m-1)(m+1) \equiv 1 \pmod{n}$. Це означає, що або

$m-1$, або $m+1$ ділиться на n. Звідси робимо висновок, що або $m=1$, або $m=p-1$. Для всіх інших m число $m' \neq m$. Таким чином, всі числа $2, \ldots, p-2$ можна розбити на пари $m \leftrightarrow m'$. Тому

$$(n-1)! = 1 \cdot (n-1) \cdot \prod_{\frac{n-1}{2} \text{ пар}} mm' \equiv n-1 \pmod{n},$$

оскільки $mm' \equiv 1 \pmod{n}$. Отримана конгруенція рівносильна (2).

Припустимо тепер, що виконано конгруенцію (2); доведемо, що n є простим числом. Якщо n не є простим числом, тобто має дільник $1 < k < n$, то $(p-1)!$ ділиться на k. З іншого боку, з конгруенції (2) випливає, що $(p-1)!+1$ ділиться на p, а отже і на k. Отримане протиріччя доводить, що n є простим числом. $\square$

2. Псевдопрості числа

Мала теорема Ферма (теорема 6.3) стверджує, що

$$a^{p-1} \equiv 1 \pmod{p},$$

якщо p є простим числом, а a не ділиться на p.

Припустимо, що нам необхідно дізнатись чи є простим деяке число n. Ми будемо напевно знати, що n не є простим числом, якщо ми зможемо знайти ціле число b, яке не ділиться на n і яке задовольняє умову $b^{n-1} \not\equiv 1 \pmod{n}$. ② Таке число b будемо називати *свідком* (того, що n не є простим числом). Таким чином, ми маємо спосіб для перевірки чи є непарне число n складеним: для кожного b,

яке не ділиться на n, необхідно знайти остачу $b^{n-1} \pmod n$ від ділення b^{n-1} на n; якщо $b^{n-1} \not\equiv 1 \pmod n$ для хоча б одного b, то n є складеним числом.

Для скорочення запису цього алгоритму, який називається *тестом Ферма*, ми використовуємо позначення $k \nmid m$, яке означає, що k не ділить m (або, іншими словами, що m не ділиться на k).

Алгоритм 1. Тест Ферма

Вхідні дані: натуральне число n;

Вихідні дані: висновок відносно простоти n;

якщо $2 \nmid n$ та $2^{n-1} \not\equiv 1 \pmod n$, то ‘‘$n$ є складеним’’ STOP.

якщо ж $3 \nmid n$ та $3^{n-1} \not\equiv 1 \pmod n$, то ‘‘$n$ є складеним’’ STOP.

якщо ж $4 \nmid n$ та $4^{n-1} \not\equiv 1 \pmod n$, то ‘‘$n$ є складеним’’ STOP.

. . . . . .

Недоліком цього алгоритму є те, що він буде працювати поки не буде знайдено свідка, тобто, як здається, необмежено довго у разі відсутності свідка. Втім для пошуку свідка достатньо випробувувати лише натуральні числа з інтервалу $1 < b \leq n-1$. ③ Оскільки n є непарним, то $(n-1)^{n-1} \equiv 1 \pmod n$, ④ тобто з пошуку можна виключити також і число $n-1$ й вважати, що в тесті Ферма еобхідно перевірити лише натуральні числа $1 < b < n-1$.

Теорема 2 (*умова складеності числа*)**.** *Нехай n — непарне натуральне число. Якщо існує таке ціле число b, що*

А) $1 < b < n-1$ *та*
В) $b^{n-1} \not\equiv 1 \pmod{n}$,

то n *є складеним числом.*

Оскільки нас більше цікавлять прості числа, а не складені, то варто задатись питанням: чи можна тест Ферма пристосувати для перевірки чисел на простоту?

Точне формулювання цього питання є таким. Припустимо, що n є непарним натуральним числом, для якого $b^{n-1} \equiv 1 \pmod{n}$ при деякому цілому b, $1 < b < n-1$. Чи є n простим числом? Вважається, що у стародавньому Китаї на це питання давали ствердну відповідь для $b = 2$.

Але ця китайська відповідь є невірною!

Приклад 1. Все ж таки треба віддати належне інтуіції китайських математиків, оскільки для більшості випадків їхня гіпотеза справджується.

Нехай $n = 7$. Тоді $2^{7-1} = 64 \equiv 1 \pmod{7}$ і тому 7 є простим числом згідно китайської гіпотези (це ясно і без неї!). Якщо ж $n = 9$, то $2^{9-1} = 256 \equiv 5 \pmod{9}$ і тому 9 не є простим числом згідно до теореми 2. Далі, $2^{11-1} = 1024 \equiv 1 \pmod{11}$ і китайська гіпотеза знову є вірною.

Приклад 2. Китайська гіпотеза є вірною для всіх чисел $n < 341$. При $n = 341$ маємо $2^{341-1} \equiv 1 \pmod{341}$, ⑤ але $341 = 11 \cdot 31$ є складеним числом, тобто при $b = 2$ метод Ферма для визначення простоти не спрацьовує для $n = 341$ і китайська гіпотеза є хибною.

Означення 1. Будь-яке непарне складене число n, для якого $b^{n-1} \equiv 1 \pmod{n}$ для деякого цілого b, $1 < b < n-1$, називають *псевдопростим за основою* b.

Таким чином, 341 є псевдопростим за основою 2.

Без сумніву, китайський метод є корисним, хоча він і не є абсолютно точним. Для малих n, обраних випадковим чином, такий спосіб частіше дає правильну відповідь, ніж неправильну. Дійсно, між 1 та 10^9 є 50,847,534 простих чисел й лише 5597 псевдопростих за основою 2. Таким чином, число з цього проміжка, яке витримало китайський тест, є скоріше простим, ніж псевдопростим за основою 2.

Крім того, якщо застосувати цей тест не для однієї основи, а для кількох, то кількість невірних відповідей зменшиться ще більше. Наприклад, $3^{341-1} \equiv 56 \pmod{341}$, тобто 3 є свідком для числа 341 (тобто, 3 свідчить про те, що 341 є складеним числом). Нагадаємо, що 2 не є свідком для числа 341 (приклад 2).

Додамо, що між 1 и 10^9 є 1272 псевдопростих за двома основами 2 и 3 й тільки 685 псевдопростих за трьома основами 2, 3 и 5. Чи існує хоча б одне натуральне n, яке є псевдопростим за довільною основою? Іншими словами,

(3) чи існують складені числа n, які є псевдопростими за кожною з основ $2, 3, \ldots, n-2$? ⑥

Відповідь на це питання є негативною.

Теорема 3. *Нехай $n > 2$. Якщо $b^{n-1} \equiv 1 \pmod{n}$ для будь-якого $1 < b < n-1$, то n є простим числом.*

Доведення. Оскільки $b^{n-1} = b \cdot b^{n-2}$, то з умови теореми випливає, що існує обернене $b^{-1} \pmod{n}$. ⑦ Теорема про існування оберненого числа (теорема 3.1) стверджує, що це можливо лише у випадку $(b, n) = 1$. Але якщо n було б

складеним, то кожен з його дільників не задовольняв би цю умову. ⑧ □

Теорему 3 можна використати для доведення простоти заданого числа n. Але, якщо n має невеликий дільник, то для цього простіше виконати алгоритм 1 з глави 1 й перевірити чи є число складеним. У будь-якому випадку простіше знайти дільник великого числа n, ніж перевірити, що воно не є псевдопростим для кожного $1 < b < n - 1$.

3. Числа Кармайкла

Якщо $(b, n) \neq 1$, то n не може бути псевдопростим за основою b. ⑨ Якщо ж число b є взаємно простим з n, то конгруенція $b^n \equiv b \pmod{n}$ після скорочення на b зводиться до $b^{n-1} \equiv 1 \pmod{n}$. ⑩ Тому питання (3) можна у цьому випадку поставити таким чином:

(4) чи існує таке непарне складене число n, для якого $b^n \equiv b \pmod{n}$ для всіх цілих b?

Хоча питання (3) та (4) є схожими, відповіді на них є абсолютно різними.

Відомо, що числа n, які мають властивість (4), існують. Першим, хто детально дослідив (у 1912 році) такі числа був американський математик Р. Д. Кармайкл. Тому зараз вони називаються *числами Кармайкла*, хоча про існування таких чисел знали і до нього.

Означення 2. Непарне натуральне n називають числом Кармайкла, якщо воно є складеним та $b^n \equiv b \pmod{n}$ для всіх цілих b.

Зауважимо, що, як і у випадку тесту Ферма, перевірку конгруенції в означенні 2 необхідно здійснювати лише для $1 < b < n - 1$. ⑪

3.1. Найменше з чисел Кармайкла. Сам Кармайкл знайшов, що найменшим з розглянутих ним чисел є 561. Цей факт можна було б перевірити безпосередньо, виходячи з означення 2. Але ця процедура не є оптимальною, оскільки необхідно перевіряти конгруенції $b^{561} \equiv b \pmod{561}$ для $b = 2, 3, 4, \ldots, 559$, тобто зробити 558 доволі складних обчислень. Існує більш розумний шлях.

Перш за все, число 561 нескладно факторизувати:

$$561 = 3 \cdot 11 \cdot 17.$$

Тепер будемо перевіряти конгруенції

$$b^{561} \equiv b \pmod{561}. \tag{5}$$

Ми доведемо, що $b^{561} - b$ ділиться на кожне з чисел 3, 11 та 17. Оскільки ці три числа є простими, то $b^{561} - b$ повинно ділитися на їхній добуток 561. ⑫ Цим самим властивість (5) буде доведено.

Спочатку доведемо, що $b^{561} - b$ ділиться на 17, тобто

$$b^{561} \equiv b \pmod{17}. \tag{6}$$

Розглянемо два випадки:

Випадок 1: *число b ділиться на 17.* Тоді обидві частини конгруенції (6) діляться на 17, тобто (6) є вірною.

Випадок 2: *число b не ділиться на 17.* Тоді з малої теореми Ферма випливає, що $b^{16} \equiv 1 \pmod{17}$. Оскільки $561 = 35 \cdot 16 + 1$, то

$$b^{561} \equiv \left(b^{16}\right)^{35} \cdot b \pmod{17} = b \pmod{17}.$$

Теорема Ферма настільки сильно зменшила наші обчислення через те, що остача від ділення 561 на $16 = 17 - 1$ дорівнює 1. Таку ж властивість мають й інші прості дільники числа 561, тобто $561 \equiv 1 \pmod 3$ та $561 \equiv 1 \pmod{11}$. Тому обчислення, що залишились, є дослівним повторенням того, що ми вже здійснили для перевірки конгруенції (6). ⑬

3.2. Необмеженість множини чисел Кармайкла. В своїй роботі 1912 року Кармайкл писав, що існує безкінечно багато досліджених ним чисел, але не наводив жодного обгрунтування своєї гіпотези. Його гіпотеза чекала свого доведення більше 80 років: тільки в 1994 році В. Альфорд, Е. Гранвиль та К. Померанц довели її істинність.

3.3. Теорема Корселта. Як зрозуміти чи є задане n числом Кармайкла? Відповідь на це питання була дана німецьким математиком А. Корселтом за п'ятнадцять років до (!) публікації роботи Кармайкла на цю тему.

Теорема 4 (*Корселт*). *Непарне натуральне число n є числом Кармайкла тоді і тільки тоді, коли для кожного його простого дільника p виконано наступні дві умови*:

А) *n не ділиться на p^2*;
В) *$n - 1$ ділиться на $p - 1$.*

Щоб використати теорему Корселта, необхідно факторизувати число n, тобто знайти всі його прості дільники, а це є складною задачею, якщо n є великим. З іншого боку, існують великі числа Кармайкла, які мають невеликі дільники й для яких теорема Корселта є корисною. Таким числом, наприклад, є ⑭

(7) $11{\cdot}13{\cdot}17{\cdot}19{\cdot}29{\cdot}31{\cdot}37{\cdot}41{\cdot}43{\cdot}61{\cdot}71{\cdot}73{\cdot}97{\cdot}101{\cdot}109{\cdot}113{\cdot}151{\cdot}181{\cdot}193{\cdot}641.$

Доведення теореми 4. Покажемо спочатку, що якщо n задовольняє умови A) та B), то воно є числом Кармайкла. Нехай p — простий дільник числа n. Тоді для будь-якого $b \in \mathbf{N}$

$$b^n \equiv b \pmod{p}. \tag{8}$$

Дійсно, якщо b ділиться на p, то конгруентність (8) очевидна, оскільки обидва числа b та b^n діляться на p.

Якщо ж b не ділиться на p, то з малої теореми Ферма (теорема 6.3) випливає, що $b^{n-1} \equiv 1 \pmod{n}$. Далі, $n-1 = (p-1)q$ для деякого цілого q згідно умові B) й тому

$$n = (n-1) + 1 = (p-1)q + 1.$$

Звідси

$$b^n = \left(b^{p-1}\right)^q \cdot b \equiv b \pmod{p}$$

(друга конгруенція є вірною на підставі малої теореми Ферма ⑮). Таким чином, властивість (8) повністю доведено.

Тепер з умови A) отримуємо $n = p_1 \dots p_k$, де $p_1, \dots, p_k$ — різні прості числа. Оскільки $b^n - b$ ділиться на кожне з цих чисел, то $b^n - b$ ділиться на добуток $p_1 \dots p_k = n$. Іншими словами, $b^n \equiv b \pmod{n}$. У цьому міркуванні b є довільним, тому n є числом Кармайкла.

Покажемо, що довільне число Кармайкла задовольняє умову A). Нехай $n > 2$ є числом Кармайкла. Покажемо, що припущення про те, що n ділиться на p^2 для деякого свого простого дільника p, приводить до протиріччя. Ми отримаємо зазначене протиріччя, якщо знайдемо таке ціле b, для якого $b^n \not\equiv b \pmod{n}$.

У якості такого числа b можна обрати сам дільник p, тобто візьмемо $b = p$. Тоді $p^n \equiv p \pmod{n}$, оскільки є числом Кармайкла. Звідси та на підставі $p^2 \mid n$ випливає $p^n \equiv p \pmod{p^2}$. ⑯ Це протирічить конгруенції $p^n \equiv 0 \pmod{p^2}$ при $n > 2$. Тепер робимо висновок про те, що $p^n \not\equiv p \pmod{n}$, а це є неможливим для числа Кармайкла. Звідси ми отримуємо $p^2 \nmid n$.

Доведення умови B) для будь-якого числа Кармайкла спирається на теорему про примітівні корені (означення див. в §7.1, глава 10). Деталі цієї частини доведення ми не наводимо. Повне доведення цієї частини теореми можна знайти у багатьох підручниках з теорії чисел (див., наприклад, [20]). □

Зауваження 1. Числа Кармайкла зустрічаються не часто у послідовності натуральних чисел. Наприклад, існує тільки 105,212 чисел Кармайкла, які є меншими за один квадрильйон, тобто за 1,000,000,000,000,000 (якби таких чисел Кармайкла було в мільйон разів більше, то це складало б лише 1% від загальної кількості натуральних чисел від 1 до одного квадрильйона). Тим не менше, як ми зазначили в §3.2, множина чисел Кармайкла є необмеженою.

4. Тест Соловея–Штрассена

Щоб уникнути проблеми кармайклових чисел, які неможливо відрізнити від простих за допомогою малої теореми Ферма, Р. Соловей та Ф. Штрассен в 1977 році запропонували метод, оснований на використанні так званого *символа Якобі*, який є узагальненням *символа Лежандра*.

Означення 3. Число a називається *квадратичним лиш-*

ком за модулем n, якщо існує таке x, що

$$x^2 \equiv a \pmod{n}. \tag{9}$$

В іншому випадку a називається *квадратичним нелишком* за модулем n. Множину квадратичних лишків за модулем n позначимо через $\operatorname{qres}(n)$.

Нехай p — непарне просте число. *Символом Лежандра* натурального числа a за модулем p називається число

$$\operatorname{Leg}(a,p) = \begin{cases} 1, & \text{якщо } a \in \operatorname{qres}(p) \text{ та } a \not\equiv 0 \pmod{p}, \\ -1, & \text{якщо } a \notin \operatorname{qres}(p) \text{ та } a \not\equiv 0 \pmod{p}, \\ 0, & \text{якщо } a \equiv 0 \pmod{p}. \end{cases}$$

Якщо канонічним представленням натурального числа n у добуток простих дільників є $n = p_1 p_2 \dots p_k$, то символ Якобі (позначається тим же чином, що і символ Лежандра) дорівнює

$$\operatorname{Jac}(a,n) = \operatorname{Leg}(a,p_1)\operatorname{Leg}(a,p_2)\dots\operatorname{Leg}(a,p_k).$$

4.1. Тест Соловея–Штрассена. Алгоритм Соловея–Штрассена використовує випадково обране натуральне число a й робить один з двох висновків: ‘‘можливо n є простим’’ або ‘‘n є складеним’’.

Перший з цих висновків не здається корисним: більш важливим для нас був би висновок ‘‘n є простим’’, але алгоритм 2 зробити його не в змозі. Процедуру Соловея–Штрассена можна повторити кілька разів, якщо кожного разу її висновком є ‘‘можливо n є простим’’. Повторивши процедуру достатню кількість разів й отримавши кожного разу цей

висновок, ми з достатньою впевненістю вважаємо, що ‘‘n є простим’’ (див. §4.4).

Алгоритм 2. Тест Соловея–Штрассена

Вхідні дані: непарне число $n > 2$;

Вихідні дані: один з двох висновків, а саме ‘‘n є складеним’’ або ‘‘можливо n є простим’’;

обрати випадкове число $1 < a < n - 1$;

якщо $(a, n) > 1$ або $a^{(n-1)/2} \not\equiv \operatorname{Jac}(a, n) \pmod{n}$,

то висновком є ‘‘n є складеним’’;

інакше висновком є ‘‘можливо n є простим’’.

Висновок, який робить алгоритм 2, пояснюється наступним результатом (ми доводимо його нижче).

Теорема 5 (*Ойлер*). *Нехай p — просте число, а a — ціле. Тоді*

$$a^{(p-1)/2} \equiv \operatorname{Leg}(a, p) \pmod{p}. \tag{10}$$

Зауваження 2. Конгруенція (10) є цілком зрозумілою, якщо $(a, p) > 1$. В цьому випадку a ділиться на p, тобто $\operatorname{Leg}(a, p) = 0$ за означенням символу Лежандра; зрозуміло також, що $a^{(p-1)/2} \equiv 0 \pmod{p}$.

Приклад 3. Нехай $n = 7$. У наступних таблицях наведено значення $b \equiv a^{(n-1)/2} \pmod{7}$ для $a = 2, 3, 4, 5, 6$, а

також $y \equiv x^2 \pmod 7$ для $x = 2, 3, 4, 5, 6$:

a	2	3	4	5	6
b	1	-1	1	-1	1

x	2	3	4	5	6
y	4	2	2	4	1

З другої таблиці робимо висновок про те, що

$$\begin{aligned}
&\mathrm{Leg}\,(2,7) = 1, \quad \text{оскільки} \quad 4^2 \equiv 2 \pmod 7;\\
&\mathrm{Leg}\,(3,7) = -1, \quad \text{оскільки} \quad x^2 \not\equiv 3 \pmod 7 \quad \text{для } x \le 6;\\
&\mathrm{Leg}\,(4,7) = 1, \quad \text{оскільки} \quad 2^2 \equiv 4 \pmod 7;\\
&\mathrm{Leg}\,(5,7) = -1, \quad \text{оскільки} \quad x^2 \not\equiv 5 \pmod 7 \quad \text{для } x \le 6;\\
&\mathrm{Leg}\,(6,7) = 1, \quad \text{оскільки} \quad 6^2 \equiv 6 \pmod 7.
\end{aligned}$$

Порівнюючи ці результати з першою таблицею, бачимо, що $b = \mathrm{Leg}\,(a, 7)$ для будь-якого $1 < a < 7$, тобто висновком тесту Соловея–Штрассена буде ‘‘можливо n є простим’’ для будь-якого $1 < a < 7$. Таким чином, алгоритм Соловея–Штрассена кожного разу робить один і той же висновок, що додає нам впевненості у тому, що ‘‘n є простим’’.

Приклад 4. Нехай $n = 9$. У наступних таблицях наведено значення $b \equiv a^{(n-1)/2} \pmod 9$ для $a = 2, 3, 4, 5, 6, 7, 8$, а також $y \equiv x^2 \pmod 9$ для $x = 2, 3, 4, 5, 6, 7, 8$:

a	2	3	4	5	6	7	8
b	7	0	4	4	0	7	1

x	2	3	4	5	6	7	8
y	4	0	7	7	0	4	1

З цих таблиць видно, що $b \ne \mathrm{Jac}\,(a, 9)$ для $a = 2, 4, 5, 7$, оскільки $b \notin \{-1, 0, 1\}$. Крім того, $(a, 9) > 1$ для $a = 3, 6$. Тому висновком алгоритму 2 є ‘‘n є складеним’’, якщо $a = 2, 3, 4, 5, 6, 7$. Якщо ж $a = 8$, то висновком алгоритму 2 є

‘‘можливо n є простим’’. Таким чином, в одному випадку з 8 алгоритм Соловея–Штрассена не дасть певну відповідь. Одне з його повторень обов'язково буде виконано з $a \neq 8$ й тому врешті буде зроблено правильний висновок, що ‘‘n є складеним’’. ⑰

4.2. Оптимальність тесту Соловея–Штрассена. Існування кармайклових чисел є неприємним фактом для тесту Ферма, оскільки для кожного кармайклового числа n тест Ферма дає відповідь ‘‘можливо n є простим’’, яким би не було a. Чи існують подібні числа для алгоритму Соловея–Штрассена? Виявляється, що таких чисел не існує: якби ми дозволили алгоритму 2 перевірити усі можливі натуральні a, то його висновок був би абсолютно правильним: або на певному кроці висновком було би ‘‘n є складеним’’, або на кожному кроці висновком було би ‘‘можливо n є простим’’. Другий випадок, на відміну від тесту Ферма, означає, що ‘‘n є простим’’. Це випливає з такої теореми.

Теорема 6 (*Соловей, Штрассен*)**.** *Нехай n — непарне складене натуральне число. Тоді існує ціле a, яке є взаємно простим з n та задовольняє співвідношення*

$$a^{(n-1)/2} \not\equiv \operatorname{Jac}(a,n) \pmod{n}, \tag{11}$$

Для доведення теореми 6 нам необхідні наступні факти стосовно квадратичних лишків.

Лема 1. *Припустимо, що p — непарне просте число. Нехай a є таким, що $(a,p) = 1$ та існує розв'язок рівняння* (9)*. Тоді рівняння* (9) *має рівно два розв'язки за модулем p.*

Лема 2. *Припустимо, що p — непарне просте число. Серед чисел $1, 2, \ldots, p-1$ квадратичних лишків стільки ж, скільки квадратичних нелишків.*

Доведення леми 1. Оскільки $(a, p) = 1$, то $a \not\equiv 0 \pmod{p}$ і тому розв'язок x рівняння (9) є таким, що $x \not\equiv 0 \pmod{p}$. ⑱ Легко бачити, що $-x \pmod{p}$ також є розв'язком рівняння (9). ⑲ Ясно, що $x \pmod{p} \neq -x \pmod{p}$, бо інакше $2x = x - (-x) \equiv 0 \pmod{p}$, чого не може бути, оскільки p є непарним, а $x \not\equiv 0 \pmod{p}$.

Нарешті, якщо існує ще один (третій) розв'язок рівняння (9) (позначимо його через y), то $x^2 - y^2 \equiv 0 \pmod{p}$. Це означає, що або $x - y \equiv 0 \pmod{p}$, або $x + y \equiv 0 \pmod{p}$. Перший випадок означає, що $y \equiv x \pmod{p}$, а другий — що $y \equiv -x \pmod{p}$. Таким чином, рівняння (9) дійсно має тільки два розв'язки. □

Доведення леми 2. Нехай $A = \left\{1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2\right\}$. Квадратичними лишками можуть бути тільки ті числа a, для яких $a^2 \equiv z \pmod{p}$ для деякого $z \in A$. Це твердження є очевидним, якщо $a \leq (p-1)/2$, оскільки в цьому випадку $a^2 \in A$. Якщо ж $(p-1)/2 < a < p$, то $p - a \leq \frac{p-1}{2}$ й тому $(p-a)^2 \in A$ й $a^2 \equiv (p-a)^2 \pmod{p}$. Тому кількість квадратичних лишків дорівнює кількості елементів в множині A.

Покажемо, що $|A| = \frac{p-1}{2}$. Якби це було не так, то знайшлися б два натуральних числа k та l, $1 \leq k < l \leq \frac{p-1}{2}$, для яких $k^2 \equiv l^2 \pmod{p}$. Тоді рівняння $x^2 \equiv l^2 \pmod{p}$ мало б чотири розв'язки $x = \pm l$ та $x = \pm k$, що протирічило б лемі 1. Таким чином, всі елементи множини A є різними й тому $|A| = \frac{p-1}{2}$. □

Доведення теореми 6. Ми доведемо теорему лише для випадку $n = pq$, де p та q є різними простими числами. У загальному випадку необхідно окремо розглянути випадок, коли канонічний розклад n у добуток простих дільників містить множники вигляду p^2.

Оберемо довільний квадратичний нелишок за модулем p (він існує згідно до леми 2), тобто ми обираємо b, для якого $(b, p) = 1$ та $\mathrm{Leg}\,(b, p) = -1$. За китайською теоремою про остачі (теорема 5.5) існує розв'язок a системи

$$\begin{cases} a \equiv b \pmod{p}, \\ a \equiv 1 \pmod{q}. \end{cases}$$

Зрозуміло, що $(a, p) = 1$, ⑳ звідки $(a, n) = 1$. ㉑ Крім того,

$$\mathrm{Leg}\,(a, p) = \mathrm{Leg}\,(b, p) = -1, \quad \mathrm{Leg}\,(a, q) = \mathrm{Leg}\,(1, q) = 1. \quad ㉒$$

Тому $\mathrm{Jac}\,(a, n) = -1$. ㉓ Припустимо, що тим не менше

$$a^{(n-1)/2} \equiv \mathrm{Jac}\,(a, n) \pmod{n}$$

або іншими словами, що $a^{(n-1)/2} \equiv -1 \pmod{pq}$. Звідси $a^{(n-1)/2} \equiv -1 \pmod{q}$. ㉔ Оскільки $a \equiv 1 \pmod{q}$ за означенням a, то $1 \equiv -1 \pmod{q}$. Цього не може бути для $q > 2$. □

4.3. Обгрунтування тесту Соловея–Штрассена. Для обгрунтування алгоритму Соловея–Штрассена ми доводимо теорему 5.

Доведення теореми 5. Якщо $(a, p) > 1$, то $a = cp$ для деякого $c \in \mathbf{N}$, звідки випливає, що $a^{\frac{p-1}{2}} \equiv 0 \pmod{p}$. Тому далі розглядатимемо лише випадок $(a, p) = 1$. В цьому

випадку з малої теореми Ферма (теорема 6.3) отримуємо $a^{p-1} \equiv 1 \pmod{p}$, звідки

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod{p}.$$

Це означає, що виконано одну з двох конгруенцій

$$(12) \qquad a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \quad \text{або} \quad a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Доведемо, що перша конгруенція в (12) є еквівалентною тому, що $\operatorname{Leg}(a,p) = 1$ або $a \in \operatorname{qres}(p)$.

По-перше, якщо $a \in \operatorname{qres}(p)$, то існує таке натуральне число x, що $x^2 \equiv a \pmod{p}$. Тому

$$a^{\frac{p-1}{2}} = x^{p-1} \pmod{p} = 1,$$

оскільки $(x,p) = 1$. ㉕ Тому першу конгруенцію в (12) виконано.

По-друге, нехай $a \notin \operatorname{qres}(p)$ й $a \not\equiv 0 \pmod{p}$. Оберемо довільне натуральне число $b \in \{1, 2, \ldots, p-1\}$. Оскільки $(b,p) = 1$, то рівняння $bx \equiv a \pmod{p}$ має єдиний розв'язок (див. теорему 5.1). Позначимо цей розв'язок через b'. Зауважимо, що $b' \neq b$ (інакше $b^2 \equiv a \pmod{p}$ й $a \in \operatorname{qres}(p)$). Таким чином, всі числа $1, 2, \ldots, p-1$ можна розбити на пари за правилом $b \leftrightarrow b'$. Тому

$$(p-1)! = \prod_{\frac{p-1}{2} \text{ пар}} bb' \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

З іншого боку, $(p-1)! \equiv -1 \pmod{p}$ за теоремою Вільсона (теорема 1), тому для $a \notin \operatorname{qres}(p)$ виконана друга конгруенція в (12). $\square$

4.4. Кілька ітерацій тесту Соловея–Штрассена. Відповідь ‘‘n є складеним’’ завжди є точною в алгоритмі 2. Інша відповідь ‘‘можливо n є простим’’ є непевною. Алгоритм можна повторити кілька разів, якщо кожного разу його висновком є ‘‘можливо n є простим’’. Якщо цей висновок інтерпретувати як ‘‘n є простим’’, то на кожному кроці може виникнути помилка, ймовірність якої є меншою за $1/2$ (теорема 7). Якщо алгоритм 2 повторити l разів, то ймовірність помилки буде меншою за $1/2^l$. Обираючи l достатньо великим, ймовірність помилки можна зробити як завгодно малою. Наприклад, вже для $l = 10$ ймовірність помилки є меншою за $\frac{1}{1000}$.

Теорема 7 (*Соловей, Штрассен*)**.** *Нехай n — непарне натуральне число. Позначимо через A множину*

$$\left\{1 \le a < n : (a,n) = 1,\ a^{(n-1)/2} \equiv \operatorname{Jac}(a,n) \pmod{n}\right\}.$$

Тоді $|A| < \frac{n-1}{2}$.

Теорема 7 означає, що більше половини чисел від 1 до $n-1$ або не є взаємно простими з n, або задовольняють умову (11). Іншими словами, якщо висновок ‘‘можливо n є простим’’ в алгоритмі 2 замінити на ‘‘n є простим’’, то для більше ніж половини чисел $1 \le a < n$ він буде правильним, тобто якщо a обрати випадковим чином, то ймовірність помилки при такому висновку є меншою за $\frac{1}{2}$.

Доведення теореми 7. Нагадаємо, що $\operatorname{Jac}(a,n) = \pm 1$, якщо a та n є взаємно простими, й $\operatorname{Jac}(a,n) = 0$, якщо $(a,n) > 1$. Нехай B — це множина

$$\left\{1 \le a < n : (a,n) = 1,\ a^{(n-1)/2} \not\equiv \operatorname{Jac}(a,n) \pmod{n}\right\},$$

а $C = \{1 \le a < n : (a, n) > 1\}$. Множини A, B та C не перетинаються, а їхнім об'єднанням є $\{1, 2, \ldots, n-1\}$. Множина A не порожня, оскільки $1 \in A$; множина C не порожня, оскільки n є складеним числом. За теоремою 6 множина B також непорожня. Зафіксуємо довільне $b_0 \in B$. Тоді для будь-якого $a \in A$ число ab_0 є взаємно простим з n, причому

$$(ab_0)^{(n-1)/2} \equiv \mathrm{Jac}\,(a, n) b_0^{(n-1)/2} \pmod{n}.$$

Зрозуміло, що $ab_0 \pmod{n} \in A \cup B$. ㉖ Доведемо, що $ab_0 \pmod{n} \in B$. Якщо навпаки $ab_0 \pmod{n} \in A$, то

$$(ab_0)^{(n-1)/2} \equiv \mathrm{Jac}\,(ab_0, n) \equiv \mathrm{Jac}\,(a, n)\,\mathrm{Jac}\,(b_0, n) \pmod{n}.$$

Зауважимо, що $(a, n) = 1$ й тому $\mathrm{Jac}\,(a, n) = \pm 1$. Порівнюючи останні два співвідношення, отримуємо

$$\mathrm{Jac}\,(b_0, n) \equiv b_0^{(n-1)/2} \pmod{n}.$$

Це протирічить умові $b_0 \in B$, тобто насправді вірним є включення $ab_0 \pmod{n} \in B$ для довільного числа $a \in A$ і тому $Ab_0 \subset B$, де

$$Ab_0 = \{ab_0 \pmod{n} : a \in A\}.$$

Нехай a та a' — це два різних натуральних числа з множини A. Тоді й $ab_0 \not\equiv a'b_0 \pmod{n}$. Дійсно, якщо припустити, що $ab_0 \equiv a'b_0 \pmod{n}$, то отримаємо $a \equiv a' \pmod{n}$, звідки $a = a'$, оскільки $a, a' < n$. Тому кількість елементів в множині Ab_0 дорівнює $|A|$. Тепер з доведеного включення $Ab_0 \subset B$ ми отримуємо $|A| = |Ab_0| \le |B|$. Таким чином,

$$n - 1 = |A| + |B| + |C| \ge |A| + |A| + 1 > 2|A|,$$

тобто $|A| < \frac{n-1}{2}$, що і треба було довести. □

Приклад 5. Нехай $n = 5,605,236$. Нижче наведено обчислення для трьох випадково обраних a. Для перших двох чисел a виявилось, що $a^{(n-1)/2} \equiv \mathrm{Jac}\,(a,n) \pmod{n}$: це свідчить про те, що ‘‘можливо n є простим’’. Для третього числа a вийшло $a^{(n-1)/2} \not\equiv \mathrm{Jac}\,(a,n) \pmod{n}$: це свідчить про те, що насправді ‘‘n є складеним’’.

a	$a^{(n-1)/2} \pmod{n}$	$\mathrm{Jac}\,(a,n)$
40715161	1	1
18267097	1	1
55146139	1	-1

Зауважимо, що алгоритм Соловея–Штрассена лише стверджує, що число 5605236 є складеним, але його дільники не знаходить. Насправді ж, $5605236 = 2^2 \cdot 3^2 \cdot 7 \cdot 13 \cdot 29 \cdot 59$.

Приклад 6. Нехай $n = 7,427,466,391$. Нижче наведено обчислення для десяти випадково обраних a. Для всіх з них виявилось, що $a^{(n-1)/2} \equiv \mathrm{Jac}\,(a,n) \pmod{n}$.

a	$a^{(n-1)/2} \pmod{n}$	$\mathrm{Jac}\,(a,n)$
3402235571	1	1
2277339183	1	1
3511612661	1	1
1892495979	-1	-1
735536755	1	1
966099371	-1	-1
3288169902	1	1
3037671250	-1	-1
270193898	1	1
7427466390	-1	-1

В цьому випадку алгоритм Соловея–Штрассена не дає певної відповіді стосовно простоти n, але якби n було б складеним, то шанси отримати такі результати, як у таблиці, не

перевищували $1/2^{10} \approx 0.00097$. Насправді ж 7427466391 є простим числом.

Зауваження 3. У наведених прикладах ми не пояснювали як можна обчислити символи Лежандра та Якобі. Для наших цілей це неактуально, оскільки існує метод перевірки чисел на простоту, оснований на зовсім іншій ідеї.

5. Тест Міллера

В 1976 році Г. Міллер запропонував у своїй кандидатський дисертації новий спосіб для перевірки простоти натуральних чисел.

Подібно до методу Соловея–Штрассена, не всі натуральні числа можна перевірити на простоту способом Міллера, оскільки у багатьох випадках його висновком є $\boxed{?}$ (скорочення для ‘‘можливо n є простим’’). Може навіть скластися враження, що результат, відмінний від $\boxed{?}$, можна отримати лише у виключних нечисельних випадках. Проте, теорема 8 свідчить, що невизначена відповідь $\boxed{?}$ отримується втричі рідше за певну відповідь.

Перевагою метода Міллера є набагато менша ймовірність помилкового висновку при такій же кількості ітерацій, як у тесті Соловея–Штрассена. Крім того, метод Міллера не використовує символи Якобі, обчислення яких потребує певного часу, і тому є більш ефективним, ніж тест Соловея–Штрассена.

Рандомізована версія алгоритму Міллера (див. розділ 6) і до цього часу є фаворитом серед всіх відомих методів перевірки натуральних чисел на простоту. За швидкістю обчислень жоден з детермінованих алгоритмів не може скласти йому конкуренцію.

Алгоритм 3. Тест Міллера

Вхідні дані: непарне натуральне число $n \geq 5$ й основа b,
натуральне число $1 < b < n-1$;

Вихідні дані: висновок ‘‘n є складеним’’ або $\boxed{?}$;

знаходимо k та непарне q, для яких $n-1 = 2^k q$;

покладемо $r_0 = b^{2^0 q} \pmod{n}$;

якщо $r_0 = 1$, то $\boxed{?}$ STOP.

якщо ж $r_0 \neq 1$, то покладемо $r_1 = b^{2^1 q} \pmod{n}$;

якщо $r_1 = n-1$, то $\boxed{?}$ STOP.

якщо ж $r_1 \neq n-1$, то покладемо $r_2 = b^{2^2 q} \pmod{n}$;

якщо $r_2 = n-1$, то $\boxed{?}$ STOP.

якщо ж $r_2 \neq n-1$, то покладемо $r_3 = b^{2^3 q} \pmod{n}$;

. . . . . .

якщо $r_{k-1} = n-1$, то $\boxed{?}$ STOP.

якщо ж $r_{k-1} \neq n-1$, то ‘‘n є складеним’’ STOP.

Останньою дією алгоритму 3 може стати перевірка рівності $r_{k-1} = n-1$: якщо вона є невірною, то висновком алгоритму є ‘‘n є складеним’’; якщо ж вірною — то висновком є $\boxed{?}$, тобто ‘‘неможливо встановити чи є n простим числом’’.

У випадку $\boxed{?}$ можливі дві ситуації: або n є простим, або n є складеним. Друга ситуація реально може виникнути для певних чисел n.

Доведення алгоритму Міллера. Нехай $n \geq 5$ — непарне на-

туральне число. Нехай $1 < b < n-1$. Оскільки n є непарним, то $n-1$ є парним. Першою дією алгоритма Міллера є знаходження такого $k \geq 1$, що $n-1 = 2^k q$ для деякого непарного числа q. ㉗.

У подальшому алгоритм обчислює остачі при діленні на n для членів послідовності

$$b^{2^0 q}, \quad b^{2^1 q}, \quad \ldots, \quad b^{2^{k-1} q}. \tag{13}$$

З'ясуємо, які властивості має ця послідовність, якщо n є простим числом. В цьому випадку з малої теореми Ферма (теорема 6.3) випливає

$$b^{2^k q} = b^{n-1} \equiv 1 \pmod{n},$$

тобто остача при діленні $b^{2^k q}$ на n обов'язково дорівнює 1. Серед остач $r_0, r_1, \ldots, r_{k-1}$ можуть бути й інші, які дорівнюють 1. Позначимо через j найменше число, для якого $r_j = b^{2^j q} \equiv 1 \pmod{n}$. Якщо $j = 0$, то $r_0 = b^q \equiv 1 \pmod{n}$. Якщо ж $j \geq 1$, то

$$b^{2^j q} - 1 = \left(b^{2^{j-1} q} - 1\right)\left(b^{2^{j-1} q} + 1\right).$$

Оскільки n — просте число і є дільником різниці квадратів $b^{2^j q} - 1$, ㉘ то воно є дільником або $b^{2^{j-1} q} - 1$, або $b^{2^{j-1} q} + 1$. ㉙ Зауважимо також, що n не може бути дільником $b^{2^{j-1} q} - 1$. ㉚ Тому залишається тільки одна можливість: n є дільником числа $b^{2^{j-1} q} + 1$, тобто

$$b^{2^{j-1} q} \equiv -1 \pmod{n} \equiv n-1 \pmod{n}.$$

Ці міркування доводять, що якщо n є простим числом, то серед членів послідовності

$$b^{2^1 q}, \quad b^{2^2 q}, \quad \ldots, \quad b^{2^{k-1} q}$$

знайдеться хоча б одне число, конгруентне з $n-1$ за модулем n.

Таким чином, якщо n є простим числом, то або перший же член послідовності остач при діленні чисел (13) на n дорівнює 1, або у цій послідовності з'явиться такий, що дорівнює $n-1$. Іншими словами, якщо $b^{2^0 q} \not\equiv 1 \pmod{n}$ та

$$b^{2^1 q} \not\equiv n-1 \pmod{n}, \quad \ldots, \quad b^{2^{k-1} q} \not\equiv n-1 \pmod{n},$$

то n є складеним числом. $\square$

Зауваження 4. Для обчислення остач у тесті Міллера немає потреби застосовувати на кожному кроці алгоритм 4.1 (алгоритм Евкліда знаходження частки та остачі), оскільки кожна наступна остача дорівнює квадрату попередньої за модулем n. Дійсно, $b^{2^j q} = \left(b^{2^{j-1} q}\right)^2$ при $j \geq 1$.

До речі, звідси випливає, що як тільки у послідовності остач за модулем n зустрінеться число $n-1$, то всі решта дорівнюють 1. ㉛

Приклад 7. Ми бачили у прикладі 2, що хоча число 341 не є простим, воно є псевдопростим за основою 2. Який же висновок робить тест Міллера стосовно цього числа? Маємо $340 = 2^2 \cdot 85$, тобто $k = 2$, $q = 85$. Тепер

$$\begin{aligned} r_0 &= 2^{85} \pmod{341} \equiv 32 \pmod{341}, \\ r_1 &= 2^{170} \pmod{341} \equiv 32^2 \pmod{341} = 1. \end{aligned}$$

㉜ Оскільки $r_0 \neq 1$ та $r_{k-1} \neq n-1$, то на підставі тесту Міллера робимо висновок про те, що 341 є складеним числом.

Приклад 8. Перевіримо число Кармайкла 561 на тесті Міллера з основою 2. Перш за все, $560 = 2^4 \cdot 35$, тобто $k = 4$, $q = 35$. Тепер обчислимо остачі r_0, r_1, r_2, r_3 від ділення чисел $b^{2^0 q}, b^{2^1 q}, b^{2^2 q}, b^{2^3 q}$ на 561:

	$b^{2^j q}$	$2^{2^0 \cdot 35}$	$2^{2^1 \cdot 35}$	$2^{2^2 \cdot 35}$	$2^{2^3 \cdot 35}$
$b^{2^j q}$	$(\mathrm{mod}\ n)$	263	166	67	1

㉝ Оскільки $r_0 \neq 1$, $r_1 \neq n-1$, $r_2 \neq n-1$, $r_3 \neq n-1$, то і в цьому випадку тест Міллера правильно свідчить, що 561 є складеним числом.

Наведемо ще один приклад, який показує, що алгоритм Міллера дійсно може закінчуватись невизначеним висновком $\boxed{?}$.

Приклад 9. Застосуємо тест Міллера з основою $b = 7$ до $n = 25$. Оскільки $24 = 2^3 \cdot 3$, то $k = 3$, $q = 3$. Тому

	$b^{2^j q}$	$7^{2^0 \cdot 3}$	$7^{2^1 \cdot 3}$	$7^{2^2 \cdot 3}$
$b^{2^j q}$	$(\mathrm{mod}\ n)$	18	24	1

㉞ Оскільки $r_0 \neq 1$, але $r_1 = n-1$, то в цьому випадку тест Міллера робить висновок $\boxed{?}$. Відзначимо також, що тест розпізнав би, що $n = 25$ є складеним числом, якщо замість $b = 7$ у якості основи ми обрали б $b = 2$. ㉟

Означення 4. Нехай $n > 0$ є непарним числом, а $1 < b < n-1$. Якщо n є складеним, але тест Міллера з основою b закінчився з результатом $\boxed{?}$, то n називають називають *строго псевдопростим за основою b*.

Приклад 9 показує, що 25 є строго псевдопростим за основою 7. Кожне строго псевдопросте число за основою b є псевдопростим за цією ж основою. ㊱

6. Тест Рабіна–Міллера

Ми вже відзначили, що число 25 не є строго псевдопростим за основою 2. Можна довести, що найменшим строго псевдопростим за основою 2 є 2047. ㊲ Більш того, існують тільки 1282 строго псевдопростих чисел за основою 2, які знаходяться між 1 та 10^9. Нагадаємо, що у цьому ж діапазоні існує 5597 псевдопростих чисел за основою 2. Це свідчить про достатньо високу эфективність тесту Міллера. Звичайно, тест Міллера можна застосувати послідовно для кількох основ й це ще більше підвищить його ефективність. Наприклад, найменшим строго псевдопростим числом одночасно для трьох основ 2, 3 та 5 є 25,326,001.

Якщо результатом тесту Міллера вважати ‘‘n є простим’’ замість [?], то наведені дані означають, що тест Міллера, застосований для трьох основ 2, 3 та 5, дасть абсолютно вірну відповідь, якщо $n < 25,326,001$.

6.1. Рандомізований алгоритм. Для скорочення запису ми позначаємо в алгоритмі 4, наведеному нижче, через [!] висновок тесту Міллера ‘‘n є складеним’’ (див. алгоритм 3).

Алгоритм 4 циклічно використовує алгоритм 3, причому основи обираються випадковим чином. Тому висновок алгоритму 4 також є випадковим. Чи є це прийнятним у практичних задачах?

Перш за все, зауважимо, що алгоритм 4 робить один з двох висновків [!] або [?], тобто ‘‘n є складеним’’ або ‘‘можливо n є простим’’. Кожен з них є цілком певним, жодної ви-

падковості у них немає. Проте, висновок [?] навряд чи є бажаним, оскільки включає елемент непевності, яка входить разом зі словом *можливо*. Звичайно, замість [?] ми хотіли би отримати висновок ‘‘n є простим’’. Саме тут з'являється випадковість, оскільки цей висновок є випадковою подією! Заміна висновку [?] однією з двох його частин ‘‘n є простим’’ приводить до ігнорування іншої частини ‘‘n не є простим’’. При цьому може виникнути помилка, ймовірність виникнення якої необхідно знати.

Алгоритм 4. Рандомізований тест Міллера–Рабіна

Вхідні дані: непарне число $n \geq 5$;

Вихідні дані: висновок про простоту n або [?];

обрати випадкове число $1 < b_1 < n-1$;

застосувати тест Міллера з основою b_1;

якщо результатом теста Міллера є [!], то STOP.

якщо ж результатом є [?], то

обрати випадкове число $1 < b_2 < n-1$, $b_2 \neq b_1$;

застосувати тест Міллера з основою b_2;

якщо результатом теста Міллера є [!], то STOP.

якщо ж результатом є [?], то

обрати випадкове число $1 < b_3 < n-1$,

$b_3 \neq b_1$, $b_3 \neq b_2$;

. . . . . .

Зауважимо, що не існує жодного "строго Кармайклового числа". ㊳ Це випливає з наступного результата М. О. Рабіна.

Теорема 8 (*Рабіна*)**.** *Нехай $n > 0$ є непарним числом. Якщо тест Міллера, застосований до n для більш, ніж $n/4$ основ $1 < b < n - 1$, не закінчиться жодного разу з висновком ''n є складеним'', то n є простим числом.*

З теореми Рабіна випливає, що правдоподібною є гіпотеза про те, що ймовірність невизначеного результату в алгоритмі 4 не перевищує $1/4$. Це дає змогу запропонувати рандомізований тест, у якому основи обираються випадковим чином.

Кількість повторень цього тесту визначається тим наскільки малою ми хочемо зробити ймовірність невизначеної відповіді. Якщо його повторити m разів і кожного разу отримати $\boxed{?}$, то ймовірність того, що число є складеним, не перевищуватиме $1/4^m$, тобто правдоподібним є те, що ймовірність того, що число n є простим у випадку невизначеної відповіді, перевищуватиме $1 - 1/4^m$. ㊴

Зауваження 5. Зрозуміло, що ми хочемо бути абсолютно впевненими у тому, що числа, які пройшли тест, є дійсно простими. Для цього ми обираємо m настільки великим, щоб похибка тесту Міллера–Рабіна була настільки малою, що нею можна було знехтувати. Якщо, наприклад, обрати $m = 40$, то ймовірність невизначеної відповіді алгоритму Міллера–Рабіна не перевищуватиме $1/4^{40} \approx 1/10^{24}$. Вважатимемо, що подіями з такою (або меншою) ймовірністю можна знехтувати. Чи не ризиковано нехтувати подіями такої малої ймовірності?

Якщо, наприклад, у якості основ обрати перші 40 простих чисел, то можна вказати число Кармайкла (яке має 397 десяткових цифр), для якого тест Міллера дає невизначену відповідь. Для потреб сучасної криптографії це можливо є надто ризикованим!

6.2. PRIMES is in P. В 2002 році індійський математик М. Агравал та два його студенти Н. Каян та Н. Саксена запропонували детерміністський алгоритм (AKC) перевірки на простоту довільного натурального числа n за час $O(\log^{12} n)$. Трьома роками пізніше нідерландський вчений Х. Ленстра покращив алгоритм AKC так, що він закінчується за час $(\log^6 n)$. Згідно з гіпотезою Агравала існує варіант алгоритму з часом виконання $(\log^3 n)$, але певні евристичні міркування показують хибність цієї гіпотези.

На відміну від алгоритмів Соловея–Штрассена та Міллера–Рабіна, які визначають простоту тільки з певною ймовірністю, алгоритм AKC абсолютно точно визначає чи є простим задане число і тому він має важливе теоретичне значення. На практиці ж алгоритм AKC не застосовується, оскільки його обчислювальна складність значно вище, ніж у кращих імовірнісних алгоритмів.

Якщо вірною є знаменита гіпотеза Рімана про нулі ζ функції (див. [Гіпотеза Рімана], стор. 378), то алгоритм Міллера–Рабіна можна перетворити у детерміністський з вищою швидкодією, ніж у алгоритма AKC. Це випливає з наступної гіпотези, яка автоматично стає вірною, якщо доведено гіпотезу Рімана.

Гіпотеза. *Для кожного складеного натурального числа n існує таке $b < 2\log^2 n$, для якого тест Міллера визнає n складеним числом.*

7. КОНТРОЛЬНІ ПИТАННЯ

1. Чому число λ в формулі Міллса (формула (1)) не є натуральним? (стор. 308).

2. Чому n не є простим, якщо існує b для якого $b^{n-1} \not\equiv 1 \pmod{n}$? (стор. 309).

3. Чому свідків в алгоритмі 1 можна не шукати після числа $n-1$? (стор. 310).

4. Чому $(n-1)^{n-1} \equiv 1 \pmod{n}$, якщо n є непарним? (стор. 310).

5. Перевірити конгруенцію $2^{341-1} \equiv 1 \pmod{341}$. (стор. 311).

6. Чому основи $n-1, n, \ldots$ в питанні (3) не враховано? (стор. 312).

7. Показати, що якщо $b^{n-1} \equiv 1 \pmod{n}$ та $n > 2$, то існує обернене число $b^{-1} \pmod{n}$. (стор. 312).

8. Чому кожен з дільників n не є свідком його простоти, якщо n є складеним числом? (стор. 312).

9. Впевнитись, що якщо $(b, n) \neq 1$, то n не є псевдопростим за основою b. (стор. 313).

10. Довести, що якщо $(b, n) = 1$, то конгруенція $b^n \equiv b \pmod{n}$ випливає з $b^{n-1} \equiv 1 \pmod{n}$. (стор. 313).

11. Пояснити чому конгруенцію в означенні 2 достатньо перевіряти лише для $1 < b < n-1$? (стор. 313).

12. Довести, що $b^{561} - b$ ділиться на 561, якщо воно ділиться на 3, 11 та 17. (стор. 314).

13. Закінчити доведення (5). (стор. 314).

14. Чи просто перевірити умови теореми Корселта для числа (7)? (стор. 315).

15. Довести, що $(b^{p-1})^q \equiv 1 \pmod{p}$. (стор. 316).

16. Чому з $p^n \equiv p \pmod{n}$ випливає $p^n \equiv p \pmod{p^2}$, якщо $p^2 \mid n$? (стор. 316).

17. Пояснити фразу у прикладі 4: "Одне з повторень алгоритму Соловея–Штрассена обов'язково буде виконано з $a \neq 8$ й тому врешті буде зроблено правильний висновок, що ''n є складеним''". (стор. 320).

18. Чому $x \not\equiv 0 \pmod{p}$, якщо x є розв'язком рівняння (9), причому $a \not\equiv 0 \pmod{p}$ та $(a, p) = 1$? (стор. 322).

19. Чому $-x \pmod{p}$ також є розв'язком рівняння (9)? (стор. 322).

20. Чому $(a,p)=1$ в доведенні теореми 6? Вказівка. $(a,p)>1 \Rightarrow a=cp \Rightarrow b=0$. (стор. 323).

21. Чому в доведенні теореми 6 з $(a,p)=1$ випливає, що $(a,n)=1$? Вказівка. Лема 8.4. (стор. 323).

22. При доведенні теореми 6 показати, що $\mathrm{Leg}\,(a,p)=\mathrm{Leg}\,(b,p)=-1$ та $\mathrm{Leg}\,(a,q)=\mathrm{Leg}\,(1,q)=-1$. Вказівка. $\left(\frac{b}{p}\right)=-1$ та $a \equiv b \pmod p$; $1^2 \equiv a \pmod p$ та $a \equiv b \pmod p$ (стор. 323).

23. Чому $\left(\frac{a}{n}\right)=-1$ в доведенні теореми 6? (стор. 323).

24. При доведенні теореми 6 використано таку імплікацію: якщо $a^{(n-1)/2} \equiv -1 \pmod{pq}$, то $a^{(n-1)/2} \equiv -1 \pmod q$. Покажіть, що ця імплікація є вірною. (стор. 323).

25. Чому $(x,p)=1$, якщо $x^2 \equiv a \pmod p$ та $(a,p)=1$? (стор. 324).

26. Чому $ab_0 \pmod n \in A \cup B$ у доведенні теореми 7? (стор. 326).

27. Чому для кожного непарного n існують такі натуральне k та непарне q, що $n-1=2^k q$? (стор. 329).

28. Чому n є дільником різниці квадратів $b^{2^j q}-1$ в доведенні алгоритму Міллера? (стор. 330).

29. Чому n не є дільником обох чисел $b^{2^{j-1}q}-1$ та $b^{2^{j-1}q}+1$ в доведенні алгоритму Міллера? (стор. 330).

30. Чому n не може бути дільником $b^{2^{j-1}q}-1$ в доведенні алгоритму Міллера? (стор. 330).

31. Довести, що якщо у послідовності остач при діленні на n чисел (13) зустрінеться $n-1$, то всі решта дорівнюють 1. (стор. 331).

32. Обчислити $2^{85} \pmod{341}$ та $2^{170} \pmod{341}$. (стор. 331).

33. Обчислити $2^{2^j \cdot 35}$ для $j=0,1,2,3$. (стор. 332).

34. Обчислити $7^{2^j \cdot 3}$ для $j=0,1,2$. (стор. 332).

35. Провести обчислення для даних з прикладу 9 та основи $b=2$. (стор. 332).

36. Чому кожне строго псевдопросте число за основою b є псевдопростим за цією ж основою? (стор. 332).

37. Як довести, що 2047 є найменшим строго псевдопростим за основою 2? (стор. 333).

38. Як можна було б означити поняття “строго Кармайклового числа”? (стор. 334).

39. Пояснити, чому якщо повторити тест Міллера–Рабіна m разів, то ймовірність того, що число n є простим у випадку невизначеної відповіді, перевищуватиме $1 - 1/4^m$? (стор. 335).

8. ЗАДАЧІ

Задача 1. *Довести, що* $2^{1105} \equiv 2 \pmod{1105}$.

Задача 2. *Доведіть, що складене число n є псевдопростим за базою b:*

a) $n = 45$, $b = 17$;
b) $n = 49$, $b = 18$.

Задача 3. *Доведіть, що складене число n є псевдопростим за базою b:*

a) $n = 51$, $b = 35$;
b) $n = 55$, $b = 21$.

Задача 4. *Доведіть, що складене число n є псевдопростим за базою b:*

a) $n = 57$, $b = 20$;
b) $n = 65$, $b = 14$.

Задача 5. *Перевірити, що* 341, 561, 645 *та* 1105 *є найменшими псевдопростими числами за базою* 2, *які не є простими.*

Задача 6. *Які з чисел, що перераховані у задачі* 5, *є псевдопростими за базою* 3? *А за базою* 5?

Задача 7. *Нехай n є пседопростим за базою* 2, *а також за базою* 3. *Доведіть, що n є псевдопростим за базою* 6.

Задача 8. *Доведіть, що кожне складене число Ферма $f_m = 2^{2^m} + 1$ є псевдопростим за базою* 2.

Задача 9. *У прикладі* 2 *було доведено, що* $341 = 11 \cdot 31$ *є псевдопростим числом за базою* 2. *Насправді таких чисел нескінченна кількість. Доведіть цей факт, виконавши наступні кроки.*

a) *Покажіть, що* $(2^d - 1) \mid (2^n - 1)$, *якщо* $d \mid n$.

b) *Нехай* $n = dt$, $1 < d, t < n$, — *складене псевдопросте число за базою* 2. *Позначимо* $m = 2^n - 1$. *Тоді* m *є складеним числом на підставі задачі* a). *Покажіть, що існує таке натуральне число* k, *для якого* $m - 1 = kn$.

c) *За допомогою* a) *доведіть, що* $m \mid 2^{m-1} - 1$.

d) *За допомогою* c) *доведіть, що* m *є псевдопростим числом за базою* 2.

e) *За допомогою* d) *доведіть, що існує нескінченно багато псевдопростих чисел за базою* 2.

Задача 10. *Доведіть, що якщо* $b^{n-1} \equiv 1 \pmod{n}$, *але* n *є складеним та* $(b-1, n) = 1$, *то число*

$$N = \frac{b^n - 1}{b - 1}$$

має ті ж властивості, тобто $b^{N-1} \equiv 1 \pmod{N}$, $(b-1, N) = 1$ *й* N *є складеним. Це означає, що з псевдопростого числа за базою* b *можна побудувати більше псевдопросте число за тією ж базою, тобто таких чисел нескінченна кількість.*

Для цього покажіть, що

a) n *ділить* $\frac{b^n-1}{b-1}$;

b) nb *ділить* $N - 1$;

c) $b^n - 1$ *ділить* $b^{N-1} - 1$; N *ділить* $b^{N-1} - 1$;

d) $b-1 \equiv -1 \pmod{b}$, *звідки випливає* $N \equiv 1 \pmod{b}$, *тобто* $(b-1, N) = 1$.

Задача 11. *Нехай* $b \geq 2$, *а* $p > 2$ — *просте число, яке не ділить* $b(b-1)(b+1)$. *Доведіть, що число*

$$N = \frac{b^p - 1}{b - 1} \cdot \frac{b^p + 1}{b + 1}$$

є псевдопростим за базою b, *але не є простим.*

Для цього покажіть, що

a) $N - 1 = \frac{b^2((b^2)^{p-1}-1)}{b^2-1}$;

b) p *ділить* $(b^2)^{p-1} - 1$; p *ділить* $\frac{(b^2)^{p-1}-1}{b^2-1}$;

c) $b^2((b^2)^{p-1}-1)b^2-1$ *є парним*;
d) b^N-1 *ділиться на* $b^{2p}-1$;
e) b^N-1 *ділиться на* N.

Задача 12. *Довести, що* 1729 *та* 2821 *є числами Кармайкла.*

Задача 13. *Знайти число Кармайкла вигляду* $7\cdot 23\cdot p$, *де* p — *просте число.*

Задача 14. *Знайдіть* 5 *псевдопростих чисел за базою*
a) 2; b) 3.

Задача 15. *Знайдіть* 5 *чисел, які є псевдопростими за обома базами* 2 *та* 3.

Задача 16. *Знайдіть* 6 *псевдопростих чисел за базою* 7.

Задача 17. *Довести, що кожне число Кармайкла має принаймні три прості дільники.*

Задача 18. *Довести, що кожне число Кармайкла є непарним.*

Задача 19. *Нехай* $n=1387$. *Довести, що*
a) n *є псевдопростим за базою* 2;
b) *тест Соловея–Штрассена з* $b=2$ *показує, що* n *є складеним.*

Задача 20. *Нехай* p *є простим числом, а* a — *натуральним. Довести, що* $a^2\equiv 1 \pmod p$ *тоді і тільки тоді, коли* $a\equiv 1 \pmod p$ *або* $a\equiv -1 \pmod p$.

Задача 21. *Ми кажемо, що число* n *пройшло тест Міллера з базою* b, *якщо* $b^t\equiv 1 \pmod n$ *або* $b^{2^j t}\equiv -1 \pmod n$ *для деякого* $0\le j\le s-1$, *де* $n-1=2^s t$ *для деяких цілих* s *та* t, *причому* $s\ge 1$, *а* t *непарне. Довести, що якщо складене число* n *пройшло тест Міллера з базою* b, *то воно є псевдопростим за базою* b.

Задача 22. *Нехай непарне число* n *пройшло тест Міллера з базою* b (*див. задачу* 21). *Довести, що*
a) $b^{(n-1)/2}\equiv \pm 1 \pmod n$;
b) n *є строго псевдопростим за базою* b (*див. означення 4*).

Задача 23. *Довести, що перше число Кармайкла* $n = 561$ *не пройшло тест Міллера з базою* 2 (*див. задачі* 21 *та* 22).

Задача 24. *Довести, що перше число Кармайкла* $n = 561$ *не пройшло тест Міллера з базою* 3 (*див. задачі* 21 *та* 22).

Задача 25. *Довести, що перше число Кармайкла* $n = 561$ *не пройшло тест Міллера з базою* 5 (*див. задачі* 21 *та* 22).

Задача 26. *Нехай* n *натуральне число. Припустимо, що властивість* а) *задачі* 22 *не виконується за жодною за базою* b. *Довести, що* n *є складеним числом.*

Задача 27. *Доведіть, що властивість* а) *задачі* 22 *виконано для числа* $n = 25$ *та бази* $b = 7$.

Задача 28. *Доведіть, що* 1387 *є псевдопростим, але не є строго псевдопростим, за базою* 2.

Задача 29. *Доведіть, що* 25,326,001 *є строго псевдопростим за базами* 2, 3 *та* 5.

Задача 30. *Доведіть, що* $n = 2047$ *проходить тест Міллера для бази* $b = 2$.

Задача 31. *Нехай* n *є строго псевдопростим за основою* a (*означення* 4). *Доведіть, що* n *є строго псевдопростим за основою* a^{2j+1} *для будь-якого* $j \geq 1$.

Задача 32. *Англійський фізик Генрі Поклінгтон цікавився математикою. Йому належить цікавий результат, який використовується для перевірки простоти натуральних чисел.*

Теорема Поклінгтона. *Нехай* $n = ab + 1$, $a, b \in \mathbf{N}$, $b > 1$. *Припустимо, що для кожного простого дільника* q *числа* b *існує таке* m, *що* $m^{n-1} \equiv 1 \pmod{n}$ *та* $(m^{(n-1)/q}, n) = 1$. *Тоді* $p \equiv 1 \pmod{b}$ *для кожного* $p \mid b$. *Крім того, якщо* $b > \sqrt{n} - 1$, *то* n *є простим числом*

За допомогою теореми Поклінгтона визначити, чи є $n = 54419$ *простим числом*?

Вказівка. Використати властивість $n - 1 = 2 \cdot 27209$, де 27209 є простим. Тоді $b = 27209$ та $a = 2$. Впевнитись, що для $q = 27209$ можна взяти $m = 2$.

Задача 33. *Один з зручних способів перевірки чисел на простоту належить Франсуа Проту, французькому фермеру, який цікавився математикою.*

Теорема Прота. *Нехай $k, t \in \mathbf{N}$, причому t є непарним числом, а $2^k > t$. Тоді $n = 2^k t + 1$ є простим числом тоді і тільки тоді, коли $c^{(n-1)/2} \equiv -1 \pmod{n}$, де число c є квадратичним нелишком за модулем n (див. означення 3).*

Доведіть теорему Прота.

Вказівка. Якщо n є простим, то з теореми 5 випливає конгруенція $c^{(n-1)/2} \equiv -1 \pmod{n}$. Обернене твердження випливає з теореми Поклінгтона з $a = t$, $b = 2k$ та $m = c$ (див. задачу 32).

Задача 34. *Числа $M_p = 2^p - 1$ у випадку простих p носять ім'я Мерсенна.*

a) *Доведіть теорему Мерсенна: якщо $2^n - 1$ є простим, то n також є простим.*

Для доведення теореми Мерсенна

b) *покажіть, що якщо $a \in \mathbf{N}$, то*

$$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a^2 + a + 1);$$

c) *більше того, якщо $n = rs$, то*

$$a^{rs} - 1 = (a^r - 1)(a^{r(s-1)} + a^{r(s-2)} + \cdots + a^{2r} + a^r + 1);$$

d) *зокрема, якщо $a^n - 1$ є простим, то $a = 2$ та n є простим.*

Задача 35. *В 1644 році Мерсенн довів, що числа M_p є простими для*

$$p = 2,\ 3,\ 5,\ 7,\ 13,\ 17,\ 19,\ 31,\ 67,\ 127,\ 257$$

(числа Мерсенна M_p означено в задачі 34). Крім того, він вважав, що всі M_p є простими для $p \le 257$.

a) *Доведіть, що M_{11} є складеним;*

b) *Чи може тест Ферма розпізнати, що M_{61} є складеним?*

c) *Чи може тест Міллера розпізнати, що M_{61} є складеним?*

Задача 36. *Для визначення простоти чисел Мерсенна (див. задачу* 34*) використовують так званий тест Люка–Лемера.*

Тест Люка–Лемера. *M_p, $p > 2$, є простим числом тоді і тільки тоді, коли M_p є дільником числа S_p, де послідовність $\{S_k, k \geq 2\}$ задано рекурентно*:

$$S_2 = 2, \qquad S_k = S_{k-1}^2 - 2.$$

За допомогою теста Люка–Лемера визначити чи є простим числом

a) M_{89}? b) M_{107}?

Задача 37. *Число n називається досконалим, якщо воно дорівнює сумі своїх дільників без n (див. задачу* 7.23*).*

Евклід 2300 *років тому довів, що якщо M_k є простим, то $2^k M_k$ є досконалим. Ойлер довів й обернене твердження про те, що якщо $2^{k-1} M_k$, $k > 1$, є досконалим, то M_k є простим.*

a) *Довести теорему Евкліда про числа Мерсенна.*

b) *Довести теорему Ойлера про числа Мерсенна.*

Позначимо $p = 2^k - 1$ та $n = 2^{k-1}(2^k - 1)$.

c) *Для* **a)** *необхідно довести, що $\sigma(n) = 2n$, де $\sigma(n)$ — це сума дільників числа n (функцію σ означено в задачі* 7.21*). Це випливає з властивостей $\sigma(p) = 2^k$ та $\sigma(n) = \sigma(2^{k-1})\sigma(p)$. Остання рівність називається мультиплікативністю функції σ (див. задачу* 7.22*).*

d) *Для* **b)** *припустимо, що n є парним досконалим числом та запишемо його у вигляді $n = 2^{k-1}m$, де $k > 1$, m непарне. Тоді $\sigma(n) = \sigma(2^{k-1})\sigma(m)$ та $\sigma(n) = 2^k m$, звідки випливає $m = (2^k - 1)M$ для деякого натурального числа M. Тоді $2^k M = \sigma(m)$. Оскільки m та M є дільниками m, то $2^k M \geq m + M = 2^k M$, тобто $\sigma(m) = m + M$. Іншими словами, m має тільки два дільника.*

9. БІОГРАФІЇ

Агравал, *Маніндра* (нар. 1966), індійський математик, спеціаліст у галузі складності обчислень та компьютерної теорії чисел. Найбільш відомою є його стаття (спільна з його студентами Н. Каялом та Н. Саксеною), у якій описано детерміністський алгоритм перевірки чисел на простоту. За цю роботу її співавтори отримали в 2006 році премію Геделя, якою нагороджують за видатні досягнення у теорії компьютерних наук, та премію Фулкерсона, яку вручають за видатні статті у галузі дискретної математики.

Альфорд, *Уільям* (1937–2003), американський математик, відомий спеціаліст у галузі теорії чисел. Певний час працював юристом (як у свій час П. Ферма (див. [Ферма], стор. 30)), оскільки також мав диплом юриста. Але найбільше відомий своїми трудами у галузі аналітичної теорії чисел. Разом з К. Померанцем (див. [Померанц], стор. 266) та Гранвілем (див. [Гранвіль], стор. 347) довів, що існує нескінченно багато чисел Кармайкла (див. [Кармайкл], стор. 347).

Гаусс, *Карл Фрідріх* (1777–1855), видатний німецький математик, астроном, геодезист, фізик. Дослідження з математики почав проводити у 1995 році, коли став студентом Геттінгенського університету. Серед його відкриттів у той час був метод найменших квадратів. У 1908 році закінчив математичний шедевр "*Арифметичні дослідження*" (лат. "*Disquisitiones Arithmeticae*"), надрукований через 3 роки. У цій праці він детально виклав теорію порівнянь в сучасних (введених ним) позначеннях, розробив методи розв'язання конгруенцій довільного порядку, глибоко дослідив квадратичні форми, вказав роль комплексних коренів з одиниці для

побудови правильних n-кутників циркулем та лінійкою (це дослідження багато в чому було прообразом теорії Галуа), виклав властивості квадратичних лишків, довів квадратичний закон взаємності, один з центральних результатів теорії чисел, тощо. Постановка і розробка цих питань Гауссом визначили дальший розвиток цих дисциплін.

К. Гаусс довів, що за допомогою циркуля та лінійки можна побудувати такий правильний n-кутник, число сторін якого виражається формулою $n = 2^{2^r} + 1$, де r — деяке натуральне число або нуль. Побудови трикутника ($r = 0$) і п'ятикутника ($r = 1$) були відомі ще давнім грекам, але Гаусс першим здійснив побудову правильного 17-кутника ($r = 2$).

Можна без перебільшень сказати, що теорія чисел, як наука, почала своє справжнє існування саме з досліджень Гаусса. "*Арифметичні дослідження*" Гаусса в математичній науці створили цілу епоху, а Гаусс був визнаний найвизначнішим математиком світу. На медалі, виготовленій у 1855 р. на його честь, вигравірувано напис: "*Король математиків*".

К. Гаусс любив говорити, що математика — це цариця наук, а теорія чисел — цариця математики.

Дуже важливе значення має доведена Гауссом у 1799 р. основна теорема алгебри про існування кореня алгебраїчного рівняння. На основі цієї теореми доведено таку властивість рівнянь: "*Алгебраїчне рівняння має стільки коренів дійсних чи комплексних, скільки одиниць у показнику його степеня*". За працю, в якій доведено ці теореми, Гаусс дістав звання приват-доцента.

З 1796 року К. Гаусс вів короткий щоденник своїх відкриттів. Він, подібно до Ньютона, не публікував багато своїх результатів, хоча вони були виняткової важливості (еліптичні функції, неевклідова геометрія тощо). Своїм друзям він пояснював, що публікує тільки ті результати, якими задоволений і вважає завершеними. Багато відкладених або покинутих ним ідей пізніше воскресли в працях Абеля, Якобі, Коші, Лобачевського і інших. Кватерніони він теж відкрив за 30 років до Гамільтона.

Всі численні опубліковані праці Гаусса містять значні результати, сирих і прохідних робіт не було жодної. Незаперечними є досягнення Гауссса у галузі астрономії та фізики. У 1809 р. учений написав і свою фундаментальну працю "*Теорія руху небесних тіл, які оберта-*

ються навколо Сонця по конічних перерізах", а наступного року французький астрономічний інститут за розв'язання задачі про рух малої планети Паллади присудив йому золоту медаль. Хоча Гаусс плідно працював у різних галузях науки, але він сам часто говорив: "*Я весь відданий математиці*".

К. Гаусс був настільки піднесений своїм відкриттям методу побудови правильного 17-кутника за допомогою циркуля та лінійки, що при житті заповів, щоб правильний сімнадцятикутник викарбували на його могилі. Скульптор відмовився це зробити, стверджуючи, що побудова буде настільки складною, що результат не можна буде відрізнити від кола. Але пам'ятник Гауссу, збудований у Брауншвейзі, встановлено на сімнадцятикутній плиті.

Гранвіль, *Ендрю* (нар. 1962 р.), британський математик, який працює у галузі теорії чисел; його спеціалізацією є алгебраїчна теорія чисел. У статті, написаній у 1994 році спільно з К. Померанцем (див. [Померанц], стор. 266) та У. Альфордом (див. [Альфорд], стор. 345), довів, що існує нескінченно багато чисел Кармайкла (див. [Кармайкл], стор. 347). Доведення Альфорда, Гранвіля та Померанца було основано на одній з ідей Ердеша (див. [Ердеш], стор. 379). Основний результат роботи Альфорда, Гранвіля та Померанца полягає в оцінці $C(x) > x^{\alpha}$ для достатньо великих x та деякого $\alpha > 0$ (можна, наприклад, взяти $\alpha > 2/7$), де $C(x)$ — це кількість чисел Кармайкла до x.

У 2007 та 2009 роках Е. Гранвіля було нагороджено премією Форда, а в 2008 — премією Шавені за найкращий математичний твір.

Кармайкл, *Роберт Деніел* (1879–1967), американський математик. Сучасним математикам Кармайкл відомий в першу чергу своїм дослідженням так званих чисел Кармайкла. Він є автором двох невеликих книжок з теорії чисел: "*The Theory of Numbers*" (1914) та "*Diophantine analysis*" (1915). З першою книгою пов'язано цікаву історію. Задачу 8 у главі 2 сформульовано наступним чином: *Довести, що якщо рівняння* $\phi(x) = n$

має розв'язок, то він не є єдиним. Тут n є параметром, а x — невідомим. Тут, як завжди, ϕ — це функція Ойлера. У якості розв'язку Кармайкл використав доведення відповідного факту зі своєї статті 1907 року. Проте це "доведення" є невірним, що було помічено ним самим у 1922 році. Однак невірне доведення не означає, що саме твердження є невірним. Він зауважив, що якщо його твердження є невірним, то це може статися лише при $x > 10^{37}$. До цього часу невідомо, чи є вірним його твердження (воно тепер називається гіпотезою Кармайкла). Зусиллями багатьох математиків вдалося лише довести, що якщо гіпотеза Кармайкла є невірною, то це може статися лише тоді, коли

$$x > 10^{10,000,000}.$$

Корселт, *Алвін Рейнголд* (1864–1947), німецький математик. Він відкрив критерій Корселта для чисел Кармайкла (див. [Кармайкл], стор. 347). В 1902 році захистив кандидатську дисертацію на тему "*Про можливість розв'язання задач про дивні властивості трикутників за допомогою поділу кута*". Відомий також своєю дискусією з Г. Фреге стосовно аксіоматизації евклідової геометрії, запропонованої Гільбертом.

Зберіглися свідчення його знайомих про те, що всі свої гроші він витрачав на придбання книг та сигар, тому завжди мав дуже пошарпану зовнішність.

Ленстра, *Хендрік* (нар. 1949 р.), нідерландський математик, спеціаліст з алгебри, теорії чисел, теорії алгоритмів. Відомими є його роботи стосовно факторизації на еліптичних кривих, а також швидкого обчислення майже ортогональних базисів. Його алгоритм визначення простоти чисел є найшвидшим серед детерміністських алгоритмів такого роду. Крім того, він (разом з Померанцем (див. [Померанц], стор. 266)) навів міркування, які показують, що гіпотеза Агравала (див. [Агравал], стор. 345) стосовно швидкодії алгоритму AKC, є невірною.

Його нагороджено преміями Фулкерсона (1985) та Спінози (1998). В 2009 році Німецька математична спілка відзначила його досягнення, нагородивши премією Гаусса, яка передбачає цикл лекцій перед широкою аудиторією з предмета, який визначає сам автор.

Міллер, *Гаррі Лі* (нар. у XX сторіччі), американський математик та спеціаліст у галузі компьютерних наук. Захистив кандидатську дисертацію "*Гіпотеза Рімана та перевірка чисел на простоту*" у 1975 році. Разом з М. Рабіном (див. [Рабін], стор. 349) він є одним з авторів відомого ймовірнісного метода перевірки натуральних чисел на простоту. В 2003 році разом з трьома іншими колегами отримав престижну премію Каннелакіса за "*розробку і аналіз алгоритмів у теорії чисел та обчислювальній геометрії*".

Його метод у випадку справедливості гіпотези Рімана дає змогу визначити простоту числа за поліноміальний час. Це використовується для різного роду спекуляцій стосовно "загибелі" криптографії у випадку справедливості гіпотези Рімана (див. [Гіпотеза Рімана], стор. 378).

Рабін, *Майкл Осер* (нар. 1.09.1931), ізраільський спеціаліст у галузі компьютерних наук. Він є відомим через свій ймовірнісний тест перевірки натуральних чисел на простоту. Рабін розробив цей метод на базі ранішньої роботи Г. Міллера (див. [Міллер], стор. 349), який запропонував детермінований метод перевірки на простоту у припущенні, що вірною є узагальнена гіпотеза Рімана. М. Рабін позбувся цього припущення ціною допущення певної ймовірності похибки алгоритма. В 2003 році Рабін разом з Г. Міллером (див. [Міллер], стор. 349), Ф. Штрассеном (див. [Штрассен], стор. 350) та Р. Соловеем (див. [Соловей], стор. 350) отримав престижну премію Асоціації компьютерних обчислень (премію імені Каннелакіса).

Він є автором однієї з криптографічних систем з відкритими ключами, яка зараз носить його ім'я (див. задачу 9.27). Його система основана на складності обчислення квадратних коренів за модулем.

За одну з своїх ранніх робіт був нагороджений (разом з Д. Скоттом) премією Тьюрінга.

Соловей, *Роберт* (нар. 15.12.1938), американський математик, який працює у галузі теорії множин. Одним з його результатів у теорії множин є твердження про те, що (за деяких припущень) твердження "*кожна підмножина дійсних чисел є вимірною за Лебегом*" є узгодженою з моделлю Цермело–Френкеля без аксіоми вибору. Є автором (спільно з Ф. Штрассеном (див. [Штрассен], стор. 350)) алгоритму перевірки чисел на простоту.

Штрассен, *Фолькер* (нар. 29.04.1936), німецький математик, знаний спеціаліст з теорії ймовірностей та аналізу алгоритмів. Його називають батьком алгебраїчної теорії складності. Широко відомим є так званий *функціональний закон повторного логарифму Штрассена*, який він довів в 1964 році. Він є автором багатьох алгоритмів для швидких обчислень, які зараз працюють на мільйонах комп'ютерів. В 1969 році він відкрив абсолютно новий спосіб множення двох матриць розміру $n \times n$ за час $O\left(n^{2.81}\right)$, тоді як звичайний спосіб здійснюється за час $O\left(n^3\right)$. Алгоритм Шенхаге–Штрассена множення великих чисел вважався найшвидшим у світі до 2007 року, але і досі є стандартним методом у компьютерних обчисленнях (алгоритм виконує множення за час $O(N \cdot \log N \cdot \log\log N)$, де N це кількість двійкових розрядів у бінарному представленні добутку).

Ф. Штрассена нагороджено медалью Кантора в 1999 році, премією Кнута в 2008 році. В 2003 році він разом з Р. Соловеем (див. [Соловей], стор. 350), Г. Міллером (див. [Міллер], стор. 349) та М. Рабіном (див. [Рабін], стор. 349) отримав престижну премію Каннелакіса за роботи стосовно перевірки чисел на простоту.

Глава 13

ТЕОРЕМА ЧЕБИШОВА

Нашою головною метою у цій главі є оцінити $\pi(x)$, кількість простих чисел, які не перевищують x. Для цього спочатку оцінимо функцію Чебишова.

Множину простих чисел позначимо через $\mathcal{P}$. *Функцією Чебишова* називається

$$\vartheta(x) = \sum_{\substack{p\in\mathcal{P}\\ p\le x}} \ln(p), \qquad x \ge 2,$$

де $\ln(p)$ — це натуральний логарифм числа p. Покладемо також $\vartheta(x) = 0$, $0 \le x < 2$. Безпосередньо з означення випливає, що

x	2	3	4	5
$\vartheta(x)$	$\ln(2)$	$\ln(2)+\ln(3)$	$\ln(2)+\ln(3)$	$\ln(2)+\ln(3)+\ln(5)$

Почнемо з необхідних оцінок для біноміальних коефіцієнтів.

Лема 1. *Для всіх $n \ge 1$ виконуються нерівності*

$$\frac{4^n}{2\sqrt{n}} \le C_{2n}^n < 4^n.$$

Доведення леми 1. За формулою бінома Ньютона

$$4^n = (1+1)^{2n} = \sum_{k=0}^{2n} C_{2n}^k > C_{2n}^n,$$

й тому верхню оцінку доведено. Нижню оцінку доведемо методом математичної індукції. Вона очевидна для $n = 1$. Вважаючи, що вона є вірною для $n = k$, маємо за припущенням індукції

$$C_{2(k+1)}^{k+1} = \frac{2(2k+1)}{k+1} C_{2k}^{k} \geq \frac{2(2k+1)}{k+1} \frac{4^k}{2\sqrt{k}} > \frac{4^{k+1}}{2\sqrt{k+1}}. \qquad ①$$

Лему доведено. □

Тепер ми можемо отримати оцінку зверху для функції Чебишова $\vartheta(x)$.

Лема 2. *Для всіх $x \geq 0$ має місце нерівність*

$$\vartheta(x) \leq (4\ln(2))x.$$

Точність оцінки з леми 2 для декількох перших значень аргументу продемонстровано у наступній таблиці.

x	2	3	5	7
$2(\ln(2))x - \vartheta(x)$	$\approx 2,1$	$\approx 2,3$	$\approx 3,5$	$\approx 4,3$
$\frac{2(\ln(2))x}{\vartheta(x)}$	≈ 4	$\approx 2,3$	≈ 2	$\approx 1,8$

З таблиці видно, що різниця між оцінкою та функцією Чебишова зростає, але відношення їх значень зменшується. ②

Зауваження 1. Для скорочення будемо надалі писати

$$\prod_{p<2n} \quad \text{замість} \quad \prod_{\substack{p\in\mathcal{P}\\ p<2n}}.$$

Інші добутки будемо розуміти аналогічно. Вважатимемо, що добуток дорівнює 0, якщо множина індексів є порожньою. Наприклад, $\prod_{p<2} \cdots = 0$.

Доведення леми 2. Зауважимо, що для всіх $n \geq 1$

$$C_{2n}^{n} > \prod_{n<p<2n} p. \tag{1}$$

Дійсно,

$$\frac{(n+1)\ldots(2n)}{n!} = \left(\prod_{n<p<2n} p \right) \cdot \left(\frac{1}{n!} \prod_{\substack{k \notin \mathcal{P} \\ n<k\leq 2n}} k \right) \stackrel{\text{def}}{=} A \cdot B.$$

Зрозуміло, що ліва частина дорівнює C_{2n}^{n} ③ і тому права частина є натуральним числом. Оскільки $n!$ не може ділитися на жодний з дільників числа A ④, то B є натуральним числом. ⑤ Більше того, $B > 1$. ⑥ Таким чином, нерівність (1) доведено.

Тепер, згідно з верхньою оцінкою для біноміальних коефіцієнтів, отриманою в лемі 1,

$$4^n > C_{2n}^{n} > \prod_{n<p<2n} p,$$

звідки $2n \ln(2) > \vartheta(2n) - \vartheta(n)$. ⑦ Підсумовуючи нерівності, які відповідають $n = 2^0, 2^1, \ldots, 2^{m-1}$, отримуємо для кожного $m \geq 1$

$$\vartheta(2^m) \leq 2\ln(2)(1 + 2 + \cdots + 2^{m-1}) < 2\ln(2) \cdot 2^m.$$

Це доводить бажаний результат для $x = 2^m$. Для іншого аргументу $x \geq 2$ знайдемо $m \geq 1$, для якого $2^{m-1} < x < 2^m$. Тоді

$$\vartheta(x) \leq \vartheta(2^m) < 2\ln(2) \cdot 2^m = 4\ln(2) \cdot 2^{m-1} < (4\ln(2))x.$$

Лему доведено. □

Наступний результат містить оцінку знизу для функції Чебишова $\vartheta(x)$.

Лема 3. *Для довільного натурального* $m > 4$

$$\vartheta(m) > \frac{m}{2}. \tag{2}$$

Доведення леми 3. Для будь-якого простого числа p та натурального числа n позначимо через $\nu_p(n)$ степінь, у якій простий дільник p входить до канонічного розкладу числа n у добуток простих множників. У добутку $n! = 1 \cdot 2 \cdot \ldots \cdot n$ на $p \leq n$ діляться рівно $\left[\frac{n}{p}\right]$ множників, ⑧ на p^2 — рівно $\left[\frac{n}{p^2}\right]$ множників, і так далі. ⑨ Зауважимо, що множина чисел, які діляться на p^i, включає множину чисел, які діляться на p^{i+1}. Тому для кожного $i \geq 1$ існує рівно $\delta_i = \left[\frac{n}{p^i}\right] - \left[\frac{n}{p^{i+1}}\right]$ чисел, які не перевищують n та діляться на p^i, але не діляться на p^{i+1}. ⑩ Кожне з таких чисел можна записати у вигляді kp^i, де k — певний множник (свій для кожного числа), який не ділиться на p. Це означає, що добуток всіх таких чисел ділиться на $p^{i\delta_i}$, тобто $n!$ ділиться на p в степені $\sum_{i\geq 1} i\delta_i$. ⑪ Таким чином,

$$\nu_p(n!) = \sum_{i\geq 1} i\delta_i = \sum_{i\geq 1} \left[\frac{n}{p^i}\right]. \tag{3}$$

⑫

Оскільки степінь кожного простого числа p у канонічному розкладі C_{2n}^n на прості множники дорівнює $\nu_p((2n)!) - 2\nu_p(n!)$, то з (3) випливає

$$\nu_p\left(C_{2n}^n\right) = \nu_p\left(\frac{(2n)!}{(n!)^2}\right) = \sum_{i\geq 1}\left[\frac{2n}{p^i}\right] - 2\sum_{i\geq 1}\left[\frac{n}{p^i}\right] \qquad (13)$$

$$= \sum_{i=1}^{\left[\log_p(2n)\right]}\left(\left[\frac{2n}{p^i}\right] - 2\left[\frac{n}{p^i}\right]\right) \leq \left[\log_p(2n)\right], \qquad (14)$$

на підставі $[2x] - 2[x] \leq 1$ для всіх x. (15) Звідси отримуємо

$$C_{2n}^n = \prod_{p<2n} p^{\nu_p(C_{2n}^n)} \leq \prod_{p<2n} p^{\left[\log_p(2n)\right]} \qquad (16)$$

$$\leq \prod_{p\leq\sqrt{2n}} p^{\log_p(2n)} \prod_{\sqrt{2n}<p<2n} p^{\log_p(2n)}$$

$$\leq (2n)^{\left(\sqrt{2n}+1\right)/2} \prod_{\sqrt{2n}<p<2n} p. \qquad (17)$$

Остання нерівність є вірною на підставі оцінки кількості простих чисел $p \leq \sqrt{2n}$: їх не більше, ніж $(\sqrt{2n}+1)/2$. (18) Використовуючи першу нерівність з леми 1, отримуємо

$$\vartheta(2n) > \sum_{\sqrt{2n}<p\leq 2n} \ln(p) \geq \ln\left(C_{2n}^n\right) - \frac{1}{2}\left(\sqrt{2n}+1\right)\ln(2n)$$

$$\geq n\ln(4) - \ln(2) - \frac{1}{2}\ln(n) - \frac{1}{2}\left(\sqrt{2n}+1\right)\ln(2n) = nt_n,$$

де

$$t_n = \ln(4) - \frac{\ln(2)}{n} - \frac{\ln(n)}{2n} - \frac{\left(\sqrt{2n}+1\right)\ln(2n)}{2n}.$$

Константа t_n є не меншою за 1, якщо $n \geq 134$. ⑲

Таким чином, якщо число $m \geq 268$ є парним, то нерівність (2) доведено. Якщо ж $m \geq 268$ є непарним, то $\vartheta(m) = \vartheta(m+1) > (m+1)/2 > m/2$ і нерівність (2) також справджується.

Нерівність (2) перевіряється безпосередньо для всіх чисел $m < 268$. ⑳ □

Теорема 1 (*Чебишов*). *Для $n \geq 2$ маємо*

$$\frac{1}{2} \cdot \frac{\ln(n)}{n} < \pi(n) < 5 \cdot \frac{\ln(n)}{n}. \tag{4}$$

Доведення теореми 1. Покладемо $y = n^{2/3}$. Тоді

$$\vartheta(n) \geq \sum_{\substack{p \in \mathcal{P} \\ y < p \leq n}} \ln(p) \geq (\pi(n) - \pi(y)) \ln(y). \tag{5}$$ ㉑

Оскільки $\pi(y) \leq y$, то з леми 2 випливає

$$\pi(n) \leq c_n \frac{n}{\ln(n)}, \qquad \text{де} \quad c_n = 6\ln(2) + \frac{\ln(n)}{n^{1/3}}. \tag{6}$$ ㉒

Максимальне значення $\frac{3}{e}$ функції $\frac{\ln(x)}{x^{1/3}}$ в області $x \geq 1$ досягається при $x = e^3$. ㉓ Тому

$$\pi(n) \leq \left(6\ln(2) + \frac{3}{e}\right) \frac{n}{\ln(n)} < 5 \cdot \frac{n}{\ln(n)} \tag{7}$$ ㉔

і праву нерівність в (4) доведено. Фактично замість константи 5 у правій частині (7), а отже і в (4), можна записати константу 4.9.

Ліва нерівність в (4) доводиться за допомогою леми 3:

$$\frac{n}{2} < \vartheta(n) \le \pi(n)\ln(n). \qquad (8)$$

□

Зауваження 2. Насправді, П. Л. Чебишов в 1848 році довів більш точну нерівність

$$\frac{7}{8}\cdot\frac{\ln(n)}{n} < \pi(n) < \frac{9}{8}\cdot\frac{\ln(n)}{n}. \qquad (9)$$

1. Асимптотика кількості простих чисел

З оцінок Чебишова (9) випливає, що

$$\liminf_{x\to\infty}\frac{\pi(x)}{x/\ln(x)} \ge \frac{7}{8}, \qquad \limsup_{x\to\infty}\frac{\pi(x)}{x/\ln(x)} \le \frac{9}{8}. \qquad (10)$$

З теореми 1 аналогічний результат можна отримати з константами $\frac{1}{2}$ замість $\frac{7}{8}$ та 5 замість $\frac{9}{8}$. Ці дві нерівності правильно описують асимптотику функції $\pi(x)$, але результат не є точним. Точним ми називаємо такий результат, в якому знайдено точне значення границі відношення $\pi(x)$ до $x/\ln(x)$, а не тільки асимптотичні оцінки для нього. Остаточну відповідь на питання про асимптотику функції $\pi(x)$ при $x\to\infty$ дає наступний результат.

Теорема 2 (*теорема про прості числа*)**.**

$$\lim_{x\to\infty}\frac{\pi(x)}{x/\ln(x)} = 1. \qquad (11)$$

1.1. Про доведення теореми про прості числа. Гіпотезу про асимптотику простих чисел, яка є еквівалентною теоремі 2, висловив в 1797 або 1798 році французький математик А. Лежандр. К. Гаусс в 1849 році писав, що те ж саме питання він розглядав ще в 1792 або 1793 році (тоді йому було 15 або 16 років).

Саму теорему 2 довели наприкінці XIX сторіччя майже одночасно та незалежно один від іншого математики Ж. Адамар з Франції та Ш. Валле Пуссен з Бельгії. Оскільки в цих доведеннях використовувались методи комплексного аналізу, що не вважається природним у задачах теорії чисел, пошуки "елементарного" доведення тривали і надалі.

В 1949 році з'явились відразу два елементарні доведення теореми 2, які знайшли А. Сельберг (Швеція) та П. Ердеш (Угорщина) (див. [Теорема про прості числа], стор. 382).

2. Постулат Бертрана

В 1845 році Ж. Бертран (Франція) висловив гіпотезу, що у кожному інтервалі $(x, 2x]$, $x > 3$, знайдеться принаймні одне просте число. Сам Ж. Бертран не зміг довести свою гіпотезу; це зміг зробити П. Л. Чебишов в 1852 році. Найпростіший спосіб доведення цього результату спирається на теорему 2; Чебишов довів його іншим методом.

Покажемо, що постулат Бертрана дійсно випливає з теореми 2. З теореми 2 отримуємо

$$\lim_{x\to\infty} \frac{\pi(2x) - \pi(x)}{x/\ln(x)} = 1. \qquad (12)$$

Оскільки $\pi(2x) - \pi(x)$ — це кількість простих чисел в ін-

тервалі $(x, 2x]$, то останнє співвідношення означає, що

$$\pi(2x) - \pi(x) > \frac{1}{2} \cdot \frac{x}{\ln(x)}$$

для достатньо великих x. Оскільки $x/\ln(x)$ прямує до нескінченості при $x \to \infty$, то ми отримуємо такий результат.

Твердження 1. *Нехай задано натуральне число N. Тоді інтервал $(x, 2x)$ містить більше, ніж N простих чисел, якщо x є достатньо великим.*

Зауваження 3. Твердження 1 є набагато більш змістовним, ніж постулат Бертрана. З іншого боку, в твердженні 1 не вказується точно нижня межа для x, після якої результат є вірним.

Такі ж міркування доводять, що якщо $c > 1$ — довільне число, а $N > 1$ — довільне натуральне число, то інтервал (x, cx) містить більше, ніж N простих числа, якщо x є достатньо великим. ㉗

Доведення постулату Бертрана. Позначимо

$$A(x) = \text{НСК}\,(1, 2, 3, \ldots, [x]), \qquad x > 0.$$

Нагадаємо, що через $\text{НСК}\,(m_1, m_2, \ldots, m_k)$ ми позначаємо найбільше спільне кратне натуральних чисел $m_1, \ldots, m_k$. Нехай p — просте число, а $k_p = k_p(x)$ — це максимальне ціле число k, для якого $p^k \leq x$. Іншими словами, k_p — це кількість розв'язків нерівності $p^k \leq x$, де невідомим є натуральне k. Кожне просте число p входить у канонічний розклад $A(x)$ на прості множники у степені k_p. ㉘

Визначимо тепер показник $a_p(x)$, з яким просте число p входить у добуток

$$T(x) \stackrel{\text{def}}{=} A(x) \cdot A(x/2) \cdot A(x/3) \cdot \ldots \cdot A(x/[x]). \tag{13}$$

Зрозуміло, що $a_p(x) = k_p(x) + k_p(x/2) + \cdots + k_p(x/[x])$, тобто $a_p(x)$ дорівнює кількості розв'язків нерівності $np^k \leq x$, де невідомими є натуральні k та n. Для кожного фіксованого k існує $[x/p^k]$ розв'язків цієї нерівності відносно n, ㉙ тобто

$$a_p(x) = [x/p] + [x/p^2] + \ldots \stackrel{\text{def}}{=} \nu_p(x). \qquad ㉚$$

Таким чином, розклад на прості множники добутку (13) співпадає з розкладом на прості множники числа $[x]!$ (формула (3)). ㉛ Це доводить відому *тотожність Чебишова*:

$$T(x) = [x]!. \tag{14}$$

Покажемо, що постулат Бертрана випливає з нерівності

$$\frac{A(x)}{A(x/2)} > A^2\left(\sqrt{x}\right), \qquad x > 0. \tag{15}$$

Дійсно, якщо (15) виконується, а постулат Бертрана не виконується, то для деякого $x = 2n$ не існує жодного простого числа p, для якого $\frac{x}{2} < p \leq x$.

Показник $b_p(x)$, з яким кожне просте число p входить в канонічний розклад $A(x)/A(x/2)$ ㉜ на прості множники, дорівнює кількості тих натуральних k, які є розв'язком нерівності $x/2 < p^k \leq x$. ㉝ Можна також сказати, що цей показник дорівнює сумі кількостей розв'язків нерівностей

$x/2 < p^{2k} \le x$ та $x/2 < p^{2k+1} \le x$, в яких невідомим є натуральне k. Очевидно, що ця сума не перевищує помноженої на 2 кількості розв'язків нерівності $p^k \le \sqrt{x}$. ㉞ Це означає, що $b_p(x)$ не перевищує показник, з яким p входить в канонічний розклад числа $A^2(\sqrt{x})$ на прості множники. ㉟ Звідси випливає, що $A(x)/A(x/2) \le A^2(\sqrt{x})$, а це протирічить (15).

Таким чином, постулат Бертрана дійсно випливає з (15), тому зосередимось на доведенні цієї нерівності. Будемо вважати, що $x \ge 2000$ (при менших значеннях x постулат Бертрана перевірити нескладно).

Застосуємо тотожність Чебишова (14) для x та $x/2$:

$$\frac{[x]!}{([x/2]!)^2} = \frac{A(x)A(x/2)A(x/3)\ldots}{A^2(x/2)A^2(x/4)A^2(x/6)\ldots}.$$

Оскільки $A(x)$ є неспадною функцією аргументу x, ㊱ то

$$\frac{A(x)}{A(x/2)} \overset{/1/}{\le} \frac{[x]!}{([x/2]!)^2} \overset{/2/}{\le} \frac{A(x)A(x/3)}{A(x/2)}. \qquad (16)$$

㊲

Нехай $[x/2] = m$, тобто $m \le x/2 < m+1$. Тому

$$\frac{A(x)}{A(x/2)} \le \frac{[x]!}{([x/2]!)^2} \overset{/3/}{\le} \frac{(2m+1)!}{(m!)^2} \overset{/4/}{\le} 4^m < 6^m \le 6^{x/2}. \qquad (17)$$

㊳ Нерівність /4/ є вірною на підставі верхньої оцінки з леми 1. Аналогічно,

$$\frac{A(x)A(x/3)}{A(x/2)} \ge \frac{[x]!}{([x/2]!)^2} \overset{/5/}{\ge} \frac{(2m)!}{(m!)^2} \overset{/6/}{\ge} \frac{4^m}{2\sqrt{m}} \overset{/7/}{\ge} \frac{2^{2m}}{2m+1} \overset{/8/}{\ge} \frac{2^{x-2}}{x+1}. \qquad (18)$$

㊴

Нерівність /5/ є наслідком означення числа m, а нерівність /6/ випливає з верхньої оцінки у лемі 1.

Нерівність (17) можна використати для оцінки значень функції $A(x)$. Зрозуміло, що для $x > 2$

$$A(x) \overset{/9/}{=} \prod_{k=0}^{[\log_2(x)]-1} \frac{A(x/2^k)}{A(x/2^{k+1})} \leq \prod_{k=0}^{[\log_2(x)]-1} 6^{x/2^{k+1}} \overset{/10/}{\leq} 6^x. \qquad (19)$$ ㊵

Застосовуючи цю формулу для $\sqrt{x}$ та $x/3$, отримуємо такі дві оцінки:

$$A^2\left(\sqrt{x}\right) \leq 6^{2\sqrt{x}}, \qquad A(x/3) \leq \left(\sqrt[3]{6}\right)^x.$$

Використовуючи оцінку (18), отримуємо

$$\frac{A(x)}{A(x/2)} \geq \frac{2^{x-2}}{(x+1)A(x/3)} \geq \left(\frac{2}{\sqrt[3]{6}}\right)^x \cdot \frac{1}{4(x+1)} \geq \frac{1.1^x}{4(x+1)}.$$

Таким чином, для доведення (15), а значить і самого постулату Бертрана, необхідно показати, що для цілих $x \geq 2000$ виконується нерівність

$$1.1^x > 4(x+1)6^{2\sqrt{x}}. \qquad (20)$$

Безпосередні обчислення показують, що нерівність (20) справджується при $x = 2000$. Зауважимо, що при збільшенні x на одиницю ліва частина (20) збільшується в 1.1 рази, а права — менше, ніж в 1.05 рази, оскільки при $x \geq 2000$

$$\frac{x+2}{x+1} \cdot 6^{2\left(\sqrt{x+1}-\sqrt{x}\right)} \overset{/11/}{<} \left(1 + \frac{1}{2000}\right) \cdot 6^{\frac{1}{2000}} \overset{/12/}{<} 1.05. \qquad (21)$$ ㊶

Таким чином, нерівність (15) залишається справедливою для всіх цілих $x \geq 2000$, що і треба було довести.

Підсумовуючи, ми довели постулат Бертрана для всіх натуральних чисел $n \geq 1000$. Для менших значень n постулат Бертрана перевіряється безпосередньо. Це можна зробити, наприклад, за допомогою таблиць простих чисел. $\square$

2.1. Теорема Райта. У попередній главі ми відзначали (див. розділ 1 глави 12), що не існує формул, які можна ефективно використати на практиці для отримання нових простих чисел (стосовно формули Міллса див. §1.1, глава 12). З метою продемонструвати можливі застосування постулату Бертрана наведемо ще одну з подібних формул, яка отримана англійським математиком Е. Райтом.

Теорема 3 (*теорема Райта*)**.** *Існує дійсне число μ, при якому всі числа*

$$\left[2^{2^{\cdot^{\cdot^{\cdot^{2^{\mu}}}}}}\right] \tag{22}$$

є простими. Іншими словами, при будь-якій кількості піднесень до степеня число (22) *є простим.*

Доведення. Оберемо послідовність простих чисел $\{q_n\}$ так, щоб

$$2^{q_n} < q_{n+1} < 2^{q_n+1} - 1, \qquad n > 1. \tag{23}$$

Число q_1 оберемо довільним чином. Така послідовність існує на підставі постулату Бертрана. ㊷ Позначимо

$$\exp(n, x) \stackrel{\text{def}}{=} 2^{2^{\cdot^{\cdot^{\cdot^{2^{x}}}}}}$$

(тут n позначає кількість піднесень до степеня; іншими словами, n — це кількість символів "2" у записі цього числа). Обернену до $\exp(n,x)$ функцію $\log_2\log_2\ldots\log_2 x$ позначимо через $\log(n,x)$. Нашою метою є знайти таке дійсне число μ, що

$$[\exp(n,\mu)] = q_n, \qquad n \geq 1. \tag{24}$$

Властивість (24) і означатиме справедливість твердження теореми Райта.

Властивість (24) еквівалентна подвійній нерівності

$$q_n \leq \exp(n,\mu) < q_n + 1$$

за означенням цілої частини числа. Якщо n разів застосувати логарифм за основою 2 до кожної з частин цієї двосторонньої нерівності, то отримаємо ще одну еквівалентну двосторонню нерівність

$$\log(n,q_n) \leq \mu < \log(n,q_n+1). \tag{25}$$

З першої нерівності в (23) випливає, що $q_n < \log_2(q_{n+1})$, тобто послідовність $\{\log(n,q_n)\}$ є зростаючою. ㊸ З другої нерівності в (23) випливає, що $\log_2(q_{n+1}+1) < q_n+1$, тобто послідовність $\{\log(n,q_n+1)\}$ є спадною. ㊹ Крім того,

$$\begin{aligned}\log(n,q_n) &< \log(n+1,q_{n+1}+1) < \log(n,q_n+1) < \ldots\\ &< \log(1,q_1+1),\end{aligned}$$

що означає, що послідовність $\{\log(n,q_n)\}$ обмежена зверху числом $\log(1,q_1+1)$, тобто вона має скінчену границю. Значення цієї границі візьмемо у якості μ. Нескладно побачити, що це μ задовольняє не тільки нерівність (25), але й

$$\log(n,q_n) < \mu < \log(n,q_n+1).$$

Таким чином властивість (24) виконано. □

3. Асимптотика функції Чебишова

Насправді теорема про асимптотику функції $\pi(x)$ є еквівалентною певному результату про асимптотику функції Чебишова. Саме через це Чебишов вивчав поведінку функції $\vartheta(x)$ (вона здалася йому простішою, ніж $\pi(x)$).

Теорема 4. *Формула* (11) *виконується тоді і тільки тоді, коли границя відношення дорівнює одиниці, тобто*

$$\lim_{n\to\infty} \frac{\vartheta(n)}{n} = 1. \tag{26}$$

Оцінки, отримані в лемах 2 та 3, дозволяють лише стверджувати, що нижня та верхня границя відношення $\vartheta(n)/n$ є скінченими:

$$\frac{1}{2} \le \liminf_{n\to\infty} \frac{\vartheta(n)}{n} \le \limsup_{n\to\infty} \frac{\vartheta(n)}{n} \le 4\ln(2). \tag{27}$$

Звичайно, співвідношення (26) означає більше, ніж нерівності (27). Теорема 4) стверджує, що формулу (11) вивести з нерівностей (27) неможливо.

Доведення теореми 4. Спочатку ми покажемо, що вірною є імплікація (11)$\Longrightarrow$(26). З нерівності (5) випливає, що для будь-якого $0 < y < n$

$$(\pi(n) - \pi(y))\ln(y) \le \vartheta(n) \le \pi(n)\ln(n). \tag{28}$$

Зафіксуємо $0 < \varepsilon < 1$ та оберемо $y = n^{1-\varepsilon}$. Тоді з нерівностей (28) отримуємо

$$1 = \lim_{n\to\infty} \frac{\pi(n) - \pi(n^{1-\varepsilon})}{n/\ln(n)} \qquad ㊻$$

$$\le \liminf_{n\to\infty} \frac{\vartheta(n)}{(1-\varepsilon)n} \le \limsup_{n\to\infty} \frac{\vartheta(n)}{(1-\varepsilon)n}$$

$$\le \frac{1}{1-\varepsilon} \limsup_{n\to\infty} \frac{\pi(n)}{n/\ln(n)} = \frac{1}{1-\varepsilon}. \qquad ㊼$$

Оскільки число $\varepsilon > 0$ є довільним у цих міркуваннях, то співвідношення (26) доведено.

Тепер доведемо обернену імплікацію (26)$\Longrightarrow$(11).

З другої нерівності в (28) випливає, що

$$\liminf_{n\to\infty} \frac{\pi(n)}{n/\ln(n)} \ge 1. \qquad (29)\ ㊽$$

З першої нерівності в (28) з $y = n^{1-\varepsilon}$, $0 < \varepsilon < 1$, випливає, що

$$\limsup_{n\to\infty} \frac{\pi(n) - \pi(n^{1-\varepsilon})}{n/\ln(n)} \le \limsup_{n\to\infty} \frac{\vartheta(n)}{(1-\varepsilon)n} = 1. \qquad (30)\ ㊾$$

Тепер з верхньої оцінки в (4) отримуємо

$$\limsup_{n\to\infty} \frac{\pi(n^{1-\varepsilon})}{n/\ln(n)} \le 5 \limsup_{n\to\infty} \frac{n^{1-\varepsilon}/\ln(n^{1-\varepsilon})}{n/\ln(n)} = 0,$$

що разом з (30) доводить

$$\limsup_{n\to\infty} \frac{\pi(n)}{n/\ln(n)} \le \frac{1}{1-\varepsilon}. \qquad (31)\ ㊿$$

Оскільки число $\varepsilon > 0$ є довільним, то це разом з (29) завершує доведення теореми 4. $\square$

4. Асимптотика n-ого простого числа

Нехай p_n позначає n-те просте число. За означенням, $p_1 = 2$, $p_2 = 3$, $p_3 = 5, \ldots$. За допомогою теореми 2 можна знайти порядок зростання p_n при $n \to \infty$. Більше того, теорема 2 є еквівалентною твердженню про правильну асимптотику послідовності $\{p_n\}$.

Теорема 5. *Формула* (11) *виконується тоді і тільки тоді, коли*

$$\lim_{n\to\infty} \frac{p_n}{n\ln(n)} = 1. \tag{32}$$

Позначимо $f(x) = x/\ln(x)$, $x \geq 3$. Нехай $f^{-1}(x)$ — це обернена функція до $f(x)$. ⑤①

Лема 4.

$$\lim_{x\to\infty} \frac{f^{-1}(x)}{x\ln(x)} = 1.$$

Доведення леми 4. Зауважимо, що

$$f'(x) = \frac{\ln(x) - 1}{(\ln(x))^2}.$$

Тому за правилом Лопіталя

$$\begin{aligned}
\lim_{x\to\infty} \frac{f^{-1}(x)}{x\ln(x)} &= \lim_{x\to\infty} \frac{\left(f^{-1}(x)\right)'}{\left(x\ln(x)\right)'} = \lim_{x\to\infty} \frac{1/f'(f(x))}{1+\ln(x)} \\
&= \lim_{x\to\infty} \frac{(\ln(f(x)))^2}{(\ln(f(x))-1)(\ln(x)-1)} \\
&= \lim_{x\to\infty} \frac{(\ln(x)-\ln(\ln(x)))^2}{(\ln(x)-\ln(\ln(x))-1)(\ln(x)-1)} = 1.
\end{aligned}$$

Це і доводить лему 4. □

Доведення теореми 5. Спочатку ми доведемо, що вірною є імплікація (11)$\Longrightarrow$(32). Оскільки $\pi(p_n) = n$, то з (11) випливає, що

$$\lim_{n\to\infty} \frac{n}{p_n/\ln(p_n)} = 1. \tag{33}$$

Тому для будь-якого $0 < \varepsilon < 1$ існує натуральне число n_ε, для якого

$$1 - \varepsilon \le \frac{n}{p_n/\ln(p_n)} \le 1 + \varepsilon, \qquad n \ge n_\varepsilon,$$

або

$$\frac{n}{1+\varepsilon} \le \frac{p_n}{\ln(p_n)} \le \frac{n}{1-\varepsilon}, \qquad n \ge n_\varepsilon,$$

або

$$f^{-1}\left(\frac{n}{1+\varepsilon}\right) \le p_n \le f^{-1}\left(\frac{n}{1-\varepsilon}\right), \qquad n \ge n_\varepsilon. \tag{34}$$

Нерівності (34) разом з лемою 4 доводять, що

$$1 \le \liminf_{n\to\infty} \frac{p_n}{\frac{n}{1+\varepsilon}\ln\left(\frac{n}{1+\varepsilon}\right)}, \qquad \limsup_{n\to\infty} \frac{p_n}{\frac{n}{1-\varepsilon}\ln\left(\frac{n}{1-\varepsilon}\right)} \le 1. \tag{35}$$

Це, в свою чергу, означає, що

$$\frac{1}{1+\varepsilon} \le \liminf_{n\to\infty} \frac{p_n}{n\ln(n)}, \qquad \limsup_{n\to\infty} \frac{p_n}{n\ln(n)} \le \frac{1}{1-\varepsilon}. \tag{36}$$

Оскільки $\varepsilon > 0$ є довільним, то звідси отримуємо (32).

Тепер доведемо імплікацію (32)$\Longrightarrow$(11). Перш за все зауважимо, що з (32) випливають співвідношення

$$\lim_{n\to\infty}\frac{p_{n+1}}{p_n}=1,\qquad \lim_{n\to\infty}\frac{\ln(p_n)}{\ln(n)}=1. \tag{37}$$

Для кожного $x\ge 2$ знайдемо n, при якому $p_n\le x<p_{n+1}$. Тоді $\pi(x)=n$. Тому

$$\begin{aligned}\frac{\pi(x)}{x/\ln(x)}&=\frac{n}{x/\ln(x)}\le\frac{n\ln(p_{n+1})}{p_n}\\&=\frac{\ln(p_{n+1})}{\ln(p_n)}\cdot\frac{n\ln(n)}{p_n}\cdot\frac{\ln(p_n)}{\ln(n)}.\end{aligned}$$

Звідси та з (37) випливає, що

$$\limsup_{x\to\infty}\frac{\pi(x)}{x/\ln(x)}\le 1.$$

Доведення нерівності

$$\liminf_{x\to\infty}\frac{\pi(x)}{x/\ln(x)}\ge 1$$

є цілком аналогічним. $\square$

5. КОНТРОЛЬНІ ПИТАННЯ

1. Чому $C_{2(k+1)}^{k+1}=\frac{2(2k+1)}{k+1}C_{2k}^{k}$ та $\frac{2(2k+1)}{k+1}\frac{4^k}{2\sqrt{k}}>\frac{4^{k+1}}{2\sqrt{k+1}}$? (стор. 352).

2. Перевірити обчислення точності відносної похибки апроксимації функції Чебишова її оцінкою з леми 2. (стор. 352).

3. Перевірити, що $\frac{(n+1)\ldots(2n)}{n!}=C_{2n}^{n}$. (стор. 353).

4. Пояснити, чому $n!$ не може ділитися на жодний з дільників числа A у доведенні леми 2? (стор. 353).

5. Чому B є натуральним числом у доведенні леми 2? (стор. 353).

6. Показати індукцією за n, що $B > 1$ для доведення леми 2. (стор. 353).

7. Чому $2n\ln(2) > \vartheta(2n) - \vartheta(n)$? (стор. 353).

8. Чому рівно $\left[\frac{n}{p}\right]$ множників в $n!$ діляться на $p \le n$? (стор. 354).

9. Чому рівно $\left[\frac{n}{p^2}\right]$ множників в $n!$ діляться на p^2? (стор. 354).

10. Чому для кожного $i \ge 1$ існує рівно $\delta_i = \left[\frac{n}{p^i}\right] - \left[\frac{n}{p^{i+1}}\right]$ чисел, які не перевищують n та діляться на p^i, але не діляться на p^{i+1}? (стор. 354).

11. Чому добуток чисел, які діляться на p^i, але не діляться на p^{i+1}, ділиться на $p^{i\delta_i}$, тобто $n!$ ділиться на p в степені $\sum_{i\ge1} i\delta_i$? (стор. 354).

12. Довести, що $\sum_{i\ge1} i\delta_i = \sum_{i\ge1}\left[\frac{n}{p^i}\right]$. (стор. 354).

13. Довести, що $\nu_p\left(\frac{(2n)!}{(n!)^2}\right) = \sum_{i\ge1}\left[\frac{2n}{p^i}\right] - 2\sum_{i\ge1}\left[\frac{n}{p^i}\right]$. (стор. 355).

14. Довести, що $\sum\limits_{i\ge1}\left(\left[\frac{2n}{p^i}\right] - 2\left[\frac{n}{p^i}\right]\right) = \sum_{i=1}^{\left[\ln_p(2n)\right]}\left(\left[\frac{2n}{p^i}\right] - 2\left[\frac{n}{p^i}\right]\right)$. (стор. 355).

15. Довести, що $[2x] - 2[x] \le 1$ для всіх x. (стор. 355).

16. Пояснити, чому ми пишемо $C_{2n}^n = \prod_{p<2n} p^{\nu_p(C_{2n}^n)}$, а не $C_{2n}^n = \prod_{p\le2n} p^{\nu_p(C_{2n}^n)}$? (стор. 355).

17. Чому кількість простих чисел $p \le \sqrt{2n}$ не перевищує $\frac{\sqrt{2n}+1}{2}$? (стор. 355).

18. Чому $[\ln_p(2n)] = 1$ для $\sqrt{2n} < p < 2n$? (стор. 355).

19. Довести, що $n\ln(4) - \ln(2) - \frac{1}{2}\ln(n) - \frac{1}{2}\left(\sqrt{2n}+1\right)\ln(2n) \ge n$ при $n \ge 134$. (стор. 355).

20. Перевірити нерівність (2) для $m < 268$. (стор. 356).

21. Пояснити другу нерівність в (5). (стор. 356).

22. Довести, що (6) випливає з $\pi(y) \le y$. (стор. 356).

23. Пояснити, чому максимальне значення $\frac{3}{e}$ функції $\frac{\ln(x)}{x^{1/3}}$ в області $x \ge 1$ досягається при $x = e^3$? (стор. 356).

24. Перевірити нерівність $3\ln(2) + \frac{3}{e} < 4$ в (7). (стор. 356).

25. Яким чином нерівності (8) випливають з леми 3? (стор. 356).

26. Вивести (12) з теореми 2. (стор. 358).

27. Довести, що для будь-яких фіксованих $c > 1$ та $m \in \mathbf{N}$ інтервал $(x, cx]$ містить більше, ніж m простих чисел, якщо x є достатньо великим. (стор. 359).

28. Чому кожне просте число p входить у канонічний розклад $A(x)$ на прості множники у степені k_p? (стор. 359).

29. Чому існує $[x/p^k]$ розв'язків нерівності $np^k \le x$ відносно n для кожного фіксованого k? (стор. 359).

30. Чому $a_p(x) = [x/p] + [x/p^2] + \ldots \stackrel{\text{def}}{=} \nu_p(x)$? (стор. 360).

31. Чому розклад на прості множники добутку (13) співпадає з розкладом на прості множники числа $[x]!$? (стор. 360).

32. Чому $A(x)/A(x/2)$ є натуральним числом? (стор. 360).

33. Чому показник, з яким кожне просте число p входить в канонічний розклад $A(x)/A(x/2)$, на прості множники, дорівнює кількості тих натуральних k, які є розв'язком нерівності $x/2 < p^k \le x$? (стор. 360).

34. Чому сума кількостей розв'язків нерівностей $x/2 < p^{2k} \le x$ та $x/2 < p^{2k+1} \le x$, в яких невідомим є натуральне k не перевищує помноженої на 2 кількості розв'язків нерівності $p^k \le \sqrt{x}$? (стор. 360).

35. Чому $b_p(x)$ не перевищує показник, з яким p входить в канонічний розклад числа $A^2\left(\sqrt{x}\right)$ на прості множники? (стор. 360).

36. Чому $A(x)$ є неспадною функцією аргументу x? (стор. 361).

37. Довести нерівності /1/ та /2/ в (16). (стор. 361).

38. Довести нерівність /3/ в (17). (стор. 361).

39. Довести нерівності /7/ та /8/ в (18). (стор. 361).

40. Пояснити рівність /9/ та нерівність /10/ в (19). (стор. 362).

41. Перевірити нерівності /11/ та /12/ в (21). (стор. 362).

42. Чому послідовність простих чисел $\{q_n\}$ можна обрати так, щоб виконувалась властивість (23)? (стор. 363).

43. Чому послідовність $\{\log(n, q_n)\}$, означена в доведенні теореми 3, є зростаючою? (стор. 364).

44. Чому послідовність $\{\log(n, q_n + 1)\}$, означена в доведенні теореми 3, є спадною? (стор. 364).

45. Перевірити нерівності (28). (стор. 365).

46. Довести, що $1 = \lim_{n\to\infty} \frac{\pi(n) - \pi(n^{1-\varepsilon})}{n/\ln(n)}$. (стор. 366).

47. Пояснити нерівність $\lim_{n\to\infty} \frac{\pi(n)-\pi(n^{1-\varepsilon})}{n/\ln(n)} \le \liminf_{n\to\infty} \frac{\vartheta(n)}{(1-\varepsilon)n}$. (стор. 366).

48. Пояснити формулу (29). (стор. 366).

49. Пояснити формулу (30). (стор. 366).

50. Вивести формулу (31) з (30) та нижньої оцінки в (4). (стор. 366).

51. Чому обернена функція $f^{-1}(x)$ існує в області $x > 1$? (стор. 367).

52. Чому (33) є вірним? (стор. 368).

53. Нерівності (34) є вірними тільки для зростаючих функцій. Чи є f^{-1} зростаючою? (стор. 368).

54. Чому нерівності (35) випливають з леми 4? (стор. 368).

55. Нерівності (36) виконуються, якщо $\ln\left(\frac{n}{1-\varepsilon}\right) \sim \ln(n) \sim \ln\left(\frac{n}{1+\varepsilon}\right)$. Чи є це вірним? (стор. 368).

56. Пояснити, чому $\lim_{n\to\infty} \frac{p_{n+1}}{p_n} = 1$ та $\lim_{n\to\infty} \frac{\ln(p_n)}{\ln(n)} = 1$ випливають з (32)? (стор. 368).

57. Пояснити, чому $\pi(x) = n$, якщо $p_n \le x < p_{n+1}$? (стор. 368).

58. Доведіть, що $\limsup_{x\to\infty} \frac{\pi(x)}{x/\ln(x)} \le 1$. (стор. 369).

59. Доведіть нерівність $\liminf_{x\to\infty} \frac{\pi(x)}{x/\ln(x)} \ge 1$. (стор. 369).

6. З А Д А Ч І

Задача 1. *Нехай n — це натуральне число, $p_1, p_2, \ldots, p_t$ — всі прості числа, які не перевищують $\sqrt{n}$.*

а) *Довести, що*

$$\pi(n) = n - 1 + \pi(\sqrt{n}) - \sum_{i=1}^{t} \left[\frac{n}{p_i}\right] + \sum_{i<j} \left[\frac{n}{p_i p_j}\right] - \sum_{i<j<k} \left[\frac{n}{p_i p_j p_k}\right] + \cdots + (-1)^t \left[\frac{n}{p_1 p_2 \ldots p_t}\right].$$

b) *Використовуючи* а), *підрахувати* $\pi(100)$.

Задача 2. а) *Не використовуючи результати цієї глави, довести, що*

$$\pi(n) \ge (2\ln(2))^{-1} \ln(n).$$

b) *Порівнять оцінку в* а) *з точною формулою в задачі 1.*

Задача 3. *Не використовуючи результати цієї глави, довести, що* $\pi(n) \le \frac{1}{2}n - 1$ *для всіх* $n \ge 14$.

Задача 4. *Не використовуючи результати цієї глави, довести, що* $p_n \le 2^{2^{n-1}}$, *де* p_n *— це* n*-те просте число.* Вказівка. Як у доведенні Евкліда про нескінченість множини простих чисел, розглянути $p_1 p_2 \dots p_k + 1$ і використати індукцію.

Задача 5. *Використати задачу* 4 *для доведення нерівності* $\pi(x) \ge [\ln(\ln(x))] + 1$.

Задача 6. *Використовуючи задачу* 2, *довести, що* $p_k < 2^{2^k}$, *де* p_k *— це* k*-те просте число.*

Задача 7. *Довести, що* $\vartheta(x) \sim \pi(x)\ln(x)$, $x \to \infty$.

Задача 8. *Нехай* $\{p_n\}$ *— послідовність простих чисел. Довести, що* $p_n + p_{n+1} > p_{n+2}$.

Задача 9. *Довести, що ряд*

$$\sum_{p \in \mathcal{P}} \frac{1}{p}$$

розбігається.

Задача 10. *З теореми* 1 *вивести, що існує така константа* $\Delta > 1$, *для якої кожен з інтервалів* $(n, \Delta n]$, $n > 1$, *містить хоча б одне просте число.*

Задача 11. *Довести, що з теореми 2 випливає, що*

$$\pi(x) \sim \int_2^x \frac{dx}{\ln(x)}, \qquad x \to \infty.$$

Задача 12. *Довести, що нерівність*

$$\frac{\pi(n-1)}{n-1} < \frac{\pi(n)}{n}$$

виконується тоді і тільки тоді, коли n *є простим числом.*

Задача 13. *Нехай $m \in \mathbf{N}$. Знайти розв'язки рівняння $\pi(x) = m$ для $x \in \mathbf{N}$.*

Задача 14. *За допомогою формули* (3) *знайти кількість нулів, якими закінчується число* 100!.

Задача 15. *Нехай $n \in \mathbf{N}$, $p \in \mathcal{P}$. Позначимо $t = \log_p(n)$.*

a) *Довести, що степінь p в канонічному розкладі C_{2n}^n дорівнює*

$$\left(\left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right]\right) + \left(\left[\frac{2n}{p^2}\right] - 2\left[\frac{n}{p^2}\right]\right) + \cdots + \left(\left[\frac{2n}{p^t}\right] - 2\left[\frac{n}{p^t}\right]\right).$$

b) *Використати* a) *для доведення нерівності $p^r \leq 2n$, якщо $p^r \mid C_{2n}^n$.*

Задача 16. *Використати задачу* 15 *для доведення нерівності*

$$C_{2n}^n \leq (2n)^{\pi(2n)}.$$

Задача 17. *Довести, що добуток всіх простих чисел, які знаходяться між n та $2n$, лежить між C_{2n}^n та $n^{\pi(2n)-\pi(n)}$.* Вказівка. Використайте властивість, що кожне просте число, яке знаходиться між n та $2n$, ділить $(2n)!$, але не ділить $(n!)^2$.

Задача 18. *Використайте задачі* 16 *та* 17, *щоб довести, що*

$$\pi(2n) - \pi(n) \leq \ln(4) \cdot \frac{n}{\ln(n)}.$$

Задача 19. *Використайте задачу* 18, *щоб довести, що*

$$\begin{aligned}\pi(2n) &= (\pi(2n) - \pi(n)) + (\pi(n) - \pi(n/2)) + (\pi(n/2) - \pi(n/4)) + \ldots \\ &\leq \ln(64)\frac{n}{\ln(n)}.\end{aligned}$$

Задача 20. *Використайте постулат Бертрана* (*розділ* 2), *щоб довести, що кожне число $n \geq 7$ є сумою двох різних простих чисел.*

Задача 21. *Нехай $n, m \in \mathbf{N}$. Використайте постулат Бертрана (розділ 2), щоб довести, що*

$$\frac{1}{n} + \frac{1}{n+1} + \cdots + \frac{1}{n+m}$$

не є натуральним числом.

Задача 22. *Нехай p_k — це k-те просте число. Довести, що*

a) $p_n^2 < p_{n-1}p_{n-2}p_{n-3}$ *для* $n \geq 6$;
b) *ця нерівність є невірною для* $n = 3$, 4 *та* 5.

Вказівка. Використайте постулат Бертрана, щоб довести нерівності $p_n < 2p_{n-1}$ та $p_{n-1} < 2p_{n-2}$.

Задача 23. *Нехай $a > 0$ та $x_0 > 1$. Припустимо, що для всіх $x \geq x_0$ виконано нерівність $\pi(x) \leq ax/\ln(x)$. Довести, що в цьому випадку $p_n \geq \frac{n}{a}\ln\left(\frac{n}{a}\right)$ для всіх $n \geq n_0$, де натуральне число $n_0 > ae$ є таким, що $p_{n_0} \geq x_0$.*

Задача 24. *Нехай $n > 3$, а $p \in \mathcal{P}$ є таким, що $2n/3 < p < n$. Довести, що p не може бути дільником C_{2n}^n.*

Задача 25. *Нехай p є простим дільником біноміального коефіцієнта C_{2n}^n. Довести, що якщо $p \geq \sqrt{n}$, то C_{2n}^n не ділиться на p^2.*

Задача 26. *Нехай p є простим дільником біноміального коефіцієнта C_{2n}^n. Довести, що якщо $n < p < 2n$, то C_{2n}^n не ділиться на p^2.*

Задача 27. *Позначимо через R_n добуток всіх простих чисел $n < p < 2n$. Довести, що*

a) $R_n \mid C_{2n}^n$, *тобто* $C_{2n}^n = Q_n R_n$ *для деякого натурального* Q_n;
b) *жодне з чисел* $n < p < 2n$ *не ділить* Q_n;
c) *має місце оцінка*

$$R_n > \frac{4^{n/3}}{2\sqrt{n}(2n)^{\sqrt{n/2}}}.$$

Задача 28. *Використати результат задачі* 27, *щоб довести, що* $R_n > 2n$ *для* $n \geq 648$.

Задача 29. *Не використовуючи постулат Бертрана, вивести з результату задачі* 28, *що між* n *та* $2n$ *знайдеться принаймні одне просте число, якщо* $n \geq 648$.

Задача 30. *Не використовуючи постулат Бертрана, вивести з результату задачі* 29, *що між* n *та* $2n$ *знайдеться принаймні одне просте число, якщо* $n > 5$.

Задача 31. *Використати результат задачі* 30, *щоб довести постулат Бертрана: між* n *та* $2n - 2$ *знайдеться принаймні одне просте число, якщо* $n > 3$.

Задача 32. *Знайти натуральні числа* n, *які дорівнюють сумі всіх простих чисел, які не перевищують* n.

7. БІОГРАФІЇ

Адамар, *Жак Соломон* (1865–1863), французький математик й механік. Автор багатьох фундаментальних робіт з теорії чисел, геометрії, функціональному аналізу, дифференциальній геометрії, математичної фізики, топології, теорії ймовірностей. За роботу, в якій довів теорему про прості числа (теорема 2), отримав в 1892 році премію французької Академії наук. Конкурс було оголошено у грудні 1890 року на тему "*Кількість простих чисел, менших заданої величини*". Ш. Ерміт, який у той час був президентом Академії наук, особисто запросив до участі Т. Стільтьеса, який, як тоді вважалось, знайшов доведення гіпотези Рімана (див. [Гіпотеза Рімана], стор. 378). Мабуть, звернення голови означало, що комітет по присудженню премії сподівався, що саме Стільтьес прийме участь і стане переможцем конкурсу. Проте у березні 1891 року Стільтьес у листі до Ерміта визнав, що знайшов помилку у своєму доведенні. В результаті Стільтьес так і не представив свою роботу, але до комітету надійшло дві статті інших авторів, одну з яких було відхилено через порушення формальних вимог та занадто елементарний характер питань, які в ній порушувались. Другу роботу було представлено під девізом

> *Мистецтво обгрунтування істин, вже відкритих, та ясне пояснення їх ... — ось до чого я прагну.*

Ці слова Б. Паскаля для девізу своєї роботи обрав Ж. Адамар. В цій роботі Адамар розвинув результати своєї кандидатської дисертації й досяг видатного результату у доведенні теореми про прості числа. Девіз роботи Адамара пояснюється тим, що він вважав її продовженням досліджень Рімана стосовно гіпотези про нулі ζ функції (див. [Гіпотеза Рімана], стор. 378).

У журнальному варіанті роботу Адамара було опубліковано у 1896 році. У тому ж році з'явилась стаття Валле Пуссена (див. [Валле Пуссен], стор. 378), у якій було отримано такий же результат.

Бертран, *Жозеф Луи Франсуа* (1822–1900), відомий французький математик, що працював в області теорії чисел, диференціальної геометрії, теорії ймовірності та термодинаміки. Його гіпотеза, висловлена в 1845 році про те, що між n та $2n-2$, $n>3$, знайдеться просте число, зараз називається постулатом Бертраном (доведення цього результату знайшов в 1850 році П. Л . Чебишов (див. [Чебишов], стор. 383)). В теорії ймовірностей відомим є *парадокс Бертрана*. Інший парадокс Бертрана стосується положення рівноваги Неша (див. [Неш], стор. 179) у теорії ігор.

Валле Пуссен, *Шарль Жан де ла* (1866–1962), бельгійський математик, відомий своїми глибокими результатами в теорії чисел, математичному аналізі та інших областях математики. Найбільш відомою його роботою є стаття 1896 року (у той же рік з'явилась робота Ж. Адамара (див. [Адамар], стор. 377)), в якій доведено теорему про прості числа (див. [Теорема про прості числа], стор. 382). Як і в роботі Адамара, Валле Пуссен для доведення використав складний метод, оснований на тонких фактах комплексного аналізу. Елементарне доведення (без використання комплексного аналізу) теореми про прості числа отримано А. Селбергом (див. [Селберг], стор. 382) та П. Ердешом (див. [Ердеш], стор. 379).

У 1920 році став першим президентом Міжнародного математичного союзу. У 1930 році за видатні наукові заслуги бельгійський король присвоїв Валле Пуссену титул барона.

Гіпотеза Рімана, (1859–????), висловлена німецьким математиком Б. Ріманом в роботі "*Про кількість простих чисел, менших заданої величини*", опублікованій у 1859 році. Гіпотеза полягає у тому, що всі нетривіальні нулі функції

$$\zeta(z)=\sum_{n=1}^{\infty}\frac{1}{n^z},\qquad \mathrm{Re}\,(z)>1,$$

розташовано на лінії

$$\mathrm{Re}\,(z) = \frac{1}{2}.$$

Тривіальними нулями ζ функції називають $z = -2, -4, -6, \ldots$. Рівність $\zeta(z) = 0$ для таких z випливає з функціонального рівняння Рімана

$$\zeta(z) = 2^z \pi^{z-1} \Gamma(1-z) \cdot \sin\left(\frac{\pi z}{2}\right) \cdot \zeta(z-1).$$

Про зв'язок гіпотези Рімана з поведінкою функції $\pi(x)$ (кількість простих чисел до x) краще за все свідчить еквівалентне її формулювання, знайдене в 1901 році Н. Кохом:

$$\pi(x) = \int_2^x \frac{dt}{\log t} + O\left(\sqrt{x}\log x\right), \qquad x \to \infty.$$

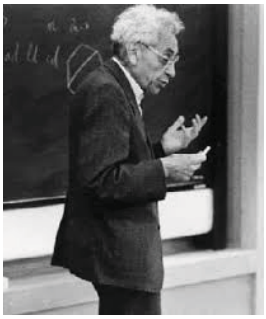
Доведена в 1896 році Адамаром (див. [Адамар], стор. 377) та Валле Пуссеном (див. [Валле Пуссен], стор. 378) теорема про прості числа (див. [Теорема про прості числа], стор. 382) зводиться до більш слабкого твердження

$$\zeta(z) \neq 0, \quad \text{якщо} \quad \mathrm{Re}\,(z) = 0 \ \text{ або } \ \mathrm{Re}\,(z) = 1.$$

В 1900 році Д. Гільберт включив гіпотезу Рвмана у список 23 нерозв'язаних проблем как частину восьмої проблеми разом гіпотезою Гольдбаха. В 2000 році Інституту Клея включив гіпотезу Рімана у список 7 задач тисячоліття: за розв'язання кожної з них пропонується премія у розмірі 1,000,000 долларів США.

Дуже розповсюдженою серед аматорів є думка, що доведення гіпотези Рімана знищить секретність, оскільки існуючи оцінки швидкодії багатьох алгоритмів дешифрації залежать від різноманітних наслідків гіпотези Рімана. Насправді це побоювання є несуттєвим: ніхто не заважає і зараз користуватись тими алгоритмами. Мабуть, ними тепер широко користуються, навіть не знаючи чи є вірною гіпотеза Рімана. Проте мова про "небезпеку для секретності" не йде.

Знаменитою є відповідь Гільберта на питання про те, якими будуть його дії, якщо він з якоїсь причини проспить п'ятсот років і раптом прокинеться. Математик відповів, що насамперед він запитає, чи була доведена гіпотеза Рімана.



Ердеш, *Пал* (1913–1996), угорський математик, відомий своєю надзвичайною продуктивністю. Ще за життя він став легендою серед математиків. Співпрацював одночасно з сотнями інших колег над проблемами з комбінаторики, теорії графів, теорії чисел, дискретної математики, класичного аналізу, теорії множин, теорії ймовірностей та теорії наближених обчислень. Будучи одним з гігантів серед математиків XX сторіччя, він любив ставити нові задачі та розв'язувати задачі інших математиків, якщо вони красиво та просто формулювались. Ще 1931 року, будучи студентом у Будапешті, він знайшов елегантне елементарне доведення постулату Бертрана (див. [Бертран], стор. 377).

Щоб уявити величезний внесок Ердеша в математику, достатньо перерахувати лише малу частину теорем та гіпотез, пов'язаних з його ім'ям: теореми *Ердеша–Турана* (теорія міри), *Ердеша–Галаї* (теорія графів), *Ердеша–Радо* (теорія множин), *Ердеша–Секереша* (комбінаторика), *Сюя–Роббінса–Ердеша* (теорія ймовірностей).

Вважається, що Ердеш не був так зацікавлений у розвитку теорій, як у розв'язуванні конкретних задач. Його інтерес до конкретних математичних питань привів до неймовірної кількості гіпотез Ердеша, деякі з яких є нерозв'язаними ще й досі: наприклад, гіпотези *Ердеша* про різні відстані (дискретна геометрія), *Ердеша–Грехема* (комбінаторна теорія чисел), *Камерона–Ердеша* (комбінаторика), *Ердеша–Фабера–Ловаса* (теорія графів). Свої результати та гіпотези Ердеш формулював у манері, зрозумілій навіть неспеціалістам. Наприклад, досі не розв'язана гіпотеза Ердеша–Штрауса стверджує, що *для кожного натурального числа* $n \geq 2$ *знайдуться такі три натуральні числа* x, y, z, *що*

$$\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}.$$

У 1939 р. П. Ердеш довів теорему Ердеша–Каца (*фундаментальну теорему ймовірнісної теорії чисел*) про те, що кількість простих дільників числа є, в деякому сенсі, нормально розподіленою. Ердеш дізнався про цю гіпотезу на лекції М. Каца у Принстоні (США) і після

лекції прийшов до нього з доведенням теореми.

У 1949 р. П. Ердеш одночасно з А. Селбергом (див. [Селберг], стор. 382) знайшов елементарне доведення теореми про прості числа (див. [Теорема про прості числа], стор. 382). Сталось так, що саме Селберг отримав за це доведення медаль Філдса, найвидатнішу нагороду серед математиків. Сам Ердеш у 1983 р. отримав премію Вольфа за "*елементарне доведення теореми про прості числа ... яке багато математиків вважали неможливим ...* ".

Ердеш є найпродуктивнішим математиком за усю історію. За кількістю опублікованих статей (більше 1500) йому немає рівних, але за кількістю опублікованих сторінок його випереджає Леонард Ойлер. Переважна кількість його робіт з'явилися у співавторстві. Оскільки з ним співпрацювали більш ніж 500 його колег, цілком справедливим є використання *чисел Ердеша*, що характеризують близкість кожного математика до Ердеша. Число Ердеша кожного математика визначається як довжина мінімального ланцюжка співавторів, який закінчується самим Ердешем.*

Лежандр, *Адріен-Марі* (1752–1833), видатний французький математик, чиє ім'я внесено у список найвидатніших вчених Франції, який розміщено на першому поверсі Ейфелевої вежі в Парижі. Багато сучасних понять та результатів пов'язано з ім'ям Лежандра: поліноми Лежандра, перетворення Лежандра. Його внесок у геометрію, теорію чисел, аналіз є незаперечним. Лежандр першим відкрив і застосував в обчисленнях метод найменших квадратів, широко вживаний у наш час. Його "*Елементи геометрії*" довгий час були стандартом строгості та послідовності.

---

*Наприклад, число Ердеша автора цієї книжки дорівнює 2, оскільки я маю спільну роботу з К. Х. Індлекофером, який має спільну роботу з Ердешем. Таким чином, моє число Ердеша визначається ланцюжком співавторів Клесов → Індлекофер → Ердеш. Існують й інші ланцюжки моїх співавторів, які приводять до Ердеша, наприклад Клесов → Штайнебах → Дехойвелс → Ердеш, але попередній є дійсно найменшим, хоча є ще один мінімальний: Клесов → Катаї → Ердеш.

Єдиним зображенням Лежандра, що дійшло до нашого часу, є наведене тут. Це карикатура на нього французького митця Бейлі (у повному варіанті на ній же зображено ще й іншого французького математика Жозефа Фур'є). Раніше в біографічних описах Лежандра широко використовувався інший портрет, але в 2009 році було остаточно з'ясовано, що він належить іншій людині.

Селберг, *Атле* (1917–2007), норвезький математик, спеціаліст у галузі аналітичної теорії чисел та теорії функцій. його математичні здібності виявились рано: у віці 12 років він вже вивчав математику на університетському рівні; у віці 15 років опублікував свою першу математичну роботу. Його кандидатську дисертацію було присвячено гіпотезі Рімана про нуля ζ функції. Про математичний талант Селберга краще за все свідчить розмова між видатними математиками К. Зігелем (який під час світової війни перебував у США) та Х. Бором, який весь цей час знаходився в окупованій Данії. Перший запитав у другого: "Що відбулося у Європі за ці роки?" Відповіддю Бора було: "*Селберг*".

У 1946 році А. Селберг переїхав до Принстона (США), де невдовзі зрозумів зв'язок між своїми дослідженнями стосовно гіпотези Рімана та теоремою про прості числа. Невдовзі він отримав результати, які зараз називають *решетом Селберга* та *фундаментальною формулою Селберга*. Це дозволило йому (паралельно з П. Ердешем (див. `[Ердеш]`, стор. 379)) знайти елементарне доведення теореми про прості числа (див. `[Теорема про прості числа]`, стор. 382). У 1950 році за це досягнення його було нагороджено найпрестижнішою серед математиків премією Філдса.

У 1956 році А. Селберг довів ще один результат, *формулу сліду Селберга*, яку багато хто з математиків вважають одним з найвидатніших досягнень математики XX сторіччя.

Крім премії Філдса, його було нагороджено премією Вольфа у 1986 році й почесною премією Абеля у 2002 році.

Теорема про прості числа, (1798–1896), відоме твердження про

асимптотику функції $\pi(x)$ (кількості простих чисел до x). Висловлено в 1797 або 1798 році А.-М. Лежандром після ретельного вивчення існуючих таблиць простих чисел. Гіпотеза Лежандра полягала у тому, що $\pi(x)$ добре наближається функцією

$$\frac{x}{A\log(x)+B}.$$

Числові значення $A=1$, $B=-1.08366$ Лежандр навів в 1808 році. В 1838 році П. Дірихле запропонував іншу апроксимацію для $\pi(x)$ за допомогою інтегрального логарифма

$$\int_2^x \frac{dt}{\log t}.$$

Кожна з цих апроксимацій означає, що

$$\pi(x)\sim\frac{x}{\log(x)}, \qquad x\to\infty.$$

Саме цей результат зараз називають *теоремою про прості числа*.

Важливими дослідженнями асимптотики функції $\pi(x)$ стали роботи П. Л. Чебишова (див. [Чебишов], стор. 383), опубліковані в 1848–1850 роках. В 1859 році Б. Ріман запропонував інший підхід, оснований на комплексному аналізі, який в 1896 році привів до доведення теореми про прості числа Ж. Адамаром (див. [Адамар], стор. 377) та Ш. Валле Пуссеном (див. [Валле Пуссен], стор. 378). Лише в 1949 році А. Селбергом (див. [Селберг], стор. 382) та П. Едешем (див. [Ердеш], стор. 379) були знайдені доведення цієї теореми без використання комплексного аналізу.

В XIX сторіччі один з захоплених авторів писав, що складнощі доведення теореми про прості числа можна порівняти зі складнощами, які у свій час здолав міфічний герой Геракл. Автор закінчив свою фразу так: “І винагорода за доведення теореми про прості числа буде такою ж, яку від богів отримав Геракл”. З міфів про Геракла ми знаємо, що нагородою йому стало безсмертя. П. Рібенбойм, видатний сучасний спеціаліст з теорії чисел, додає: “Боги дійсно подарували безсмертя за доведення теореми про прості числа: Адамар прожив 98

років, а Валле Пуссен — 96 років. Майже 200 років, поділені між двома, це безсмертя у людському суспільстві".

Чебишов, *Пафнутій Львович* (1821–1894), видатний російський математик і механік. З багаточисельних математичних відкриттів Чебишова треба згадати насамперед дослідження з теорії чисел. Початок ним було покладено докторською дисертацією Чебишова "*Теорія порівнянь*", надрукованою в 1849 році; вона стала першою в Російській імперії монографією з теорії чисел. Ця праця кілька разів перевидавалась, була переведена на німецьку та італійську мови. В 1850 з'явився його знаменитий мемуар "*Memorie sur les nombres premiers*", де наведено дві межі для кількості простих чисел, що знаходяться між двома даними числами. У своїй статті 1866 року "*Про одне арифметичне питанні*" він, використовуючи апарат ланцюгових дробів, досліджував діофантови наближення цілих чисел. В аналітичній теорії чисел він одним з перших використав гамма-функцію.

Загальновідомими є його досягнення у теорії ймовірностей (*нерівність Чебишова*), теорії наближення функцій (*поліноми Чебишова*), математичному аналізі (*теорема Чебишова про інтегровність диференціального бінома*). У балістиці відомою є *формула Чебишова* про дальність польоту снарядів. Кілька сконструйованих Чебишовим механізмів, які імітували рух тварин при ходьбі, були представлені на міжнародних виставках.

Список літератури

1. Н. В. Алфутова, А. В. Устинов, *Алгебра и теория чисел. Сборник задач*, МЦНМО, Москва, 2002.
2. З. И. Боревич, И. Р. Шафаревич, *Теория чисел*, "Наука", Москва, 1985.
3. А. А. Бухштаб, *Теория чисел*, "Просвещение", Москва, 1966.
4. О. Н. Василенко, *Теоретико-числовые алгоритмы в криптографии*, "МЦНМО", Москва, 2006.
5. И. М. Виноградов, *Основы теории чисел*, "Наука", Москва, 1976.
6. Е. И. Деза, Л. В. Котова, *Сборник задач по теории чисел*, УРСС, Москва, 2011.
7. С. А. Дориченко, В. В. Ященко, *25 этюдов о шифрах*, "Теис", Москва, 1994.
8. Д. Кан, *Взломщики кодов*, "Центрполиграф", Москва, 2009; пер. с англ.D. Kahn, *The Codebreakers*, New American Library, New York, 1967.
9. С. Коутинхо, *Введение в теорию чисел. Алгоритм RSA*, "Постмаркет", Москва, 2001; пер. с англ. S. Coutinho, *The Mathematics of Ciphers. Number Theory and RSA Criptography*, A. K. Peters, Natick, Massachusetts, 1999.
10. В. И. Нечаев, *Элементы криптографии*, "Высшая школа", Москва, 1996.
11. В. О. Осипян, К. В. Осипян, *Криптография в упражнениях и задачах*, Гелиос АРВ, Москва, 2004.
12. Г. Г. Харди, *Апология математика*, "УРСС", Москва, 2004; пер. с англ.G. Hardy, *A Mathematician's Apology*, Cambridge University Press, Cambridge, 1940.
13. А. В. Черемушкин, *Лекции по арифметическим алгоритмам в криптографии*, "МЦНМО", Москва, 2002.
14. В. В. Ященко (под. ред.), *Введение в криптографию*, 3-е изд., "МЦНМО", Москва, 2000.

15. J. A. Buchmann, *Introduction to cryptography*, second edition, Springer Verlag, New York, 2004.
16. L. E. Dickson, *History of the Theory of Numbers*, vol. I: Divisibility and Primality, Chelsea Publishing Company, New York, 1952; (перше видання зявилось в 1919 році).
17. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Clarendon Press, Oxford, England, 1979.
18. T. Koshy, *Elementary Number Theory with Applications*, 2nd edition, Elsevier, Amsterdam, 2007.
19. P. Ribenboim, *The New Book of Prime Number Records*, Springer-Verlag New York, Inc., New York, Berlin, Heidelberg, 1996.
20. K. H. Rosen, *Elementary Number Theory*, 6th edition, Addison Wesley, Boston MA.
21. W. Stein, *Elementary Number Theory: Primes, Congruences, and Secrets. A computational Approach*, Springer-Verlag, New York, 2009.
22. J. Talbot and D. Welsh, *Complexity and Criptography. An Introduction*, Cambridge University Press, Cambridge, 2006.
23. A. L. Young, *Mathematical Ciphers: from Caesar to RSA*, American Mathematical Society, Providence, RA, 2006.

ПРЕДМЕТНИЙ ПОКАЖЧИК

$Αριθμητικα$ 87
$Σποιχεῖα$ 88
$\mathcal{C}_{\mathtt{X}}$ 66
$E_{k,n}$ 180
$\mathrm{Jac}\,(a,n)$ 318
$\mathrm{Leg}\,(a,p)$ 318
$L_{a,b}$ 136
M_a 66
$M_{a,n}$ 72
RSA-129 237
RSA-640 209
tabula recta 52
$\mathrm{dlog}_{a,n}(h)$ 215
$\pi(x)$ 351
$\mathcal{P}_{\mathtt{X}}$ 66
$\vartheta(x)$ 351
$\phi\,(n)$ 140

A

Агравал, М. 336
Адамар, Ж. 358
азбука
— Брайля 18
— Морзе 19
“Апологія математика” 1
Аліса 229
алгоритм
— RSA, вибір параметрів 239
— RSA, дешифрування 240
— RSA, шифрування . 239
— АКС 336
— електронне голосування 286
— електронні гроші ... 284
— знаходження частки та остачі 88
— Крайчика 213
— Міллера–Рабіна 334
— перевірки чисел на простоту, послідовний перебір 11
— решето Ератосфена . 13
— сліпий цифровий підпис 279
— Ферма, факторизації 243
— цифровий підпис в методі Ель-Гамаля 288
— швидкого піднесення до степеня 190

— швидкого піднесення до степеня за модулем 191
— Шенкса 218
алгоритм Евкліда 88
— знаходження найбільшого спільного дільника 90
— знаходження оберненого за модулем 96
— розширений 99
Альфорд, В. 315
Арнольд, В. І. IX
атака на криптографічні шифри 242
аутентифікація 269

Б

Бертран, Ж. 358
бінарне представлення ... 192
Боб 229
Больцман, Л. ..... -10
Брайль, Л. 18

В

Вайлс, Е. IX
Валле Пуссен, Ш. 358
відношення
— еквівалентності 45
— рефлексивності 45
— симетричності 45
— транзитивності 45
Віженер, Б. 51
Верн, Ж. 6
Вернам, Г. 53
взаємно прості числа 47

Г

Гарднер, М. 59
Гаусс, К. 2
Гільберт, Д. ..... -10
гіпотеза Рімана 336
головоломки Меркла 230
Гранвиль, Е. 315
групування 75

Д

да Вінчі, Л. ..... -10
дайджест 273
ділення
— остача 44
— частка 44
ділення з остачею 43
Діффі, В. 230
дискретний логарифм 215

Е

Евклід 88
Еделман, Л. 232
електронні гроші 282
Ель-Гамаль, Т. 248
Ератосфен 12
Ердеш, П. 358

З

задача про рюкзак 244
— для суперзростаючих послідовностей 244
закон розподілу простих чисел 50
захист пароля 216
золотий переріз 92

К

Капіца, П. Л. VIII
Кармайкл, Р. 313
Каян, Н. 336
— лишок 317
— нелишок 318
Керкхоффс, О. 164
ключ
— відкритий 231
— відкритий RSA 234
— приватний 231
— приватний RSA 234
Кнут, Д. V
код клавіатури 38
кодування 9
Конан Дойль, А. 5
конгруентні числа 44
константа Капрекара 59
корінь
— первісний 217
— примітивний 217
Корселт, А. 315
криптосистема
— Ель-Гамаля 251
— з відкритим ключем 229
— рюкзачна 244
криптографічна стійкість . 53
криптографія 4
критерій
— Вілсона 308
— Корселта 315
— Ойлера 14

Л

лінійне рівняння за модулем
— дві невідомі 93
— одна невідома 113
Ламе, Г. 92
Лежандр, А. 317
лексикографічний порядок 77
Ленстра, Х. 336
Ляйбніц, Ґ. 7

М

Манін, Ю. І. .....-10
математичні шифри 9
Меркл, Р. 230
метод
— грубої сили 73
— Діффі–Хеллмана ... 231
— повного перебору 73

— Полларда 82
— смужок 55
— факторизації, Крайчика 211
Міллер, Г. 328
модель Чаума 283
Морган де, А. 59
Морзе, С. 19

Н

найбільший спільний дільник 46
найменше спільне кратне .104
Неш, Д. 165
Ньютон, І. 7

О

обернене число за модулем n 71
Ойлер, Л. 140
основна теорема аналіза 8
основна теорема арифметики 2

П

Пастер, Л. VIII
перестановочний шифр 16
Піфагор 3
Плейфер, Л. 123
По, Е. 5
показник кореня 184
— за модулем $n = p$ ... 186
— за модулем $n = pq$ .. 188
Поліґ, С. 180
Померанц, К. 237
постулат Бертрана 358
представлення числа
— бінарне 189
— двійкове 189
— Керкхоффса 164
— складності обчислень 164
просте число 47
протокол
— AES 301
— DES, спрощений 301
псевдопросте число
— за основою n 311
— строго 332

Р

Рабін, М. 335
Рівест, Р. 232
репюніт 25
решето
— Ератосфена 12
— квадратичне 237
розподілення секретів 293
рукопис Войніча 167

С

Саксена, Н. 336
свідок простоти числа 309

Сельберг, А. 358
символ
— Лежандра 317
— Якобі 317
система
— двох лінійних рівнянь за модулем 114
— лінійних конгруенцій 119
сліпий цифровий підпис
— абсолютна впевненість 279
— неможливість пов'язати підпис та повідомлення 279
— нульове розголошення 279
Соловей, Р. 317
Сталлмен, Р. 238
стеганографія 37
— мікрокрапка 37
— невидимі чорнила ... 37
— цифрові водяні знаки 37
суперзростаюча послідовність 244

Т

таємне голосування 285
теорема
— Вільсона 82
— китайська про остачі 120
— Корселта 315
— Ламе 92
— Ньютона–Ляйбніца ... 8
— Ойлера 145
— Поклінгтона 342
— про існування оберненого за модулем 71
— про нескінченість множини простих чисел .. 3
— про прості числа ... 357
— Прота 343
— Райта 363
— Ферма, велика IX
— Ферма, мала 147
— Чебишова 356
тест
— Люка–Лемера 344
— Міллера 329
— Міллера–Рабіна 334
— Соловея–Штрассена 319
— Ферма 310
тотожність Чебишова 360

Ф

Ферма, П. 4
формула
— включення/виключення 142
— Міллса 308
функція
— мультиплікативна .. 145

— одностороння 214
— одностороння, з секретом 214
— Ойлера 140
— Чебишова 351

Х

Харді, Ґ. IX
Хеллман, М. 180
хеш функція 275
Хілл, Л. 110

Ц

Цезарь, Юлій 39
цифра
— бінарна 189
— двійкова 189
цифровий підпис
— метод Ель-Гамаля ..287
— метод RSA 270
— сліпий 277

Ч

частотний аналіз 160
Чаум, Д. 277
Чебишов, П. Л. 351
числа
— Жермейн 223
— Кармайкла 313
— Мерсенна 343
— прості 47
— складені 47
— Ферма 26
— Фібоначчі 25

Ш

Шамір, А. 232
шифр-матриця 52
шифр
— RSA 232
— адитивний 66
— афінний 136
— блочний 110
— Вернама 53
— Віженера 51
— експоненціальний .. 180
— лінійний 136
— моноалфавітний 39
— мультиплікативний .. 66
— одноразового блокноту 53
— перестановки 16
— підстановочний 38
— Плейфера 123
— поліалфавітний 51
— простої заміни 39
— рандомізований матричний 17
— Хілла 110
— Цезаря 39
Штрассен, Ф. 317

Основні позначення

(m, n)	найбільший спільний дільник m та n
$[m, n]$	найбільше спільне кратне m та n
$m \mid n$	m ділить n
$m \div n$	m ділиться на n
$a \pmod n$	остача від ділення a на n
$a^{-1} \pmod n$	обернене до a за модулем n
$\phi(n)$	функція Ойлера для аргументу n
$\left(\frac{a}{n}\right)$	символи Лежандра та Якобі
$\pi(x)$	кількість простих чисел до x
$\vartheta(x)$	функція Чебишова для аргументу x
$(d_i \dots d_0)_{10}$	запис числа у десятковій системі
$(b_i \dots b_0)_2$	запис числа у двійковій системі
$\mathscr{A}$	алфавіт
C_a	шифр Цезаря
$M_{a,n}$	мультиплікативний шифр з параметрами a та n
M_a	мультиплікативний шифр для $n = 33$
$L_{a,b,n}$	лінійний шифр з параметрами a, b, n
$L_{a,b}$	лінійний шифр для $n = 33$
$\mathrm{dlog}_{a,n}(x)$	дискретний логарифм числа x
$\lceil z \rceil$	$\min n : n \geq x$
$\mathcal{P}_{\mathtt{X}}$	позиція букви `X` в алфавіті
$\mathcal{C}_{\mathtt{X}}$	позиція в алфавіті букви, у яку шифрується `X`
$\mathcal{S}_{\mathtt{X}}$	символ `X` оригінального підпису
$\mathcal{H}_{\mathtt{X}}$	символ `X` цифрового підпису

Підручник

ОЛЕГ ІВАНОВИЧ КЛЕСОВ

ЕЛЕМЕНТАРНА ТЕОРІЯ ЧИСЕЛ ТА ЕЛЕМЕНТИ КРИПТОГРАФІЇ

Редактор Іванов О. В.
Художник Моклячук О. М.
Коректор Попович С. І.

Оригінал-макет виготовлено за допомогою пакета $\mathcal{AMS}$-TEX
з використанням кирилізації LHamsppt © І. І. Клесова

Підписано до друку 28.3.2017. Формат 60 × 84/16
Папір офсетний. Друк високий. Друк. арк. 26,00
Умов. друк. арк. 24,25. Тираж 300 прим. Замовлення 01–215

Наукове видавництво "ТВіМС"
Свідоцтво ДК110 від 05.07.2000 р.
Київ 03189, вул. Академіка Вільямса, 6-д
відділ замовлень tbimc@online.ua