Міністерство освіти і науки України
Тернопільський національний технічний університет
імені І. Пулюя

І.В. Бойко, М.Р. Петрик, Г.Б. Цуприк

ДИСКРЕТНІ СТРУКТУРИ

(*Алгебраїчні та числові системи, комбінаторний аналіз*)

Навчально-методичний посібник

Тернопіль
Видавництво ТНТУ

УДК 511.2, 512.7, 519.1, 511.4
ББК 22.13, 22.17

Рецензенти

Пастух Олег Анатолійович, доктор технічних наук, професор.
Яворська Євгенія Богданівна, кандидат технічних наук, доцент

Затверджено до друку
Вченою радою факультету комп’ютерно-інформаційних систем і програмної інженерії Тернопільського національного технічного університету імені Івана Пулюя

Бойко І.В., М.Р. Петрик, Г.Б. Цуприк
К Дискретні структури (Алгебраїчні та числові системи, комбінаторний аналіз): навчальний посібник. Тернопіль: : ТНТУ 2017 – 62 с

Даний посібник написано згідно програм предметів “Дискретні структури” та “Комп'ютерна дискретна математика”, що читаються на факультеті комп’ютерно-інформаційних систем і програмної інженерії.

Для студентів спеціальності 121 – “Інженерія програмного забезпечення”, аспірантів та викладачів вищих навчальних закладів.

Передмова

Серед технічних наук інформаційні технології та електроніка у значній мірі використовують математику. Дійсно, якщо поглянути на програми навчання студентів в університетах США та Євросоюзу, то легко виявити, що математичні дисципліни займають в них значне місце. В останні роки особливу важливість придбали ті розділи математики, які мають відношення до галузі знань інформатики та обчислювальної техніки. Базою для викладання цих дисциплін поряд з класичними методами аналізу неперервних фізичних моделей, що становлять у свій час становили основний предмет комп'ютерної науки, стали алгебраїчні, логічні і комбінаторні методи дослідження різних моделей дискретної математики.

Проте, в середній школі та вищих навчальних закладах цим предметам не приділяється достатньої уваги. Тому особливо важливого значення набувають спеціальні курси, пов'язані з професійною орієнтацією студента. Ця книга була задумана саме як спеціальний курс з теорії дискретних структур для студентів першого та третього курсів, що навчаються на напрямом "Інженерія програмного забезпечення". Дана книга значно розширює можливість вибору матеріалу для читання або викладання з урахуванням попередньої підготовки і інтересів тієї чи іншої аудиторії.

Книга призначена як для студентів початкових курсів, які вивчають основи вищої математики, так і для студентів старших курсів, що приступають до самостійних досліджень. Матеріал книги і спосіб його викладу підбиралися таким чином, щоб її можна було використовувати і як підручник, і як спеціальний посібник. З додатковими питаннями, які лише частково порушені в книзі, можна ознайомитися , скориставшись вказаними в книзі джерелами.

Зміст

РОЗДІЛ 1. АЛГЕБРАЇЧНІ СТРУКТУРИ

1.1. Метод математичної індукції

Розглянемо два підходи до задання множини натуральних чисел. Перший підхід – конструктивний – дозволяє представляти натуральні числа у вигляді об'єктів, побудованих із пустої множини. Другий підхід – аксіоматичний. Згідно цього підходу натуральні числа утворюють множину, яка задовольняє деякому набору аксіом (властивостей), і при цьому природа елементів множини не є важливою. Таким чином, з одної сторони, вказується множина натуральних чисел, а з іншої сторони – всі важливі (визначаючі) властивості цієї множини.

Для визначеності візьмемо: $0 \Leftrightarrow \varnothing; 1 \Leftrightarrow \{0\} = \varnothing; 2 \Leftrightarrow \{0, 1\} = \{\varnothing, \{\varnothing\}\}$, …, $n = \{0, 1,..., n-1\}...$ Множини, які позначаються як $0, 1, 2,...,$ називаються натуральними числами. Об'єднуючи ці множини, отримаємо множину натуральних чисел $\{0, 1, 2,..., n,...\}$, яку позначимо N.

Таким чином, можна записати, що якщо $A = \{0, 1,.., n-1\}$, $B = 2 = \{0, 1\}$, то $2^A = B^A = \{f \mid f : n \to \{0, 1\}\}$. Це позначення узгоджується з тим, що у множині B^A міститься 2^n функцій. Дійсно, оскільки функція f на аргументі $i \in n$ може примати одне з двох значень 0 чи 1 і кількість таких елементів i є рівною n, то всього міститься $2 \cdot 2 \cdot ... \cdot 2 = 2^n$ різних функцій.

Аналогічно маємо, що $2^\omega = \{f \mid f : \omega \to \{0, 1\}\}$ - множина, яка складається з усіх можливих послідовностей нулів та одиниць.

Як уже відмічалось, другий підхід до визначення множини натуральних чисел є аксіоматичним. В подальшому розглянемо аксіоматику Дедекінда-Пеано.

Нехай маємо деяку множину N, в якій вибрано елемент, який позначається 0, і функція, яка довільному елементу $n \in N$ ставить у відповідність елемент $n' \in N$, який називається ***безпосередньо наступним*** (елемент n' відіграє роль числа $n+1$). Таким чином, за допомогою функції

$n \to n'$ можна однозначно знайти елементи $0', 0'', 0'''$ і т.д. (елемент $0^{(n)}$ відіграє роль числа n). Множина N називається множиною натуральних чисел, якщо система $N = \langle N, 0, ' \rangle$ задовольняє таким аксіомам:

1) для будь-якого $m \neq 0$ знайдеться номер $n \in N$ такий, що $n' = m$;

2) для будь-яких $m, n \in N$, якщо $m' = n'$, то $m = n$;

3) $n' \neq 0$ для будь-якого $n \in N$;

4) (аксіома математичної індукції) для будь-якої властивості P (унітарного відношення на множині N), якщо P виконується на елементі 0 (тобто має властивість P), і для будь-якого $n \in N$ з виконуваності властивості P для елемента n випливає виконуваність P для елемента n', то властивість P виконується для будь-якого елемента т $n \in N$.

Остання аксіома є найбільш змістовною, вона символічно записується наступним чином:

$$\forall P\Big(\big(P(0), \forall n(P(n) \Rightarrow P(n'))\big) \Rightarrow \forall n P(n)\Big), \qquad (1.1.1)$$

а також:

$$\frac{P(0), \forall n\,(P(n) \Rightarrow P(n+1))}{\forall n\ P(n)}$$

або

$$\frac{0 \in P, \forall n\,(n \in P \Rightarrow (n+1) \in P)}{P = N}.$$

Значить, твердження "для будь-якого $n \in N$ виконується $P(n)$" вважається доведеним, якщо встановленими є ***базис індукції*** (доведено $P(0)$) та ***крок індукції*** (доведено, що для будь-якого $n \in N$ справедливим є $P(n+1)$ в припущенні, що виконується $P(n)$). В цьому і полягає принцип математичної індукції.

Принцип математичної індукції дозволяє задавати ***індукційні визначення***, тобто визначення понять $P(n)$ для всіх натуральних чисел n, які будуються згідно такої схеми:

1) задається значення $P(0)$,

2) задається правило отримання значення $P(n+1)$ за числом n і значенням $P(n)$.

Визначимо за індукцією операції додавання $a+b$ і множення $a \cdot b$ на множині натуральних чисел. Візьмемо $a+0=a$ (базис індукції). Якщо відомо значення $a+n$, то $a+n^{/}=(a+n)^{/}$ (крок індукції). Аналогічно $a \cdot 0=0$. Якщо задано $a \cdot n$, то $a \cdot n^{/}=(a \cdot n)+a$.

Використовуючи операцію додавання, кожна вивести відношення $\leq$ на множині натуральних чисел: $a \leq b \Leftrightarrow \exists c\ (a+c=b)$.

Визначимо за індукцією функцію $n!$ (n - факторіал): $0!=1;\ (n+1)!=n! \cdot (n+1)$.

Іноді вдається встановити тільки виконання $P(k)$ для деякого $k>0$ і властивість $P(n) \Rightarrow P(n+1)$ для всіх $n \geq k$. Тоді, згідно принципу математичної індукції властивість P виконується для всіх $n \geq k$:

$$\frac{P(k),\ \forall n \geq k\ (P(n) \Rightarrow P(n+1))}{\forall n \geq k\ P(n)}. \qquad (1.1.2)$$

Іншою еквівалентною формою принципу математичної індукції є принцип повної індукції:

якщо для будь-якого $n \in N$ з припущення, що $P(k)$ є правильним для довільного натурального $k<n$, випливає, що $P(k)$ є вірним також і при $k=n$, то $P(n)$ виконується і для будь-якого натурального n:

$$\frac{\forall n((\forall k<n\ P(k)) \Rightarrow P(n))}{\forall n\ P(n)}. \qquad (1.1.3)$$

Ця форма використовується в тому випадку, якщо для доведення виконання властивості $P(n+1)$ необхідно використовувати виконуваність властивості P не тільки для елемента n, але і на попередніх елементах.

Приклад 1. Довести методом математичної індукції, що 9^n-2^n ділиться на 7 для довільного натурального n.

Доведення

Твердження $P(n)$ полягає в тому, що $9^n - 2^n$ ділиться на 7.

Перевіримо базу індукції, тобто встановимо твердження $P(0)$, яке полягає в тому, що $9^0 - 2^0 = 1 - 1 = 0$, очевидно, ділиться на 7.

Припустимо, що істинним є твердження $P(k)$, тобто $9^k - 2^k$ ділиться на 7. Перевіримо істинність твердження $P(k+1)$:

$9^{k+1} - 2^{k+1} = 9 \cdot 9^k - 2 \cdot 2^k = 7 \cdot 9^k + 2 \cdot 9^k - 2 \cdot 2^k = 7 \cdot 9^k + 2 \cdot (9^k - 2^k)$.

Перший доданок, очевидно, ділиться на 7, а другий ділиться на 7 за припущенням індукції. Таким чином, згідно із принципом математичної індукції твердження є доведеним.

Приклад 2. Довести методом математичної індукції, що $1 + 3 + ... + (2n-1) = n^2$.

Доведення

Нехай твердження $P(n)$ полягає в тому, що рівність $1 + 3 + ... + (2n-1) = n^2$ виконується для заданого n. Необхідно довести, що твердження $P(n)$ є істинним для всіх $n \geq 1$.

Для $n = 1$ маємо, що $1 = 1^2$, що є правильним.

Нехай $P(k)$ є істинним для деякого k, тобто $1 + 3 + ... + (2k-1) = k^2$.

Доведемо істинність твердження $P(k+1)$:

$1 + ... + (2k-1) + (2k+1) = (1 + 3 + ... + (2k-1)) + (2k+1) = k^2 + 2k + 1 =$
$= (k+1)^2$.

Таким чином, з істинності $P(k)$ випливає істинність твердження $P(k+1)$, а значить, згідно принципу математичної індукції тотожність є доведеною.

Приклад 3. Довести методом математичної індукції, що для будь-якого натурального n виконується нерівність $3^n > n^2$.

Доведення

Перевіримо базу індукції: $3^0 > 0^2$, оскільки $1 > 0$.

Нехай нерівність виконується при $n = k$, тобто $3^k > k^2$. Маємо: $3^{k+1} = 3 \cdot 3^k > 3k^2$, згідно індуктивної гіпотези. Для завершення доведення

треба довести, що $3k^2 \geq (k+1)^2$, так як в цьому випадку отримаємо, що $3^{k+1} > (k+1)^2$. Розв'яжемо нерівність $3k^2 \geq (k+1)^2$:

$3k^2 > k^2 + 2k + 1;\ 2k^2 - 2k - 1 > 1$.

Значить, $k \in \left(-\infty, \frac{1-\sqrt{3}}{2}\right] \cup \left[\frac{1+\sqrt{3}}{2}, \infty\right)$.

Оскільки $\frac{1+\sqrt{3}}{2} < 2$, отримаємо $3k^2 \geq (k+1)^2$ для $k \geq 2$. Проте для $k = 0; 1$ ця нерівність не виконується. Тому ми не зможемо довести, що $3^{k+1} > (k+1)^2$ для цих значень k і для них прийдеться перевірити виконання нерівності безпосередньо:

$3^1 > 1^2$, оскільки $3 > 1$,

$3^2 > 2^2$, так як $9 > 4$.

Список рекомендованих до розв'язування задач.

1. Довести методом математичної індукції тотожності.

а) $1 \cdot 1! + 2 \cdot 2 + \ldots + n \cdot n! = (n+1)! - 1$;

б) $0 \cdot 3 + 1 \cdot 4 + \ldots + n(n+3) = \frac{n(n+1)(n+5)}{3}$;

в) $1 \cdot 0! + 2 \cdot 1! + 5 \cdot 2! + \ldots + (n^2+1) \cdot n! = n(n+1)! + 1$;

г) $1 \cdot 3^0 + 3 \cdot 3^1 + \ldots + (2n+1) \cdot 3^n = n \cdot 3^{n+1} + 1$;

д) $1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$;

е) $\frac{2^3-1}{2^3+1} \cdot \frac{3^3-1}{3^3+1} \cdot \ldots \cdot \frac{n^3-1}{n^3+1} = \frac{2}{3}\left(1 + \frac{1}{n(n+1)}\right)$.

2. Довести методом математичної індукції твердження:

а) $n^3 - n$ ділиться на 6;

б) $12^n - 5^n$ ділиться на 7;

в) $8^{2n+1} + 1$ ділиться на 9;

г) $2^{2n+1} + 9^{2n+1}$ ділиться на 11;

д) $7^n - 6n - 1$ ділиться на 9.

3. Довести методом математичної індукції нерівності:

а) $2^n > n$ для натуральних n;

б) $2^n < n!$ для натуральних $n \geq 4$;

в) $3^n > n \cdot 2^n$ для натуральних n;

г) $3^n > n \cdot 2^{n+1}$ для натуральних $n \geq 7$;

д) $\frac{(2n)!}{(n!)^2} \geq \frac{4^n}{n+1}$ для натуральних n;

е) $\frac{1}{n+1} + \frac{1}{n+2} + ... + \frac{1}{2n} \geq \frac{1}{2}$ для натуральних $n \geq 1$;

д) $\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + ... + \frac{1}{\sqrt{n}} \geq \sqrt{n}$ для натуральних $n \geq 1$.

3. Довести, що число, складене з 3^n одиниць, ділиться на 3^n.

4. Довести методом математичної індукції, що число елементів в множині $P(A)$ рівне 2^n, де n - кількість елементів в множині A.

5. Перевіривши співвідношення $C_n^{k-1} + C_n^k = C_{n+1}^k$, довести формулу бінома Ньютона методом математичної індукції.

1.2. Властивості цілих чисел

Впорядкованість.

Позначимо через Z множину усіх цілих чисел. Цілі числа мають природній порядок: $...-3,-2,-1,0,1,2,3...$

Це означає, що цілі числа пов'язані співвідношенням "більше-менше", яке установлює, що число, яке знаходиться справа завжди є більшим від числа, яке знаходиться зліва від нього. Множину усіх додатних цілих чисел позначимо як Z^+. При цьому запис співвідношення $a < b$, яке означає, що у приведеній вище послідовності число a знаходиться зліва від числа b є еквівалентним тому, що $b - a \in Z^+$.

Визначимо бінарне відношення "≤", яке має три очевидні властивості:

а) (Рефлексивність): $a \le a$;

б) (Антисиметричність): якщо $a \le b$ і $b \le a$, то $a = b$;

с) (Транзитивність): якщо $a \le b$ і $b \le c$, то $a \le c$.

Згадані властивості називаються аксіомами порядку. Крім співвідношення порівняння цілих чисел аксіомам порядку задовольняють також співвідношення включення $\subset$, що справедливі з діями над множинами. Якщо на деякій множині G визначене бінарне відношення "≤", яке задовольняє аксіомам а)-с), то множина G називається упорядкованою. Якщо для довільних елементів $x, y \in Z$, обов'язково $x \le y$ або $y \le x$, то таку упорядкованість називають повною, а в іншому випадку її називають частково упорядкованою. Відношення "більше-менше" у множині Z є відношенням повної упорядкованості.

Мінімальним елементом непустої множини S називається елемент $s \in S$, такий, що $s \le x$ для будь-якого $x \in S$.

Якщо довільна непуста підмножина впорядкованої множини G має мінімальний елемент, то множина G називається цілком впорядкованою множиною.

Теорема 1.2.1. Множина всіх цілих додатних чисел є цілком впорядкованою множиною відносно відношення “більше-менше”, а його мінімальним елементом є число 1.

Наприклад, мінімальний елемент множини додатних парних чисел є число 2. Множина всіх цілих чисел Z мінімального елемента не має і тому не є цілком впорядкованою множиною.

Наслідок з Теореми 1.2.1. Нехай деяка множина цілих додатній чисел S задовольняє наступні умови: 1) $1 \in S$; 2) якщо $n \in S$, то $n+1 \in S$. Тоді $S = Z^+$.

Якщо для чисел $a, b, q \in Z$ виконується співвідношення $a = bq$, то кажуть, що a є кратним b, а b - дільником a. При цьому також кажуть, що b ділить a, і записують це у вигляді: $b \mid a$.

Очевидно, що виконуються такі властивості:

1. Закон рефлексивності: $a \mid a$;

2. Закон транзитивності. Якщо $a \mid b$ і $b \mid c$, то $a \mid c$.

При цьому закон анти симетричності не виконується. Наприклад числа 2 і -2 діляться одне на одне, але рівними при цьому не є.

Теорема 1.2.2. Дільниками числа 1 є тільки числа +1 і -1.

Наслідок 1 з теореми 1.2.2. Якщо $a \mid b$ і $b \mid a$, то $a = b$ або $a = -b$.

Доведення

Оскільки $a = bd_1$ і $b = ad_2$, то тоді: $a = ad_1d_2$. Тому $1 = d_1d_2$ і, згідно теореми, $d_1 = \pm 1$.

Даний наслідок показує, що в множині цілих додатних чисел закон антисиметричності виконується.

Наслідок 2 з теореми 1.2.2. Якщо $a, b \in Z^+$ і $a \mid b$ і $b \mid a$, то тоді $a = b$.

Найбільш часто використовувані властивості подільності виражаються у наступних теоремах.

Теорема 1.2.3. Якщо всі цілі числа, які містяться у рівності $k + l + ... + m = p + q + ... + s$, за виключенням одного, є кратними числу b, то і число яке залишилося також є кратним до b.

Теорема 1.2.4. Для довільного цілого числа $a \in Z$ і цілого додатного числа $b \in Z^+$ однозначно визначаються неповна частка q і остача r такі, що $a = bq + r,\ 0 \le r < b$.

Припустимо, що деяка непуста множина цілих чисел S є замкнутою відносно операції додавання і віднімання. Інакше кажучи, ми будемо уважати, що для довільних чисел $a, b \in S$ їх сума $a + b$ та різниця $a - b$ також є елементами множини S. Припустимо, що S містить елемент $a \neq 0$. Тоді $a - a = 0$ і значить, $0 - a = -a \in S$. Тоді або a, або $-a$ - ціле додатне число, множина S містить, як мінімум одне ціле додатне число. Значить, в множині S міститься мінімальне додатне число b.

Якщо поділити довільне число $a \in S$ на b, то неповну частку q і остачу r, які задовольняють умовам теореми 1.3. Так як $a \in S$ і $bq \in S$, то $r = a - bq \in S$. Таким чином, якщо $r > 0$, то нерівність $r < b$ суперечить тому, що b - це мінімальне число в S. Значить, $r = 0$, і число a є кратним числу b. Це виражається наступною теоремою.

Теорема 1.2.5. Непуста множина цілих чисел, замкнута відносно операцій додавання та віднімання, складається або тільки з одного числа 0, або в ньому міститься тільки мінімальне додатне число b і множина складається з усіх чисел кратних b.

1.3. Найбільший спільний дільник.

Число p називається спільним кратним чисел $a, b, ..., l$, якщо воно є кратним до кожного з цих чисел. Очевидно, що множина S усіх спільних кратних чисел $a, b, ..., l$ є замкнутим відносно операцій додавання і віднімання. За виключенням випадку, коли одне з чисел $a, b, ..., l$ є рівним 0, в S завжди міститься додатне ціле число. Це число називається найменшим спільним кратним. Іншими словами, найменшим спільним кратним деякої сукупності відмінних від нуля чисел називається є найменше ціле число з цієї

сукупності. Згідно теореми 1.5. множина всіх спільних кратних S співпадає з множиною всіх цілих чисел, кратних найменшому спільному кратному.

Число p називається спільним дільником чисел $a, b,..., l$ якщо воно є дільником кожного з них. За винятком особливого випадку, коли всі числа $a, b,..., l$ є рівними нулю, серед спільних дільників зажди міститься найбільший, оскільки всі вони по абсолютній величині не є більшими від найменшого з чисел $|a|, |b|,..., |l|$. Цей дільник називається найбільшим спільним дільником і позначається $(a, b,..., l)$. Якщо $(a, b,..., l) = 1$, то числа $a, b,..., l$ є взаємно простими.

Приклад 1. Покажіть, що якщо $b \mid a$ і $b \in Z^+$, то множина спільних дільників чисел a і b та множина дільників числа b співпадають, зокрема, $(a, b) = b$.

Розв'язання

Очевидно, що спільний дільник a і b є дільником b. Навпаки, якщо $x \mid b$, то $x \mid a$, оскільки $b \mid a$. Значить x є спільним дільником a і b. Тому сукупність спільних дільників чисел a і b співпадає з сукупністю дільників b. Оскільки $b \in Z^+$, то серед дільників b найбільшим є воно саме, так що $(a, b) = b$.

Приклад 2. (самостійно). Якщо $a \in Z^+$, то $(a, 0) = a$; якщо $-a \in Z^+$, то $(a, 0) = -a$.

Алгоритм Евкліда. Доведіть, що якщо $a = bq + r$, то сукупність спільних дільників чисел a і b співпадає з сукупністю спільних дільників чисел b і r, зокрема $(a, b) = (b, r)$.

Для визначення найбільшого спільного дільника (a, b) для чисел $a, b \in Z$ з використанням наслідків прикладів 1 і 2 справедлива така схема:

$$\left.\begin{aligned} a &= bq_1 + r_2, \quad 0 < r_2 < b; \\ b &= r_2 q_2 + r_3, \quad 0 < r_3 < r_2; \\ r_2 &= r_3 q_3 + r_4, \quad 0 < r_4 < r_3; \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n, \quad 0 < r_n < r_{n-1}. \end{aligned}\right\} \qquad (1.3.1)$$

Оскільки остача від ділення з кожним кроком алгоритму зменшується, тому кількість кроків алгоритму Евкліда є скінченою. Тоді, оскільки $(a, b) = (b, r_2), (b, r_2) = (r_2, r_3),...,$ то $(a, b) = (r_{n-1}, r_n)$.

Тоді з схеми алгоритму (1) маємо:

$r_2 = a + (-q_1)b,$

$r_3 = (-q_2)a + (1 + q_1 q_2)b.$

Продовжуючи процес, знаходимо такі $s, t \in Z$, що $r_n = sa + tb$.

Таким чином, отримуємо таку лему.

Лема 1.3.1. Для будь яких цілих не рівних одночасно нулю чисел a і b існують числа $s, t \in Z$, такі, що

$$(a, b) = sa + tb. \qquad (1.3.2)$$

Нехай S - множина всіх цілих чисел, що отримують ся при додаванні чисел, кратних числу a і чисел, кратних числу b, тобто: $S = \{n \in Z\}\ n = sa + tb,\ st \in Z\}$.

Очевидно, що множина S є замкнутою відносно операцій додавання та віднімання, таким чином:

$(s_1 a + t_1 b) \pm (s_2 a + t_2 b) = (s_1 \pm s_2)a + (t_1 \pm t_2)b$.

Оскільки a і b одночасно не є рівними нулю, то в множині S міститься числа, які є відмінними від нуля. Згідно теореми 1.2.5, в множині S міститься мінімальне ціле додатне число:

$$k = s'a + t'b, \qquad (1.3.3)$$

і множина S співпадає з сукупністю кратних цього числа k. Тому $k \mid (a, b)$.

Оскільки $(a, b) \mid a$ і $(a, b) \mid b$, то враховуючи (1.3.3):

$$(a, b) \mid k. \qquad (1.3.4)$$

Тоді з (1.3.3) і (1.3.4) і наслідку з теореми (1.2.2) випливає, що $(a, b) = k$.

На основі отриманої доведеної леми 1.3.1. доводяться наступні теореми.

Теорема 1.3.1. Нехай a і b - два цілих числа, одночасно не рівні нулю. Мінімальне ціле додатне число в множині всіх чисел виду $sa+tb$, де s і t - довільні цілі числа, є найбільшим спільним дільником (a, b) чисел a і b.

Зауважимо, що якщо $c \mid a$ і $c \mid b$ то згідно (2.2) $c \mid (a, b)$, тобто множина всіх спільних дільників чисел a і b співпадає з множиною дільників числа (a, b).

Теорема 1.3.2. Якщо $(a, b) = 1$, $b \mid ac$, то $b \mid c$.

Доведення

Як слідує з леми 1.3.1, існують такі числа $s, t \in Z$, що $sa+tb=1$. Якщо цю рівність помножити на c, і врахувати, що $ac = bq$, маємо: $sbq+tbc=c$, тобто $b(sq+tc)=c$. Це і доводить твердження теореми.

Приклад 2.3. (самостійно). Доведіть, що якщо $m \in Z^+$, то $(am, bm) = m(a, b)$.

1.4. Розкладання на прості співмножники

Довільне ціле число a завжди має дільники $\pm a$ і 1. Якщо ціле додатне число $p>1$ не має інших дільників окрім $\pm p$ і 1, то воно називається простим. Додані цілі числа, які не є простими і більші за 1 називаються складеними.

Для перечислення всіх простих чисел, які не перевищують задане ціле число N, існує метод “решета Ератосфена” який полягає в такому.

Виписуються всі числа: 1, 2, ..., N. Число 1 не є простим, а тому з заданої сукупності видаляється. Число 2 є простим і тому залишається. Далі з заданої сукупності видаляються всі числа, кратні 2. Найменше число, з тих, які залишились, число 3, воно є простим, а тому залишається Далі з заданої сукупності чисел видаляються числа, кратні 3. Повторюючи ці операції, можна отримати всі числа, що містяться в сукупності 1, 2, ..., N.

Теорема 1.4.1. Якщо a - ціле додатне число, більше від 1, то мінімальний відмінний від 1 дільник числа a є простим числом.

Доведення

Нехай $q>1$ - мінімальний відмінний від 1 додатний дільник числа $a>1$. Якщо q - складене число то $q=q_1q_2$, $q>q_1>1$, $q>q_2>1$, звідки слідує, що q_1 і q_2 є дільниками a, меншими від q. Суперечність доводить теорему.

Прості числа, що є дільниками цілого числа a, називаються простими співмножниками a.

Теорема 1.4.2. Якщо p - просте число, то для довільного цілого числа a або $p\mid a$, або $(p, a)=1$.

Доведення

Так як додатними дільниками числа p є тільки числа p і 1, то або $(p, a)=p$, що рівносильне $p\mid a$, або $(p, a)=1$.

Наслідок з теореми 1.4.2. Нехай a, b - ненульові цілі числа, $d=(a, b)$. Тоді числа a/d і b/d взаємно прості.

Теорема 1.4.3. Якщо p - просте число і $p\mid ab$, то або $p\mid a$, або $p\mid b$.

Доведення

Якщо $p\mid a$, то враховуючи попередню теорему $(p, a)=1$. Оскільки $p\mid ab$, то з теореми 1.4.2 випливає, що $p\mid b$.

Наслідок. Якщо p - просте число і $p\mid a_1a_2...a_n$, то $p\mid a_i$ для деякого $1\le i\le n$.

Теорема 1.4.4. (Основна теорема елементарної теорії чисел). Будь-яке ціле число, яке більше від 1, однозначно розкладається у вигляді добутку простих чисел.

Доведення

Розглянемо довільне ціле число $a>1$. Якщо p_1 - мінімальний простий співмножник числа a, то $a=p_1a_1$. Якщо $a_1>1$ і p_2 - мінімальний простий співмножник a_1, то $a_1=p_2a_2$. Цей процес можна продовжити. Оскільки $a>a_1>a_2...$, то в деякий момент $a_n=1$, і процес закінчиться. При цьому число $a_{n-1}=p_n$ буде простим.

Таким чином:

$$a=p_1p_2...p_n, \qquad (1.4.1)$$

тобто числа a розкладається у добуток простих чисел.

Нехай число a іншим способом розкладається у добуток простих чисел $a = q_1 q_2 ... q_m$, тоді:

$$p_1 p_2 ... p_n = q_1 q_2 ... q_m . \qquad (1.4.2)$$

У розкладі на прості множники (1.4.2) деякі множники можуть співпадати, тому використовується стандартний розклад у вигляді:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k} , \qquad (1.4.3)$$

де $\alpha_1, \alpha_2, ...\alpha_k \in Z^+$ і $p_1, p_2, ..p_k$ - прості числа.

Наслідок з теореми 1.4.4. Якщо (1.4.3) стандартний розклад числа $a > 1$ на прості співмножники, то стандартний розклад числа $d \in Z^+$, $d \mid a$ на прості співмножники має вигляд:

$$d = p_1^{\beta_1} p_2^{\beta_2} ... p_k^{\beta_k} , \; 0 \le \beta_i \le \alpha_i \; (i = 1,...,k) . \qquad (1.4.4)$$

Приклад 1. Маємо: $588800 = 2^5 \cdot 3 \cdot 5^3 \cdot 7^2$.

1.5. Конгруенції простих чисел.

Розглянемо остачі, які отримуються при діленні цілих чисел на число $m \in Z^+$, яке називається модулем. Цілі числа a і b називаються конгруенціями за модулем m, якщо $m \mid (a - b)$. Символічно це записується так:

$$a \equiv b (\mathrm{mod}\, m) . \qquad (1.5.1)$$

Розділяючи числа a і b на m, маємо:

$$a = mq_1 + r_1, \;\; 0 \le r_1 < m;$$

$$b = mq_2 + r_2, \;\; 0 \le r_2 < m.$$

Зрозуміло, що a і b будуть порівняними за модулем m тоді і тільки тоді, якщо $r_1 = r_2$. Відношення порівнянності задовольняє таким законам:

1. Рефлексивність: $a \equiv a$;
2. Симетричність: якщо $a \equiv b$, то $b \equiv a$;
3. Транзитивність: : якщо $a \equiv b$ і $b \equiv c$, то $a \equiv c$.

З використанням законів порівнянності випливають такі теореми.

Теорема 1.5.1. До будь-якої з частин конгруенції можна додати число, яке є кратним модулю. До обох частин порівняння можна додати одне і теж саме число. Крім того, обидві частини порівняння можна помножити на одне і те ж саме число. Іншими словами, якщо $a \equiv b(\mathrm{mod}\, m)$ і $k \in Z$, то:

$$a + mk = b;\ \ a + k = b + k;\ ak \equiv bk \bmod(m). \qquad (1.5.2)$$

Теорема 1.5.2. Конгруенції можна почленно додавати та перемножувати. Тобто, якщо $a_1 \equiv b_1;\ a_2 \equiv b_2 \bmod(m)$, тоді:

$$a_1 + a_2 = b_1 + b_2;\ a_1 a_2 \equiv b_1 b_2 \bmod(m). \qquad (1.5.3)$$

Порівняння залишається справедливим при множенні обох його частин на одне і те ж число, але при діленні обох частин на одне і теж саме число, воно може порушуватися. Наприклад з порівняння $ca \equiv cb \bmod(m)$ не обов'язково випливає, що $a \equiv b \bmod(m)$. Для цього наприклад розглянемо порівняння для якого $c = 5;\ a = 1;\ b = 2;\ m = 5$. З даною властивістю пов'язана така теорема.

Теорема 1.5.3. Якщо $ca \equiv cb \bmod(m)$ і $(c, m) = 1$, то $a \equiv b \bmod(m)$.

Доведення

Оскільки $m \mid c(a-b),\ (c, m) = 1$, то враховуючи **теорему 1.3.2.** маємо, що $m \mid (a-b)$, звідки $a \equiv b \bmod(m)$.

Приклад 1. Якщо $a \equiv b \bmod(m)$, то $(a, m) = (b, m)$.

Оскільки $a \equiv b \bmod(m)$, то $a = mt + b$. Використовуючи алгоритм Евкліда, маємо, що $(a, m) = (b, m)$.

Припустимо, що на множині G задано відношення порівняння, яке задовольняє умови 1-3. Відношення, яке задовольняє цим умовам, називають відношенням еквівалентності. При цьому сукупність елементів, еквівалентних елементу $a \in Z$,

$$C_a = \{b \in G \mid a \equiv b\} \qquad (1.5.4)$$

називають класом еквівалентності, що визначається елементом a. Згідно закону рефлексивності $a \equiv a;\ a \in C_a;\ C_a \neq \varnothing$.

Два класи еквівалентності C_a, C_b або не мають жодних спільних елементів або співпадають між собою, тобто:

$$C_a \cap C_b = \varnothing \text{ або } C_a = C_b. \qquad (1.5.5)$$

Нехай перше з заданих співвідношень не виконується. Тоді знайдеться такий елемент $x \in G$, що $x \in C_a$ і $x \in C_b$, тобто $a \equiv x$ і $b \equiv x$. Проте в цьому випадку з закону симетричності випливає, що $a \equiv x$ і $x \equiv b$, а з закону транзитивності маємо: $a \equiv b$. Звідси видно, що якщо $a \equiv y$, то $b \equiv y$ і якщо $b \equiv y$, то $a \equiv y$. Значить $C_a = C_b$.

Кожний елемент G належить до одного і тільки одного класу еквівалентності, а значить, можна говорити про розбиття G на класи еквівалентності. Розглянемо розбиття множини цілих чисел Z на класи еквівалентності з допомогою відношення еквівалентності $\equiv (\mathrm{mod}\, m)$. Для спрощення класи еквівалентності будемо визначати відповідно до остач $0, 1, 2, ..., m-1$, що отримуються при діленні цілих чисел на m:

$$\begin{aligned} &C_0 = \{..., -2m, -m, 0, m, 2m\}; \\ &C_1 = \{..., -2m+1, -m+1, 1, m+1, 2m+1\}; \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &C_{m-1} = \{..., -m-1, -1, m-1, 2m-1, 3m-1, ...\} \end{aligned} \qquad (1.5.6)$$

Таке розбиття називають розбиттям на класи лишків за модулем m. При цьому класи еквівалентності (лишків) позначаються як:

$$(0)_m, (1)_m, ..., (m-1)_m. \qquad (1.5.7)$$

В загальному випадку клас лишків, що містить ціле число a, позначається $(a)_m$.

Якщо взяти по одну числу в кожному з m класів лишків $(0)_m, (1)_m, ..., (m-1)_m$, то отримана сукупність цілих чисел буде називатися повною системою лишків. Для прикладу повною системою лишків є сукупність $\{0, 1, ..., m-1\}$, яка отримується, якщо вибрати у кожному з m суміжних класів найменший невід'ємний лишок.

Теорема 1.5.4. Якщо жодні два числа з заданої множини цілих чисел $a_1, a_2, ..., a_m$ не порівняні між собою за модулем m, то ця множина є повною системою лишків за модулем m.

Так як жодні два числа не належать одночасно до одного і того ж класу лишків, то зрозуміло, що сукупність з m цілих чисел отримується вибором тільки одного лишку з загальної кількості m лишків.

Наслідок з теореми 1.5.4. Нехай $(c, m) = 1$. Тоді, якщо $\{a_1, a_2, ..., a_m\}$ - повна систем лишків за модулем m і b - ціле число, то сукупність $\{ca_1 + b, ca_2 + b, ..., ca_m + b\}$ також буде повною системою лишків за модулем m.

Доведення

Нехай $i \neq j$. Якщо припустити, що $ca_i + b \equiv ca_i + b (\mathrm{mod}\, m)$, то легко прийти до суперечності. Дійсно, якщо до обох частин попередньої конгруенції $-b$, отримаємо: $ca_i \equiv ca_i (\mathrm{mod}\, m)$. Оскільки $(c, m) = 1$, то згідно **теореми 1.5.3.**, $a_i \equiv a_i (\mathrm{mod}\, m)$. Але це суперечить тому, що $\{a_1, a_2, ..., a_m\}$ є повною системою лишків.

Для прикладу розглянемо порівняння першого порядку, що містить невідоме число x:

$$ax \equiv b (\mathrm{mod}\, m). \qquad (1.5.8)$$

У деяких випадках це порівняння може не мати розв'язків. Наприклад порівняння $2x \equiv 3$ або $2x - 3 \equiv 0 (\mathrm{mod}\, 2)$. Оскільки $2x$ є парним числом для будь-якого x, а $2x - 3$ - непарним, то дане порівняння не має розв'язків. Розглянемо також порівняння $2x \equiv 0 (\mathrm{mod}\, 4)$, розв'язки якого $x = 0$ і $x = 2$. В цьому випадку обидва класи лишків $\{..., -8, -4, 0, 4, 8, ...\}$ і $\{..., -6, -2, 2, 6, ...\}$ відображають розв'язки даного порівняння.

При розв'язуванні задач часто корисною є наступна теорема.

Теорема 1.5.5. Якщо $(a, m) = 1$, то конгруенція $ax \equiv b (\mathrm{mod}\, m)$ має розв'язок у цілих числах, при цьому сукупність усіх розв'язків утворює один клас лишків.

Доведення

Згідно із лемою 2.1, існують такі числа s і t, що $sa + tm = 1$. Домножуючи цю рівність на b, отримуємо $a(sb) + (bt)m = b$, тобто $a(sb) \equiv b(\mathrm{mod}\, m)$. Тому $x = sb$ є розв'язком розглядуваного порівняння, при цьому розв'язками будуть всі цілі числа, порівняні з sb за модулем m.

Приклад 1. Розв'язати конгруенцію $6x \equiv 1(\mathrm{mod}\, 7)$.

Розв'язання

Підставимо замість x в це порівняння числа $0,1,..., 6$. Отримаємо:

$6 \cdot 0 = 0;\ 6 \cdot 1 = 6;\ 6 \cdot 2 = 12 \equiv 5(\mathrm{mod}\, 7);\ 6 \cdot 3 = 18 \equiv 4(\mathrm{mod}\, 7);\ 6 \cdot 4 = 24 \equiv 3(\mathrm{mod}\, 7);$

$6 \cdot 5 = 30 \equiv 2(\mathrm{mod}\, 7);\ 6 \cdot 6 = 36 \equiv 1(\mathrm{mod}\, 7)$.

Отже, розв'язком даного порівняння є клас лишків $(6)_7 = \{..., -8, -1, 6, 13, ...\}$.

1.6. Області цілісності та поля.

Досі ми користувались чотирма арифметичними операціями над цілими числами, уважаючи при цьому їх властивості відомими.

У множині цілих чисел Z є визначеними дві операції: додавання "+" і множення "·". Перерахуємо їх основні властивості:

А1. Асоціативність додавання : $(x + y) + z = x + (y + z)$.

А2. Комутативність додавання: $x + y = y + x$.

З асоціативності додавання випливає, що при додаванні дужки можна розставляти довільним чином або ж взагалі їх не писати, тобто використовувати спрощену рівність: $(x + y) + z = x + (y + z) = x + y + z$. Крім цього, з комутативності випливає, що при додаванні доданки можна міняти місцями.

А3. Існування одиничного по відношенню до додавання елемента. Тобто існує таке число θ, що $x + \theta = x$ для довільного x.

У множині цілих чисел роль одиничного по відношенню до додавання елемента відіграє число 0. В єдності існування такого елемента можна

упевнитися наступним чином. Якщо числа θ, θ' є одиничними по відношенню до додавання елементами, то $\theta = \theta + \theta' = \theta' + \theta = \theta'$. Це означає, що роль елемента θ в множині цілих чисел відіграє число 0.

А4. Існування оберненого по відношенню до додавання елемента. Для будь-якого x існує елемент x', такий, що $x + x' = 0$. В множині цілих чисел роль елемента x' відіграє число $-x$.

Описаними вище властивостями операція додавання володіє не тільки в множині цілих чисел, але й у множині всіх раціональних чисел, у множині всіх дійсних чисел, у множині всіх комплексних чисел. Загалом, множина G, з визначеною на ній операцією додавання "+", що задовольняє законам А1-А4, називається комутативною групою по відношенню до операції додавання.

Розглянемо множину класів лишків за модулем:

$$Z_m = \{(0)_m, (1)_m, .., (m-1)_m\}. \qquad (1.6.1)$$

Клас лишків $(i)_m$ представляє собою деяку множину цілих чисел. Проте при дослідженні множин Z_m він розглядається як один елемент. Якщо $a_1,\ a_2 \in (a)_m$, $b_1,\ b_2 \in (b)_m$, то згідно з **теоремою 1.5.2**.: $a_1 + b_1 = a_2 + b_2 (\mathrm{mod}\, m)$, тобто $(a_1 + b_1)_m = (a_2 + b_2)_m$.

Це означає, що сума доданків:

$$(a)_m + (b)_m = (a + b)_m. \qquad (1.6.2)$$

однозначно визначає операцію додавання в множині Z_m.

Теорема 1.6.1. Z_m є групою по відношенню до операції додавання.

Доведення

Асоціативність. Рівність $((a)_m + (b)_m) + (c)_m = (a)_m + ((b)_m + (b)_m)$ є наслідком того, що в силу асоціативності додавання чисел як ліва так і права частини рівності є $(a + b + c)_m$.

Комутативність. Рівність $(a)_m + (b)_m = (b)_m + (a)_m$ випливає з того, що обидві його частини в силу комутативності додавання чисел співпадають з $(a + b)_m$.

Очевидно, що одиничним по відношенню до операції додавання в даному випадку є клас лишків $(0)_m$, а оберненим класом по відношенню до класу $(a)_m$ - клас $(-a)_m$.

Множення цілих чисел має такі властивості:

А5. Асоціативність множення: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

А6. Комутативність множення: $a \cdot b = b \cdot a$.

А7. Існування одиничного елемента по відношенню до операції множення. Існує елемент, такий, що $x \cdot e = e \cdot x = x$ для усіх x.

В множині цілих чисел одиничним по відношенню до множення є елемент 1. Як і для додавання, існує тільки один елемент по відношенню до операції множення. В множині цілих чисел обернений елемент по відношенню до операції множення, зазвичай є відсутнім. Одиничний елемент по відношенню до операції множення позначається як 1, і точка $(\cdot)$, яка позначає операцію множення в подальшому буде опускатися.

А8. Дистрибутивність.

Для довільних чисел x, y, z виконується рівність: $x(y+z) = xy + xz$.

З властивості дистрибутивності випливають такі важливі співвідношення:

$$x0 = 0 \text{ для будь-якого } x, \tag{1.6.3}$$

$$x(-y) = -xy, \tag{1.6.4}$$

$$x(y-z) = xy - xz. \tag{1.6.5}$$

Для отримання рівності (1.6.3), до обох частин рівності $x0 = x(0+0) = x0 + x0$ треба додати $-(x0)$. При цьому: $0 = x0 + (-(x0)) = x0 + (x0 + (-(x0))) = x0 + 0 = x0$.

Далі з рівності $xy + x(-y) = x(y + (-y)) = x0 = 0$ випливає справедливість рівності (1.6.4).

З рівності $x(y-z) = x(y + (-z)) = xy + x(-z) = xy - xz$ випливає рівність (1.6.5).

Аналогічно, які і у випадку операції додавання доводиться справедливість співвідношення:

$$(a)_m(b)_m = (ab)_m, \qquad (1.6.6)$$

що однозначно визначає операцію множення в Z_m.

Операція множення, що визначена на множині цілих чисел Z має крім вище зазначених, ще такі властивості.

А9. Правило скорочення. Якщо $x \neq 0$ і $xy = xz$, то $y = z$.

Згідно даного правила, будь-які частини рівності можна розділити на спільний відмінний від нуля спільний множник.

Приведене вище правило скорочення А9 є також еквівалентним такому:

А9 (*). Правило скорочення. Якщо $x \neq 0$ і $y \neq 0$, то $xy \neq 0$.

Дійсно, якщо припустити, що $x \neq 0$, $y \neq 0$, але $xy = 0$, то $xy = x0$. Тоді звідси і правила А9 випливає, що $y = 0$. Отримали протиріччя. Таким чином, з властивості А9 випливає властивість А9 (*). Навпаки, якщо виконується властивість А9 (*), то з рівності $xy = xz$, випливає, що $0 = xy - xz = x(y - z)$. Таким чином, якщо $x \neq 0$, то $y - z = 0$ і $y = z$.

Якщо на множині G визначені операції додавання та множення, що визначаються згідно законів А1-А9, то множина G називається областю цілісності.

Якщо m складене число, то його можна записати у вигляді: $m = ab$, причому $m > a > 1$ і $m > b > 1$. Значить: $(a)_m \neq (0)_m$, $(b)_m \neq (0)_m$, але $(a)_m(b)_m = (m)_m = (0)_m$, тобто добуток ненульових елементів рівний нульовому. Це означає, що в даному випадку Z_m для складених m не є областю цілісності.

Приклад 1. Доведіть, що як число p - просте число, то Z_p - область цілісності.

Розв'язання

Нехай $(a)_p \neq (0)_p$ і $(b)_p \neq (0)_p$. Припустимо, що ні a, ні b не є дільниками числа p, а $(a)_p(b)_p = (ab)_p = (0)_p$. Тоді $p \mid ab$, і згідно з теоремою 1.10 або $p \mid a$, або $p \mid a$. Отримали суперечність.

В множині цілих чисел Z обернений по відношенню до операції множення елемент може бути відсутнім. Але він завжди існує в множині раціональних чисел, та в множині дійсних чисел.

А.10. Існування оберненого по відношенню до операції множення елемента. Для кожного $x \neq 0$ існує елемент $x^{/}$ такий, що $xx^{/} = 1$.

Обернений елемент визначається однозначно, будемо позначати його x^{-1}. З властивості А.10 відразу випливає правило скорочення А.9 Дійсно, якщо $x \neq 0$ і $xy = xz$, то помножуючи останню рівність на x^{-1}, отримуємо:

$x^{-1}(xy) = (x^{-1}x)y = 1y = y = x^{-1}(xz) = (x^{-1}x)z = 1z = z$.

Якщо на множині G визначені операції додавання та множення, що задовольняють законам А1.-А8. і А.10, то G називається полем. В полі завжди можливою є операція ділення. Тобто, якщо $y \neq 0$, то результат ділення y на x визначається як xy^{-1}. Крім поля раціональних чисел і поля дійсних чисел існую інші поля, наприклад поле комплексних чисел.

Теорема 1.6.2. Якщо p - просте число, то Z_p є полем.

Доведення

Якщо $(a)_p \mid (0)_p$, то $p \mid a$. Звідси і з **теореми 1.5.2.**. випливає, що $(p, a) = 1$. Згідно **теореми 1.5.5.**, порівняння $ax = 1 (\mathrm{mod}\, p)$ має розв'язок $x = b$. Оскільки $(a)_p(b)_p = (ab)_p = (1)_p$, то $(b)_p$ є оберненим по відношенню до операції множення елементом для $(a)_p$.

Область цілісності і поле, яке містить скінчене число елементів, називається відповідно скінченою областю цілісності і скінченим полем. Завжди можна довести, що скінчена область цілісності завжди є полем. Слід зауважити, що Z_p є скінченою областю цілісності, що складається з p елементів. Якщо G - поле, то для будь-якого елемента сукупності $G - \{0\}$,

яка отримується з G видаленням одиничного по відношенню до операції додавання елемента 0, існує обернений елемент по відношенню до операції множення, значить $G - \{0\}$ є групою по відношенню до множення.

Для визначення елементів скінченого поля Z_p замість $(0)_p, (1)_p, (2)_p, ...(p-1)_p$ можна використовувати символи $1, 2, ..., p-1$. Найбільш широко використовувана множина Z_2 є полем, що складається з одиничного по відношенню до операції додавання елемента 0 і одиничного по відношенню до множення елемента 1. Додавання та множення в цій множині задаються формулами:

$0+0=0;\ 0+1=1+0=1;\ 1+1=0;\ 0\cdot 0=1\cdot 0=0\cdot 1=0;\ 1\cdot 1=1$. Всі ці рівності, за виключенням рівності $1+1=0$, виконуються по відношенню до одиничного по додаванню елемента 0 і одиничного по відношенню до одиничного по множенню елемента 1. Якщо припустити, що в полі, яке не містить інших елементів окрім 0 і 1, то операція додавання є такою, що $1+1=1$, то $1+0=1$, і, відповідно, для елемента 1 не існує оберненого по відношенню до додавання елемента. Таким чином, в полі, яке складається з двох елементів, повинна виконуватися рівність $1+1=0$. Це означає, що Z_2 - єдине поле, яке складається тільки з одиничного по відношенню до додавання елемента 0 і одиничного по відношенню до множення елемента 1.

Приклад 1. Знайти $(84, 66)$.

Розв'язання

Маємо:

$84 = 66\cdot 1 + 18;$

$66 = 18\cdot 3 + 12;$

$18 = 12\cdot 1 + 6;$

$12 = 6\cdot 2.$

Остання, відмінна від нуля остача рівні 6, значить, $(84, 66) = 6$.

Приклад 2. Розв'язати діофантове рівняння $35x + 22y = 1$.

Розв'язання

Використаємо алгоритм Евкліда, записуючи усі викладки у стовбець. Маємо:

$35 = 22 \cdot 1 + 13; \Rightarrow 13 = 35 - 22;$

$22 = 13 \cdot 1 + 9; \Rightarrow 9 - 22 - 13;$

$13 = 9 \cdot 1 + 4; \Rightarrow 4 = 13 - 9;$

$9 = 4 \cdot 2 + 1; 1 = 9 - 4 \cdot 2$

Останнього кроку можна не виконувати, так як очевидно, що будь-яке число без остачі ділиться на 1. Тепер будемо почергово розглядати рівності правого стовбця знизу вверх і підставляти їх одна в одну з метою виразити число 1 через 35 і 22. Отримуємо:

$1 = 9 - 4 \cdot 2 \qquad = 9 - (13 - 9) \cdot 2 =$

$= 9 \cdot 3 - 13 \cdot 2 \quad = (22 - 13) \cdot 3 - 13 \cdot 2 =$

$= 22 \cdot 3 - 13 \cdot 5 = 22 \cdot 3 - (35 - 22) \cdot 5 =$

$= 22 \cdot 9 - 35 \cdot 5.$

Таким чином, частковий розв'язок рівняння: $x_0 = -5,\ y_0 = 8$. Оскільки $(35,\ 22) = 1$, то загальний роз'язок рівняння:

$\{x,\ y\} = \{(-5 - 22m,\ 8 + 35m) \mid m \in Z\}$.

Приклад 3. Розв'язати порівняння $23x \equiv 4 (\mathrm{mod}\, 36)$.

Розв'язання

Спочатку розглянемо порівняння $23x' \equiv 4 (\mathrm{mod}\, 36)$. Якщо x' - розв'язок цього порівняння, то існує y' таке, що $23x' + 36y' = 1$.

Використаємо алгоритм Евкліда:

$36 = 23 \cdot 1 + 13; \Rightarrow 13 = 36 - 23;$

$23 = 13 \cdot 1 + 10; \Rightarrow 10 = 23 - 13;$

$13 = 10 \cdot 1 + 3; \ \Rightarrow \ 3 = 13 - 10;$

$10 = 3 \cdot 3 + 1; \ \Rightarrow \ 1 = 10 - 3 \cdot 3.$

Розглядаючи рівності правого стовбця знизу вверх і підставляючи їх одна в одну, маємо:

$$
\begin{aligned}
1 &= 10 - 3\cdot 3 \qquad = 10 - (13-10)\cdot 3 \quad = \\
&= 10\cdot 4 - 13\cdot 3 \;= (23-13)\cdot 4 - 13\cdot 3 \;= \\
&= 23\cdot 4 - 13\cdot 7 \;= 23\cdot 4 - (36-23)\cdot 7 = \\
&= 23\cdot 11 - 36\cdot 7.
\end{aligned}
$$

Таким чином, $x' = 11$. Так як права частина початкової рівності рівна 4, то отримуємо: $x = 11\cdot 4 = 44$. Тому розв'язком заданого порівняння є будь-яке значення x, таке, що $x \equiv 44 \bmod(36)$. Якщо необхідно знайти найменший відмінний від нуля лишок, то враховуючи, що від даного порівняння можна віднімати числа кратні 36, маємо:

$x \equiv 44 - 1\cdot 36 = 8 \ (\mathrm{mod}\, 36)$.

Приклад 4. Розв'язати систему порівнянь:

$$
\begin{cases}
x \equiv 2 \ (\mathrm{mod}\, 5); \\
x \equiv 1 \ (\mathrm{mod}\ 8); \\
x \equiv 4 \ (\mathrm{mod}\ 9).
\end{cases}
$$

Розв'язання

З першого рівняння маємо:

$x = 5x_1 + 2$.

Підставимо цей вираз в друге порівняння системи. Маємо:

$5x_1 + 2 \equiv 1 (\mathrm{mod}\ 8)$, тоді отримуємо: $5x_1 \equiv -1 (\mathrm{mod}\ 8)$.

Розв'яжемо порівняння $5x_1' \equiv 1 (\mathrm{mod}\ 8)$. З нього випливає, що $5x_1' + 8y_1' = 1$.

Використовуючи алгоритм Евкліда, маємо:

$8 = 5\cdot 1 + 3; \Rightarrow 3 = 8 - 5;$

$5 = 3\cdot 1 + 2; \Rightarrow 2 = 5 - 3;$

$3 = 2\cdot 1 + 1; \Rightarrow 1 = 3 - 2.$

Підставляючи почергово рівності правого стовбця один в одного знизу вгору, будемо мати:

$$
\begin{aligned}
1 &= 3 - 2 \qquad = 3 - (5-2) = \\
&= 3\cdot 2 - 5 \qquad = (8-5)\cdot 2 - 5 = \\
&= 8\cdot 2 - 5\cdot 3.
\end{aligned}
$$

Таким чином, $x_1^{/} = -3 (\mathrm{mod}\ 8)$. Домножуючи на -1, отримує, що розв'язком порівняння $5x_1 + 2 \equiv 1 (\mathrm{mod}\ 8)$ є $x_1 = 3 (\mathrm{mod}\ 8)$, тобто: $x_1 = 8x_2 + 3$.

Підставляючи у розв'язок першого порівняння, знаходимо:

$x = 5(8x_2 + 3) + 2 = 40x_2 + 17$.

Підставляючи в третє порівняння системи, будемо мати:

$40x_2 + 17 \equiv 4 (\mathrm{mod}\ 9)$. Оскільки до обох частин цього порівняння можна додавати числа кратні 9 за модулем, то від цього розв'язок порівняння не зміниться. Маємо:

$40x_2 - 9 \cdot 4x_2 + 17 - 2 \cdot 9 \equiv 4 \ (\mathrm{mod}\ 9)$, звідки $4x_2 - 1 \equiv 4 \ (\mathrm{mod}\ 9)$, тобто:

$4x_2 \equiv 5 \ (\mathrm{mod}\ 9)$.

Знайдемо розв'язок порівняння $4x_2^{/} \equiv 1 \ (\mathrm{mod}\ 9)$. Використовуючи алгоритм Евкліда, маємо:

$9 = 4 \cdot 2 + 1; \Rightarrow 1 = 9 - 4 \cdot 2$.

Звідси випливає, що $x_2^{/} = -2 \equiv 7 \ (\mathrm{mod}\ 9)$. Щоб отримати розв'язок порівняння $4x_2 \equiv 5 \ (\mathrm{mod}\ 9)$, домножимо отриманий результат на 5. Тоді отримуємо:

$x_2 \equiv 7 \cdot 5 = 35 \ (\mathrm{mod}\ 9)$. Знайдемо найменший невід'ємний лишок: $x_2 \equiv 35 - 9 \cdot 3 = 8 \ (\mathrm{mod}\ 9)$. Тому $x_2 = 9x_3 + 8$. Повертаючись до розв'язку другого порівняння, знаходимо:

$x = 40(9x_3 + 8) + 17 = 360x_3 + 337$.

Значить, розв'язком системи порівнянь є: $x \equiv 337 \ (\mathrm{mod}\ 360)$.

Список рекомендованих до розв'язування задач

1. Доведіть, що якщо $(a, b) = 1$, то $(ac, b) = (c, b)$.

2. Доведіть, що якщо $(m_1, m_2) = 1$, то система порівнянь $x \equiv b_1 (\mathrm{mod}\, m_1),\ x \equiv b_2 (\mathrm{mod}\, m_2)$ має розв'язок, і, крім того, множина всіх її розв'язків співпадає з одним із класів лишків за модулем $m_1 m_2$.

3. Доведіть, що якщо деяка множина цілих чисел S є не пустою і замкнутою про відношенню до операції віднімання, то вона буде закритою і по відношенню до операції додавання.

4. Побудуйте таблиці множення та додавання для скінченого поля Z_5.

5. Знайти НСД чисел за допомогою алгоритму Евкліда:

а) 122 і 305; б) 124 і 48;

в) 852 і 483; г) 588 і 861.

6. Довести, що для довільних цілих чисел a, b, c виконується рівність:

$(a, b, c) = ((a, b), c) = (a, (b, c))$.

7. Довести, що якщо $(a, b) = d$, то $(a/d, b/d) = 1$.

8. Довести, що якщо $a \mid b$ і $b \mid c$, то $a \mid c$.

9. Довести, що для довільних чисел $a, b, c, d \in N$ справедлива рівність:

$(a, b)(c, d) \mid (ac, bd)$.

10. Розв'язати лінійні діофантові рівняння:

а) $35x + 82y = 1$; б) $42x + 65y = 1$; в) $28x + 37y = 4$;

г) $57x + 74y = 5$; д) $44x + 62y = 6$; е) $63x + 108y = 12$;

ж) $76x + 52y = 10$; з) $45x + 81y = 18$.

11. Розв'язати порівняння:

а) $43x \equiv 1 (\mathrm{mod}\, 82)$; б) $39x \equiv 1 (\mathrm{mod}\, 25)$; в) $38x \equiv 3 (\mathrm{mod}\, 45)$;

г) $45x \equiv 8 (\mathrm{mod}\, 64)$; д) $35x \equiv 14 (\mathrm{mod}\, 91)$; е) $84x \equiv 12 (\mathrm{mod}\, 36)$;

ж) $82x \equiv 7 (\mathrm{mod}\, 38)$; з) $108x \equiv 15 (\mathrm{mod}\, 72)$.

12. Розв'язати систему порівнянь:

а) $\begin{cases} x \equiv 5 (\mathrm{mod}\, 7); \\ x \equiv 3 (\mathrm{mod}\, 5); \\ x \equiv 2 (\mathrm{mod}\, 9); \end{cases}$ б) $\begin{cases} x \equiv 3 (\mathrm{mod}\, 7); \\ x \equiv 2 (\mathrm{mod}\, 11); \\ x \equiv 1 (\mathrm{mod}\, 3); \end{cases}$

в) $\begin{cases} x \equiv 2 (\mathrm{mod}\, 5); \\ x \equiv 1 (\mathrm{mod}\, 3); \\ x \equiv 6 (\mathrm{mod}\, 7); \\ x \equiv 9 (\mathrm{mod}\, 11); \end{cases}$ г) $\begin{cases} x \equiv 1 (\mathrm{mod}\, 3); \\ x \equiv 4 (\mathrm{mod}\, 7); \\ x \equiv 4 (\mathrm{mod}\, 117); \\ x \equiv 10 (\mathrm{mod}\, 13); \end{cases}$

д) $\begin{cases} x \equiv 3 (\mathrm{mod}\, 7); \\ x \equiv 2 (\mathrm{mod} 13); \\ x \equiv 1 (\mathrm{mod} 11); \end{cases}$ е) $\begin{cases} x \equiv 2 (\mathrm{mod} 15); \\ x \equiv 7 (\mathrm{mod}\, 25); \\ x \equiv 7 (\mathrm{mod}\, 40). \end{cases}$

РОЗДІЛ 2. КОМБІНАТОРНИЙ АНАЛІЗ. РОЗМІЩЕННЯ, КОМБІНАЦІЇ, ПРИНЦИП ВКЛЮЧЕННЯ-ВИКЛЮЧЕННЯ

2.1. Властивості цілих чисел.

Спосіб розміщення в певному визначеному порядку деякого числа елементів з заданої множини S, чи те саме, що спосіб вибору цих елементів з множини S, коли важливою є послідовність вибору елементів, називається розміщенням. Якщо ж послідовність вибору елементів, є несуттєвою то такий спосіб вибору називається сполученням. При цьому є можливість повторення або не повторення вибору одних і тих же елементів. Наприклад, коли повторення елементів є неможливим, то з трьох елементів a, b, c два елементи можна вибрати шістьома різними способами, якщо при цьому враховувати послідовність вибору елементів ab, ac, ba, bc, ca, cb, і трьома різними способами, якщо не враховувати послідовність вибору елементів a, b, a, c, b, c. Якщо є повторення елементів є можливим, то існує дев'ять розміщень $aa, ab, ac, ba, bb, bc, ca, cb, cc$ і шість сполучень $a, a;\ a, b;\ a, c;\ b, b;\ b, c;\ c, c$.

Загальне число розміщень без повторення з n різних елементів по r позначається як ${}_nP_r$. При цьому:

$$ {}_nP_r = n(n-1)...(n-r+1),\ n \geq r \geq 1. \qquad (2.1.1) $$

Оскільки повторення елементів є неможливим, то завжди $n \geq r$. Будемо уважати, що при $r = 0$ є лише одне розміщення (елементи взагалі не вибираються), тобто справедлива рівність:

$$ {}_nP_0 = 1. \qquad (2.1.1)(*) $$

Розміщення r елементів можна уявити собі як заповнення деяких r позицій елементами заданої множини. При цьому першу позицію можна заповнити n різними способами. Після того, як 1-а позиція заповнена, то елемент для заповнення 2-ї позиції можна вибрати вже $(n-1)$-а способами.

Якщо цей процес продовжувати, то після заповнення позицій з 1-ої по $(r-1)$ -у буде міститися по $(n-r+1)$ способів заповнення останньої r -ї позиції. Перемножуючи ці числа, отримаємо формулу (2.1). Добуток, який міститься у правій частині рівності (2.1) позначимо як $n^{(r)}$. В частковому випадку, коли $r=n$, маємо:

$$_nP_n = n(n-1)...3\cdot 2\cdot 1 = n!. \qquad (2.1.2)$$

Число різних комбінацій без повторення n різних елементів будемо позначати як $_nC_r$. При цьому, кожному сполученню відповідає $r!$ різних способів упорядкування елементів, що входять до нього. Якщо таке упорядкування виконати для усіх сполучень, то ми тримаємо усі розміщення без повторень з n елементів по r і, відповідно:

$$_nC_r = \frac{_nP_r}{r!} = \frac{n(n-1)...(n-r+1)}{r!},\ n\ge r\ge 1. \qquad (2.1.3)$$

Будемо уважати, що при $r=0$ існує лише одна можливість для вибору елементів – не вибирати їх узагалі, тобто:

$$_nC_0 = 1. \qquad (2.1.3)(*)$$

Вирази, які розміщені у правій частині виразу (2.3), називаються біноміальними коефіцієнтами і позначають $\binom{n}{r}$. При цьому:

$$\binom{n}{r} = \frac{n(n-1)...(n-r+1)}{r!} = \frac{n!}{r!(n-r)!},\ n\ge r\ge 0, \qquad (2.1.4)$$

де $0!=1$.

2.2. Перестановки та підстановки.

Нехай задана множина $M=\{a_1, a_2,..., a_2\}$. Перестановкою елементів множини M називається будь-який кортеж $(a_{i_1}, a_{i_2},..., a_{i_n})$, який складається з n різних елементів множини M.

Перестановки відрізняються одна від одної тільки порядком входячих до них елементів. Число всіх перестановок множини з n елементів рівне: $P_n = n!$.

Бієкція $\sigma : M \leftrightarrow M$ називається підстановкою множини M. Нехай σ - підстановка множини $M = \{1, 2, ..., n\}$. Тоді $\sigma(k) = s_k$, де $1 \le s_k \le n,\ k = 1, 2, ..., n$, $\{s_1, s_2, ..., s_2\} = \{1, 2, ..., n\}$, і тому підстановку σ можна представити у вигляді матриці, яка містить два рядки:

$$[\sigma] = \begin{pmatrix} 1 & 2 & ... & n \\ s_1 & s_2 & ... & s_n \end{pmatrix}. \qquad (2.2.1)$$

Зрозуміло, що якщо в матриці $[\sigma]$ переставити місцями стовбці, то отримана матриця буде також визначати підстановку σ. Множина всіх підстановок множини $\{1, 2, ..., n\}$ позначається як S_n. Для підстановок $\sigma, \tau \in S_n$ можна визначити добуток $\sigma \cdot \tau$ як добуток двох функцій. Знаючи матриці підстановок $[\sigma] = \begin{pmatrix} 1 & 2 & ... & n \\ s_1 & s_2 & ... & s_n \end{pmatrix}$ і $[\tau]$, і переставивши стовбці матриці $[\tau]$ так, щоб її перший рядок співпав з другим рядком матриці $[\sigma]$:

$$\begin{pmatrix} t_1 & t_2 & ... & t_n \\ s_1 & s_2 & ... & s_n \end{pmatrix},$$

отримуємо:

$$[\sigma\tau] = \begin{pmatrix} 1 & 2 & ... & n \\ s_1 & s_2 & ... & s_n \end{pmatrix}\begin{pmatrix} s_1 & s_2 & ... & s_n \\ t_1 & t_2 & ... & t_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & ... & n \\ t_1 & t_2 & ... & t_n \end{pmatrix}.$$

Теорема 2.2.1. Алгебра $\langle S_n \rangle$ є групою. При $n \ge 3$ вона є некомутативною.

Доведення

Операція "$\cdot$"є асоціативною як операція добутку функцій. Легко перевірити, що існує одинична підстановка ε з матрицею $\begin{pmatrix} 1 & 2 & ... & n \\ 1 & 2 & ... & n \end{pmatrix}$ і для

будь-якої підстановки σ з матрицею $[\sigma]=\begin{pmatrix}1 & 2 & \dots & n\\ s_1 & s_2 & \dots & s_n\end{pmatrix}$ існує обернена підстановка σ^{-1}, якій відповідає матриця $\begin{pmatrix}s_1 & s_2 & \dots & s_n\\ 1 & 2 & \dots & n\end{pmatrix}$.

Якщо $n\geq 3$, то розглянемо підстановки σ і τ з матрицями $[\sigma]=\begin{pmatrix}1 & 2 & 3 & 4 & \dots & n\\ 2 & 1 & 3 & 4 & \dots & n\end{pmatrix}$ і $[\tau]=\begin{pmatrix}1 & 2 & 3 & 4 & \dots & n\\ 3 & 2 & 1 & 4 & \dots & n\end{pmatrix}$.

Маємо: $[\sigma\tau]=\begin{pmatrix}1 & 2 & 3 & 4 & \dots & n\\ 2 & 1 & 3 & 4 & \dots & n\end{pmatrix}$, $[\tau\sigma]=\begin{pmatrix}1 & 2 & 3 & 4 & \dots & n\\ 3 & 2 & 1 & 4 & \dots & n\end{pmatrix}$, тобто $\sigma\tau\neq\tau\sigma$. Таким чином, група $\langle S_n,\cdot\rangle$ є некомутативною.

Група $\langle S_n,\cdot\rangle$ називається симетричною групою степеню n. Число елементів цієї групи $|S_n|$ рівне $P_n=n!$.

Підстановка σ називається циклом довжини r, якщо матрицю $[\sigma]$ перестановкою стовбців можна привести до вигляду:

$$\begin{pmatrix}s_1 & s_2 & s_3 & \dots & s_{r-1} & s_r & s_{r+1} & \dots & s_n\\ s_2 & s_3 & s_4 & \dots & s_r & s_1 & s_{r+1} & \dots & s_n\end{pmatrix}.$$

Очевидно, що в цьому випадку σ задає бієкцію, в якій $s_1\leftrightarrow s_2$, $s_2\leftrightarrow s_3$, ..., $s_r\rightarrow s_1$, а решта елементів є нерухомими. Описаний цикл σ позначається через $(s_1\,s_2\dots s_r)$.

Приклад 1. Підстановка з матрицею $\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 1 & 5 & 6 & 4 & 3 & 2\end{pmatrix}$ є циклом (2536), а підстановка з матрицею $\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 4 & 5 & 2 & 1 & 6 & 3\end{pmatrix}$ циклом не є, оскільки з неї можна виділити два цикли (14) і (2563).

Цикли $(s_1\,s_2\dots s_r)$ і $(t_1\,t_2\dots t_p)$ називаються незалежними, якщо $\{s_1\,s_2\dots s_r\}\bigcap\{t_1\,t_2\dots t_p\}=\varnothing$.

Теорема 2.2.2. Будь-яку підстановку можна однозначно (з точністю до порядку співмножників) представити у вигляді добутку незалежних циклів.

Використовуючи попередній приклад маємо:

$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 6 & 4 & 3 & 2 \end{pmatrix} = (2536)$, а $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 1 & 6 & 3 \end{pmatrix} = (14)(2563)$.

Двоелементний цикл $(i\ j)$ називається транспозицією. При транспозиції i-й і j-й елементи міняються місцями, а решта зберігають своє положення.

Теорема 2.2.3. Кожна підстановка є добутком транспозицій.

Доведення

Згідно **теореми 2.2.1.** достатньо встановити, що довільний цикл $(s_1\, s_2 \ldots s_r)$ можна представити у вигляді добутку транспозицій, але легко перевірити, що $(s_1\, s_2 \ldots s_r) = (s_1\, s_2)(s_1\, s_3)\ldots(s_1\, s_r)$.

Приклад 2. $(1234) = (12)(13)(14)$.

2.3. Розміщення і комбінації

Нехай M - множина, яка складається з n елементів, $m \le n$. Розміщенням з n елементів по m чи впорядкованою (n, m) - вибіркою називається будь-який кортеж $(a_{i_1}, a_{i_2}, ..., a_{i_m})$, який складається з m попарно різних елементів множини M. Розміщення можна розглядати як різнозначну функцію $f : \{1, 2, ..., m\} \to M$, для якої $f(j) = a_j$.

Приклад 1. Для множини $M = \{a, b, c\}$ пари (a,b) і (b,a) є розміщеннями з 3 по 2, трійка (a,c,b) - розміщенням з 3 по 3, а трійка (b,a,b) розміщення не утворює.

Число розміщень з n по m позначається як A_n^m чи $P(n, m)$. Доведемо, що

$$A_m^n = \frac{n!}{(n-m)!} = n(n-1)\ldots(n-m+1). \qquad (2.3.1)$$

Дійсно, розміщення m елементів можна представити як заповнення деяких m позицій елементами множини M. При цьому першу позицію можна заповнити n різними способами. Після того як 1-а позиція заповнена, елемент для заповнення 2-ї позиці можна вибрати $(n-1)$ способами. Якщо продовжувати даний процес далі, то після заповнення позицій з 1-ї по

$(m-1)$ - у будемо мати $(n-m+1)$ способів заповнення останньої, m - ї позиції. Тоді, перемножуючи ці числа, отримаємо формулу (2.3.1).

Поєднанням з n елементів по m чи невпорядкованою вибіркою (n, m) - вибіркою називається будь-яка підмножина множини M, яка складається з m елементів.

Приклад 2. Якщо $M = \{a, b, c\}$, то $\{a, b\}, \{a, c\}, \{b, c\}$ - всі комбінацій з 3 по 2.

Число комбінацій з n по m позначається C_n^m, $\binom{n}{m}$ чи $C(n, m)$.

Якщо об'єднати розміщення з n елементів по m, які складаються з одних і тих же елементів (без урахування порядку їх розміщення), в класи еквівалентності, то можна встановити бієкцію φ між комбінаціями і отриманими класами згідно правила:

$$\varphi\left(\{a_{i_1}, a_{i_2}, ..., a_{i_m}\}\right) \Leftrightarrow \{(b_1, b_2, ..., b_m) \mid \{b_1, b_2, ..., b_m\} = \{a_{i_1}, a_{i_2}, ..., a_{i_m}\}\}. \quad (2.3.2)$$

Оскільки з кожної комбінацій C можна отримати $m!$ розміщень (впорядковуючи елементи з множини C $m!$ способами за числом перестановок множини C), то кожний клас еквівалентності містить $m!$ розміщень, тобто: $A_n^m = m! \cdot C_n^m$, звідки $C_n^m = \frac{A_n^m}{m!}$. Таким чином:

$$C_n^m = \frac{n!}{(n-m)!m!}. \quad (2.3.3)$$

Число C_n^m має такі властивості:

1) $C_n^m = C_n^{n-m}$;

2) $C_n^m + C_n^{m+1} = C_{n+1}^{m+1}$;

3) $(a+b)^n = \sum_{m=0}^{n} C_n^m a^m b^{n-m}$ для будь-яких $a, b \in R, n \in N$ (біном Ньютона).

З урахування властивості 3) числа C_n^m називаються біноміальними коефіцієнтами.

2.4. Розміщення і комбінацій з повторенням

Розміщенням з повторенням із n елементів по m чи впорядкованою (n, m) - вибіркою с повтореннями називається будь-який кортеж $(a_1, ..., a_m)$ елементів множини M, для якої $|M| = n$.

Оскільки в кортеж $(a_1, a_2, ..., a_m)$ на довільне місце може претендувати будь-який з n елементів множини M, то число розміщень з повтореннями $\widehat{P}(n, m)$ рівне: $\underbrace{n \cdot n \cdot ... \cdot n}_{m \text{ разів}} = n^m$:

$$\widehat{P}(n, m) = n^m. \tag{2.4.1}$$

Визначимо відношення еквівалентності на множині розміщень з повтореннями з n по m: $(a_1, a_2, ..., a_m) \sim (b_1, b_2, ..., b_m) \Leftrightarrow$ для будь-якого $c \in M$ число елементів a_i, які дорівнюють c, співпадає з числом елементів b_i, які дорівнюють c.

Комбінацією з повторенням з n елементів по m чи невпорядкованою (n, m) - вибіркою з повтореннями називається будь-який клас еквівалентності по відношенню $\sim$ множини розміщень з повтореннями з n елементів по m. Іншими словами, комбінації з повтореннями – це властивість елементів множини, яка складається з вибраних m разів елементів множини M, причому один і той же елемент можна вибирати повторно.

Число комбінацій з повтореннями з n елементів по m позначається $\widehat{C}(n, m)$ і обчислюється згідно формули:

$$\widehat{C}(n, m) = C_{n+m-1}^m = \frac{(n+m-1)!}{m!(n-1)!}. \tag{2.4.2}$$

Приклад 1. Кількість різних результатів кидання двох однакових кубиків рівна $\widehat{C}(6, 2) = C_7^2 = 21$.

Приклад 2. Довести, що число (n, r) - перестановок без повторень рівне $(n)_r$.

Розв'язання

Скористаємося методом математичної індукції по r. При $r=1$ число способів вибору одного елемента з n рівне $n=(n)_1$. Нехай для деякого $r\geq 1$ виконується рівність $P(n,r)=(n)_r$. Доведемо аналогічну рівність для $r+1$. Будь-яка сукупність, яка складається з $r+1$ елементів може бути утвореною шляхом попереднього вибору елементів, утворюючих (n,r) - перестановку, і подальшого додавання до неї $(r+1)$ - го елемента. Якщо вибрано r елементів, то $(r+1)$ - ий елемент може бути вибраним $n-r$ способами. З урахуванням правила добутку, отримуємо, що:

$$P(n,r+1)=P(n,r)\cdot(n-r).$$

З використанням індукційного припущення звідси отримуємо, що:

$$P(n,r+1)=(n)_r\cdot(n-r)=(n)_{r+1}.$$

Також значна частина комбінаторних задач зводиться до підрахунку кількості двійкових векторів.

Приклад 3. Скількома способами можна представити число n у вигляді суми k невід'ємних доданків? (Представлення, які відрізняються тільки порядком доданків, уважаються різними.)

Розв'язання

Кожному розбиттю числа n на k цілих невід'ємних доданків поставимо у відповідність вектор довжини $n+k-1$, що містить n одиниць та $k-1$ нулів, в якому число одиниць, що містяться перед першим і другим нулями, дорівнює другому доданку і так далі. Тоді відповідність є взаємно однозначною. Зауважимо, що кожному двійковому вектору с $n+k-1$ координатами і n одиницями в свою чергу можна поставити у відповідність підмножину A множини $U=\{a_1,a_2,...,a_{n+k-1}\}$ наступним чином: i - а координата вектора рівна 1 тоді і тільки тоді, коли $a_i\in A$ $(i=1,2,...,n+k-1)$. Зрозуміло, що число таких підмножин рівна $C(n+k-1)$.

Приклад 4. Знайти найбільший член у розкладі бінома: $\left(1+\sqrt{3}\right)^{100}$.

Розв'язання

Нехай T_k - найбільший член розкладу заданого бінома $\left(1+\sqrt{3}\right)^{100}$, тоді $T_k = C_{100}^k 1^{100-k} \cdot \left(\sqrt{3}\right)^k$. Тоді очевидно, що виконуються нерівності: $T_k > T_{k-1}$ і $T_k > T_{k+1}$. Отримуємо систему нерівностей:

$$\begin{cases} C_{100}^k \cdot \left(\sqrt{3}\right)^k > C_{100}^{k-1} \cdot \left(\sqrt{3}\right)^{k-1}, \\ C_{100}^k \cdot \left(\sqrt{3}\right)^k > C_{100}^{k+1} \cdot \left(\sqrt{3}\right)^{k+1}, \end{cases} \text{ або}$$

$$\begin{cases} \dfrac{100!}{k!(100-k)!} \cdot \left(\sqrt{3}\right)^k > \dfrac{100!}{(k-1)!(101-k)!} \cdot \left(\sqrt{3}\right)^{k-1}, \\ \dfrac{100!}{k!(100-k)!} \cdot \left(\sqrt{3}\right)^k > \dfrac{100!}{(k+1)!(99-k)!} \cdot \left(\sqrt{3}\right)^{k+1}, \end{cases}$$

Після спрощення маємо: $\begin{cases} \dfrac{\sqrt{3}}{k} > \dfrac{1}{101-k}, \\ \dfrac{1}{100-k} > \dfrac{\sqrt{3}}{k+1} \end{cases}$ або

$\begin{cases} (101-k)\sqrt{3} > k, \\ k+1 > (100-k)\sqrt{3} \end{cases}$, звідки: $\begin{cases} k(1+\sqrt{3}) < 101\sqrt{3}, \\ k(1+\sqrt{3}) < 100\sqrt{3}-1 \end{cases}$, отримуємо:

подвійну нерівність для k: $\dfrac{100\sqrt{3}-1}{1+\sqrt{3}} < k < \dfrac{101\sqrt{3}}{1+\sqrt{3}}$. Підставляючи наближене значення $\sqrt{3} = 1{,}732$, отримуємо: $63{,}135 < k < 64{,}64$.

Єдине ціле значення k, яке задовольняє отриману нерівність є 64.

Значить, найбільший член розкладу бінома має номер, рівний 64 і $T_{64} = C_{100}^{64} \cdot 1^{100-64} \cdot \left(\sqrt{3}\right)^{64}$.

Приклад 5. З заданої пропорції $C_x^{y+1} : C_x^y : C_x^{y-1} = 2:2:1$ знайти x і y.

Розв'язання

Записуючи окремо відношення першого члена пропорції до другого та третього, після скорочення, отримуємо:

$$\frac{x!}{(y+1)!(x-y-1)!}:\frac{x!}{y!(x-y)!}=\frac{x-y}{y+1};$$

$$\frac{x!}{y!(x-y)!}:\frac{x!}{(y-1)!(x-y+1)!}=\frac{x-y+1}{y}.$$

Використовуючи умову, отримуємо систему рівнянь:

$$\begin{cases}\dfrac{x-y}{y+1}=1,\\[2ex] \dfrac{x-y+1}{y}=1,\end{cases}$$

звідки: $x=5,\ y=2$.

Приклад 6. Знайти коефіцієнт при x^{30} в розкладі виразу $\left(3-x^2+x^5\right)^{19}$ за поліноміальною формулою, отриманий після розкриття дужок і зведення подібних членів.

Розв'язання

Загальний член розкладу за поліноміальною формулою має вигляд: $3^m\cdot\left(-x^2\right)^n\cdot\left(x^5\right)^k\cdot P(m,\ nn\ k)$.

Для відшукання всіх випадків, в яких виникає x^{30}, отримуємо діофантове рівняння в цілих невід'ємних числах: $2n+5k=30$.

Виразимо k: $k=6-\dfrac{2n}{5}$. Видно, що k приймає цілі значення, якщо n кратне 5. Випишемо всі такі випадки:

$$n=0\Rightarrow k=6;\ n=5\Rightarrow k=4;$$

$$n=10\Rightarrow k=2;\ n=15\Rightarrow k=0.$$

Для кожної із знайдених пар значень n, k значення m знаходимо з рівняння: $m+n+k=19$. Отримуємо три набори $(m,\ n,\ k)$:

$$(13;\ 0;\ 6),\ (10;\ 5;\ 4),\ (7;\ 10;\ 2),\ (4;\ 15;\ 0).$$

Доданки, які містять x^{30}, такі:

$$3^{13}\cdot\left(-x^2\right)^0\cdot\left(x^5\right)^6\cdot P(13,\ 0,\ 6);\ 3^{10}\cdot\left(-x^2\right)^5\cdot\left(x^5\right)^4\cdot P(10,\ 5,\ 4);$$

$$3^7\cdot\left(-x^2\right)^{10}\cdot\left(x^5\right)^2\cdot P(7,\ 10,\ 2);\ 3^4\cdot\left(-x^2\right)^{15}\cdot\left(x^5\right)^0\cdot P(4,\ 15,\ 0).$$

Таким чином коефіцієнт при x^{30} має вигляд:

$$19!\left(\frac{3^{13}}{13!0!6!}-\frac{3^{10}}{10!5!4!}+\frac{3^{7}}{7!10!2!}-\frac{3^{4}}{4!15!0!}\right).$$

Список рекомендованих до розв'язування задач.

1. Скількома способами можна розподілити три білети серед 20 студентів, якщо:

1) розподіляються білети в різні театри, а кожен студент може отримати не більше одного білета;

2) розподіляються білети в різні театри і на різні дні, а кожний студент може отримати будь-яке (не перевищуюче трьох) число білетів;

3) розподіляються рівноцінні білети на вечір і кожен студент може отримати не більше одного білета?

2. З'ясувати, скількома способами можна в вистроїти дев'ять чоловік:

1) у колону по одному;

2) в колону по три, якщо в кожній шерензі люди вистроюються за ростом і при цьому нема людей однакового росту?

3. Довести, що:

1) $\widehat{P}(n,r)=n^r$; 2) $C(n,r)=\binom{n}{r}$; 3) $\widehat{C}(n,r)=\binom{n+r-1}{n-1}$.

4. 1) Якою є кількість матриць, що містять n рядків і m стовбців з елементами з множини $\{0,1\}$?

2) Те ж саме при умові, що рядки матриці є попарно різними?

5. Дано m предметів одного сорту і n іншого. Знайти число вибірок, складених з предметів першого сорту і s предметів іншого сорту.

6. Довести властивості біноміальних коефіцієнтів:

1) $\binom{n}{k}=\binom{n}{n-k}$; 2) $\binom{n}{k}=\binom{k}{r}=\binom{n-r}{k-r}\binom{n}{r}$;

3) $\binom{n}{k}=\binom{n-1}{k}+\binom{n-1}{k-1}$; 4) $\dfrac{\binom{n}{k-r}}{\binom{n}{k}}=\dfrac{(k)_r}{(n-k+r)_r}$;

5) $\binom{n}{k}=\sum_{r=0}^{n}\binom{n-r-1}{k-r}$; 6) $\dfrac{\binom{n-r}{k-r}}{\binom{n}{k}}=\dfrac{(k)_r}{(n)_r}$;

7) $\dfrac{\binom{n+1}{k}}{\binom{n}{k}}=\dfrac{n+1}{n-k+1}$; 8) $\sum_{r=k}^{n}\binom{r}{k}=\binom{n+1}{k+1}$.

7. Довести , що:

1) $\binom{n}{k}$ зростає по n при фіксованому k;

2) $\binom{n-r}{k-r}$ спадає по r при фіксованих n і k;

3) якщо n фіксоване, то $\binom{n}{k}$ зростає по k при $k \le \left[\frac{n}{2}\right]$ і спадає при $k > \left]\frac{n}{2}\right[$.

8. Індукцією по n з використанням співвідношення $\binom{n+1}{k}=\binom{n}{k}+\binom{n}{k-1}$ довести тотожність:

$$(1+t)^n=\sum_{k=0}^{n}\binom{n}{k}t^k . \qquad (1)$$

9. Нехай n і m - цілі додатні числа. З використанням тотожності (1) чи іншим способом довести наступні рівності:

1) $\sum_{k=0}^{n}\binom{n}{k}=2^n$; 2) $\sum_{k=0}^{n}(-1)^k\binom{n}{k}=0$; 3) $\sum_{k=1}^{n}k\binom{n}{k}=n2^{n-1}$;

4) $\sum_{k=2}^{n}k(k-1)\binom{n}{k}=n(n-1)2^{n-2}$; 5) $\sum_{k=0}^{n}(2k+1)\binom{n}{k}=(n+1)2^n$;

6) $\sum_{k=0}^{n}\frac{1}{k+1}\binom{n}{k}=\frac{1}{n+1}\left(2^{n+1}-1\right)$; 7) $\sum_{k=0}^{n}(-1)^k\frac{1}{k+1}\binom{n}{k}=\frac{1}{n+1}$;

8) $\sum_{k=1}^{n}\frac{(-1)^{k-1}}{k}\binom{n}{k}=1+\frac{1}{2}+\ldots+\frac{1}{n}$;

9) $\sum_{r=0}^{k}\binom{m}{r}\binom{n}{k-r}=\binom{n+m}{k}$; 10) $\sum_{k=0}^{n}\binom{n}{k}^2=\binom{2n}{n}$;

11) $\sum_{r=k}^{n}(-1)^{k-r}\binom{n}{r}=\sum_{r=0}^{n-k}(-1)^{n-r-k}\binom{n}{r}$; 12) $\sum_{r=0}^{n-k}\binom{n}{k+r}\binom{m}{r}=\binom{m+n}{n-k}$;

15) $\sum_{k=n}^{m}(-1)^{k-n}\binom{k}{n}\binom{m}{k}=\begin{cases}0 & \text{при } m\neq n,\\ 1 & \text{при } m=n.\end{cases}$

10. Довести тотожності:

1) $\sum_{k}\binom{n}{2k}=\sum_{k}\binom{n}{2k+1}=2^{n-1}$;

2) $4\sum_{k}\binom{n}{4k}=2^n+2^{n/2+1}\cos\frac{\pi n}{4}$.

11. Визначити, скільки раціональних членів міститься в розкладів:

1) $\left(\sqrt{2}+\sqrt[3]{3}\right)^{20}$; 2) $\left(\sqrt{3}+\sqrt[4]{5}\right)^{50}$; 3) $\left(\sqrt[3]{6}+\sqrt[4]{2}\right)^{100}$;

4) $\left(\sqrt[3]{12}+\sqrt[6]{3}\right)^{30}$.

12. Знайти коефіцієнт при t^k в розкладі:

1) $(1+2t-3t^2)^8$, $k=9$; 2) $(1-t+2t^2)^{10}$, $k=7$;

3) $(2+t-2t^3)^{10}$, $k=5$; 4) $(2+t^4+t^7)^{15}$, $k=17$.

13. Виходячи з комбінаторних міркувань, довести, що для будь-яких цілих невід'ємних $k_1, k_2,\ldots,k_s, n$ таких, що $k_1+k_2+\ldots+k_s=n$, справедлива рівність:

$$\binom{n}{k_1}\binom{n-k_1}{k_2}\cdots\binom{n-k_1-k_2-\ldots-k_{s-1}}{k_s}=\frac{n!}{k_1!k_2!\ldots k_s!}.$$

14. Індукцією по s довести тотожність:

$$(t_1+t_2+\ldots+t_s)^n=\sum_{\substack{k_1,\ldots,k_s\\ k_1+\ldots+k_s=n}}\frac{n!}{k_1!k_2!\ldots k_s!}t_1^{k_1}t_2^{k_2}\ldots t_s^{k_s}.$$

2.5. Розбиття

Нехай M - множина потужності n, $\{M_1, M_2, ..., M_k\}$ - розбиття множини M на k підмножин, $|M_i| = m_i$, $m_1 + m_2 + ... + m_k = n$. Кортеж $(M_1, M_2, ..., M_k)$ називається впорядкованим розбиттям множини M.

Якщо $k = 2$, то впорядковане розбиття множини M на дві підмножини, які містять відповідно по m_1 і m_2 елементів, визначається комбінацією без повторень з n елементів по m_1 чи з n по m_2 ($m_2 = n - m_1$). Значить, число розбиттів $R(m_1, m_2)$ дорівнює біноміальному коефіцієнту $C_n^{m_1} = C_n^{m_2}$. Таким чином:

$$R(m_1, m_2) = \frac{n!}{m_1!(n-m_1)!} = \frac{n!}{m_1!m_2!}. \qquad (2.5.1)$$

В загальному випадку кількість $R(m_1, m_2, ..., m_k)$ впорядкованих розбиттів $(M_1, M_2, ..., M_k)$, для яких $|M_i| = m_i$ дорівнює $\frac{n!}{m_1!m_2!...m_k!}$, а кількість $R(n, k)$ впорядкованих розбиттів на k підмножин визначається формулою:

$$R(n, k) = \sum_{\substack{m_1+m_2+...+m_k=n, \\ m_i>0}} R(m_1, m_2, ..., m_k). \qquad (2.5.2)$$

Числа $R(m_1, m_2, ..., m_k)$ називаються поліноміальними коефіцієнтами, оскільки для всіх $a_1, a_2, ..., a_k \in R$ є справедливим співвідношення:

$$(a_1 + a_2 + ... + a_k)^n = \sum_{\substack{m_1+...+m_k=n, \\ m_i>0}} \frac{n!}{m_1!...m_k!} a_1^{m_1} a_2^{m_2} ... a_k^{m_k}. \qquad (2.5.3)$$

Число $\widehat{R}(m_1, m_2, ..., m_k)$ розбиттів вихідної множини M на k підмножин $M_1, M_2, ..., M_k, |M_i| = m_i$, не впорядкованих між собою, обчислюється за формулою:

$$\widehat{R}(m_1, m_2, ..., m_k) = \frac{n!}{m_1!...m_k!(1!)^{m_1}...(n!)^{m_k}}, \qquad (2.5.4)$$

а кількість всіх можливих розбиттів множини M на k підмножин, не впорядкованих між собою рівна:

$$\sum_{\substack{m_1+\ldots+m_k=n,\\ m_i>0}} \widehat{R}(m_1, m_2, ..., m_k).$$

2.6. Метод включень та виключень

Нехай множина A містить N елементів та n одномісних бінарних відношень $P_1, P_2, ..., P_n$. Кожен з N елементів може мати чи не мати будь-яку із згаданих властивостей. Позначимо через $N_{i_1 \ldots i_k}$ число елементів, які мають властивості $P_{i_1}, ..., P_{i_k}$ і, можливо деякими іншими. Тоді число $N(0)$ елементів, які не мають можної з властивостей $P_1, P_2, ..., P_n$, визначається формулою, яка називається формулою включень і виключень:

$$N(0) = S_0 - S_1 + S_2 - \ldots + (-1)^n S_n, \tag{2.6.1}$$

де $S_0 = N;\ S_k = \sum_{1 \le i_1 < \ldots < i_k \le n} N_{i_1 \ldots i_k}, k = 1, 2, ..., n$.

Використовуючи формулу (2.6.1), отримуємо, що число $N(0)$ розміщень, при яких можна з властивостей P_i не виконується, рівна:

$$\sum_{k=0}^{n} (-1)^k S_k = n! \sum_{k=0}^{n} (-1)^k \frac{1}{k!}. \tag{2.6.2}$$

Тоді, узагальнюючи формулу (2.6.1), отримаємо формулу, яка дозволяє обчислити число $N(r)$ елементів, які мають рівно r властивостей $(1 \le r \le n)$:

$$N(r) = \sum_{k=0}^{n-r} (-1)^k C_{r+k}^{r} S_{r+k}. \tag{2.6.3}$$

2.7. Рекурентні відношення. Зворотні послідовності.

Рекурентним співвідношенням, рекурентним рівнянням чи рекурентною функцією називається співвідношення виду $a_{n+k} = F(n, a_n, a_{n+1}, ..., a_{n+k+1})$, яке дозволяє обчислювати всі члени послідовності $a_0, a_1, a_2, ...$, якщо задані перші k членів послідовності.

Приклад 1.

1. Формула $a_{n+1} = a_n + d$ визначає арифметичну прогресію;

2. Формула $a_{n+1} = q \cdot a_n$ визначає геометричну прогресію;

3. Формула $a_{n+2} = a_{n+1} + a_n$ задає послідовність чисел Фібоначчі.

У випадку, коли рекурентне співвідношення є лінійним і однорідним, тобто виконується співвідношення виду:

$$a_{n+k} + p_1 a_{n+k-1} + ... + p_k a_n = 0\,,\ \forall n \geq 0 \qquad (2.7.1)$$

$(p = \text{const})$, послідовність $a_0, a_1, a_2, ...$ називається зворотною. Многочлен:

$$P_a(x) = x^k + p_1 x^{k-1} + ... + p_k \qquad (2.7.2)$$

називається характеристичним для зворотної послідовності $\{a_n\}$. Корені многочленна $P_a(x)$ називаються характеристичними.

Множина усіх послідовностей, задовольняючих дане рекурентне співвідношення, називається загальним розв'язком.

Твердження 2.7.1. Множина U послідовностей $\{a_n\}_{n=0}^{\infty}$, які задовольняють співвідношення (2.7.1), є лінійним простором, що має розмірність k.

Доведення

Множина всіх нескінченних числових послідовностей с операціями додавання (не компонентно) і множення (покомпонентно) є лінійним простором. Тому, щоб довести, що послідовності $\{a_n\}_{n=0}^{\infty}$, які задовольняють співвідношення (2.7.1) утворюють лінійний підпростір, достатньо упевнитися в замкнутості множини таких послідовностей відносно операції додавання та множення на число. Якщо $\{a_n\}_{n=0}^{\infty}$ і $\{b_n\}_{n=0}^{\infty}$ задовольняють співвідношення (2.7.1), α і β - довільній дійсні числа, а n - довільне невід'ємне ціле, то:

$$\begin{aligned}&(\alpha a_{n+k} + \beta b_{n+k}) + p_1(\alpha a_{n+k-1} + \beta b_{n+k-1}) + ... + p_k(\alpha a_n + \beta b_n) = \\ &= \alpha(a_{n+k} + p_1 a_{n+k-1} + ... + p_k a_n) + \beta(b_{n+k} + p_1 b_{n+k-1} + ... + p_k b_n) = 0.\end{aligned} \qquad (2.7.3)$$

Значить, U - лінійний простір.

Якщо послідовність $\{a_n\}_{n=0}^{\infty}$ задовольняє співвідношення (2.7.1) і задані числа $a_0, ..., a_{k-1}$, то всі решта чисел a_i визначаються з (2.7.1) однозначно. Значить, розмірність U не перевищує k. З іншого боку, для $j = 0$, 1,..., $k-1$

послідовність A_j можна побудувати таким чином: $a_j = 1, a_i = 0$ для $i \in \{0, 1, ..., k-1\} \setminus \{j\}$: решта a_{n+k} для $n \geq 0$ визначаються із (2.7.1). Тоді послідовності $A_j \ (j = 0, 1, ..., k-1)$ є лінійно незалежними у загальній сукупності.

Описання загального розв'язку співвідношення (2.7.1) має аналоги с описання розв'язків звичайного диференціального рівняння з постійними коефіцієнтами.

Теорема 2.7.1. 1. Нехай λ - корінь характеристичного многочлена (2.7.2). Тоді послідовність $\{c\lambda_n\}$, де c - довільна постійна, задовольняє співвідношенню (2.7.1).

2. Якщо $\lambda_1, \lambda_2, ..., \lambda_k$ - прості корені характеристичного многочлена (2.7.2), то загальний розв'язок рекурентного співвідношення (2.7.1) має вигляд $a_n = c_1\lambda_1^n + c_2\lambda_2^n + ... + c_n\lambda_n^n$, де $c_1, c_2, ..., c_k$ - довільні константи.

3. Якщо λ_i - корінь кратності r_i $(i = 1, ..., s)$ характеристичного многочлена (2.7.2), то розв'язок рекурентного співвідношення (2.7.1) має вигляд $a_n = \sum_{i=1}^{s} \left(c_{i1} + c_{i2}n + ... + c_{ir_i} n^{r_i - 1} \right) \lambda_i^n$, де c_{ij} - довільні константи.

Знаючи розв'язок рекурентного рівняння (2.7.1), за початковим умовами $a_0, a_1, ..., a_{k-1}$ можна знайти невідомі постійні c_{ij} і таким чином, отримати розв'язок рівняння (2.7.1) з заданими початковими умовами.

Твердження 2.7.2. (Наслідок з Теореми2.7.1). Нехай λ - корінь многочлена (2.7.2) кратності s $(s \geq 1)$. Тоді для будь-якого $t, 1 \leq t \leq s$, послідовність $\{b_n(t)\}_{n=0}^{\infty}$, де $b_n = n^{t-1}\lambda^n$, задовольняє співвідношення (2.7.1).

Доведення

Випадок 1. $t = 1$. Тоді $b_n = \lambda^n$ $(n = 0, 1, ...)$ і:

$$\begin{aligned} b_{n+k} + p_1 b_{n+k-1} + ... + p_k b_n = \lambda^{n+k} + p_1\lambda^{n+k-1} + ... + p_k\lambda^n = \\ = \lambda^n \left(\lambda^k + p_1\lambda^{k-1} + ... + p_k \right) = 0. \end{aligned} \tag{2.7.4}$$

Випадок 2. $t>1$. Зауважимо, що $\lambda \neq 0$, оскільки $p_k \neq 0$. Визначимо функцію $\varphi(f(x)) = xf'(x)$ і $\varphi_m(f(x)) = \underbrace{\varphi(\varphi(...\varphi}_{m \text{ разів}}(f(x)...))$. З урахуванням **Твердження 7.1** легко встановлюється лінійність функції $\varphi(f(x))$, що полягає у тому, що: $\varphi(f(x)+g(x)) = \varphi(f(x)) + \varphi(g(x))$, і що $\varphi(ax^r) = arx^r$. Оскільки λ - корінь кратності не менше t многочлена $P_n(x) = x^n P(x)$, то λ є і коренем многочлена:

$$\varphi_{t-1}(P_n(x)) = \varphi_{t-1}(x^{n+k} + p_1 x^{n+k-1} + ... + p_k x^n) =$$
$$= \varphi_{t-1}(x^{n+k}) + \varphi_{t-1}(p_1 x^{n+k-1}) + ... + \varphi_{t-1}(p_k x^n) = (n+k)^{t-1} x^{x+k} +$$
$$+ (n+k-1)^{t-1} p_1 x^{n+k-1} + ... + (n+1)^{t-1} p_{k-1} x^{n+1} + n^{t-1} p_k x^n.$$

Оскільки $\lambda \neq 0$, отримуємо:

$$(n+k)^{t-1}\lambda^k + (n+k-1)^{t-1}\lambda^{k-1} p_1 \lambda^{k-1} + ... + (n+1)^{t-1} p_{k-1}\lambda + n^{t-1} p_k = 0,$$

що і необхідно було довести.

Таким чином, якщо $\lambda_1, ..., \lambda_m$ - корені многочлена (2.7.2) і λ_i - корінь кратності s_i $(1 \le i \le m,\ s_1 + ... + s_m = k)$, то довільна послідовність $\{a_n\}_{n=0}^{\infty}$ виду:

$$\begin{aligned} a_n &= (a_{1,1} + a_{1,2} n + ... + a_{1,s_1} n^{s_1-1})\lambda_1^n + ... \\ &.... + (a_{m,1} + a_{m,2} n + ... + a_{m,s_m} n^{s_m-1})\lambda_m^n \qquad (n = 0, 1, 2, ...), \end{aligned} \tag{2.7.5}$$

де $\alpha_{i,j}$ - довільні константи, задовольняє (2.7.1).

Використовуючи наведений вище прийом можна установити лінійну незалежність усіх k послідовностей із **Прикладу 1.**

Приклад 2. Якщо усі корені $\lambda_1, ..., \lambda_k$ характеристичного многочлена (2.7.2) різні, то визначник Вандермонда: $W = W(\lambda_1, ..., \lambda_k)$ не рівний нулю.

$$W = \begin{vmatrix} 1 & \lambda_1 & \lambda_1^2 & ... & \lambda_1^{k-1} \\ 1 & \lambda_2 & \lambda_2^2 & ... & \lambda_2^{k-1} \\ ... & ... & ... & ... & ... \\ 1 & \lambda_k & \lambda_k^2 & ... & \lambda_k^{k-1} \end{vmatrix}.$$

Випадок 1. Усі корені (2.7.2) мають кратність 1. Для доведення того, що послідовності $\{\lambda_i^n\}_{n=0}^{\infty}$ $(i=1,..,k)$ є лінійно незалежними, достатньо встановити, що лінійно незалежними є вектори $(1, \lambda_i, \lambda_i^2, ..., \lambda_i^{k-1})$ $(i=1,2,...,k)$, тобто вектори, складені з їх перших k координат. Останнє твердження є еквівалентним до вихідного.

Випадок 2. Корінь λ має кратність k. Тоді достатньо довести, що $D_k \neq 0$, де:

$$D_k = \begin{vmatrix} 1 & \lambda & \lambda^2 & ... & \lambda^{k-1} \\ 0 & \lambda & 2\lambda^2 & ... & (k-1)\lambda^{k-1} \\ 0 & \lambda & 2^2\lambda^2 & ... & (k-1)^2\lambda^{k-1} \\ ... & ... & ... & ... & ... \\ 0 & \lambda & 2^{k-1}\lambda^2 & ... & (k-1)^2\lambda^{k-1} \end{vmatrix}.$$

Але оскільки:

$$D_k = \lambda^{k(k-1)/2} \begin{vmatrix} 1 & 1 & 1 & 1 & ... & 1 \\ 0 & 1 & 2 & 3 & ... & k-1 \\ 0 & 1 & 2^2 & 3^2 & ... & (k-1)^2 \\ ... & ... & ... & ... & ... & ... \\ 0 & 1 & 2^{k-1} & 3^{k-1} & ... & (k-1)^{k-1} \end{vmatrix} \neq 0,$$

що й доводить задане твердження.

Приклад 3. Характеристичним многочленом для послідовності чисел Фібоначчі $a_{n+2} = a_{n+1} + a_n$ є $P(x) = x^2 - x - 1$. Коренями характеристичного многочлена $P(x)$ є $\lambda_1 = \frac{1+\sqrt{5}}{2}$ і $\lambda_2 = \frac{1-\sqrt{5}}{2}$. Відповідно, для деяких α_1 і α_2 маємо:

$$F_n = \alpha_1\lambda_1^n + \alpha_2\lambda_{12}^n, \ \forall n.$$

Знайдемо α_1 і α_2, враховуючи, що для послідовності чисел Фібоначчі: $F_0 = F_1 = 1$:

$$\alpha_1 + \alpha_2 = 1 \text{ і } \alpha_1\lambda_1 + \alpha_2\lambda_2 = 1.$$

Звідси знаходимо, що:

$$\alpha_1 = \frac{1+\sqrt{5}}{2\sqrt{5}},\ \alpha_2 = -\frac{1-\sqrt{5}}{2\sqrt{5}} \text{ і тоді:}$$

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right).$$

Приклад 4. Знайти послідовність $\{a_n\}$, яка задовольняє рекурентне співвідношення $a_{n+2} - 4a_{n+1} + 3a_n = 0$ і початкові умови $a_1 = 10,\ a_2 = 16$.

Розв'язання

Коренями характеристичного многочлена $P_a = x^2 - 4x + 3$ є числа $x_1 = 1$ і $x_2 = 3$. З урахуванням **Теореми 2.7.1.** загальний розв'язок має вигляд: $a_n = c_1 + c_2 \cdot 3^n$. Використовуючи початкові умови, отримуємо систему:

$$\begin{cases} c_1 + 3c_2 = 10, \\ c_1 + 9c_2 = 16, \end{cases}$$

звідки знаходимо, що $c_1 = 7$ і $c_2 = 1$. Таким чином, $a_n = 7 + 3^n$.

Розглянемо неоднорідне лінійне рекурентне рівняння:

$$a_{n+k} + p_1 a_{n+k-1} + ... + p_k a_n = f(n),\ n = 0, 1, ... \qquad (2.7.6)$$

Нехай $\{b_n\}$ - загальний розв'язок однорідного рівняння (2.7.6), а $\{c_n\}$ - частинний розв'язок неоднорідного рівняння (2.7.6). Тоді послідовність $\{b_n + c_n\}$ утворює загальний розв'язок рівняння (2.7.6), і тому є справедливою.

Теорема 2.7.3. Загальний розв'язок лінійного рекурентного рівняння зображається у вигляді суми загального розв'язку відповідного однорідного лінійного рекурентного рівняння і деякого частинного розв'язку неоднорідного рівняння.

Таким чином, в силу **Теореми 2.7.3.** задача зі знаходження загального розв'язку рекурентного рівняння (2.7.6) зводиться до знаходження деякого частинного розв'язку.

В окремих випадках можливими є загальні підходи до знаходження частинного розв'язку.

Якщо $f(n)=\beta^n$ (де β не є характеристичним коренем), то підставляючи $a_n=c\beta^n$ в (2.7.3), отримуємо $c(\beta^k+p_1\beta^{k-1}+...+p_k)\cdot\beta^k=\beta^n$ і звідси $c\cdot P_a(b)=1$, тобто частковий розв'язок можна задати формулою $a_n=\frac{1}{P_a(b)}\cdot\beta^n$.

Нехай $f(n)$ - Многочлен степеня r від змінної n, і число 1 не є характеристичним коренем. Тоді $P_a(1)=1+p_1+...+p_k\neq 0$ і частинний розв'язок треба шукати у вигляді $a_n=\sum_{i=0}^{r}d_i n^i$. Підставляючи многочлени у формулу (2.7.6), отримуємо:

$$\begin{aligned}&\sum_{i=0}^{r}d_i(n+k)^i+p_1\sum_{i=0}^{r}d_i(n+k-1)^i+...+p_k\sum_{i=0}^{r}d_i n^i=\\&=\sum_{i=0}^{r}d_i((n+k)^i+p_1(n+k-1)^i+...+p_k n^i)=\sum_{i=0}^{r}d_i(g_1 n^i+...)=f(n).\end{aligned}\qquad(2.7.7)$$

Прирівнюючи коефіцієнти в лівій та правій частинах останньої рівності, отримаємо співвідношення для чисел d_i, які дозволяють визначити ці числа.

Приклад 5. Знайти розв'язок рівняння:

$$a_{n+1}+2a_n=n+1$$

з початковою умовою $a_0=1$.

Розв'язання

Розглянемо характеристичний многочлен $P_a(x)=x+2$. Так як $P_a(1)=3\neq 0$ і права частина $f(n)$ рівняння (2.7.6) рівна $n+1$, то частинний розв'язок будемо шукати у вигляді $c_n=d_0+d_1\cdot n$. Підставляючи c_n у вихідне рівняння, отримуємо:

$$(d_0+d_1(n+1))+2(d_0+d_1\cdot n)=(3d_0+d_1)+3d_1\cdot n=1+n.$$

Прирівнюючи коефіцієнти в лівій і правій частинах останньої рівності, отримуємо систему:

$$\begin{cases} 3d_0 + d_1 = 1, \\ 3d_1 = 1, \end{cases}$$

звідки знаходимо, що $d_0 = \frac{2}{9}, d_1 = \frac{1}{3}$. Таким чином, частинний розв'язок заданого рівняння має вигляд: $c_n = \frac{2}{9} + \frac{1}{3}n$. За **Теоремою 7.1.** загальний розв'язок однорідного рівняння $a_{n+1} + 2a_n = 0$ виражається формулою $b_n = c \cdot (-2)^n$ і згідно із **Теоремою 2.7.3.** отримуємо загальний розв'язок вихідного рівняння:

$$a_n = \frac{2}{9} + \frac{1}{9}n + c \cdot (-2)^n.$$

З початкової умови $a_0 = 1$ знаходимо: $\frac{2}{9} + c = 1$, тобто $c = \frac{7}{9}$. Таким чином:

$$a_n = \frac{2}{9} + \frac{1}{3}n + \frac{7}{9}(-2)^n.$$

2.8. Утворюючі функції.

З будь-якою послідовністю $\{a_n\}_{n=0}^{\infty}$ можна пов'язати формальний степеневий ряд $A(t) = a_0 + a_1 t + a_2 t^2 + a_3 t^3 + ...,$ який називається утворюючою функцією для послідовності $\{a_n\}_{n=0}^{\infty}$. Якщо $|a_n|$ зростає не дуже швидко, то в деякому околі нуля цей ряд абсолютно сходиться і $A(t)$ можна спів ставити з деякою отримуваною аналітичною функцією.

Приклад 1.

1. $a_n = \binom{k}{n}$. Тоді: $A(t) = 1 + kt + \binom{k}{2}t^2 + ... + \binom{k}{k}t^k = (1+t)^k$.

2. $a_n = 1$. Тоді: $A(t) = 1 + t + t^2 + t^3 + ... = \frac{1}{1-t}$.

3. $a_n = \frac{1}{n!}$. Тоді: $A(t) = 1 + \frac{t}{1!} + \frac{t^2}{2!} + ... = e^t$.

4. $a_n = F_n$. Тоді:

$$A(t)=\sum_{n=0}^{\infty}F_n t^n = 1+t+\sum_{n=2}^{\infty}(F_{n-2}+F_{n-1})t^n =$$

$$=1+t+t^2\sum_{n=0}^{\infty}F_n t^n + t\sum_{n=1}^{\infty}F_n t^n = 1+t^2A(t)+tA(t).$$

З рівняння $A(t)=1+t^2A(t)+tA(t)$ отримуємо: $A(t)=\dfrac{1}{1-t-t^2}$.

Знаючи утворюючу функцію $A(t)$, можна знайти будь-яке a_n, використовуючи розклад у ряд Тейлора. Маємо: $a_n=\dfrac{A(0)^{(n)}}{n!}$.

Приклад 2.

1. $A(t)=\dfrac{1}{1-2t}$.

Тоді:

$A^{(n)}(t)=(-1)(-2)...(-n)(-2)^n(1-2t)^{-1-n}$.

Значить, $A(0)=1$, $\dfrac{A^{/}(0)}{1!}=2$; $\dfrac{A^{//}(0)}{2!}=2^2$,..., $\dfrac{A^{(n)}(0)}{n!}=2^n$.

2. $A(t)=(1+t)^{-m}$, де число $-m$ не є натуральним.

Тоді: $A^{(n)}(t)=(-m)(-m-1)...(-m-n+1)(1+t)^{-m-n}$.

Значить: $a_n=\dfrac{A(0)^{(n)}}{n!}=\dfrac{[-m]_n}{n!}=\begin{pmatrix}-m\\ n\end{pmatrix}=(-1)^n\begin{pmatrix}m+n-1\\ n\end{pmatrix}$.

Формальні ряди можна додавати і перемножувати: якщо $A(t)=\sum_{n=0}^{\infty}a_n t^n$, $B(t)=\sum_{n=0}^{\infty}b_n t^n$, то:

$$A(t)B(t)=\sum_{n=0}^{\infty}d_n t^n, \text{ де } d_k=a_0b_k+a_1b_{k-1}+...+a_kb_0. \qquad (2.8.1)$$

Властивість (2.8.1) можна використовувати при виведенні ряду тотожностей.

Приклад 3.

Розпишемо очевидну рівність $(1+t)^k(1+t)^{-m}=(1+t)^{k-m}$ через ряди:

$$\left(\sum_{n=0}^{\infty}\begin{pmatrix}k\\ n\end{pmatrix}t^n\right)\left(\sum_{n=0}^{\infty}(-1)^n\begin{pmatrix}m+n-1\\ n\end{pmatrix}t^n\right)=\sum_{n=0}^{\infty}\begin{pmatrix}k-m\\ n\end{pmatrix}t^n.$$

Прирівнюючи коефіцієнти при t^n, отримуємо справа $\binom{k-m}{n}$, а зліва:

$$\sum_{i=0}^{n}\binom{k-m}{i}(-1)^{n-i}\binom{m+n-1-i}{n-i}.$$

Таким чином:

$$\binom{k-m}{n}=\sum_{i=0}^{n}\binom{k-m}{i}(-1)^{n-i}\binom{m+n-1-i}{n-i}.$$

Використовуючи означення чисел Каталана, знайдемо утворюючу функцію $C(t)$ цієї послідовності и таким чином, виведемо їх явну формулу. Маємо:

$$C(t)=\sum_{n=0}^{\infty}c_n t^t=1+\sum_{n=1}^{\infty}(c_0c_{n-1}+...+c_{n-1}c_0)t^n=$$

$$=1+t\sum_{n=0}^{\infty}(c_0c_{n-1}+...+c_{n-1}c_0)t^n=1+t\big(C(t)\big)^2.$$

Розв'язуючи квадратне рівняння відносно $C(t)$, отримуємо:

$$C(t)=\frac{1\pm\sqrt{1-4t}}{2t}.$$

Оскільки $C(0)=1$, в останньому виразі слід залишити знак "-".

Знаходимо n - у похідну від $\sqrt{1-4t}$:

$$\frac{d^n}{dt^n}\left(\sqrt{1-4t}\right)=\binom{1/2}{n}n!(1-4t)^{\frac{1}{2}-n}(-4)^n=2^n(-1)(2n-3)!!(1-4t)^{\frac{1}{2}-n}.$$

Отже:

$$1-\sqrt{1-4t}=\sum_{n=1}^{\infty}\frac{2^n(2n-3)!!}{n!}t^n$$

і

$$C(t)=\sum_{n=1}^{\infty}\frac{2^n(2n-3)!!}{n!}t^n.$$

Врахуємо, що:

$$\frac{2^n(2n-3)!!}{n!} = \frac{(2n)!}{n!(n+1)!} = \frac{1}{n+1}\binom{2n}{n}$$, тому:

$$C(t) = \sum_{n=1}^{\infty} \frac{1}{n+1}\binom{2n}{n} t^n .$$

Список рекомендованих до розв'язування задач.

1. 1) Довести, що зворотна послідовність повністю визначається заданням її перших k членів і співвідношенням $a_{n+k} + p_1 a_{n+k-1} + ... + p_k a_n = 0$ (1).

2) Нехай λ - корінь характеристичного многочлена $P(x) = x^k + p_1 x^{k-1} + ... + p_k$ (2). Довести, що послідовність $\{c\lambda^n\}$, де c - константа, задовольняє співвідношення (1).

3) Довести, що якщо $\lambda_1, ..., \lambda_k$ - прості (не кратні) корені характеристичного многочлена (2), то загальний розв'язок рекурентного співвідношення (1) має вигляд:

$$a_n = c_1\lambda_1^n + ... + c_k\lambda_k^n .$$

4) Нехай λ_i - корінь характеристичного многочлена (2) кратності r_i $(i = 1, ..., s)$. Довести, що тоді загальний розв'язок рекурентного співвідношення (1) має вигляд:

$$a_n = \sum_{i=1}^{s} (c_{i1} + c_{i2}n + ... + c_{ir_i} n^{r_i - 1})\lambda_i^n ,$$

де c_{ij} $(i = 1, ..., s,\ j = 1, ..., r_i)$ - деякі константи.

2. Найти загальні розв'язки рекурентних співвідношень:

1) $a_{n+2} - 4a_{n+1} + 3a_n = 0$; 2) $a_{n+2} + 3a_n = 0$;

3) $a_{n+2} - a_{n+1} - a_n = 0$; 4) $a_{n+2} + 2a_{n+1} + a_n = 0$;

5) $a_{n+3} + 10a_{n+2} + 32a_{n+1} + 32a_n = 0$;

6) $a_{n+3} + 3a_{n+2} + 3a_{n+1} + a_n = 0$.

3. Знайти a_n за заданими рекурентними співвідношеннями и початковими умовами:

1) $a_{n+2} - 4a_{n+1} + 3a_n = 0,\ a_0 = 10,\ a_1 = 16$;

2) $a_{n+3} - 3a_{n+2} + a_{n+1} - 3a_n = 0,\ a_0 = 3,\ a_1 = 7,\ a_2 = 27$;

3) $a_{n+3} - 3a_{n+1} + 2a_n = 0,\ a_0 = a,\ a_1 = b,\ a_2 = b$;

4) $a_{n+2} - 2\cos\alpha\, a_{n+1} + a_n = 0,\ a_0 = 1,\ a_1 = \cos\alpha$;

5) $a_{n+2} - a_n = 0,\ a_0 = 0,\ a_1 = 2$;

6) $a_{n+2} - 6a_{n+1} + 9a_n = 0,\ a_0 = 6,\ a_1 = 6$.

4. Знайти розв'язки лінійних неоднорідних рекурентних співвідношень:

1) $a_{n+1} - a_n = n,\ a_1 = 1$;

2) $a_{n+2} + 2a_{n+1} - 8a_n = 27 \cdot 5^n,\ a_0 = 0,\ a_1 = -9$;

3) $a_{n+2} - 2a_{n+1} + 2a_n = 2^n,\ a_0 = 1,\ a_1 = 2$;

4) $a_{n+2} + a_{n+1} - 2a_n = n,\ a_0 = 1,\ a_1 = -2$;

5) $a_{n+2} - 4a_{n+1} + 4a_n = 2^n,\ a_0 = 1,\ a_1 = 2$;

6) $a_{n+2} + a_{n+1} - 6a_n = 5 \cdot 2^{n+1},\ a_0 = 2,\ a_1 = 1$.

5. 1) Нехай $\{a_n\}$ і $\{b_n\}$ - дві послідовності, члени яких задані співвідношеннями:

$$a_{n+1} = p_1 a_n + q_1 b_n,$$

$$b_{n+1} = p_2 a_n + q_2 b_n,$$

$$\Delta = p_1 q_2 - p_2 q_1 \equiv 0,$$

де p_1, q_1, p_2, q_2 - задані числа. Знайти вирази для a_n і b_n, уважаючи, що a_1 і b_1 задані.

2) Знайти розв'язок системи рекурентних співвідношень:

$$a_{n+1} = 3a_n + b_n,$$

$$b_{n+1} = -a_n + b_n,$$

$$a_1 = 15,\ b_1 = 6.$$

3) Знайти загальний розв'язок системи рекурентних співвідношень:

$$a_{n+1} = b_n + 5,$$

$$b_{n+1} = -a_n + 3.$$

6. Знайти утворюючу функцію $f(t)$ для послідовності $\{a_n\}$, якщо:

1) $a_n = 1$ для всіх $n \geq 0$;

2) $a_n = 1$ для всіх $0 \leq n \leq N$ і $a_n = 0$ при всіх $n > N$;

3) $a_n = \alpha^n$; 4) $a_n = \dfrac{\alpha^n}{n!}$; 5) $a_n = (-1)^n$; 6) $a_n = n$;

7) $a_n = n(n-1)$; 8) $a_n = \binom{m}{n}$, m - натуральне число;

9) $a_n = \binom{\alpha}{n}$, α - дійсне число; 10) $a_n = n^2$;

11) $a_n = \sin \alpha n$; 12) $a_n = \cos \alpha n$.

7. Найти експоненціальні утворюючі функції $E(t)$ для послідовності $\{a_n\}$, якщо:

1) $a_n = 1$; 2) $a_n = \alpha^n$; 3) $a_n = n$; 4) $a_n = n(n-1)$;

5) $a_n = (m)_n$; 6) $a_n = n^2$.

8. За допомогою тотожностей, що зв'язують утворюючі функції, вивести тотожності для біноміальних коефіцієнтів:

1) $(1+t)^n (1+t)^m = (1+t)^{n+m}$, $\displaystyle\sum_{s=0}^{k} \binom{n}{s}\binom{m}{k-s} = \binom{n+m}{k}$;

2) $(1-t)^{-1-n}(1-t)^{-1-m} = (1-t)^{-2-n-m}$, $\displaystyle\sum_{s=0}^{k} \binom{n+s}{s}\binom{m+k-s}{m} = \binom{n+m+k+1}{k}$;

3) $(1+t)^n (1+t)^{-m} = (1+t)^{n-m}$, $\displaystyle\sum_{s=0}^{k} (-1)^{k-s}\binom{n}{s}\binom{m+k-s+1}{k-s} = \binom{n-m}{k}$;

4) $(1-t)^{-1-n}(1+t)^{-1-n} = (1-t^2)^{-1-n}$, $\displaystyle\sum_{s=0}^{2k} (-1)^{k-s}\binom{n+s}{n}\binom{n+2k-s}{n} = \binom{n+k}{k}$;

9. Знайти загальний член a_n послідовності, для якої функція $A(t)$ є утворюючою:

1) $A(t) = (q + pt)^m$; 2) $A(t) = \dfrac{1}{1-t}$; 3) $A(t) = \sqrt{1-t}$;

4) $A(t) = t^m (1-t)^m$; 5) $A(t) = (t + t^2 + \ldots + t^r)^m$;

6) $A(t) = \left(1 + \dfrac{t^2}{2}\right)^{-m}$; 7); $A(t) = \ln(1+t)$ 8) $A(t) = \operatorname{arctg} t$;

9) $A(t) = \arcsin t$; 10) $A(t) = e^{-2t^2}$.

10. Довести тотожності:

1) $\sum\limits_s (-1)^{n-s} \binom{n}{s} \binom{m+s}{m+1} = \binom{m}{n-1}$;

2) $\sum\limits_s (-1)^s \binom{m}{s} \binom{m}{2n-s} = (-1)^n \binom{m}{n}$;

3) $\sum\limits_s (-1)^s \binom{m}{m-k+s} \binom{n+s}{n} = (-1)^n \binom{m-n-1}{k}$.

Список використаних джерел

1. Новиков Ф. А. Дискретная математика для программистов. - СПб.: Питер, 2004.

2. Бондаренко М. Ф., Білоус Н. В., Руткас А. Г. Комп'ютерна дискретна математика: Підручник. Харків: “Компанія СМІТ”, 2004. - 480 с.

3. Яблонский С.В. Введение в дискретную математику. — М.: Наука, 2006. — 384 с.

4. Гаврилов Г. П., Сапоженко А. А. Сборник задач по дискретной математике. — М: ФИЗМАТЛИТ, 2005.

5. Гаврилов Г.П., Сапоженко А.А. Задачи и упражнения по курсу дискретной математики. — М.: Наука, 2007. —408с.

6. Судоплатов С.В., Овчинникова Е.В. Элементы дискретной математики. – М.: ИНФРА-М; Новосибирск: НГТУ, 2003. – 280 с.

7. Иванов Б.Н. Дискретная математика. Алгоритмы и программы. Расширенный курс. - М: Известия, 2011. - 512 с.

8. Холл М. Комбинаторика. - М.: «Мир», 1970. - 424 с.

9. Нікольський Ю. В. Дискретна математика: підручник: гриф МОН України / Ю. В. Нікольський, В. В. Пасічник, Ю. М. Щербина. - 3-тє вид., випр. і доп. - Львів : Магнолія-2006, 2008. - 608 с.

10. Липский В. Комбинаторика для программистов. - М.: «Мир», 1988. -200 с.

11. Белоусов А. И., Ткачев С. Б. Дискретная математика: Учеб. для вузов. - М.: Изд-во МГТУ им. Н.З. Баумана, 2003. - 440 с. (Сер. Математика в техническом университете; Вып. XIV).

12. Виленкин Н. Я. Комбинаторика. - М.: Изд. «Наука», 1969. - 328 с.

13. Кривий С. Л. Дискретна математика: Вибр. питання: Навч. посіб. для студ. вищ. навч. закл. -К.: Вид. дім «Києво-Могилянська академія», 2007.-572 с.

14. Кузнецов О. П., Адельсон-Вельский Г. М., Дискретная математика для инженера. М.: Знергоатомиздат, 1988. -476 с.

15. Сигорский В. П., Математический апарат инженера. К.: Техніка, 1977. -768 с.
16. Фудзисава Т., Касами Т., Математика для инженеров. Теория дискретных структур. М.: Радио и связь, 1984. -240 с.
16. Тишин В.В., Дискретная математика в примерах и задачах. СПб .: БХВ-Петербург, 2008. -352 с.