МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
імені В. Н. КАРАЗІНА

ЕЛЕМЕНТИ ТЕОРІЇ ЧИСЕЛ

Навчально-методичний посібник
з елементів алгебри та теорії чисел

Харків – 2024

УДК 51: 511.172
Г 51

Рецензенти:

Ямпольський О. Л. – професор кафедри фундаментальної математики факультету математики і інформатики Харківського національного університету імені В. Н. Каразіна, доктор фізико-математичних наук, професор;

Ігнатович С. Ю. – професор кафедри прикладної математики факультету математики і інформатики Харківського національного університету імені В. Н. Каразіна, доктор фізико-математичних наук, доцент.

Затверджено до друку рішенням Навчально-методичної ради
Харківського національного університету імені В.Н. Каразіна
(протокол № 3 від 19 грудня 2023 року)

Гиря Н. П.

Г 51 Елементи теорії чисел : навчально-методичний посібник з елементів алгебри та теорії чисел / укладачі Н. П. Гиря, О. О. Заварзіна, Є. О. Каролінський, Л. Ю. Полякова. – Харків : ХНУ імені В. Н. Каразіна, 2024. – 48 с.

У виданні розглядаються наступні розділи елементарної теорії чисел: цілі числа, подільність та її властивості, ділення з остачею, найбільший спільний дільник та алгоритм Евкліда, найменше спільне кратне, лінійні діофантові рівняння, прості числа, існування та єдиність розкладання на прості, конгруенції та класи лишків, розв'язання лінійних конгуенцій, китайська теорема про остачі, мала теорема Ферма та теорема Ейлера. Крім того, посібник містить стисле викладення методу математичної індукції та елементів комбінаторики. Посібник буде корисним для студентів математичних спеціальностей при вивченні курсів, що містять ці теми.

УДК 51: 512.642 (512.643, 512.644)

© Харківський національний університет
імені В. Н. Каразіна, 2024
© Гиря Н. П., Заварзіна О. О., Каролінський Є. О.,
Полякова Л. Ю., уклад., 2024
© Дончик І. М., макет обкладинки, 2024

Навчальне видання

Гиря Наталія Петрівна
Заварзіна Олеся Олегівна
Каролінський Євген Олександрович
Полякова Людмила Юріївна

Елементи теорії чисел

Навчально-методичний посібник
з елементів алгебри та теорії чисел

Коректор *Л. Є. Стешенко*
Комп'ютерне верстання авторів
Макет обкладинки *І. М. Дончик*

Формат 60x84/16. Ум. друк. арк. 3,33. Наклад 50 пр. Зам. № 214/23.

Видавець і виготовлювач
Харківський національний університет імені В. Н. Каразіна,
61022, м. Харків, майдан Свободи, 4.
Свідоцтво суб'єкта видавничої справи ДК №3367 від 13.01.2009

Видавництво ХНУ імені В. Н. Каразіна

Зміст

Вступ

Посібник призначений для вивчення елементарної теорії чисел. А саме, розглянуто наступні теми: цілі числа, подільність та її властивості, ділення з остачею, найбільший спільний дільник та алгоритм Евкліда, найменше спільне кратне, лінійні діофантові рівняння, прості числа, існування та єдиність розкладання на прості, конгруенції та класи лишків, розв'язання лінійних конгуенцій, китайська теорема про остачі, мала теорема Ферма та теорема Ейлера. Крім того, посібник містить стисле викладення методу математичної індукції та елементів комбінаторики.

Кожен розділ посібника містить теоретичні відомості з докладними доведеннями всіх необхідних результатів. Далі розглядаються приклади розв'язання «типових» задач. Наприкінці розділів наведена низка задач для самостійного розв'язання.

До посібника включено матеріали, які багато років використовувались при викладанні курсу «Елементи алгебри та теорії чисел» студентам першого курсу факультету математики і інформатики Харківського національного університету імені В.Н. Каразіна.

Автори щиро вдячні Анні Вишняковій, Ірині Ільїнській, Дмитру Селютіну та Нгуєн Тху Хієн, що допомагали в апробації матеріалів посібника, а також Світлані Ігнатович за низку зауважень, що призвели до суттєвого покращення тексту.

Перелік умовних позначень

$\mathbb{N}$ – множина натуральних чисел;
$\mathbb{Z}$ – множина цілих чисел;
$\mathbb{Z}_+$ – множина цілих невід'ємних чисел;
$|A|$ – число елементів скінченної множини A;
$A \times B$ – декартів добуток множин A і B;
$A \cup B$ – об'єднання множин A і B;
$A \cap B$ – перетин множин A і B;
Δ_A – діагональ декартова квадрата $A \times A$;
$n!$ – n-факторіал;
$(n)_k$ – число k-вибірок без повернень з n елементів;
$\binom{n}{k}$ – число k-комбінацій без повернень з n елементів;
$a \mid b$ – a ділить b;
$a \nmid b$ – a не ділить b;
НСД(a, b) – найбільший спільний дільник чисел a і b;
НСК(a, b) – найменше спільне кратне чисел a і b;
$[a]_n$ – клас лишків числа a за модулем n;
$\varphi(n)$ – функція Ейлера;
$\mathbb{Z}(n)$ – множина всіх класів лишків за модулем n.
$\mathbb{Z}(n)^\times$ – множина всіх оборотних класів лишків за модулем n.

1 Метод математичної індукції

Розглянемо множину натуральних чисел $\mathbb{N} = \{1, 2, 3, \ldots\}$. Ми приймаємо без доведення, що у будь-якій непорожній підмножині $A \subset \mathbb{N}$ знайдеться найменше число, тобто $a \in A$ таке, що $a \leq b$ для всіх $b \in A$.

Розглянемо твердження (вислів) $p(n)$, що залежить від натурального числа n. Метод математичної індукції дає техніку доведення того, що $p(n)$ є правильним для всіх $n \in \mathbb{N}$.

Твердження 1.1 (принцип математичної індукції)**.** *Нехай*
(1) $p(1)$ є правильним;
(2) для всіх $n \in \mathbb{N}$, $n > 1$, з $p(n-1)$ випливає $p(n)$.
Тоді $p(n)$ є правильним для всіх $n \in \mathbb{N}$.

Доведення. Нехай це не так. Розглянемо (непорожню!) підмножину A всіх тих натуральних чисел, для котрих $p(n)$ не є правильним. Нехай a – найменше число в A, тобто, зокрема, $p(a)$ не є правильним. Тоді $a > 1$ відповідно до (1). Далі, $p(a-1)$ є правильним за вибором a. Це суперечить (2). □

Умова (1) називається базою індукції, умова (2) – індуктивним переходом.

Зазначимо, що умову (2) можна переформулювати таким чином:
(2') для всіх $n \in \mathbb{N}$ з $p(n)$ випливає $p(n+1)$.

Існують різноманітні варіанти методу математичної індукції. Наприклад, множину $\mathbb{N}$ натуральних чисел можна замінити множиною $\mathbb{Z}_+ = \{0, 1, 2, 3, \ldots\}$ цілих невід'ємних чисел; в цьому випадку базою індукції буде твердження, що $p(0)$ є правильним.

Окрім того, буває, що для перевірки $p(n)$ потрібне не одне твердження $p(n-1)$, а, скажімо, два: $p(n-1)$ і $p(n-2)$. У цьому випадку базою індукції буде перевірка істинності $p(1)$ і $p(2)$; індуктивний перехід – перевірка того, що з $p(n-2)$ і $p(n-1)$ випливає $p(n)$.

Приклад 1.1. Доведіть, що при будь-якому натуральному n виконується рівність

$$1 \cdot 2 + 2 \cdot 3 + \ldots + n(n+1) = \frac{n(n+1)(n+2)}{3}. \tag{1}$$

Розв'язок. Доведемо твердження за допомогою методу математичної індукції.

1. **База індукції.**

   Перевіримо, що твердження справедливе при $n = 1$: ліва частина виразу (1) дорівнює $1 \cdot 2 = 2$, права частина виразу (1) дорівнює $\frac{1 \cdot 2 \cdot 3}{3} = 2$.

2. **Індуктивне припущення.**

   Припустимо, що твердження (1) справедливе при деякому $n = k, k \geq 1$:

$$1 \cdot 2 + 2 \cdot 3 + \ldots + k(k+1) = \frac{k(k+1)(k+2)}{3}. \tag{2}$$

3. **Індуктивний перехід** (крок індукції).

   Доведемо, що твердження (1) справедливе при $n = k + 1$, тобто

$$1 \cdot 2 + 2 \cdot 3 + \ldots + k(k+1) + (k+1)(k+1+1) = \frac{(k+1)(k+1+1)(k+1+2)}{3}$$

   або

$$1 \cdot 2 + 2 \cdot 3 + \ldots + k(k+1) + (k+1)(k+2) = \frac{(k+1)(k+2)(k+3)}{3}. \quad (3)$$

   Розглянемо ліву частину виразу (3):

$$1 \cdot 2 + 2 \cdot 3 + \ldots + k(k+1) + (k+1)(k+2) =$$

$$[\text{застосуємо (2) для перших } k \text{ доданків}]$$

$$= \frac{k(k+1)(k+2)}{3} + (k+1)(k+2) =$$

$$[\text{винесемо за дужки спільні множники } (k+1), (k+2)]$$

$$= (k+1)(k+2)\left(\frac{k}{3} + 1\right) = \frac{(k+1)(k+2)(k+3)}{3},$$

   ми отримали праву частину виразу (3).

Таким чином, з припущення, що формула (1) є правильною при $n = k$, ми вивели, що вона також справедлива при $n = k + 1$.

За принципом математичної індукції формула (1) доведена для всіх натуральних n.

Приклад 1.2. Доведіть, що для кожного натурального n справедлива нерівність $2^n > n$.

Розв'язок. Наведемо доведення за допомогою методу математичної індукції.

1. **База індукції.**

   При $n = 1$ маємо $2^1 > 1$.

2. **Індуктивне припущення.**

   Припустимо, що нерівність є правильною для деякого $n = k, k \geq 1$: $2^k > k$.

3. **Індуктивний перехід.**

   Доведемо, що нерівність є правильною при $n = k+1$, тобто $2^{k+1} > k+1$. Для цього запишемо ліву частину нерівності так: $2^{k+1} = 2 \cdot 2^k$ і, використовуючи індуктивне припущення, отримаємо: $2^{k+1} = 2 \cdot 2^k > 2k \geq k + 1$ при $k \geq 1$.

   Таким чином, нерівність $2^{k+1} > k + 1$ є правильною, а отже, за принципом математичної індукції нерівність $2^n > n$ є правильною для кожного натурального n.

Приклад 1.3. Доведіть, що число 5 є дільником числа $2^{4n-2}+1$ для кожного натурального n.

Розв'язок. Наведемо доведення за допомогою методу математичної індукції.

1. **База індукції.**

   Перевіримо, що твердження є правильним при $n=1$: дійсно, $2^{4\cdot 1-2}+1 = 2^2+1 = 5$ ділиться на 5.

2. **Індуктивне припущення.**

   Припустимо, що твердження справедливе при деякому $n=k, k\geq 1$, тобто число 5 є дільником $2^{4k-2}+1$.

3. **Індуктивний перехід.**

   Доведемо, що твердження справедливе при $n=k+1$, тобто, що число 5 є дільником $2^{4(k+1)-2}+1$. Розглянемо наступний ланцюжок рівностей: $2^{4(k+1)-2}+1 = 2^{4k+4-2}+1 = 2^4\cdot 2^{4k-2}+1 = (16\cdot 2^{4k-2}+16)+(1-16) = 16(2^{4k-2}+1)-15$.

   Число 15 ділиться на 5 і за індуктивним припущенням $2^{4k-2}+1$ ділиться на 5, отже, різниця $16(2^{4k-2}+1)-15$ ділиться на 5. Таким чином, за принципом математичної індукції доведено, що число 5 є дільником $2^{4n-2}+1$ для будь-якого натурального n.

* * *

1.1. Користуючись методом математичної індукції, доведіть для всіх натуральних n:

1) $1+3+5+\ldots+(2n-1)=n^2$; придумайте також геометричне доведення цієї тотожності;

2) $1+2+3+\ldots+n=\dfrac{n(n+1)}{2}$;

3) $1\cdot 4+2\cdot 7+3\cdot 10+\ldots+n(3n+1)=n(n+1)^2$;

4) $1^2+2^2+\ldots+n^2=\dfrac{n(n+1)(2n+1)}{6}$;

5) $1^3+2^3+\ldots+n^3=\dfrac{n^2(n+1)^2}{4}$;

6) $\dfrac{1^2}{1\cdot 3}+\dfrac{2^2}{3\cdot 5}+\ldots+\dfrac{n^2}{(2n-1)(2n+1)}=\dfrac{n(n+1)}{2(2n+1)}$;

7) $\dfrac{1}{2!}+\dfrac{2}{3!}+\ldots+\dfrac{n}{(n+1)!}=1-\dfrac{1}{(n+1)!}$;

8) $1\cdot 1!+2\cdot 2!+\ldots+n\cdot n!=(n+1)!-1$;

9) $\dfrac{1}{1\cdot 2}+\dfrac{1}{2\cdot 3}+\ldots+\dfrac{1}{(n-1)n}=\dfrac{n-1}{n}$;

10) $1^2 + 3^2 + 5^2 + \ldots + (2n-1)^2 = \dfrac{n(2n-1)(2n+1)}{3}$;

11) $1^5 + 2^5 + \ldots + n^5 = \dfrac{1}{12}n^2(n+1)^2(2n^2+2n-1)$;

12) $1^2 - 2^2 + 3^2 - 4^2 + \ldots + (-1)^{n-1}n^2 = \dfrac{n(n+1)}{2}$;

13) $(a_1 + a_2 + \ldots + a_n)^2 = a_1^2 + a_2^2 + \ldots + a_n^2 + 2a_1a_2 + 2a_1a_3 + \ldots + 2a_{n-1}a_n$;

14*) $\sin x + \sin 2x + \ldots + \sin nx = \dfrac{\sin \frac{nx}{2} \sin \frac{n+1}{2}x}{\sin \frac{x}{2}}$;

15*) $\cos x + 2\cos 2x + \ldots + n\cos nx = \dfrac{(n+1)\cos nx - n\cos(n+1)x - 1}{4\sin^2 \frac{x}{2}}$.

1.2. Користуючись методом математичної індукції, доведіть наступні нерівності:

1) $\dfrac{1}{n+1} + \dfrac{1}{n+2} + \ldots + \dfrac{1}{2n} > \dfrac{13}{24}$, $n \geq 2$;

2) $\dfrac{1}{2} \cdot \dfrac{3}{4} \cdot \dfrac{5}{6} \cdot \ldots \cdot \dfrac{2n-1}{2n} < \dfrac{1}{\sqrt{3n+1}}$, $n \geq 2$;

3) $\dfrac{(2n)!}{(n!)^2} > \dfrac{4^n}{n+1}$, $n \geq 2$;

4) $n^{n+1} > (n+1)^n$, $n \geq 3$;

5) $\dfrac{1}{\sqrt{1}} + \dfrac{1}{\sqrt{2}} + \ldots + \dfrac{1}{\sqrt{n}} \geq \sqrt{n}$;

6) $\dfrac{1}{n} + \dfrac{1}{n+1} + \ldots + \dfrac{1}{3n-2} > 1$, $n \geq 2$;

7) $\dfrac{1 \cdot 2 + 2 \cdot 3 + \ldots + n(n+1)}{n(n+3)} \geq \dfrac{n+1}{4}$, $n \geq 2$ (порівняйте з прикладом 1.1);

8) $(1+x)^n \geq 1 + nx$, $x > -1$ (нерівність Бернуллі);

9) $3^n \geq n^3$, $n \in \mathbb{N}$;

10) $2^n \geq 5n - 3$, $n \geq 5$;

11) $1 + \dfrac{1}{2} + \dfrac{1}{4} + \ldots + \dfrac{1}{2^n} < 2$, $n > 1$.

1.3. Доведіть, що нерівність $\sqrt{4 + \sqrt{4 + \ldots + \sqrt{4}}} < 3$ виконується для будь-якої кількості коренів у лівій частині.

1.4. Доведіть за допомогою методу математичної індукції, що при будь-якому натуральному n:

1) $n(2n^2 - 3n + 1)$ ділиться на 6;

2) $11^{n+1} + 12^{2n-1}$ ділиться на 133;

3) $4^n + 15n - 1$ ділиться на 9;

4) $10^n - 9n - 1$ ділиться на 81;

5) $111\ldots1$ (3^n одиниць) ділиться на 3^n;

6) $7^n + 8^{2n-3}$ ділиться на 19 при $n \geq 2$;

7) $5^n + 2 \cdot 3^n + 5$ ділиться на 8;

8) $15^n + 6$ ділиться на 7;

9) $n^3 + 9n^2 + 26n + 24$ ділиться на 6.

10) $5^n - 3^n + 2n$ ділиться на 4.

1.5. Доведіть, що число $\frac{n^4}{24} + \frac{n^3}{4} + \frac{11n^2}{24} + \frac{n}{4}$ є цілим при всіх $n \in \mathbb{N}$.

1.6. Доведіть, що сума кубів трьох послідовних натуральних чисел завжди ділиться на 9.

1.7.* Доведіть, що $1^k + 2^k + \ldots + n^k$ – многочлен від n степеня $k+1$.

1.8.* Доведіть, що якщо число $x + \dfrac{1}{x}$ ціле, то для всіх натуральних n число $x^n + \dfrac{1}{x^n}$ теж ціле.

1.9.* Доведіть, що число $1 + \sqrt{2} + \ldots + \sqrt{n}$ є ірраціональним при $n > 1$.

1.10.* Обчисліть добуток $\dfrac{2^3-1}{2^3+1} \cdot \dfrac{3^3-1}{3^3+1} \cdot \ldots \cdot \dfrac{n^3-1}{n^3+1}$.

1.11. На скільки частин ділять площину n прямих, кожні дві з яких перетинаються й жодні три не проходять через одну точку?

1.12. На скільки частин ділять простір n площин, що проходять через одну точку, якщо жодні три не мають спільної прямої?

1.13. На скільки частин ділять площину n таких кіл, що будь-які два з них перетинаються у парі точок, і жодні три не проходять через одну точку?

1.14.* На яку максимальну кількість частин ділять площину графіки n квадратних тричленів вигляду $y = a_i x^2 + b_i x + c_i$, $i = 1, \ldots, n$?

1.15. Доведіть, що для кожного натурального $n \geq 3$ одиницю можна подати у вигляді суми рівно n різних дробів з чисельником, рівним 1 (тобто знайдуться такі різні натуральні числа $k_1, k_2, \ldots, k_n$, що $1 = \frac{1}{k_1} + \frac{1}{k_2} + \ldots + \frac{1}{k_n}$).

1.16. Доведіть, що для даних натуральних чисел $a_1, a_2, \ldots, a_n$ число

$$(1 + a_1^2)(1 + a_2^2) \cdot \ldots \cdot (1 + a_n^2)$$

можна подати у вигляді суми квадратів двох натуральних чисел.

2 Основні принципи комбінаторики

Комбінаторика – наука про підрахунок числа елементів у скінченних множинах.

Число елементів скінченної множини A позначається $|A|$. Таким чином, «основна задача» комбінаторики може бути сформульована наступним чином: для даної скінченної множини A знайти $|A|$.

Зрозуміло, якщо множина задана явним переліком своїх елементів, то ця задача є тривіальною. Наприклад, якщо $A = \{0, 1, 2, 3\}$, то $|A| = 4$.

Однак на практиці множина може бути задана неявною конструкцією, тобто її елементи будуються з простих «об'єктів» за допомогою деяких правил. Інакше кажучи, з простих «об'єктів» будуються більш складні «комбінації» (звідси термін «комбінаторика»), і вимагається знайти їхню кількість.

Крім того, часто буває необхідно знайти $|A|$ не для однієї множини A, а для сім'ї множин, що залежать від параметра. Наприклад, для сім'ї скінченних множин A_n (що мають «одноманітний» опис), де n – натуральне число, знайти послідовність чисел $a_n = |A_n|$. Ідеалом зазвичай є отримання явної формули для a_n, однак це не завжди можливо, і тоді бажано отримати якомога більше інформації про a_n.

Важливу роль відіграють також алгоритми, що перелічують елементи у неявно заданих скінченних множинах.

Якщо не буде вказано протилежне, то всі множини, що будуть розглядатися далі в цьому розділі, вважаються скінченними.

Ми почнемо з базових прийомів підрахунку числа елементів у скінченних множинах.

Якщо $A \subset B$, то, очевидно, $|A| \leq |B|$.

Якщо $f\colon A \to B$ – бієктивне відображення (тобто взаємно однозначна відповідність), то $|A| = |B|$. Це дає можливість проводити «комбінаторні» доведення формул для числа елементів у множинах: якщо відповідь відома для A, і побудована бієкція з A в B, то відоме й число елементів у B. Більше того, якщо існує алгоритм переліку елементів A і бієкція з A в B задана явно, то отримаємо алгоритм переліку елементів у B.

Якщо $f\colon A \to B$ – ін'єктивне відображення, то $|A| \leq |B|$; якщо ж $f\colon A \to B$ – сюр'єктивне відображення, то $|A| \geq |B|$ (подумайте, чому це справджується).

«Правило додавання». Нехай множини A, B такі, що $A \cap B = \varnothing$. Тоді $|A \cup B| = |A| + |B|$.

Узагальнення: якщо множини $A_1, \ldots, A_n$ такі, що $A_i \cap A_j = \varnothing$ для всіх $i \neq j$, то $|A_1 \cup \ldots \cup A_n| = |A_1| + \ldots + |A_n|$.

Таким чином, якщо множина розбита на частини, що попарно не перетинаються, то число елементів у ній дорівнює сумі чисел елементів частин розбиття.

«Правило доповнення». Якщо $A \subset X$, то $|X \setminus A| = |X| - |A|$. Насправді, $X = A \cup (X \setminus A)$, причому $A \cap (X \setminus A) = \varnothing$, тобто за правилом додавання маємо $|X| = |A| + |X \setminus A|$.

«Правило множення». Нехай множини $A_1, \ldots, A_n$ такі, що $A_i \cap A_j = \varnothing$ для всіх $i \neq j$, причому $|A_i| = m$ для всіх i. Тоді $|A_1 \cup \ldots \cup A_n| = |A_1| + \ldots + |A_n| = mn$.

Зручним є наступне інтуїтивне формулювання цього правила: якщо першу дію можна виконати n способами, а другу дію (незалежно від першої) – m способами, то дві дії у вказаному порядку можна виконати $m \cdot n$ способами.

Зокрема, з цього правила випливає, що $|A \times B| = |A| \cdot |B|$. Насправді, нехай $|A| = m$, $|B| = n$. Запишемо $B = \{b_1, \ldots, b_n\}$. Тоді $A \times B = A_1 \cup \ldots \cup A_n$, де $A_i = \{(a, b_i) \,|\, a \in A\}$. Оскільки, очевидно, $A_i \cap A_j = \varnothing$ для всіх $i \neq j$, причому $|A_i| = m$ для всіх i, то $|A \times B| = mn$.

Правило множення за індукцією поширюється на випадок декартового добутку декількох множин: $|C_1 \times \ldots \times C_N| = |C_1| \cdot \ldots \cdot |C_N|$.

Приклад 2.1. На вершину гори ведуть п'ять доріг.

а) Скількома способами турист може піднятися на гору і спуститися з неї?

б) Те саме запитання, але з умовою підйому і спуску різними дорогами.

Розв'язок. а) Шукане число – це число впорядкованих пар доріг, тобто елементів множини $A \times A$, де A – множина доріг. Оскільки $|A| = 5$, то, за правилом множення, $|A \times A| = 5 \cdot 5 = 25$.

б) З загальної кількості пар доріг потрібно, за правилом доповнення, виключити пари однакових доріг. Інакше кажучи, нас цікавить $|(A \times A) \setminus \Delta_A| = 25 - 5 = 20$.

Приклад 2.2. Скільки існує підмножин у n-елементної множини?

Розв'язок. Зауважимо, що кожен з n елементів множини може або належати, або не належати шуканій підмножині, тобто є 2 можливості для кожного елемента, тобто отримуємо $2 \cdot 2 \ldots \cdot 2 = 2^n$ підмножин n-елементної множини. Зауважимо, що при $n = 0$ відповідь залишається правильною, оскільки у порожньої множини рівно одна підмножина (вона сама).

* * *

2.1. Скількома способами у класі з 27 осіб можна обрати старосту та заступника старости?

2.2. Множина A містить n елементів, а її підмножина B містить k елементів. Скільки існує підмножин $B \subset C \subset A$?

2.3. Скільки існує різних семицифрових номерів телефонів (вважається, що номер починатися з нуля не може)?

2.4. З міста A у місто B ведуть 5 доріг, а з міста B у місто C ведуть 3 дороги. Скількома способами можна дістатися з міста A в місто C? Побудували ще одне місто D і кілька нових доріг: дві з A в D і три з D в C. Скількома способами можна тепер дістатися з A до C?

2.5. Скільки існує п'ятицифрових чисел, які діляться на 5?

2.6. Скільки існує п'ятицифрових чисел, у записах яких є хоча б одна парна цифра?

2.7. Скільки існує п'ятицифрових чисел, які однаково читаються справа наліво та зліва направо?

2.8. Скількома способами можна розкласти 6 монет різної вартості по трьох різних кишенях?

2.9. Скільки існує трицифрових чисел, що містять лише парні цифри? Лише непарні цифри?

2.10. Записують усі трицифрові числа, в записі яких є рівно одна двійка. Скільки таких чисел?

2.11. У мові племені Мумбо-Юмбо 3 голосних і 4 приголосних літери. При складанні слів голосні та приголосні літери неодмінно чергуються. Скільки слів з 8 літер може бути у мові цього племені?

3 Вибірки

Нехай X – множина («генеральна сукупність»), $|X| = n$.

Вибірка з поверненням об'єму k з X – це впорядкований набір $(x_1, \ldots, x_k)$, де $x_i \in X$. Інакше кажучи, така вибірка – це елемент множини $X^k = X \times \ldots \times X$ (декартів добуток k однакових співмножників).

Інтуїтивна інтерпретація: є урна з n різними предметами, з неї по черзі витягують k предметів, при цьому після кожного витягування черговий предмет кладеться назад в урну (і може бути витягнутий знову).

Число таких вибірок, згідно з правилом множення, дорівнює $|X^k| = n^k$.

Множина всіх вибірок з поверненням об'єму k з n-елементної множини X знаходиться у взаємно однозначній відповідності з множиною всіх відображень $f : Y \to X$, де Y – деяка k-елементна множина (наприклад, $Y = \{1, 2, \ldots, k\}$). Справді, задати таку вибірку означає для кожного $i \in Y$ задати $x_i \in X$, тобто задати відображення $f : Y \to X$ формулою $f(i) = x_i$.

Таким чином, якщо $|Y| = k$, $|X| = n$, то число всіх відображень з Y в X дорівнює n^k.

Вибірка без повернення об'єму k з X (або *розміщення* з n по k) — це впорядкований набір $(x_1, \ldots, x_k)$, де всі $x_i \in X$ попарно різні, тобто $x_i \neq x_j$ для всіх $i \neq j$.

Інтуїтивна інтерпретація: є урна з n різними предметами, з неї по черзі витягують k предметів, при цьому після кожного витягування черговий предмет **не** кладеться назад до урни (і **не** може бути витягнутий знову).

Позначимо кількість таких вибірок через $(n)_k$. Є й інше популярне у літературі позначення: A_n^k.

Твердження 3.1. $(n)_k = n(n-1)(n-2)\ldots(n-k+1)$.

Доведення. Зазначимо спочатку, що для $k > n$ очевидно $(n)_k = 0$. Те саме дає і права частина формули, що доводиться. Тому вважатимемо $k \leq n$.

Перший елемент вибірки можна взяти n способами, другий – $n-1$ способом (можна взяти будь-який елемент з X, крім обраного на 1-му кроці), третій – $n-2$ способами, і т. д. Для останнього, тобто k-го, елемента маємо $n-(k-1)$ можливостей. Відповідно до правила множення, отримуємо $(n)_k = n(n-1)(n-2)\ldots(n-(k-1))$. $\square$

Число, що стоїть у правій частині формули для $(n)_k$, іноді називають «n у k-му спадному степені» (бо це добуток k співмножників, починаючи з n, і кожен наступний співмножник на 1 менший за попередній). Зазначимо, що якщо $k \leq n$, то $(n)_k = \frac{n!}{(n-k)!}$.

Множина всіх вибірок без повернення об'єму k з n-елементної множини X перебуває у взаємно однозначній відповідності з множиною всіх ін'єктивних відображень $f : Y \to X$, де Y – деяка k-елементна множина (наприклад, $Y = \{1, 2, \ldots, k\}$). Справді, задати таку вибірку означає для кожного $i \in Y$ задати $x_i \in X$, тобто задати відображення $f : Y \to X$ формулою $f(i) = x_i$. Умова $x_i \neq x_j$ для всіх $i \neq j$ в точності означає ін'єктивність відображення f.

Таким чином, якщо $|Y| = k$, $|X| = n$, то число всіх ін'єктивних відображень з Y в X дорівнює $(n)_k$.

Важливий окремий випадок отримуємо при $k = n$. А саме, *перестановка* n-елементної множини X – це вибірка без повернення об'єму n з X. Таким чином, у такій вибірці кожен елемент бере участь рівно один раз, тобто ми дійсно отримуємо розстановку елементів множини X в деякому порядку.

Число всіх перестановок множини з n елементів, таким чином, дорівнює $(n)_n = n!$.

Зазначимо ще, що множина всіх перестановок n-елементної множини X перебуває у взаємно однозначній відповідності з множиною всіх бієктивних відображень $f : X \to X$ (подумайте, чому). Таким чином, якщо $|X| = |Y| = n$, то число бієктивних відображень з Y в X дорівнює $n!$.

Зауважимо також, що якщо $|X| \neq |Y|$, то бієктивних відображень із Y в X не існує (подумайте, чому).

Приклад 3.1. Скількома способами можна витягнути з колоди в 52 карти чотири карти різних мастей та різних найменувань?

Розв'язок. У колоді в 52 карти чотири масті, у кожній масті $52/4 = 13$ найменувань карт. За умовою потрібно витягнути по одній карті кожної масті з різними найменуваннями. Тобто з 13 найменувань потрібно взяти вибірку без повернення (бо масті різні) обсягу 4. Таким чином, відповіддю буде $(13)_4 = 13 \cdot 12 \cdot 11 \cdot 10 = 17160$.

* * *

3.1. Скількома способами з колоди в 36 карт можна вибрати три карти різних мастей та найменувань?

3.2. Скількома способами з 12 працівників відділу можна вибрати 7 чергових, по одному на кожен день тижня?

3.3. Скільки існує способів розставити 8 тур на шахівниці так, щоб вони не били одна одну?

3.4. Семеро дівчаток водять хоровод. Скількома різними способами вони можуть стати в коло?

3.5. Скільки існує чотирицифрових пін-кодів, що складаються з різних цифр? А якщо цифри можуть повторюватись?

3.6. Скількома способами у спортивній команді з 11 осіб можна вибрати капітана та заступника капітана?

3.7. Скількома способами можна вибрати чотирьох осіб на чотири різні посади, якщо є дев'ять кандидатів на ці посади?

3.8. Анаграмою деякого слова називається довільне слово (необов'язково осмислене), отримане з нього перестановкою літер. Скільки анаграм можна скласти зі слів: а) точка; б) корова; в) коловорот; г) переселення; д) абракадабра; е) комбінаторика?

3.9. Алфавіт племені Мумбо-Юмбо складається з трьох літер. Словом є будь-яка послідовність, що складається не більше ніж з чотирьох літер. Скільки слів у мові племені Мумбо-Юмбо?

3.10. Скільки існує десятицифрових чисел, у записі яких є хоча б дві однакові цифри?

3.11. Яких семицифрових чисел більше: тих, у записі яких є одиниця, чи всіх інших?

3.12. Потрібно надіслати 6 посилок. Скількома способами це можна зробити, якщо для передачі посилки можна запросити трьох кур'єрів і кожну посилку можна дати будь-якому з кур'єрів?

3.13. У кімнаті гуртожитку мешкають чотири студенти. Вони мають 5 чашок, 6 блюдець, 7 чайних ложок, серед яких немає однакових. Скількома способами вони можуть накрити стіл для чаювання, якщо кожен студент отримує одну чашку, одне блюдце та одну ложку?

3.14. З'ясуйте, чи є справедливими наступні твердження:

1) $(n)_k + k(n)_{k-1} = (n+1)_k$;

2) якщо $(n)_k = (n)_l$, то $k = l$;

3) якщо $(n)_k = (m)_k$, то $n = m$.

4 Комбінації та біном Ньютона

Нехай $n, k \in \mathbb{Z}_+$. *Комбінація з n по k* – це підмножина з k елементів у множині з n елементів. Інші назви: *сполука* або *сполучення з n по k*.

Зазначимо, що оскільки комбінація є підмножиною, то, на відміну від вибірки, порядок перерахунку елементів комбінації несуттєвий.

Позначимо через $\binom{n}{k}$ кількість комбінацій з n до k. Інше позначення: C_n^k.

Твердження 4.1. $\binom{n}{k} = \frac{(n)_k}{k!} = \frac{n(n-1)(n-2)\ldots(n-k+1)}{k!}$.

Доведення. Нехай $|X| = n$. Розглянемо множину всіх вибірок без повернення об'єму k із X. З одного боку, кількість таких вибірок дорівнює $(n)_k$. З іншого боку, кожну вибірку можна однозначно одержати за допомогою наступної двокрокової процедури:

1) Вибір підмножини $A \subset X$ з k елементів (тобто комбінації з n по k),

2) Розміщення елементів A у певному порядку.

Число способів виконати перший крок дорівнює $\binom{n}{k}$, другий – $k!$. Звідси за правилом множення отримуємо $(n)_k = \binom{n}{k} \cdot k!$. □

Приклад 4.1. $\binom{n}{0} = 1$, $\binom{n}{1} = n$, $\binom{n}{2} = \frac{n(n-1)}{2}$, $\binom{n}{3} = \frac{n(n-1)(n-2)}{6}$, і т. д.

Очевидно, що $\binom{n}{k} = 0$ при $k > n$. Часто зручно також довизначити числа комбінацій при $k < 0$ і вважати в цьому випадку $\binom{n}{k} = 0$.

Змістовний випадок – це випадок $0 \le k \le n$. У цьому випадку $(n)_k = \frac{n!}{(n-k)!}$ і, отже, $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

Наведемо деякі найпростіші властивості кількості комбінацій.

Твердження 4.2.

1. $\binom{n}{k} = \binom{n}{n-k}$;
2. $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$.

Доведення. Ці формули неважко перевірити, якщо скористатися явними формулами для кількості комбінацій (див. задачу 4.7). Ми, однак, надамо комбінаторне доведення.

1) Рівність очевидна, якщо $k > n$ або $k < 0$. Далі, нехай $0 \le k \le n$. Нехай $|X| = n$. Формула $A \mapsto X \setminus A$ визначає взаємно однозначну відповідність між комбінаціями з n по k і комбінаціями з n по $n-k$, звідки і випливає необхідна рівність.

2) Рівність очевидна, якщо $k \ge n$ або $k \le 0$ (наприклад, $\binom{n}{0} = \binom{n-1}{0} + \binom{n-1}{-1}$, тобто $1 = 1+0$, і т. д.). Далі, нехай $1 \le k \le n-1$. Нехай $|X| = n$, $X = \{x_1, \dots, x_n\}$. Множина всіх комбінацій $A \subset X$ з n по k розбивається на дві підмножини, що не перетинаються: 1) $A \not\ni x_n$, 2) $A \ni x_n$. У першій з них $\binom{n-1}{k}$ елементів, у другій – $\binom{n-1}{k-1}$ елементів, звідки і випливає формула, що доводиться. □

Числа комбінацій можна впорядкувати у так званий *трикутник Паскаля*:

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
. & . & . & . & . & . & . & . & . & . & .
\end{array}$$

Тут у n-му рядку (нумерація рядків починається з 0) стоять числа комбінацій $\binom{n}{k}$, $k = 0, 1, \dots, n$. Кожне з чисел, згідно з другою формулою з твердження 2, є сумою двох чисел, що стоять у попередньому рядку вище та ліворуч і вище та праворуч. Таким чином, ця формула дає просте рекурентне правило обчислення кількості комбінацій.

Твердження 4.3 (формула бінома Ньютона)**.** *Нехай $n \in \mathbb{Z}_+$, x, y – числа. Тоді*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Доведення. Розкриємо дужки у виразі $(x+y)^n = (x+y)(x+y)\dots(x+y)$. Отримаємо суму доданків вигляду $x^k y^{n-k}$, де $0 \le k \le n$. Доданок $x^k y^{n-k}$ повторюється стільки разів, скільки можна вибрати з множини n множників $x+y$ ті k з них, у яких при розкритті дужок був обраний x. Це число, за означенням, дорівнює $\binom{n}{k}$. □

«На честь» того, що числа комбінацій з'являються як коефіцієнти в цій формулі, вони називаються також *біноміальними коефіцієнтами.*

Приклад 4.2. $(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$. При $n=5$ отримуємо $(1+x)^5 = 1 + 5x + 10x^2 + 10x^3 + 5x^4 + x^5$.

Приклад 4.3. Рота складається з 3 офіцерів, 6 сержантів та 60 рядових. Скількома способами можна виділити з них загін, що складається з одного офіцера, двох сержантів і 20 рядових? А якщо в загін повинен увійти командир роти і старший з сержантів?

Розв'язок. 1) Потрібно обрати незалежно один від одного 1 офіцера з 3, 2 сержантів з 6, 20 рядових з 60, тобто число можливих загонів дорівнює $\binom{3}{1}\binom{6}{2}\binom{60}{20} = 3 \cdot 15 \cdot \binom{60}{20}$. 2) За додаткової умови (у загін повинен увійти командир роти і старший з сержантів) залишилося вибрати 1 сержанта з 5 і 20 рядових з 60, тобто відповіддю буде $\binom{5}{1}\binom{60}{20} = 5 \cdot \binom{60}{20}$.

Приклад 4.4. Розв'яжіть рівняння $5\binom{n}{3} = \binom{n+2}{4}$.

Розв'язок. Очевидно, що при $n=0, n=1$ рівність є правильною, а при $n=2$ – ні.

При $n \ge 3$ запишемо рівняння у вигляді:

$$5\frac{n(n-1)(n-2)}{6} = \frac{(n+2)(n+1)n(n-1)}{24}.$$

Після множення на 24 і перенесення праворуч, отримуємо

$$n(n-1)((n+2)(n+1) - 20(n-2)) = 0.$$

Звідси $n(n-1)(n^2 - 17n + 42) = 0$.
Таким чином, $n_1 = 0$, $n_2 = 1$, $n_3 = 3$, $n_4 = 14$.

Приклад 4.5. Обчисліть суму $1 + 3\binom{7}{1} + 3^2\binom{7}{2} + 3^3\binom{7}{3} + \dots + 3^7\binom{7}{7}$.

Розв'язок. Даний вираз – розгорнутий вигляд бінома $(1+3)^7 = 4^7 = 16384$.

* * *

4.1. Скількома способами з 25 студентів можна обрати чотирьох студентів на конференцію профспілки?

4.2. На прямій позначили 6 точок, а на паралельній їй прямій – 7 точок. Учень малює трикутники з вершинами у позначених точках. Скільки трикутників він може намалювати?

4.3. У школі працюють 8 вчителів математики. Директор хоче розділити їх на групи по 4 особи для перевірки контрольної роботи у 10 та 11 класах. Скількома способами він може це зробити?

4.4. У класі 10 дівчат та 11 хлопців. Скількома способами можна скласти команду з 2 дівчат та 3 хлопців для участі у спортивній грі?

4.5. За допомогою бінома Ньютона зведіть вирази до вигляду $a+b\sqrt{n}$, де a, b, n – цілі числа. 1) $(2-\sqrt{3})^4$; 3) $(1-3\sqrt{2})^5$; 2) $(3+\sqrt{3})^5$; 4) $(2-\sqrt{2})^6$.

4.6. З'ясуйте, чи справедливі наступні твердження:

1) якщо $\binom{n}{k}=\binom{n}{l}$, то $k=l$;

2) якщо $\binom{n}{k}=\binom{m}{k}$, то $n=m$.

4.7. Доведіть тотожності

1) правило симетрії $\binom{n}{k}=\binom{n}{n-k}$;

2) правило Паскаля $\binom{n-1}{k-1}+\binom{n-1}{k}=\binom{n}{k}$;

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

4) $\binom{n-1}{k-1}=\frac{k}{n}\binom{n}{k}$;

5) $\binom{n-1}{k-1}\binom{n}{k+1}\binom{n+1}{k}=\binom{n-1}{k}\binom{n+1}{k+1}\binom{n}{k-1}$;

6) $\binom{n}{m}\binom{m}{k}=\binom{n}{k}\binom{n-k}{m-k}$;

7) $\binom{n-s}{k-r}\binom{n}{k+s}\binom{n+r}{k}=\binom{n-s}{k}\binom{n+r}{k+s}\binom{n}{k-r}$.

4.8. Випишіть перші 11 рядків трикутника Паскаля.

4.9. Доведіть формулу бінома Ньютона за допомогою методу математичної індукції:

$$(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k.$$

4.10. У розкладі $(x+y)^n$ за формулою бінома Ньютона другий член дорівнював 240, третій – 720, а четвертий – 1080. Знайдіть x, y, n.

4.11. Розв'яжіть рівняння:

1) $(2n)_3=20(n)_2$;

2) $\binom{n+2}{3}=2\binom{n}{2}+\binom{n+1}{2}$;

3) $5\binom{n+4}{n-1}=3(n+2)_3$;

4) $\binom{n}{3}+\binom{n}{2}=15(n-1)$.

4.12. Обчисліть суми

1) $\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n}$;
2) $\binom{n}{0} - \binom{n}{1} + \ldots + (-1)^n \binom{n}{n}$;
3) $\binom{n}{0} + \binom{n}{2} + \ldots$;
4) $\binom{n}{1} + \binom{n}{3} + \ldots$;
5) $\binom{7}{0} + 2\binom{7}{1} + 4\binom{7}{2} + \ldots + 2^7\binom{7}{7}$;
6) $\binom{6}{0} + 3\binom{6}{1} + 9\binom{6}{2} + \ldots + 3^5\binom{6}{5}$.

4.13. Доведіть, що при будь-яких натуральних n і k сума $\binom{n+k}{2} + \binom{n+k+1}{2}$ є квадратом натурального числа.

4.14. Знайдіть всі такі натуральні n і m, що

$$\binom{n+2}{m} : \binom{n+2}{m+1} : \binom{n+2}{m+2} = 0,6 : 1 : 1.$$

4.15.* При яких значеннях n всі коефіцієнти у розкладі бінома Ньютона $(a+b)^n$ непарні?

4.16.* Доведіть тотожність $\binom{n}{0}^2 + \binom{n}{1}^2 + \ldots + \binom{n}{n}^2 = \binom{2n}{n}$.

4.17.* Обчисліть суми:

1) $\binom{n}{0}\binom{m}{k} + \binom{n}{1}\binom{m}{k-1} + \ldots + \binom{n}{k}\binom{m}{0}$;
2) $\sum\limits_{k=1}^{n} k\binom{n}{k}$.

4.18.* Скільки розв'язків має рівняння $x_1 + x_2 + \ldots + x_k = n$ в натуральних числах? У цілих невід'ємних числах?

5 Подільність цілих чисел

Нехай $\mathbb{Z}$ – множина цілих чисел, $\mathbb{N}$ – її підмножина натуральних чисел. Натуральні числа можна додавати і множити, причому результат цих дій – знову натуральне число. Цілі числа можна додавати, віднімати і множити, і результат цих дій – знову ціле число. Ділення, однак, цієї властивості не має.

Нехай $a, b \in \mathbb{Z}$. Зазначимо, що якщо $ab = 0$, то $a = 0$ або $b = 0$. Інакше кажучи, якщо $ab = 0$ і $a \neq 0$, то $b = 0$. Звідси випливає, що якщо a, b, c – цілі числа, $ac = bc$ і $c \neq 0$, то $a = b$.

Нехай a, b – цілі числа. Говорять, що a *ділить* b (синоніми: b ділиться на a, b кратне a), якщо знайдеться таке ціле число c, що $b = ac$. Позначення: $a \mid b$. Якщо a не ділить b, пишуть $a \nmid b$.

Приклад 5.1. $3 \mid 6$, але $4 \nmid 6$.

Зауважимо, що

1) $a \mid 0$ для будь-якого цілого числа a. Справді, $0 = a \cdot 0$. З іншого боку, $0 \mid a$ тоді і тільки тоді, коли $a = 0$.

2) $1 \mid a$ для будь-якого цілого числа a. Справді, $a = a \cdot 1$. Таку ж властивість «універсального дільника» має і число -1, бо $a = (-a) \cdot (-1)$. Інших таких чисел немає: якщо $a \mid 1$, то $a = 1$ або $a = -1$.

3) Заміна знака числа на протилежний не змінює його властивостей, пов'язаних із подільністю. Справді, якщо $b = ac$, то $-b = a(-c)$, і т. п.

4) Якщо $a \mid b$ і $b \neq 0$, то $|a| \leq |b|$. Справді, $b = ac$, де ціле число $c \neq 0$. Тому $|c| \geq 1$, тобто $|b| \geq |a|$.

Твердження 5.1 (загальні властивості подільності)**.**

1) $a \mid a$ для будь-якого цілого числа a.

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

3) Якщо $a \mid b$, то $a \mid bc$ для будь-якого цілого числа c.

4) Якщо $a \mid b_1$ і $a \mid b_2$, то $a \mid b_1c_1 + b_2c_2$ для будь-яких цілих чисел c_1, c_2.

5) Якщо $a \mid b_1$ і $a \mid b_2$, то $a \mid b_1 + b_2$, $a \mid b_1 - b_2$.

6) Якщо $a_1 \mid b_1$ і $a_2 \mid b_2$, то $a_1a_2 \mid b_1b_2$.

Доведення. Див. задачу 5.1. □

Твердження 5.2.

1) Якщо $ac \mid bc$ і $c \neq 0$, то $a \mid b$.

2) Нехай a, b – цілі числа. Тоді $a \mid b$ і $b \mid a$ у тому і тільки тому випадку, коли $|a| = |b|$, тобто $a = \pm b$.

Доведення. 1) За умовою, $bc = acd$ для деякого цілого числа d. Тоді $(b - ad)c = 0$, і оскільки $c \neq 0$, то $b = ad$, отже, $a \mid b$.

2) Якщо, наприклад, $a = 0$ і при цьому $a \mid b$, то $b = 0$, тобто, зокрема, $|a| = |b|$. Далі, нехай $a \neq 0$ і $b \neq 0$. Якщо $a \mid b$, то $|a| \leq |b|$; якщо $b \mid a$, то $|b| \leq |a|$. Отже, $|a| = |b|$. Навпаки, якщо $|a| = |b|$, то $a = \pm b$, і тоді $a \mid b$, $b \mid a$. □

Твердження 5.3 (ділення з остачею)**.** *Нехай a, b – цілі числа, $b \neq 0$. Тоді існує єдина пара цілих чисел q, r така, що $a = bq + r$, $0 \leq r < |b|$.*

Доведення. Нехай $b > 0$. Розіб'ємо числову пряму на напівінтервали $[bq, b(q + 1))$ довжини b, де $q \in \mathbb{Z}$. Існує єдине ціле число q, для якого число a потрапляє на відповідний напівінтервал, тобто $bq \leq a < b(q + 1)$. Покладемо $r = a - bq$. За побудовою, числа q і r – шукані.

Якщо $b < 0$, то застосуємо твердження до чисел $a, -b$ (оскільки $-b > 0$, цей випадок вже доведено): існує єдина пара цілих чисел $-q$ і r така, що $a = (-q)(-b) + r$, $0 \leq r < -b = |b|$. Тоді числа q і r – шукані. □

Число q називається (неповною) часткою, а число r – остачею при діленні a на b.

Приклад 5.2. 1) Розділимо з остачею 7 на 3. Маємо: $7 = 3 \cdot 2 + 1$, тобто 2 – неповна частка, 1 – остача.

2) Розділимо з остачею -7 на -3. Маємо: $-7 = (-3) \cdot 3 + 2$, тобто 3 – неповна частка, 2 – остача.

Зазначимо, що $b \mid a$ тоді і лише тоді, коли остача від ділення a на b дорівнює 0.

Для ділення з остачею можна використовувати звичайний алгоритм ділення «стовпчиком».

Зауваження 5.1. Для застосування часто буває зручною інша версія ділення з остачею: $a = bq + r$, де $|r| \leq \frac{|b|}{2}$. Зауважимо, однак, що результат такого ділення не завжди єдиний. Наприклад, $5 = 2 \cdot 2 + 1 = 2 \cdot 3 - 1$.

* * *

5.1. Доведіть твердження 5.1.

5.2. Доведіть наступні твердження:
1) якщо $a - c$ ділить $ab + cd$, то $a - c$ ділить і $ad + bc$.
2) якщо $a + c$ ділить $ab + cd$, то $a + c$ ділить і $ad + bc$.
3) якщо $a + b$ ділить $a^2 + ab + b^2$, то $(a + b)^2$ ділить $a^4 + b^4$.

5.3. Розділіть з остачею:

1) 28 на 3;
2) -5 на 3;
3) 143 на 2;
4) 2 на 143;
5) -39 на 8;
6) 30 на 7;
7) -30 на 7;
8) 149 на 5;
9) 5 на 149;
10) -149 на 5;
11) 168 на -35;
12) -168 на 35.

5.4. Остачею при діленні a на b є r, а неповною часткою q. Знайдіть b, q, якщо:
1) $a = 100$, $r = 6$;
2) $a = 148$, $r = 37$.

5.5. Остачею при діленні a на b є r, а неповною часткою q. Знайдіть b, r, якщо:
1) $a = 534$, $q = 26$;
2) $a = 741$, $q = -14$;
3) $a = 109$, $q = 14$;
4) $a = -239$, $q = -15$.

5.6. Доведіть, що для будь-якого натурального n число $n(n+1)(n+2)$ ділиться на 6.

5.7. Доведіть, що сума $2n + 1$ послідовних цілих чисел кратна $2n + 1$. Чи завжди буде кратною $2n$ сума $2n$ послідовних цілих чисел?

5.8. Доведіть, що якщо п'ятицифрове число ділиться на 41, то й усі числа, що отримуються шляхом циклічної перестановки цифр цього числа, діляться на 41.

5.9. Доведіть, що якщо $a > b > 0$, то остача при діленні a на b менша за $\frac{a}{2}$.

5.10. З'ясуйте, які з наступних тверджень справедливі:

1) з восьми цілих чисел завжди можна вибрати два таких, що їхня різниця ділиться на 7;

2) з п'яти цілих чисел завжди можна вибрати два таких, що різниця їхніх квадратів ділиться на 7;

3) зі ста цілих чисел завжди можна вибрати 15 таких чисел, що різниця будь-яких двох із них ділиться на 7.

5.11. Було 8 аркушів паперу. Деякі з них розрізали на 8 шматків кожен. Потім деякі з шматків, що отримали, знову розрізали на 8 шматків і так зробили кілька разів. Чи могло в результаті вийти 5555 шматків?

6 Найбільший спільний дільник

Нехай a, b – цілі числа. Ціле число d називається *найбільшим спільним дільником* чисел a і b, якщо:

1) $d \mid a$, $d \mid b$;

2) якщо ціле число c таке, що $c \mid a$, $c \mid b$, то $c \mid d$.

Таким чином, найбільший спільний дільник чисел a і b – це їхній спільний дільник, кратний усім їхнім спільним дільникам. Інакше кажучи, спільні дільники чисел a і b – це дільники їхнього найбільшого спільного дільника.

Відразу зауважимо, що якщо d_1 і d_2 – два найбільші спільні дільники чисел a і b, то, відповідно до означення, вони діляться один на одного, тобто $d_1 = \pm d_2$. Отже, найбільший спільний дільник визначається однозначно з точністю до знака. Зазвичай найбільший спільний дільник вважають невід'ємним. Якщо d – невід'ємний найбільший дільник чисел a і b, пишуть $d = \text{НСД}(a, b)$. З урахуванням цих домовленостей найбільший спільний дільник єдиний. Зазначимо, що існування найбільшого спільного дільника неочевидне і потребує доведення.

Приклад 6.1. Знайдемо $\text{НСД}(8, 12)$ на основі означення. Додатні дільники числа 8 – це $1, 2, 4, 8$; додатні дільники числа 12 – це $1, 2, 3, 4, 6, 12$. Їхні спільні дільники – це $1, 2, 4$. Оскільки $1 \mid 4$, $2 \mid 4$, $4 \mid 4$, то $\text{НСД}(8, 12) = 4$.

Зауваження 6.1. 1) Відповідно до означення, $\text{НСД}(a, b) = \text{НСД}(b, a)$. Крім того, оскільки дільники числа не змінюються при зміні знака на протилежний, $\text{НСД}(a, b) = \text{НСД}(a, -b)$.

2) Знайдемо $\text{НСД}(a, 0)$. Спільні дільники чисел a і 0 – це дільники a. Таким чином, $\text{НСД}(a, 0) = a$. Зокрема, $\text{НСД}(0, 0) = 0$.

Таким чином, надалі достатньо довести існування та навчитися обчислювати найбільший спільний дільник натуральних чисел.

Вкажемо алгоритм – так званий *алгоритм Евкліда*, – що дозволяє обчислювати найбільший спільний дільник, не шукаючи явно всі дільники чисел. Зокрема, цим буде доведено існування найбільшого спільного дільника.

Лема 6.1. *Нехай a, b – цілі числа, причому $a = bq + r$ для деяких цілих чисел q, r (наприклад, r – остача при діленні a на b). Тоді спільні дільники a і b збігаються зі спільними дільниками b та r.*

Доведення. Див. задачу 1. □

Нехай a, b – натуральні числа, причому $a \geq b$. Покладемо $r_0 = b$. Нехай r_1 – остача від ділення a на b. Якщо $r_1 > 0$, то розглянемо остачу r_2 при діленні $b = r_0$ на r_1. Якщо $r_2 > 0$, то розглянемо остачу r_3 при діленні r_1 на r_2, і т. д. Оскільки $a \geq b > r_1 > r_2 > \ldots \geq 0$, то раніше чи пізніше чергова остача дорівнюватиме 0. Нехай $d = r_n$ – остання остача, що не дорівнює 0.

Теорема 6.2. *1) $d = НСД(a, b)$.*
2) Існують цілі числа u, v такі, що $d = au + bv$.

Доведення. 1) Відповідно до леми 6.1, {спільні дільники a і b} = {спільні дільники b і r_1} = {спільні дільники r_1 і r_2} = $\ldots$ = {спільні дільники r_{n-1} і r_n} = {спільні дільники r_n (тобто d) і 0} = {дільники d}. Таким чином, d – найбільший спільний дільник a та b.

2) Покладемо $r_{-1} = a$. Покажемо, що для кожного $k = -1, 0, 1, 2, \ldots, n$ знайдуться цілі числа u_k і v_k такі, що $r_k = au_k + bv_k$. (Зокрема, при $k = n$ отримаємо таке зображення для $d = r_n$.) Скористаємося індукцією за k. База індукції: $r_{-1} = a = a \cdot 1 + b \cdot 0$, $r_0 = b = a \cdot 0 + b \cdot 1$. Індуктивний перехід: нехай твердження для r_{k-2} і r_{k-1} доведене, тобто $r_{k-2} = au_{k-2} + bv_{k-2}$, $r_{k-1} = au_{k-1} + bv_{k-1}$; доведемо його для r_k. Маємо $r_{k-2} = r_{k-1}q_k + r_k$, де q_k – деяке ціле число. Звідси $r_k = r_{k-2} - r_{k-1}q_k = a(u_{k-2} - u_{k-1}q_k) + b(v_{k-2} - v_{k-1}q_k)$, тобто $u_k = u_{k-2} - u_{k-1}q_k$, $v_k = v_{k-2} - v_{k-1}q_k$. □

Зображення НСД(a, b) у вигляді $au + bv$ називається *лінійним зображенням* найбільшого спільного дільника.

Зауваження 6.2. 1) З доведення теореми 6.2 випливає, що НСД(a, b) = НСД(b, r_1) = НСД(r_1, r_2) = $\ldots$ = НСД$(r_{n-1}, r_n) = d$.

2) У теоремі 6.2 лінійне зображення НСД(a, b) отримано у припущенні, що числа a, b додатні. Проте лінійне зображення існує і для довільних цілих чисел a і b. **(Вправа: чому?)**

Приклад 6.2. Знайдіть НСД$(731, 323)$ та його лінійне зображення.

Розв'язок. Знайдемо НСД за допомогою алгоритму Евкліда. У лівому стовпці записані результати послідовного ділення з остачею, у правому – запис у буквенному вигляді.

$$\begin{array}{ll} 731 = 2 \cdot 323 + 85; & r_{-1} = 2r_0 + r_1; \\ 323 = 3 \cdot 85 + 68; & r_0 = 3r_1 + r_2; \\ 85 = 1 \cdot 68 + 17; & r_1 = r_2 + r_3. \\ 68 = 4 \cdot 17; & \end{array}$$

Числа $r_{-1} = 731$, $r_0 = 323$, $r_1 = 85$, $r_2 = 68$, $r_3 = 17$ – вихідні величини і ненульові остачі, що були отримані у процесі ділення. Остання з них, $r_3 = 17$, є шуканим НСД.

Для знаходження лінійного зображення виразимо у кожному рядку правого стовпця остачу з більшим номером через остачі з меншими номерами:

$$r_3 = r_1 - r_2; \quad r_2 = r_0 - 3r_1; \quad r_1 = r_{-1} - 2r_0.$$

Послідовно підставляючи, маємо

$$\begin{aligned} 17 = r_3 &= r_1 - r_2 = r_1 - (r_0 - 3r_1) = \\ &= 4r_1 - r_0 = 4(r_{-1} - 2r_0) - r_0 = 4r_{-1} - 9r_0. \end{aligned}$$

Отже, $17 = 4 \cdot 731 - 9 \cdot 323$.

* * *

6.1. Доведіть лему 6.1.

6.2. Доведіть, що для натурального c виконується рівність $\text{НСД}(ac, bc) = c\,\text{НСД}(a, b)$.

6.3. Знайдіть за допомогою алгоритму Евкліда $d = \text{НСД}(a, b)$ і такі цілі числа n, m, що $d = na + mb$ (лінійне зображення НСД).

1) $a = 595$, $b = 217$;
2) $a = 614$, $b = 213$;
3) $a = 1147$, $b = 899$;
4) $a = 23521$, $b = 75217$;
5) $a = 315$, $b = 231$;
6) $a = 9877$, $b = 3569$.

6.4. Доведіть, що для $a, b \in \mathbb{Z}$ виконується рівність $\text{НСД}(5a + 3b, 13a + 8b) = \text{НСД}(a, b)$.

6.5. При яких натуральних n дріб є скоротним:

1) $\dfrac{n^2 + 2n + 4}{n^2 + n + 3}$; 2) $\dfrac{n^3 - n^2 - 3n}{n^2 - n + 3}$?

6.6. Нехай a, b – цілі числа, $a \neq b$ і дріб $\frac{a+b}{a-b}$ скоротний. Що можна сказати про скоротність дробу $\frac{a}{b}$?

6.7. Знайдіть натуральні числа x і y, якщо $\frac{x}{y} = \frac{11}{7}$ та $\text{НСД}(x, y) = 45$.

6.8. Знайдіть натуральні числа x і y, якщо $x + y = 180$ та $\text{НСД}(x, y) = 30$.

6.9. Доведіть, що якщо a і b – додатні цілі числа, то кількість членів арифметичної прогресії $a, 2a, 3a, \ldots, ba$, що діляться на b, дорівнює $\text{НСД}(a, b)$.

6.10. У прямокутнику з цілими сторонами m і n, намальованому на клітчастому папері, проведена діагональ. Через яку кількість вузлів вона проходить? На скільки частин ця діагональ ділиться лініями сітки?

6.11.* Знайдіть $\text{НСД}(111\ldots111, 11\ldots11)$, якщо:

1) у першому числі 100 одиниць, а в другому 60 одиниць.
2) у першому числі n одиниць, а в другому m одиниць.

7 Взаємно прості числа

Цілі числа a і b називаються *взаємно простими*, якщо НСД$(a,b)=1$.

Твердження 7.1. *Цілі числа a і b взаємно прості тоді й тільки тоді, коли існують цілі числа u,v такі, що $au+bv=1$.*

Доведення. Нехай a та b взаємно прості. Тоді шукане зображення – це лінійне зображення НСД. Навпаки, якщо $au+bv=1$, і d – спільний дільник a і b, то $d \mid 1$, тобто НСД$(a,b)=1$. □

Наслідок 7.2. *Нехай a, b і c – цілі числа, $a \mid bc$, a і b взаємно прості. Тоді $a \mid c$.*

Доведення. Відповідно до твердження 7.1, знайдуться цілі числа u і v такі, що $au+bv=1$. Тоді число $c=a(uc)+(bc)v$ кратне a. □

* * *

7.1. Доведіть, що якщо натуральні числа a і b взаємно прості, то взаємно простими будуть:

1) a та $a+b$;
2) $a+b$ та $2a+b$;
3) a та $2a+b$.

7.2. Нехай a і b – цілі числа, хоча б одне з яких не дорівнює 0, $d=$ НСД(a,b), $a=da_1$, $b=db_1$ для цілих a_1,b_1. Доведіть, що a_1 та b_1 взаємно прості.

7.3. Нехай a,b,c – натуральні числа. Доведіть, що a і bc взаємно прості тоді й тільки тоді, коли пари a та b, a та c взаємно прості.

7.4. Нехай d ділить числа $ax-by$, $a-b$, причому d і b взаємно прості. Доведіть, що d ділить $x-y$.

7.5. Доведіть, що для будь-якого натурального n дріб є нескоротним.

1) $\dfrac{12n+1}{30n+2}$; 2) $\dfrac{2n^2-1}{n+1}$; 3) $\dfrac{n+7}{2n+13}$; 4) $\dfrac{21n+4}{14n+3}$; 5) $\dfrac{n+1}{2n+1}$.

7.6. Доведіть, що сума $\frac{1}{a}+\frac{1}{a+b}$, де НСД$(a,b)=1$, не може бути скоротним дробом.

7.7. Знайдіть всі взаємно прості числа a та b, для яких $\frac{a+b}{a^2+ab+b^2}=\frac{3}{13}$.

7.8. Нехай $\dfrac{a}{b}=\dfrac{c}{d}$, де a,b,c,d – цілі додатні числа, що задовольняють умови НСД$(a,b)=1$ і НСД$(c,d)=1$. Доведіть, що $a=c, b=d$.

7.9. Доведіть, що з п'яти послідовних цілих чисел завжди можна вибрати одне, взаємно просте з рештою.

7.10. Доведіть, що якщо натуральні числа n і m взаємно прості, то 2^n-1 і 2^m-1 теж взаємно прості.

7.11.* Числа $f_n=2^{2^n}+1$ $(n\geq 0)$ називаються числами Ферма. Доведіть, що кожні два різні числа Ферма взаємно прості.

8 Лінійні діофантові рівняння з двома змінними

Нехай a, b, c – цілі числа. Розглянемо рівняння $ax + by = c$ з *цілими* змінними x та y.

Теорема 8.1. *Рівняння $ax + by = c$ можна розв'язати в цілих числах тоді і тільки тоді, коли НСД$(a, b) \mid c$.*

Доведення. Позначимо $d = \text{НСД}(a, b)$. Оскільки $d \mid a$, $d \mid b$, $d \mid c = ax + by$ для цілих x, y. Навпаки, розглянемо лінійне зображення $d = au + bv$. Оскільки $d \mid c$, $c = dq$ для деякого цілого q, то $c = a(uq) + b(vq)$. □

Отже, якщо рівняння $ax + by = c$ має розв'язок у цілих числах, один з розв'язків можна знайти за допомогою лінійного зображення $\text{НСД}(a, b)$. Як знайти *всі* розв'язки?

Якщо $a = b = c = 0$, то рівняння $ax + by = c$ стає тривіальним, його задовольняють будь-які цілі числа x, y. Далі будемо вважати, що $a \neq 0$ або $b \neq 0$, тобто $d = \text{НСД}(a, b) \neq 0$.

Твердження 8.2. *Нехай $d = НСД(a, b) \mid c$, і x_0, y_0 – один з розв'язків рівняння $ax+by = c$ у цілих числах. Тоді всі цілі розв'язки – це в точності числа $x = x_0 + \frac{b}{d}t$, $y = y_0 - \frac{a}{d}t$, де t – будь-яке ціле число.*

Доведення. Зазначимо, що $ax + by = c$ тоді й тільки тоді, коли $a(x - x_0) + b(y - y_0) = 0$, тобто $\frac{a}{d}(x - x_0) = -\frac{b}{d}(y - y_0)$. Оскільки $\text{НСД}(\frac{a}{d}, \frac{b}{d}) = 1$, то остання умова рівносильна тому, що $\frac{b}{d} \mid (x - x_0)$, $\frac{a}{d} \mid (y - y_0)$, причому $\frac{x-x_0}{b/d} = -\frac{y-y_0}{a/d} = t$, де t – ціле число. □

Зауваження 8.1. Рівняння вигляду $ax + by = 0$ називається *однорідним*. З твердження 8.2 випливає, що його загальний розв'язок має вигляд $x = \frac{b}{d}t$, $y = -\frac{a}{d}t$, де t – будь-яке ціле число. Таким чином, загальний розв'язок рівняння $ax + by = c$ є сумою одного з його розв'язків x_0, y_0 і загального розв'язку відповідного однорідного рівняння $ax + by = 0$.

Приклад 8.1. Розглянемо рівняння $2x + 3y = 1$. Вочевидь, один з його розв'язків – це $x_0 = -1$, $y_0 = 1$. Оскільки $\text{НСД}(2, 3) = 1$, то всі розв'язки рівняння у цілих числах – це $x = -1+3t$, $y = 1-2t$, де t – ціле число. Наприклад, при $t = 1$ виходить розв'язок з найменшим цілим додатним значенням x.

Приклад 8.2. Розв'яжіть у цілих числах рівняння $24x + 66y = 42$.

Розв'язок. Скоротимо обидві частини рівняння на 6 (НСД всіх коефіцієнтів) для того, щоб коефіцієнти при x і y стали взаємно простими числами. Отримаємо рівняння

$$4x + 11y = 7. \tag{4}$$

Знайдемо загальний розв'язок однорідного рівняння

$$4x + 11y = 0. \tag{5}$$

Оскільки x, y – цілі числа, y кратне 4, тобто його можна подати у вигляді $y = 4t$, $t \in \mathbb{Z}$. Підставивши y у рівняння (5), знайдемо, що $x = -11t$.

Знайдемо частковий розв'язок неоднорідного рівняння (4). Знайдемо лінійне зображення НСД$(4, 11) = 1$. Отримати його можна за допомогою алгоритму Евкліда, проте в даному випадку неважко помітити, що $4 \cdot 3 + 11 \cdot (-1) = 1$. Помноживши обидві частини отриманої рівності на 7, отримаємо $4 \cdot 21 + 11 \cdot (-7) = 7$, звідки $x_0 = 21$, $y_0 = -7$ – частковий розв'язок рівняння (4). Отже, загальний розв'язок рівняння (4), а отже, і вихідного рівняння, має вигляд $x = 21 - 11t$, $y = -7 + 4t$, $t \in \mathbb{Z}$.

* * *

8.1. Розв'яжіть у цілих числах рівняння:

1) $45x + 37y = 25$;
2) $6x - 27y = 21$;
3) $19x + 95y = 1995$;
4) $43x + 13y = 21$;
5) $11x + 99y = 41$;
6) $34x + 21y = 1$;
7) $5x - 3y = -1$;
8) $8x + 3y = 2$;
9) $8x + 5y = 49$;
10) $3x - 2y + 11 = 0$;
11) $75x + 39y = 1$.

8.2. У деякій країні в обігу є купюри по 7 або 12 тугриків. Як розплатитися в магазині за товар, вартість якого становить 1) 505 тугриків; 2) 1 тугрик?

8.3. Є 1660 кг піску, який потрібно розсипати по мішках ємністю 40 кг і 60 кг. Як це зробити? Яка найменша кількість мішків може вийти?

9 Найбільший спільний дільник декількох чисел

Нехай $a_1, \ldots, a_n$ – цілі числа. Найбільший спільний дільник чисел $a_1, \ldots, a_n$ визначається аналогічно випадку двох чисел. А саме, ціле число d називається *найбільшим спільним дільником* чисел $a_1, \ldots, a_n$, якщо:

1) $d \mid a_1, \ldots, d \mid a_n$;

2) якщо ціле число c таке, що $c \mid a_1, \ldots, c \mid a_n$, то $c \mid d$.

Так само, як і у випадку двох чисел, найбільший спільний дільник визначений однозначно з точністю до знака. Якщо d – невід'ємний найбільший дільник чисел $a_1, \ldots, a_n$, то пишуть $d =$ НСД$(a_1, \ldots, a_n)$.

Обчислення найбільшого спільного дільника декількох чисел можна звести до послідовного обчислення найбільшого спільного дільника двох чисел.

Лема 9.1. *Спільні дільники чисел $a_1, a_2, a_3, \ldots, a_n$ співпадають зі спільними дільниками чисел НСД$(a_1, a_2), a_3, \ldots, a_n$.*

Доведення. Твердження одразу випливає з того, що спільні дільники a_1 і a_2 – це в точності дільники $\text{НСД}(a_1, a_2)$. □

З леми 9.1 негайно випливає

Наслідок 9.2. *$НСД(a_1, a_2, a_3, \ldots, a_n) = НСД(НСД(a_1, a_2), a_3, \ldots, a_n)$.* □

З наслідка 9.2 за індукцією отримуємо, що $\text{НСД}(a_1, a_2, \ldots, a_n)$ завжди існує. На цей випадок узагальнюється і лінійне зображення найбільшого спільного дільника:

Наслідок 9.3. *Існують цілі числа $u_1, \ldots, u_n$ такі, що*

$$НСД(a_1, \ldots, a_n) = a_1u_1 + \ldots + a_nu_n.$$

Доведення. Застосуємо індукцію за n. База індукції при $n = 2$ доведена раніше. Індуктивний перехід:

$$\begin{aligned}\text{НСД}(a_1, a_2, a_3, \ldots, a_n) = \text{НСД}(\text{НСД}(a_1, a_2), a_3, \ldots, a_n) = \\ \text{НСД}(a_1, a_2)v + a_3u_3 + \ldots + a_nu_n,\end{aligned}$$

$\text{НСД}(a_1, a_2) = a_1w_1 + a_2w_2$, де v, w_1, w_2 – цілі числа, звідки $\text{НСД}(a_1, a_2, a_3, \ldots, a_n) = a_1w_1v + a_2w_2v + a_3u_3 + \ldots + a_nu_n$. Позначаючи $u_1 = w_1v$, $u_2 = w_2v$, отримуємо необхідне зображення. □

Діофантове рівняння $a_1x_1 + \ldots + a_nx_n = c$ можна дослідити так само, як у випадку двох змінних. А саме, рівняння $a_1x_1 + \ldots + a_nx_n = c$ можна розв'язати в цілих числах тоді і тільки тоді, коли $\text{НСД}(a_1, \ldots, a_n) \mid c$. **(Вправа: доведіть.)**

Всі розв'язки цього рівняння можна знайти, наприклад, індуктивним зведенням до випадку двох змінних.

Приклад 9.1. Розв'яжіть у цілих числах рівняння $4x + 2y + 3z = 7$.

Розв'язок. Перенесемо $3z$ у праву частину і розглянемо рівняння $4x+2y = 7-3z$ як рівняння зі змінними x, y та параметром z.

Зауважимо, що $\text{НСД}(4, 2) = 2$, тобто отримане рівняння можна розв'язати тоді і тільки тоді, коли $7-3z = 2u$, або $3z = 7-2u$, де $u \in \mathbb{Z}$. Підставивши та скоротивши на 2, отримаємо $2x + y = u$. Розв'яжемо це рівняння, інтерпретуючи число u як параметр. Неважко бачити, що частковий розв'язок цього рівняння – це $x_0 = 0$, $y_0 = u$. Тому загальний розв'язок має вигляд $x = t$, $y = u - 2t$, де $t \in \mathbb{Z}$.

Тепер розв'яжемо рівняння $3z+2u = 7$. Оскільки $\text{НСД}(3, 2) = 1 \mid 7$, то розв'язки існують. Неважко бачити, що частковий розв'язок цього рівняння – це $z_0 = 1$, $u_0 = 2$. Тому загальний розв'язок має вигляд $z = 1 + 2s$, $u = 2 - 3s$, де $s \in \mathbb{Z}$.

Підставляючи u у формули для x і y, ми отримуємо остаточну відповідь: $x = t$, $y = 2 - 3s - 2t$, $z = 1 + 2s$, де $s, t \in \mathbb{Z}$.

* * *

9.1. Знайдіть за допомогою алгоритму Евкліда:

1) НСД$(962, 1222, 10387)$; 3) НСД$(323, 2240, 2970)$;
2) НСД$(286, 481, 832)$; 4) НСД$(697, 527, 153)$.

9.2. Доведіть, що для непарних чисел a, b, c маємо рівність

$$\text{НСД}\left(\frac{b+c}{2}, \frac{a+c}{2}, \frac{b+a}{2}\right) = \text{НСД}(a, b, c).$$

9.3. Розв'яжіть у цілих числах рівняння:

1) $10x + 3y + 11z = 7$; 4) $10x + 12y + 18z = 7$
2) $5x - 7y + 18z = 1$; 5) $4x + 10y + 15z - 21w = 1$.
3) $23x + 17y + 5z = 2$;

10 Найменше спільне кратне

Нехай $a_1, \ldots, a_n$ – цілі числа. Ціле число m називається *найменшим спільним кратним* чисел $a_1, \ldots, a_n$, якщо:

1) $a_1 \mid m, \ldots, a_n \mid m$;

2) якщо ціле число k таке, що $a_1 \mid k, \ldots, a_n \mid k$, то $m \mid k$.

Легко бачити, що найменше спільне кратне однозначно визначене з точністю до знака. Зазвичай найменше спільне кратне вважають невід'ємним і пишуть $m = \text{НСК}(a_1, \ldots, a_n)$. Зауважимо також, що найменше спільне кратне не залежить від порядку та знаків чисел, що розглядаються.

Зазначимо, що якщо одне з чисел дорівнює 0, то найменше спільне кратне цих чисел існує і дорівнює 0. Далі ми розглянемо випадок, коли всі числа $a_1, \ldots, a_n$ ненульові. Не обмежуючи загальності, можна вважати їх додатними.

Твердження 10.1. *Нехай a, b – натуральні числа. Тоді НСК(a, b) існує, причому НСК$(a, b) = \frac{ab}{\text{НСД}(a,b)}$.*

Доведення. Покладемо $d = \text{НСД}(a, b)$, $m = \frac{ab}{d}$. Вочевидь, m – спільне кратне чисел a і b. Далі, нехай $a \mid k$, $b \mid k$. Покажемо, що $m \mid k$. Запишемо $k = as = bt$ з цілими s, t. Оскільки $\frac{a}{d}s = \frac{b}{d}t$ і $\text{НСД}(\frac{a}{d}, \frac{b}{d}) = 1$, то $\frac{a}{d} \mid t$. Тому число $k = bt = \frac{abt/d}{a/d} = m\frac{t}{a/d}$ кратне m. □

Приклад 10.1. $\text{НСК}(8, 12) = \frac{8 \cdot 12}{\text{НСД}(8,12)} = 24$.

Наслідок 10.2. *Нехай числа a та b взаємно прості. Тоді НСК$(a, b) = ab$. Інакше кажучи, якщо $a \mid k$, $b \mid k$, то $ab \mid k$.* □

Найменше спільне кратне кількох чисел може бути зведене до двох чисел. А саме:

$$\text{НСК}(a_1, a_2, a_3, \ldots, a_n) = \text{НСК}(\text{НСК}(a_1, a_2), a_3, \ldots, a_n).$$

(Вправа: доведіть.)

* * *

10.1. Знайдіть:
1) НСК$(595, 217)$;
2) НСК$(286, 481, 832)$.

10.2. Знайдіть натуральні числа a та b, якщо:
1) НСД$(a, b) = 15$, НСК$(a, b) = 420$;
2) НСД$(a, b) = 5$, НСК$(a, b) = 260$;
3) $a + b = 667$, $\frac{\text{НСК}(a,b)}{\text{НСД}(a,b)} = 120$.

10.3. Доведіть, що $\frac{\text{НСК}(a,b)}{a}$ та $\frac{\text{НСК}(a,b)}{b}$ взаємно прості.

10.4. Доведіть, що якщо $c|a$ і $c|b$, то НСК$(\frac{a}{c}, \frac{b}{c}) = \frac{\text{НСК}(a,b)}{c}$.

10.5. З'ясуйте, за якої умови НСК$(a_1, a_2, \ldots, a_n) = a_1 a_2 \ldots a_n$.

10.6. Доведіть, що для натуральних чисел a, b, c мають місце рівності:
1) $\text{НСК}(a, b, c) = \dfrac{abc \cdot \text{НСД}(a, b, c)}{\text{НСД}(a, b) \cdot \text{НСД}(a, c) \cdot \text{НСД}(b, c)}$;
2) $\text{НСК}(a, b, c) = \dfrac{abc}{\text{НСД}(ab, bc, ac)}$.

11 Прості числа. Основна теорема арифметики

Ціле додатне число p називається *простим*, якщо $p > 1$, і додатні дільники p – це виключно 1 і p.

Приклад 11.1. Числа $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, \ldots$ – прості.

Натуральні числа, більші за одиницю, що не є простими, називаються *складеними*. Інакше кажучи, натуральне число a є складеним, якщо $a > 1$ і $a = bc$, де b, c – натуральні числа, $1 < b < a$, $1 < c < a$.

Твердження 11.1. *Нехай p – просте число. Тоді:*
1) Якщо a – ціле число таке, що $p \nmid a$, то НСД$(a, p) = 1$.
2) Якщо a, b – цілі числа, і $p \mid ab$, то $p \mid a$ або $p \mid b$.

Доведення. 1) Оскільки p просте і $p \nmid a$, то додатні спільні дільники a і p – це лише 1.

2) Нехай, наприклад $p \nmid a$. Тоді НСД$(a, p) = 1$, і залишається застосувати наслідок 7.2. □

За допомогою індукції отримуємо **(Вправа: доведіть)**

Наслідок 11.2. *Нехай p – просте число, $a_1, \ldots, a_n$ – цілі числа такі, що $p \mid a_1 \cdot \ldots \cdot a_n$. Тоді $p \mid a_i$ для деякого $i \in \{1, \ldots, n\}$.* □

Теорема 11.3 («основна теорема арифметики»)**.** *Кожне натуральне число однозначно (з точністю до порядку множників) можна подати у вигляді добутку простих чисел. Точніше, нехай a – натуральне число. Тоді:*

1. Існує ціле невід'ємне число n і прості числа $p_1, \ldots, p_n$ такі, що $a = p_1 \ldots p_n$;

2. Якщо $p_1 \ldots p_n = q_1 \ldots q_m$, де p_i, q_j – прості, то $m = n$, і існує така перестановка $i_1, \ldots, i_n$ чисел $1, \ldots, n$, що $p_k = q_{i_k}$ для всіх $k \in \{1, \ldots, n\}$.

Приклад 11.2. $20 = 2 \cdot 2 \cdot 5 = 2 \cdot 5 \cdot 2 = 5 \cdot 2 \cdot 2$.

Доведення. 1) Нехай це не так. Нехай a – *найменше* натуральне число, яке не є добутком простих. Тоді a – складене, тобто $a = bc$, де b, c – натуральні числа, $1 < b < a$, $1 < c < a$. Отже, числа b і c є добутками простих чисел, а тоді і число a є добутком простих чисел. Отримуємо протиріччя.

2) Нехай $p_1 p_2 \dots p_n = q_1 q_2 \dots q_m$, де для визначеності $n \le m$. Тоді маємо $p_1 \mid q_1 \dots q_m$. Оскільки p_1 просте, то, згідно з наслідком 11.2, $p_1 = q_i$ для деякого $i = i_1$. Змінюючи нумерацію співмножників, ми можемо вважати $p_1 = q_1$. Таким чином, $p_2 \dots p_n = q_2 \dots q_m$. Повторимо те саме міркування для числа p_2 і т. д. Остаточно отримаємо $1 = q_{n+1} \dots q_m$, звідки $m - n = 0$. □

Зауваження 11.1. Єдиність розкладання на прості множники нетривіальна і може порушуватися в близьких ситуаціях. Ось найпростіший із таких прикладів.

Розглянемо множину S чисел виду $4k + 1$, де k – ціле невід'ємне. Легко перевірити, що добуток чисел з S також лежить в S. Будемо говорити, що $a \in S$ не можна розкласти в S, якщо $a > 1$, і дільники a, що належать до S, – це лише 1 і a. Ясно, що якщо $a \in S$, то з простоти числа a випливає, що його не можна розкласти в S; зворотне, однак, неправильно (причина: число вигляду $4k+1$ може бути добутком чисел вигляду $4k + 3$). Наприклад, числа $9, 21, 33, 49, \dots$ не можна розкласти в S, але вони не прості. Кожне число з S розкладається на множники, що не можна розкласти в S (доведення аналогічне випадку розкладання на прості для всіх натуральних чисел), але таке розкладання, взагалі кажучи, не є єдиним: наприклад, $441 = 21 \cdot 21 = 9 \cdot 49$.

Теорема 11.4. *Простих чисел нескінченно багато.*

Доведення. Нехай це не так, і $p_1, \dots, p_n$ – всі прості числа. Розглянемо число $a = p_1 \dots p_n + 1$. Оскільки a не ділиться на жодне з чисел p_k, то a не розкладається на прості множники – протиріччя. □

Нехай a – ціле число, $a \neq 0$. Тоді $a = \pm p_1^{k_1} \dots p_n^{k_n}$, де $p_1, \dots, p_n$ – прості, $k_1, \dots, k_n$ – цілі невід'ємні.

Легко перевірити, використовуючи єдиність розкладання на прості **(Вправа: перевірте)**, що якщо $a = \pm p_1^{k_1} \dots p_n^{k_n}$, $b = \pm p_1^{l_1} \dots p_n^{l_n}$, де p_i – попарно різні прості, k_i, l_i – цілі невід'ємні, то $a \mid b$ тоді й тільки тоді, коли $k_i \le l_i$ для всіх i.

Звідси випливає **(Вправа: перевірте)**, що якщо $a = \pm p_1^{k_1} \dots p_n^{k_n}$, $b = \pm p_1^{l_1} \dots p_n^{l_n}$, де p_i – попарно різні прості, k_i, l_i – цілі невід'ємні, то $\text{НСД}(a, b) = p_1^{s_1} \dots p_n^{s_n}$, $\text{НСК}(a, b) = p_1^{t_1} \dots p_n^{t_n}$, де $s_i = \min(k_i, l_i)$, $t_i = \max(k_i, l_i)$. Цей спосіб обчислення НСД і НСК узагальнюється і на декілька чисел **(Вправа: узагальніть)**.

Приклад 11.3. Оскільки $60 = 2^2 \cdot 3 \cdot 5 = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^0$, $42 = 2 \cdot 3 \cdot 7 = 2^1 \cdot 3^1 \cdot 5^0 \cdot 7^1$, то $\text{НСД}(60, 42) = 2^1 \cdot 3^1 \cdot 5^0 \cdot 7^0 = 6$, $\text{НСК}(60, 42) = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^1 = 420$.

Приклад 11.4. Скільки різних натуральних дільників має число $n = p^3 q^2$ де p, q – прості числа?

Розв'язок. Кожен натуральний дільник числа n має вигляд $p^a q^b$, де a приймає одне зі значень 0, 1, 2, 3, а b – одне зі значень 0, 1, 2. Таким чином, у n всього $4 \cdot 3 = 12$ дільників.

Приклад 11.5. Розв'яжіть у цілих числах рівняння $xy - y + 2x = 7$.

Розв'язок. Розкладемо ліву частину рівняння на множники. Для цього перенесемо з правої частини 2 зі знаком мінус (праворуч залишиться 5) і згрупуємо доданки. Отримаємо $y(x-1) + 2(x-1) = 5$, звідки $(y+2)(x-1) = 5$.

Оскільки x і y – цілі числа, то $x-1$ і $y+2$ теж є цілими числами, добуток яких дорівнює 5. Щоб знайти всі розв'язки вихідного рівняння, розглянемо 4 випадки:

1) якщо $y+2=1$, $x-1=5$, то $x=6, y=-1$;
2) якщо $y+2=5$, $x-1=1$, то $x=2, y=3$;
3) якщо $y+2=-1$, $x-1=-5$, то $x=-4, y=-3$;
4) якщо $y+2=-5$, $x-1=-1$, то $x=0, y=-7$.

* * *

11.1. Розкладіть на прості множники числа:

1) 111; 1111; 11111;
2) 111111; 1111111;
3) 1440; 1575;
4) 3600; 1001; 5681;
5) НСК $(1, 2, \ldots, n)$;
6) $n!$.

11.2. Використовуючи розкладання числа $n!$ на прості множники (задача 11.1. 6)), доведіть, що число $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ є цілим.

11.3. Доведіть, що $\binom{p}{k}$ кратне p, якщо p просте, а $1 \le k \le p-1$.

11.4. Доведіть, що числа Каталана $\frac{1}{n+1}\binom{2n}{n}$, де $n \ge 1$, є цілими.

11.5. Доведіть, що числа вигляду $\frac{(2m)!(2n)!}{m!n!(m+n)!}$, де $n, m \ge 1$, є цілими.

11.6. Знайдіть кількість різних натуральних дільників чисел:

1) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$;
2) $22 \cdot 33 \cdot 55 \cdot 77 \cdot 1111$;
3) $2^3 \cdot 3^2 \cdot 5^{11}$;
4) $11 \cdot 111 \cdot 111111$.

11.7. Скільки різних натуральних дільників має число $n = p_1^{m_1} \ldots p_k^{m_k}$, де $p_1, \ldots, p_k$ – різні прості числа, $m_1, \ldots, m_k > 0$?

11.8. Опишіть усі числа, які мають непарну кількість натуральних дільників.

11.9. Для кожного k від 1 до 6 знайдіть найменше натуральне число, яке має k різних натуральних дільників.

11.10. Знайдіть всі прості числа p і q, для яких

1) $p - q = 17$;
2) $p^2 - 2q^2 = 1$.

11.11. При яких значеннях a всі три числа a, $a+4$ та $a+14$ будуть простими?

11.12. Розв'яжіть у цілих числах рівняння:

1) $xy = 3$;
2) $xy = 6$;
3) $x^2y = 12$;
4) $2xy - 4y + x = 7$;
5) $x^2 - xy - x + y = 1$;
6) $y + x = xy$;
7) $x^2 - 3xy = x - 3y + 2$;
8) $y^2 - 2xy - 2x = 6$.

11.13. Доведіть, що множина простих чисел вигляду
1) $p = 4k + 3$;
2) $p = 6k + 5$
нескінченна.

11.14. Доведіть, що якщо $p \neq 2, 3, 5$ – просте число, таке що $2p + 1$ – просте число, то $4p + 1$ – складене число.

11.15. Доведіть, що остача від ділення простого числа на 30 – це 1 або просте число.

11.16. Доведіть, що для простого числа $p \neq 2, 3, 5$ остача від ділення числа p^2 на 30 – це 1 або 19.

11.17. Доведіть, що складене число n завжди має простий дільник $p \leq \sqrt{n}$.

11.18. Для яких цілих n число $n^4 + 4$ – складене?

11.19. Справедливий ковбой Джо зайшов до бару і попросив у бармена пляшку віскі за 3 долари, пачку Marlboro за долар і 11 центів, шість пачок патронів для свого кольта та дюжину коробок сірників. Почувши підсумкову суму, 28 доларів і 25 центів, Джо пристрелив бармена. За що?

11.20.* Доведіть, що якщо число вигляду $a^n + 1$ просте $(a, n > 1)$, то a – парне і $n = 2^k$. При $a = 2$ виходять прості числа Ферма (див. також завдання 7.11).

11.21.* Доведіть, шо якщо число вигляду $a^n - 1$ просте, то $a = 2$ і n – просте. Прості числа вигляду $2^p - 1$ називаються числами Мерсенна.

11.22. У ребусі різним буквам відповідають різні цифри, знайдіть ці цифри: ЛИК·ЛИК=БУБЛИК.

12 Конгруенції та класи лишків

Зафіксуємо ціле невід'ємне число n. Нехай a, b – цілі числа.

Говорять, що $a \equiv b \mod n$ (читається «a конгруентне b за модулем n»), якщо $n \mid a - b$.

Приклад 12.1. $10 \equiv 4 \mod 3$, $11 \not\equiv 4 \mod 3$.

Відповідно до означення, $a \equiv b \mod 0$ тоді і тільки тоді, коли $a = b$. Далі ми вважатимемо n натуральним числом.

Лема 12.1. *$a \equiv b \mod n$ тоді й лише тоді, коли остачі від ділення a і b на n рівні.*

Доведення. Нехай $a = nq + r$, $b = nq' + r'$, де $0 \le r < n$, $0 \le r' < n$. Тоді $a - b = n(q - q') + (r - r')$, причому $-n < r - r' < n$. Тому $n \mid a - b \Leftrightarrow n \mid r - r' \Leftrightarrow r = r'$. □

З леми негайно випливає, що відношення конгруентності за модулем має властивості, аналогічні властивостям відношення рівності, а саме:

Наслідок 12.2. *1)* (рефлексивність) $a \equiv a \mod n$ *для будь-якого цілого* a*;*
2) (симетричність) *якщо* $a \equiv b \mod n$*, то* $b \equiv a \mod n$*;*
3) (транзитивність) *якщо* $a \equiv b \mod n$ *і* $b \equiv c \mod n$*, то* $a \equiv c \mod n$. □

Нехай a – ціле число. *Клас лишків* числа a за модулем n – це множина $[a]_n = \{b \mid a \equiv b \mod n\}$ всіх чисел, конгруентних a за модулем n.

Зазначимо, що кожен клас лишків за модулем n містить рівно одне число з множини $\{0, 1, 2, \ldots, n-1\}$, а саме, спільну остачу від ділення всіх чисел з класу на n.

Таким чином, $[a]_n = [b]_n$ тоді і тільки тоді, коли $a \equiv b \mod n$ (тобто класи лишків і конгруенції – це дві різні мови для одного й того ж поняття). Множина цілих чисел є об'єднанням класів лишків $[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n$, що попарно не перетинаються.

Нехай $\mathbb{Z}(n)$ – множина всіх класів лишків за модулем n. Ми встановили, що $|\mathbb{Z}(n)| = n$. Остачі від ділення на n є «стандартною» системою представників класів, але фіксувати її раз і назавжди незручно.

Класи лишків є «числоподібними» об'єктами: над ними можна робити арифметичні дії. А саме, визначимо $[a]_n + [b]_n := [a + b]_n$, $[a]_n - [b]_n := [a - b]_n$, $[a]_n \cdot [b]_n := [a \cdot b]_n$.

Приклад 12.2. 1) $[2]_3 + [2]_3 = [4]_3 = [1]_3$, $[2]_4 \cdot [2]_4 = [0]_4$, $[3]_7 \cdot [6]_7 = [4]_7$, і т. п.
2) При вимірюванні часу за допомогою годинника зі стрілками ми рутинно ведемо обчислення з класами лишків за модулем 12.

Твердження 12.3. *Визначення операцій у множині* $\mathbb{Z}(n)$ *коректне.*

Доведення. Нам потрібно довести, що сума (різниця, добуток) класів лишків не залежить від вибору чисел всередині класу. Інакше кажучи, нехай $[a_1]_n = [a_2]_n$, $[b_1]_n = [b_2]_n$. Потрібно довести, що тоді $[a_1 + b_1]_n = [a_2 + b_2]_n$, $[a_1 - b_1]_n = [a_2 - b_2]_n$, $[a_1 \cdot b_1]_n = [a_2 \cdot b_2]_n$. Те ж саме твердження мовою конгруенцій: якщо $a_1 \equiv a_2 \mod n$, $b_1 \equiv b_2 \mod n$, то $a_1 + b_1 \equiv a_2 + b_2 \mod n$, $a_1 - b_1 \equiv a_2 - b_2 \mod n$, $a_1 \cdot b_1 \equiv a_2 \cdot b_2 \mod n$ (тобто конгруенції за модулем можна почленно додавати, віднімати та множити).

Перевіримо це. За умовою числа $a_1 - a_2$ і $b_1 - b_2$ кратні n. Тоді і числа $(a_1 \pm b_1) - (a_2 \pm b_2) = (a_1 - a_2) \pm (b_1 - b_2)$ і $a_1 b_1 - a_2 b_2 = (a_1 - a_2)b_1 + a_2(b_1 - b_2)$ кратні n. □

Зауваження 12.1. Оскільки операції над класами лишків визначаються у термінах операцій над цілими числами, що їх представляють, то алгебраїчні властивості цих операцій зберігаються. Наприклад, $[a]_n + [b]_n = [b]_n + [a]_n$, і т. п.

Приклад 12.3 (ознаки подільності)**.** Доведемо, що ціле число a ділиться на 3 тоді і лише тоді, коли сума цифр числа a у десятковому записі ділиться на 3. Справді, $3 \mid a$ тоді і тільки тоді, коли $a \equiv 0 \mod 3$. Запишемо $a = a_n \cdot 10^n + \ldots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$, де $a_0, a_1, \ldots, a_n$ – цифри числа a, $0 \leq a_k \leq 9$. Зауважимо, що $10 \equiv 1 \mod 3$. Тому $10^k \equiv 1 \mod 3$ для всіх цілих невід'ємних k. Тому $a \equiv a_n + \ldots + a_2 + a_1 + a_0 \mod 3$. Таким чином, $3 \mid a$ тоді і тільки тоді, коли $a_n + \ldots + a_2 + a_1 + a_0 \equiv 0 \mod 3$, тобто $3 \mid a_n + \ldots + a_2 + a_1 + a_0$. Більше того, остачі від ділення на 3 чисел a та суми цифр $a_n + \ldots + a_2 + a_1 + a_0$ збігаються.

Аналогічно можна отримати прості та зручні ознаки подільності на $2, 4, 5, 8, 9, 10, 11$ і (складнішу і менш зручну) ознаку подільності на 7 **(Вправа: зробіть це)**.

Приклад 12.4. Знайдіть остачу від ділення на 7 числа $n = 87 \cdot 29 - 489 \cdot 313$.

Розв'язок. Зауважимо, що $87 \equiv 3 \mod 7$, $29 \equiv 1 \mod 7$, $489 \equiv -1 \mod 7$, $313 \equiv 5 \mod 7$, тому $n \equiv 3 \cdot 1 - (-1) \cdot 5 = 8 \equiv 1 \mod 7$, тобто, n дає остачу 1 при діленні на 7. Це також означає, що $[n]_7 = [1]_7$.

Приклад 12.5. Знайдіть $[2^{100}]_9$.

Розв'язок. Зауважимо, що

$2^0 = 1 \equiv 1 \mod 9$; $2^4 \equiv 7 \mod 9$;
$2^1 \equiv 2 \mod 9$; $2^5 = 2 \cdot 2^4 \equiv 2 \cdot 7 = 14 \equiv 5 \mod 9$;
$2^2 \equiv 4 \mod 9$; $2^6 \equiv 2 \cdot 5 = 10 \equiv 1 \mod 9$;
$2^3 \equiv 8 \mod 9$; $2^7 \equiv 2 \mod 9$.

Отже, остачі при діленні на 9 степенів двійки зациклюються, причому період дорівнює 6. Тоді $2^{100} = 2^{6 \cdot 16 + 4} = (2^6)^{16} \cdot 2^4 \equiv 1^{16} \cdot 7 \equiv 7 \mod 9$, тобто $[2^{100}]_9 = [7]_9$.

* * *

12.1. Чи є правильними наступні конгруенції:

1) $25 \equiv 2 \mod 3$; 4) $32 \equiv -1 \mod 11$;
2) $88 \equiv 0 \mod 6$; 5) $90 \equiv -4 \mod 43$;
3) $-2 \equiv -14 \mod 4$; 6) $1 \equiv -1 \mod 2$?

12.2. Знайдіть у класі лишків $[a]_n$ найменшого за абсолютним значенням та найменшого додатного представника, якщо

1) $a = 103$, $n = 87$;
2) $a = 185$, $n = 16$;
3) $a = 271$, $n = 19$;
4) $a = 484$, $n = 15$.

12.3. Чи утворюють числа $-40, -45, 31, 26, -48, -34$ повну систему представників класів лишків за модулем 6?

12.4. Знайдіть остачу від ділення:

1) $16^{100} - 32^{51} \cdot 8^{49}$ на 3;
2) $37^{n+2} + 16^{n+1} + 23$ на 7 ($n \geq 1$);
3) $2^{1999} + 1$ на 17;
4) $245^{23} - 57^{29} \cdot 7^{17}$ на 4;
5) $(9674^6 + 28)^{15}$ на 39;
6) $2222^{5555} + 5555^{2222}$ на 7.

12.5. Знайдіть останні дві цифри числа
1) 2^{341};
2) 289^{289}.

12.6. Доведіть за допомогою конгруенцій, що
1) для всіх $n \in \mathbb{N}$ число $15^n + 6$ ділиться на 7;
2) для всіх $n \in \mathbb{N}$ число $n^3 + 9n^2 + 26n + 24$ ділиться на 6;
3) для всіх $n \in \mathbb{N}$ число $3^{4n+3} - 17$ ділиться на 10;
4) для всіх $n \in \mathbb{N}$ число $10^n + 17$ ділиться на 3.

12.7. За яких умов на $c, m \in \mathbb{N}$ конгруенції $a \equiv b \mod m$ і $ac \equiv bc \mod m$ рівносильні для всіх $a, b \in \mathbb{Z}$?

12.8. Доведіть, що конгруенції $a \equiv b \mod m$ і $ac \equiv bc \mod mc$ рівносильні, якщо $a, b \in \mathbb{Z}$, $c, m \in \mathbb{N}$.

12.9. Доведіть, що якщо $a - 5b \equiv 0 \mod 19$, то $10a + 7b \equiv 0 \mod 19$.

12.10. Побудуйте таблиці додавання та множення для класів лишків за модулем 1) 3; 2) 5; 3) 4; 4) 6.

12.11. Обчисліть:
1) $[2]_7 \cdot [3]_7 + [4]_7 \cdot [5]_7$;
2) $[2]_9 \cdot [3]_9 + [4]_9 \cdot [5]_9$;
3) $[257]_{19} \cdot [367]_{19} - [79^2]_{19}$;
4) $[2^{100}]_7$.

12.12. Доведіть, що:
1) $20^{15} - 1$ ділиться на $11 \cdot 31 \cdot 61$;
2) $26^{30} - 1$ ділиться на $5 \cdot 7 \cdot 11 \cdot 31$;
3) $26^{15} + 1$ ділиться на $3 \cdot 7 \cdot 31$.

12.13. Складіть список різних остач, які дають числа n^2 при діленні на $3, 4, 5, \ldots, 9$.

12.14. Доведіть, що наступні рівняння не мають розв'язків у цілих числах:
1) $x^2 + y^2 = 2003$;
2) $15x^2 - 7y^2 = 9$;
3) $12x + 5 = y^2$;
4) $x^2 - 5y + 3 = 0$;
5) $-x^2 + 7y^3 + 6 = 0$;
6) $x^2 + y^2 + z^2 = 1999$.

12.15. Для яких k число $2^{2k} - 2^k + 1$ кратне 3?

12.16. Доведіть, що $p^2 - q^2$, де p і q – прості числа, більші за 3, ділиться на 24.

12.17. Доведіть, що сума квадратів п'яти цілих послідовних чисел не може бути повним квадратом.

12.18. Нехай a і b – цілі числа. Доведіть, що:
1) якщо $a^2 + b^2$ кратне 3, то $a^2 + b^2$ кратне 9;
2) якщо $a^2 + b^2$ кратне 21, то $a^2 + b^2$ кратне 441.

12.19. Цілі числа a, b, c такі, що $a^3 + b^3 + c^3$ кратне 7. Доведіть, що abc кратне 7.

12.20. Відомо, що p і $8p^2+1$ — прості. Знайдіть p.

12.21.* Розв'яжіть у натуральних числах рівняння $1!+2!+\cdots+n!=m^2$.

12.22.* *Теорема Вільсона та її обернення:*
1. Якщо p – просте, то $(p-1)!+1$ кратне p.
2. Якщо число $n!+1$ ділиться на $n+1$, то $n+1$ – просте число.

13 Лінійні конгруенції з однією невідомою

Обговоримо питання про ділення у $\mathbb{Z}(n)$: коли рівняння $[a]_n \cdot [x]_n = [b]_n$ має розв'язок, і як знайти всі розв'язки? Інакше кажучи, коли конгруенція $ax \equiv b \mod n$ має розв'язок, і як знайти всі розв'язки (попарно неконгруентні за модулем n)?

Теорема 13.1. *Позначимо $d = НСД(a,n)$. Конгруенція $ax \equiv b \mod n$ має розв'язок тоді і тільки тоді, коли $d \mid b$. При цьому кількість її розв'язків, попарно різних за модулем n, дорівнює d.*

Доведення. Той факт, що конгруенція $ax \equiv b \mod n$ має розв'язок, рівносильний тому, що знайдеться ціле число x таке, що $n \mid b-ax$. Це, в свою чергу, означає, що знайдуться цілі x і y такі, що $ax+ny=b$. За теоремою 8.1 це рівносильно умові $d \mid b$.

Якщо x_0 – один з розв'язків нашої конгруенції, то, за твердженням 8.2, всі розв'язки подаються формулою $x = x_t := x_0 + \frac{n}{d}t$, де t – ціле число. Зауважимо, що розв'язки $x_0, x_1, \ldots, x_{d-1}$ попарно не конгруентні за модулем n. Справді, якщо $0 \le k < l < d$, то $x_l - x_k = n \cdot \frac{l-k}{d}$, тобто $0 < x_l - x_k < n$, звідки $x_l \not\equiv x_k \mod n$. Далі, якщо t – ціле, $t = dq+r$, $0 \le r < d$, то $x_t = x_r + nq$, тобто $x_t \equiv x_r \mod n$. □

Приклад 13.1. Розглянемо лінійну конгруенцію $21x \equiv 15 \mod 6$. Оскільки $НСД(21,6) = 3 \mid 15$, ця конгруенція має розв'язки. Очевидно, що один з її розв'язків – це $x_0 = 1$. Далі всі (попарно неконгруентні за модулем 6) розв'язки подаються формулою $x_t = 1+2t$, де $t = 0,1,2$. Тобто всі розв'язки за модулем 6 – це $x \equiv 1 \mod 6$, $x \equiv 3 \mod 6$, $x \equiv 5 \mod 6$.

Зазначимо, що наша конгруенція еквівалентна конгруенції $7x \equiv 5 \mod 2$. Ця остання конгруенція має єдиний розв'язок за модулем 2. А саме, $x \equiv 1 \mod 2$. Усі три (попарно неконгруентні за модулем 6) розв'язки вихідної конгруенції конгруентні між собою за модулем 2.

Розглянемо важливий окремий випадок: $b = 1$.

Клас лишків $[a]_n$ називається *оборотним* (або обертовним), якщо існує такий клас лишків $[x]_n$, що $[a]_n[x]_n = [1]_n$ (інакше кажучи, конгруенція $ax \equiv 1 \mod n$ має розв'язок). Якщо $[a]_n$ оборотний, то $[x]_n$ такий, що $[a]_n[x]_n = [1]_n$, називається класом лишків, оберненим до $[a]_n$.

Наслідок 13.2. *Клас лишків $[a]_n$ оборотний тоді й тільки тоді, коли $НСД(a,n) = 1$. При цьому клас лишків, обернений до $[a]_n$, єдиний.*

Доведення. Рівняння $[a]_n[x]_n = [1]_n$ має розв'язок тоді і тільки тоді, коли НСД$(a,n) \mid 1$. Остання умова рівносильна тому, що НСД$(a,n) = 1$. При цьому кількість розв'язків цього рівняння дорівнює НСД$(a,n) = 1$. □

Якщо клас лишків $[a]_n$ оборотний, то його єдиний обернений позначається $[a]_n^{-1}$.

Приклад 13.2. $[3]_7^{-1} = [5]_7$, бо $3 \cdot 5 = 15 \equiv 1 \mod 7$.

Позначимо через $\mathbb{Z}(n)^\times$ множину всіх оборотних класів лишків за модулем n. Нехай $\varphi(n) = |\mathbb{Z}(n)^\times|$ – число оборотних класів лишків за модулем n. Інакше кажучи, $\varphi(n)$ – число цілих чисел між 0 і $n-1$, взаємно простих з n. Функція φ натурального аргументу називається *функцією Ейлера*.

Приклад 13.3. 1) $\varphi(1) = 1$.

2) Якщо p – просте число, то $\varphi(p) = p - 1$, оскільки всі цілі числа від 1 до $p-1$ взаємно прості з p. Інакше кажучи, всі ненульові класи лишків по модулю p оборотні.

3) Більш загальним чином, якщо p – просте число, то $\varphi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$. Справді, НСД$(a, p^k) = 1$ тоді і тільки тоді, коли $p \nmid a$; тобто серед цілих чисел від 0 до $p^k - 1$ кожне p-е ділиться на p (і їхні класи лишків за модулем p^k необоротні).

Приклад 13.4. Розв'яжіть лінійну конгруенцію $12x + 5 \equiv 8 \mod 7$.

Розв'язок. Перепишемо конгруенцію у вигляді $12x \equiv 3 \mod 7$. Далі, оскільки $12 \equiv -2 \mod 7$, то конгруенцію можна переписати у вигляді $-2x \equiv 3 \mod 7$.

1-й спосіб. Розв'язання цієї конгруенції, по суті, еквівалентне розв'язанню лінійного діофантового рівняння $-2x + 7y = 3$. Розв'язуючи його, отримуємо $x = 2 + 7n$, $y = 1 + 2n$, де $n \in \mathbb{Z}$. Отже, $x = 2 + 7n$, де $n \in \mathbb{Z}$ – розв'язок вихідної конгруенції.

2-й спосіб. Зауважимо, що $3 \equiv -4 \mod 7$. Запишемо конгруенцію у вигляді $-2x \equiv -4 \mod 7$ і розділимо обидві частини на -2 (остання операція обґрунтовується тим, що клас лишків $[-2]_7$ оборотний, бо НСД$(-2, 7) = 1$). Отримаємо $x \equiv 2 \mod 7$, або $[x]_7 = [2]_7$, або $x = 2 + 7n$, де $n \in \mathbb{Z}$.

Приклад 13.5. Розв'яжіть систему лінійних конгруенцій:

$$\begin{cases} 3x + 4y \equiv 4 \mod 7, \\ 4x + 5y \equiv 3 \mod 7. \end{cases}$$

Розв'язок. Помножимо першу конгруенцію системи на 4, а другу – на 3 (оскільки числа 3 і 4 оборотні за модулем 7, то в результаті розв'язки системи не зміняться):

$$\begin{cases} 12x + 16y \equiv 16 \mod 7, \\ 12x + 15y \equiv 9 \mod 7. \end{cases}$$

Віднімаючи від першої конгруенції другу, отримуємо $y \equiv 0 \mod 7$. Отже, вихідна система еквівалента системі

$$\begin{cases} y \equiv 0 \mod 7, \\ 3x \equiv 4 \mod 7. \end{cases}$$

З другого рівняння знаходимо x і отримуємо розв'язок системи $x \equiv 6 \mod 7$, $y \equiv 0 \mod 7$.

* * *

13.1. Розв'яжіть лінійні конгруенції:

1) $2x + 1 \equiv 0 \mod 13$;
2) $5x \equiv 7 \mod 21$;
3) $10x \equiv 3 \mod 49$;
4) $13x \equiv 21 \mod 29$;
5) $37x \equiv 25 \mod 117$;
6) $6x \equiv 8 \mod 26$;
7) $15x - 12 \equiv 0 \mod 33$;
8) $13x \equiv 1 \mod 27$;
9) $114x \equiv 42 \mod 87$;
10) $39x \equiv 84 \mod 93$;
11) $3x - 5 \equiv 0 \mod 3$.

13.2. Розв'яжіть системи лінійних конгруенцій з двома невідомими:

1) $\begin{cases} x + 2y \equiv 3 \mod 5, \\ 4x + y \equiv 2 \mod 5; \end{cases}$

2) $\begin{cases} 3x - 7y \equiv 1 \mod 11, \\ 6x + 5y \equiv 5 \mod 11; \end{cases}$

3) $\begin{cases} 2x - 10y \equiv 1 \mod 13, \\ 6x - 4y \equiv 3 \mod 13; \end{cases}$

4) $\begin{cases} 2x + 3y \equiv 1 \mod 6, \\ 3x + 2y \equiv 3 \mod 6; \end{cases}$

5) $\begin{cases} 3x + 4y \equiv 29 \mod 143, \\ 2x - 9y \equiv -84 \mod 143. \end{cases}$

6) $\begin{cases} 5x + 2y \equiv 3 \mod 14, \\ 6x + 8y \equiv 5 \mod 14. \end{cases}$

14 Китайська теорема про остачі

Нехай n і d – натуральні числа, $d \mid n$. Визначимо відображення $\mathbb{Z}(n) \to \mathbb{Z}(d)$ формулою $[x]_n \mapsto [x]_d$. Це визначення коректне: якщо $[x]_n = [y]_n$, тобто $x \equiv y \mod n$, то $x \equiv y \mod d$, тобто $[x]_d = [y]_d$. Зазначимо також, що це відображення узгоджується з діями над класами лишків, тобто якщо $[a]_n + [b]_n = [c]_n$, то $[a]_d + [b]_d = [c]_d$, і т. п. Це відображення, очевидно, сюр'єктивне; при $d < n$ воно не ін'єктивне.

Приклад 14.1. Відповідне відображення $\mathbb{Z}(6) \to \mathbb{Z}(2)$ влаштоване так: $[1]_6, [3]_6, [5]_6$ відображаються в $[1]_2$, оскільки $1 \equiv 3 \equiv 5 \mod 2$, а $[0]_6, [2]_6, [4]_6$ відображаються в $[0]_2$, оскільки $0 \equiv 2 \equiv 4 \mod 2$.

Нехай натуральні числа $n_1, \ldots, n_r$ попарно взаємно прості, тобто $\text{НСД}(n_i, n_j) = 1$ при $i \neq j$.

Твердження 14.1. *$НСК(n_1, \ldots, n_r) = n_1 \ldots n_r$.*

Доведення. Зауважимо, що $n_1 \ldots n_r$ – спільне кратне чисел $n_1, \ldots, n_r$. Нехай k – будь-яке спільне кратне чисел $n_1, \ldots, n_r$. Потрібно довести, що $n_1 \ldots n_r \mid k$. Скористаємося індукцією по r. База індукції при $r = 2$ нам відома (див. наслідок 10.2). Зробимо індуктивний перехід від $r - 1$ до r. Отже, нехай $n_1 \ldots n_{r-1} \mid k$, $n_r \mid k$. Зауважимо, що $\text{НСД}(n_1 \ldots n_{r-1}, n_r) = 1$: якщо це не так, то знайдеться

просте число p таке, що $p \mid n_r$, $p \mid n_1 \dots n_{r-1}$. Остання умова означає, що існує $i \in \{1, \dots, r-1\}$ таке, що $p \mid n_i$, що суперечить взаємній простоті чисел n_i і n_r. Отже, $n_1 \dots n_r = \text{НСК}(n_1 \dots n_{r-1}, n_r) \mid k$. □

Тепер покладемо $n = n_1 \dots n_r$ і розглянемо побудовані вище відображення $\mathbb{Z}(n) \to \mathbb{Z}(n_i)$ для всіх i. «Об'єднаємо» їх в одне відображення $f : \mathbb{Z}(n) \to \mathbb{Z}(n_1) \times \dots \times \mathbb{Z}(n_r)$, $f([x]_n) = ([x]_{n_1}, \dots, [x]_{n_r})$. Відображення f узгоджується з діями над класами лишків.

Теорема 14.2 (китайська теорема про остачі)**.** *Відображення f – бієкція.*

Доведення. Перевіримо ін'єктивність відображення f. Нехай $f([x]_n) = f([y]_n)$, тобто $[x]_{n_i} = [y]_{n_i}$ для всіх i, тобто $n_i \mid x - y$ для всіх i. Оскільки, згідно з твердженням 14.1, $\text{НСК}(n_1, \dots, n_r) = n$, то $n \mid x - y$. Це означає, що $[x]_n = [y]_n$.

Далі, $|\mathbb{Z}(n)| = n = n_1 \dots n_r = |\mathbb{Z}(n_1) \times \dots \times \mathbb{Z}(n_r)|$, тому з ін'єктивності відображення f випливає його бієктивність. □

Що означає китайська теорема про остачі? Бієктивність відображення f означає його оборотність, тобто для будь-яких цілих чисел $a_1, \dots, a_r$ існує єдиний клас лишків $[x]_n \in \mathbb{Z}(n)$ такий, що $[x]_{n_i} = [a_i]_{n_i}$ для всіх i. Інакше кажучи, якщо $a_1, \dots, a_r$ – цілі числа, то існує ціле число x, єдине за модулем n, таке, що

$$\begin{cases} x \equiv a_1 \mod n_1, \\ \dots \\ x \equiv a_r \mod n_r. \end{cases} \tag{6}$$

Наше доведення китайської теореми про остачі неконструктивне, і з нього не випливає способу розв'язання такої системи конгруенцій. Як розв'язувати цю систему? Вкажемо один зі способів зробити це.

Нехай $m_i = \frac{n}{n_i} = n_1 \dots n_{i-1} n_{i+1} \dots n_r$. Тоді $\text{НСД}(m_i, n_i) = 1$. Для кожного i обчислимо клас лишків $[m_i]_{n_i}^{-1}$, тобто знайдемо ціле число u_i таке, що $m_i u_i \equiv 1 \mod n_i$. Тоді $x = m_1 u_1 a_1 + \dots + m_r u_r a_r$ є розв'язком системи (6). Справді, оскільки $n_i \mid m_j$ за $i \neq j$, то $m_j u_j a_j \equiv 0 \mod n_i$ за $i \neq j$. Далі $m_i u_i a_i \equiv a_i \mod n_i$. Тому $x \equiv a_i \mod n_i$.

Приклад 14.2. Розглянемо систему конгруенцій

$$\begin{cases} x \equiv 2 \mod 5, \\ x \equiv 1 \mod 7, \\ x \equiv 3 \mod 11. \end{cases}$$

Тут $n_1 = 5$, $n_2 = 7$, $n_3 = 11$, $n = 5 \cdot 7 \cdot 11 = 385$, $m_1 = 7 \cdot 11 = 77$, $m_2 = 5 \cdot 11 = 55$, $m_3 = 5 \cdot 7 = 35$. Далі $77 \equiv 2 \mod 5$ і $2 \cdot 3 \equiv 1 \mod 5$, тобто $u_1 = 3$. Аналогічно $u_2 = -1$, $u_3 = 6$. Таким чином, $x = 77 \cdot 3 \cdot 2 + 55 \cdot (-1) \cdot 1 + 35 \cdot 3 \cdot 6 = 1037 \equiv 267 \mod 385$ – розв'язок системи конгруенцій.

Є й інші способи розв'язання «китайської» системи конгруенцій: наприклад, послідовне розв'язування кожної з конгруенцій з подальшою підстановкою розв'язку в наступну (див. приклад 14.4).

Твердження 14.3. *Нехай $n_1, \ldots, n_r$ – натуральні числа, $n = n_1 \ldots n_r$, a – ціле число. Тоді клас лишків $[a]_n$ оборотний у тому й лише тому випадку, якщо класи лишків $[a]_{n_i}$ оборотні для всіх i.*

Доведення. Якщо клас лишків $[a]_n$ оборотний, то НСД$(a, n) = 1$. Оскільки $n_i \mid n$, тоді НСД$(a, n_i) = 1$, тобто клас лишків $[a]_{n_i}$ оборотний.

Навпаки, нехай класи лишків $[a]_{n_i}$ оборотні для всіх i, тобто НСД$(a, n_i) = 1$ для всіх i. Оскільки $n = n_1 \ldots n_r$, тоді НСД$(a, n) = 1$, тобто клас лишків $[a]_n$ оборотний. □

Наслідок 14.4. *Нехай натуральні числа $n_1, \ldots, n_r$ попарно взаємно прості, $n = n_1 \ldots n_r$. Тоді звуження «китайського» відображення f на $\mathbb{Z}(n)^\times$ є біекцією між $\mathbb{Z}(n)^\times$ і $\mathbb{Z}(n_1)^\times \times \ldots \times \mathbb{Z}(n_r)^\times$.*

Доведення. Оскільки числа $n_1, \ldots, n_r$ попарно взаємно прості, то відображення $f : \mathbb{Z}(n) \to \mathbb{Z}(n_1) \times \ldots \times \mathbb{Z}(n_r)$, $f([x]_n) = ([x]_{n_1}, \ldots, [x]_{n_r})$ є біекцією. Згідно з твердженням 14.3, f переводить $\mathbb{Z}(n)^\times$ в точності у $\mathbb{Z}(n_1)^\times \times \ldots \times \mathbb{Z}(n_r)^\times$. □

Наслідок 14.5. *Нехай натуральні числа $n_1, \ldots, n_r$ попарно взаємно прості, $n = n_1 \ldots n_r$. Тоді $\varphi(n) = \varphi(n_1) \ldots \varphi(n_r)$.*

Доведення.

$$\varphi(n) = |\mathbb{Z}(n)^\times| = |\mathbb{Z}(n_1)^\times \times \ldots \times \mathbb{Z}(n_r)^\times| = |\mathbb{Z}(n_1)^\times| \ldots |\mathbb{Z}(n_r)^\times| = \varphi(n_1) \ldots \varphi(n_r).$$

□

Наслідок 14.6. $\varphi(n) = n(1 - \frac{1}{p_1}) \ldots (1 - \frac{1}{p_r})$, *де $p_1, \ldots, p_r$ – всі (попарно різні) прості дільники числа n.*

Доведення. Нехай $p_1, \ldots, p_r$ – попарно різні прості числа. Тоді $\varphi(p_1^{k_1} \ldots p_r^{k_r}) = \varphi(p_1^{k_1}) \ldots \varphi(p_r^{k_r}) = (p_1^{k_1} - p_1^{k_1 - 1}) \ldots (p_r^{k_r} - p_r^{k_r - 1}) = p_1^{k_1}(1 - \frac{1}{p_1}) \ldots p_r^{k_r}(1 - \frac{1}{p_r}) = p_1^{k_1} \ldots p_r^{k_r}(1 - \frac{1}{p_1}) \ldots (1 - \frac{1}{p_r})$. □

Приклад 14.3. $\varphi(12) = \varphi(4)\varphi(3) = (4 - 2)(3 - 1) = 4$.

Приклад 14.4. Розв'яжіть систему конгруенцій $\begin{cases} x \equiv 3 \mod 5, \\ x \equiv 7 \mod 17. \end{cases}$

Розв'язок. 1-й спосіб. З першого рівняння системи отримуємо $x = 5n + 3$, $n \in \mathbb{Z}$. Підставивши в друге рівняння, маємо $5n + 3 \equiv 7 \mod 17$. Звідси

$$5n \equiv 4 \mod 17.$$

Розв'язуючи цю конгруенцію, маємо $n \equiv 11 \mod 17$, тобто

$$\begin{cases} x = 5n + 3, \\ n = 17k + 11. \end{cases}$$

Звідси $x = 5(17k + 11) + 3 = 85k + 58$, $k \in \mathbb{Z}$.

2-й спосіб. З китайської теореми про остачі випливає, що розв'язок системи слід шукати у вигляді

$$x \equiv m_1 u_1 a_1 + m_2 u_2 a_2 \mod n_1 n_2,$$

де $n_1 = 5$, $n_2 = 17$, $a_1 = 3$, $a_2 = 7$, $m_1 = n_1 n_2 / n_1 = n_2 = 17$, $m_2 = n_1 n_2 / n_2 = n_1 = 5$, а u_i $(i = 1, 2)$ є частковим розв'язком конгруенції $m_i x \equiv 1 \mod n_i$. Розв'язуючи конгруенцію $17x \equiv 1 \mod 5$ і $5x \equiv 1 \mod 17$, знаходимо $u_1 = 3$, $u_2 = 7$, звідки

$$x \equiv 17 \cdot 3 \cdot 3 + 5 \cdot 7 \cdot 7 = 398 \equiv 58 \mod 85.$$

* * *

14.1. Розв'яжіть системи лінійних конгруенцій:

1) $\begin{cases} x \equiv 1 \mod 7, \\ x \equiv 3 \mod 11, \\ x \equiv 2 \mod 13; \end{cases}$

2) $\begin{cases} x \equiv 2 \mod 13, \\ x \equiv 5 \mod 31; \end{cases}$

3) $\begin{cases} x \equiv 2 \mod 3, \\ x \equiv 3 \mod 5, \\ x \equiv 2 \mod 7; \end{cases}$

4) $\begin{cases} x \equiv 2 \mod 10, \\ x \equiv 7 \mod 15; \end{cases}$

5) $\begin{cases} 4x \equiv 3 \mod 7, \\ 5x \equiv 4 \mod 11, \\ 11x \equiv 8 \mod 13; \end{cases}$

6) $\begin{cases} 2x \equiv 1 \mod 10, \\ 3x \equiv 5 \mod 21; \end{cases}$

7) $\begin{cases} x \equiv 4 \mod 5, \\ x \equiv 1 \mod 12, \\ x \equiv 7 \mod 14; \end{cases}$

8) $\begin{cases} x \equiv 2 \mod 10, \\ x \equiv 6 \mod 15. \end{cases}$

14.2. Знайдіть найменше натуральне число, що дає при діленні на 2, 3, 5, 7 остачі:
1) 1, 2, 4, 6 відповідно;
2) 1, 1, 2, 3 відповідно.

14.3. З'ясуйте, при яких значеннях параметра a наступні системи лінійних конгруенцій сумісні, і знайдіть розв'язок.

1) $\begin{cases} x \equiv 2 \mod 6, \\ x \equiv a \mod 8; \end{cases}$

2) $\begin{cases} x \equiv 5 \mod 18, \\ x \equiv 8 \mod 21, \\ x \equiv a \mod 35; \end{cases}$

3) $\begin{cases} x \equiv a \mod 6, \\ x \equiv 1 \mod 8; \end{cases}$

4) $\begin{cases} x \equiv 6 \mod 12, \\ x \equiv 6 \mod 16, \\ x \equiv a \mod 10. \end{cases}$

14.4. З'ясуйте, при яких значеннях параметрів наступні системи лінійних конгруенцій сумісні.

1) $\begin{cases} x \equiv 3 \mod 6, \\ x \equiv 7 \mod n; \end{cases}$

2) $\begin{cases} x \equiv 3 \mod 4, \\ x \equiv 4 \mod m, \\ x \equiv 6 \mod n. \end{cases}$

14.5. Нехай натуральні числа $n_1, \ldots, n_r$ довільні (не обов'язково попарно взаємно прості). За яких умов система конгруенцій $x \equiv a_1 \mod n_1, \ldots, x \equiv a_r \mod n_r$ має розв'язок?

14.6. Знайдіть $\varphi(375)$, $\varphi(720)$, $\varphi(1200)$, $\varphi(1440)$.

14.7. Розв'яжіть рівняння:
1) $\varphi(x) = \frac{4x}{5}$;
2) $\varphi(7^x) = 294$;

14.8. Нехай S – сума всіх цілих чисел від 0 до $n-1$, взаємно простих з n. Доведіть, що якщо $n \geq 2$, то $S = n\varphi(n)/2$.

14.9. Доведіть, що $\sum_{d|n} \varphi(d) = n$.

15 Теорема Ейлера та мала теорема Ферма

Теорема 15.1 (теорема Ейлера). *Нехай n – натуральне число, a – ціле число, $НСД(a, n) = 1$. Тоді $a^{\varphi(n)} \equiv 1 \mod n$.*

Доведення. Покладемо $\alpha = [a]_n \in \mathbb{Z}(n)^\times$. Нехай $m = \varphi(n)$, і $\mathbb{Z}(n)^\times = \{\beta_1, \ldots, \beta_m\}$. Розглянемо відображення $f : \mathbb{Z}(n)^\times \to \mathbb{Z}(n)^\times$, задане формулою $f(x) = \alpha x$. Це відображення – бієкція, бо $f^{-1}(y) = \alpha^{-1} y$. Таким чином, $\alpha\beta_1, \ldots, \alpha\beta_m$ – всі елементи множини $\mathbb{Z}(n)^\times$ без повторень (але, можливо, не в тому ж порядку, що $\beta_1, \ldots, \beta_m$). Тому

$$\beta_1\beta_2 \ldots \beta_m = \alpha\beta_1\alpha\beta_2 \ldots \alpha\beta_m = \alpha^m \beta_1\beta_2 \ldots \beta_m,$$

звідки $\alpha^m = 1$. □

Приклад 15.1. Знайдемо остачу від ділення 5^{2017} на 12. Оскільки $НСД(5, 12) = 1$ і $\varphi(12) = 4$, то $5^4 \equiv 1 \mod 12$, отже, $5^{4k} \equiv 1 \mod 12$. Оскільки $2017 \equiv 1 \mod 4$, то $5^{2017} \equiv 5 \mod 12$.

Важливий окремий випадок теореми Ейлера отримуємо у випадку, коли $n = p$ – просте число.

Наслідок 15.2 (мала теорема Ферма). *Нехай p – просте число, a – ціле число, $p \nmid a$. Тоді $a^{p-1} \equiv 1 \mod p$.*

Доведення. Якщо p просте, то $\varphi(p) = p - 1$. Залишається скористатися теоремою Ейлера. □

Буває корисною і дещо інша версія малої теореми Ферма.

Наслідок 15.3 (мала теорема Ферма). *Нехай p – просте число, a – ціле число. Тоді $a^p \equiv a \mod p$.*

Доведення. Якщо $p \nmid a$, то $a^{p-1} \equiv 1 \mod p$, звідки $a^p \equiv a \mod p$. Якщо $p \mid a$, то $a^p \equiv a \equiv 0 \mod p$. □

* * *

15.1. Знайдіть остачу від ділення:

1) 7^{393} на 13; 3) 4^{2000} на 31;
2) 9^{142} на 71; 4) 9^{378} на 17.

15.2. Доведіть, що:

1) $73^{12} - 1$ ділиться на 105;
2) $52^{60} - 1$ ділиться на 385;
3) $3^{100} - 3^{60} - 3^{40} + 1$ ділиться на 77.

15.3. Доведіть, що:

1) $1^{18} + 2^{18} + 3^{18} + 4^{18} + 5^{18} + 6^{18} \equiv -1 \mod 7$;
2) $1^{100} + 2^{100} + \cdots + 10^{100} \equiv -1 \mod 11$;
3) $1^n + 2^n + 3^n + 4^n$ кратне 5 тоді і тільки тоді, коли n не кратне 4;
4) $1^{19} + 2^{19} + 4^{19} + 5^{19} + 7^{19} + 8^{19} \equiv 0 \mod 9$;
5) $1^{14} + 3^{14} + 7^{14} + 9^{14} \equiv 0 \mod 10$.

15.4. Знайдіть остачу від ділення:

1) 19^{10} на 66; 3) 17^9 на 48;
2) 19^{14} на 70; 4) $14^{14^{14}}$ на 100.

15.5. Нехай $n = 561 = 3 \cdot 11 \cdot 17$. Доведіть, що $a^{n-1} \equiv 1 \mod n$ для всіх цілих чисел a таких, що $\text{НСД}(a, n) = 1$.

15.6. *«Покращена» теорема Ейлера.* Нехай натуральні числа $n_1, \ldots, n_r$ попарно взаємно прості, $n = n_1 \ldots n_r$, $N = \text{НСК}(\varphi(n_1), \ldots, \varphi(n_r))$. Доведіть, що якщо a – ціле число, $\text{НСД}(a, n) = 1$, то $a^N \equiv 1 \mod n$. (Наприклад, якщо $n = 12 = 4 \cdot 3$, то $N = \text{НСК}(\varphi(4), \varphi(3)) = 2$, тобто $5^2 \equiv 1 \mod 12$.)

Відповіді та вказівки

1.7. Вказівка: запишіть різниці $j^{k+1} - (j-1)^{k+1}$ у вигляді суми степенів j і підсумуйте отримані рівності за всіма $1 \leq j \leq n$.

1.10. $\frac{2}{3}(1 + \frac{1}{n(n+1)})$.

1.11. $1 + \frac{n(n+1)}{2}$.

1.13. $n^2 - n + 2$.

1.14. $n^2 + 1$.

2.1. 702.

2.2. 2^{n-k}.

2.3. $9 \cdot 10^6$.

2.4. 15; 21.

2.5. 18000.

2.6. $9 \cdot 10^4 - 5^5$.

2.7. 900.

2.8. 3^6.

2.9. 100; 125.

2.10. 225.

2.11. $2 \cdot 12^4$.

3.1. $(9)_3$.

3.2. $(12)_7$.

3.3. $(8!)^2$.

3.4. 6!.

3.5. $5040; 10^4$.

3.6. 110.

3.7. 3024.

3.8. 120; 360; 15120; $\frac{11!}{4!\cdot 2!}$; $\frac{11!}{5!\cdot 2!\cdot 2!}$; $\frac{13!}{2!\cdot 2!\cdot 2!}$.

3.9. 120.

3.10. $9 \cdot 10^9 - 9 \cdot 9!$.

3.11. З одиницею.

3.12. 3^6.

3.13. $(5)_3 \cdot (6)_3 \cdot (7)_3$.

4.5. 1) $97 - 56\sqrt{3}$; 2) $1188 + 684\sqrt{3}$; 3) $1801 - 1527\sqrt{2}$; 4) $792 - 560\sqrt{2}$.

4.10. $x = 2$, $y = 3$, $n = 5$.

4.11. 1) 3; 2) 5; 3) 5; 4) 9.

4.12. 1) 2^n; 2) 0; 3) 2^{n-1}; 4) 2^{n-1}; 5) 3^7; 6) $4^6 - 3^6$.

4.14. $n = 5$, $m = 2$.

4.15. $n = 2^k - 1$.

4.16. Вказівка: розгляньте кількість способів вибрати n предметів з $2n$ так, що рівно k береться з першої половини, а решта – з другої.

4.17. Вказівка: 1) розгляньте кількість способів вибрати k предметів із двох кошиків – по n і m різних предметів у кожному; 2) продиференціюйте обидві частини рівності $(1 + x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$.

5.3. 2) $-5 = -2 \cdot 3 + 1$; 9) $5 = 0 \cdot 149 + 5$.

5.4. 1) $b = \pm 47$, $q = \pm 2$ або $b = \pm 94$, $q = \pm 1$; 2) $b = \pm 111$, $q = \pm 1$.

5.5. 1) $b = 20$, $r = 14$; 2) $b = -52$, $r = 13$, або $b = -51$, $r = 27$, або $b = -50$, $r = 41$; 3) немає розв'язків; 4) $b = 16$, $r = 1$ або $b = 17$, $r = 16$.

5.8. Вказівка: запишіть п'ятицифрове число у вигляді $10\,000a + 1000b + 100c + 10d + e$, де a, b, c, d, e – цифри вихідного числа.

5.11. Вказівка: при розрізанні одного аркуша кількість шматків збільшується на 7.

6.3. 1) $d = 7$, $n = -4$, $m = 11$; 2) $d = 1$, $n = 17$, $m = -49$; 3) $d = 31$, $n = 11$, $m = -14$; 4) $d = 1$, $n = -7192$, $m = 2249$; 5) $d = 21$, $n = 3$, $m = -4$; 6) $d = 83$, $n = -13$, $m = 36$.

6.5. 1) $n = 3k - 1$; 2) $n = 3k$ або $n = 3k + 1$.

6.8. 150 і 30.

6.10. Проходить через $d+1$ вузол, ділиться на $n+m-d$ частин, де $d = \text{НСД}(n, m)$.

6.11. 1) число з 20 одиниць; 2) число з d одиниць, де $d = \text{НСД}(n, m)$.

7.7. $(1, -4)$, $(-4, 1)$.

7.9. Вказівка: розгляньте, чому може дорівнювати НСД числа та його «сусідів».

7.10. Вказівка: $\text{НСД}(2^m - 1, 2^n - 1) = \text{НСД}(2^{m-n} - 1, 2^n - 1)$ при $m \geq n$.

7.11. Вказівка: доведіть рівність $f_{n+1} = f_0 f_1 \cdots f_n + 2$ та скористайтеся нею.

8.1. 1) $x = 350 - 37n$, $y = -425 + 45n$; 2) $x = -1 + 9n$, $y = -1 + 2n$; 3) $x = 105 - 5n$, $y = n$; 4) $x = -63 + 13n$, $y = 210 - 43n$; 5) немає розв'язків; 6) $x = -8 + 21n$, $y = 13 - 34n$; 7) $x = 1 - 3n$, $y = 2 - 5n$; 8) $x = 1 - 3n$, $y = -2 + 8n$; 9) $x = 98 - 5n$, $y = -147 = 8n$; 10) $x = -11 + 2n$, $y = -11 + 3n$; 11) немає розв'язків.

8.2. 2) $1 = 3 \cdot 12 - 5 \cdot 7$.

8.3. Найменша кількість мішків – 28.

9.1. 1) 13; 2) 13; 3) 1; 4) 17.

9.3. 1) Вказівка: перенесіть до лівої частини доданок, що містить z і розв'яжіть як рівняння з двома невідомими x і y і параметром z. Відповідь: $x = 7 - 11m + 3n$, $y = -21 + 33m - 10n$, $z = m$; 4) немає розв'язків.

10.2. 1) $(15, 420)$, $(60, 105)$, $(420, 15)$, $(105, 60)$; 2) $(5, 260)$, $(20, 65)$, $(260, 5)$, $(65, 5)$; 3) $(232, 435)$, $(115, 552)$, $(435, 232)$, $(552, 115)$.

11.1. 5) НСК $(1, 2, \ldots, n) = \prod_p p^{k_p}$, де p^{k_p} – максимальний степінь простого числа p, що не перевищує n; 6) $n! = \prod_p p^{k_p}$, где $k_p = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots$.

11.3. Вказівка: див. 11.1. 6).

11.7. $(m_1 + 1)(m_2 + 1) \ldots (m_k + 1)$.

11.8. Квадрати натуральних чисел.

11.9. 1; 2; 4; 6; 16; 12.

11.10. 1) $p = 19, q = 2$; 2) $p = 3, q = 2$.

11.11. $a = 3$.

11.12. 4) $(-3, -1)$, $(1, -3)$, $(3, 2)$, $(7, 0)$; 5) $(0, 1)$, $(2, 1)$; 6) $(2, 2)$, $(0, 0)$; 7) $(-1, 0)$, $(2, 0)$; 8) $(-3, -6)$, $(-3, 0)$, $(1, -2)$, $(1, 4)$.

11.13. 1) Вказівка: припустіть, що $p_1(= 3), p_2, \ldots, p_s$ — всі прості числа такого вигляду, і розгляньте $N = 4p_2 \ldots p_s + 3$. Воно не кратне жодному з p_k, але повинно мати простий дільник вигляду $4k + 3$.

11.18. $n \neq \pm 1$. Вказівка: скористайтеся рівністю $n^4 + 4 = n^4 + 4n^2 + 4 - 4n^2$ і розкладіть $n^4 + 4$ на множники.

11.19. Вказівка: підсумкова сума, виражена в центах, має бути кратною 3.

11.20. Вказівка: покажіть, що a не може бути непарним, а потім подайте n у вигляді $n = 2^k m$, де m непарне, і доведіть, що $a^n + 1$ кратне $a^{2^k} + 1$.

11.21. Вказівка: $a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + \ldots + 1)$, звідки $a = 2$. Покажіть, що $2^{km} - 1$ кратне $2^k - 1$.

11.22. ЛИК = 376.

12.4. 1) 0; 2) 1, якщо $n \equiv 0 \mod 3$; 0, якщо $n \equiv 1 \mod 3$; 5, якщо $n \equiv 2 \mod 3$; 3) 10; 4) 2; 5) 14; 6) 0.

12.7. НСД$(c, m) = 1$.

12.11. 1) $[5]_7$; 2) $[-1]_9$; 3) $[13]_{19}$; 4) $[2]_7$.

12.14. Вказівка: розгляньте обидві частини рівняння за модулем 1) 4; 2) 5; 3) 3; 4) 5; 5) 7; 6) 8.

12.15. k непарне.

12.16. Вказівка: розгляньте $p^2 - q^2$ за модулями 3 і 8.

12.17. Вказівка: покажіть, що така сума кратна 5, але не кратна 25.

12.18. Вказівка: 1) доведіть, що a і b кратні 3.

12.19. Вказівка: a^3 за модулем 7 конгруентне 0, 1 або -1.

12.20. Вказівка: доведіть, що $8p^2+1$ кратне 3 при $p \neq 3$.

12.21. $n = m = 1, n = m = 3$. Вказівка: розгляньте обидві частини рівняння за модулем 10.

12.22. Вказівка: 1) розбийте класи лишків від $[2]_p$ до $[p-2]_p$ на пари взаємно обернених; 2) якщо $p < n$ – деякий простий дільник числа n, то $(n-1)! \equiv 0 \mod p$, проте $(n-1)! \equiv -1 \mod p$.

13.1. 1) $x \equiv 6 \mod 13$; 2) $x \equiv 14 \mod 21$; 3) $x \equiv 15 \mod 49$; 4) $x \equiv 15 \mod 29$; 5) $x \equiv 7 \mod 117$; 6) $x \equiv 10 \mod 13$; 7) $x \equiv 3 \mod 11$; 8) $x \equiv 25 \mod 27$; 9) $x \equiv 8 \mod 29$; 10) $x \equiv 26 \mod 31$; 11) немає розв'язків.

13.2. 1) $x \equiv 3, y \equiv 0 \mod 5$; 2) $x \equiv 9, y \equiv 10 \mod 11$; 3) система має 13 розв'язків; 4) $x \equiv 5, y \equiv 3 \mod 6$; 5) $x \equiv 100, y \equiv 111 \mod 143$; 6) система несумісна.

14.1. 1) $x \equiv 652 \mod 1001$; 2) $x \equiv 67 \mod 403$; 3) $x \equiv 23 \mod 105$; 4) $x \equiv 22 \mod 30$; 5) $x \equiv 685 \mod 1001$; 6) немає розв'язків; 7) $x \equiv 49 \mod 420$; 8) немає розв'язків.

14.2. 1) 209; 2) 157.

14.3. 1) a парне; 2) $a \equiv 1 \mod 7$; 3) a непарне; 4) a парне.

14.4. 1) n не кратне 3; 2) m, n – непарні взаємно прості.

Література

[1] Андрійчук В. І., Забавський Б. В. Алгебра і теорія чисел. Львів, 2005.

[2] Завало С. Т. та ін. Алгебра і теорія чисел: практикум. Частина 2. Київ: Вища школа, 1986.

[3] Burton D. Elementary Number Theory, McGraw-Hill, 2005.

[4] Ireland K., Rosen M. A. A Classical Introduction to Modern Number Theory. Springer, 1990.