ПІВДЕННОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ К. Д. УШИНСЬКОГО

ПИВОВАРЧИК В'ЯЧЕСЛАВ МИКОЛАЙОВИЧ, МАРТИНЮК ОЛЬГА МИКОЛАЇВНА

ОСНОВИ ТЕОРІЇ ЧИСЕЛ

Навчально-методичний посібник

Одеса – 2013

ЗМІСТ

ЧАСТИНА 1
Логіка, цілі числа і доведення

1.1. Основні положення теорії доведень і теорії цілих чисел

У даному розділі розглядаються деякі властивості цілих чисел, які будуть корисні в подальшому. Можливо, більш важлива мета – використовувати множину цілих чисел як добре відому предметну область для розвитку і застосування на практиці техніки доведення теорем. Перша проблема – з чого почати. Що можна вважати відомим і, отже, використовувати в доведенні теорем? У загальному курсі з теорії чисел можна було б почати з основних аксіом теорії чисел і розвивати виклад в цьому напрямку. У нашому випадку це не зовсім доцільно. Друга проблема – вирішити, які деталі включати в розгляд. Чи потрібно пояснювати, чому в одному місці доведення маємо $4 + x + 5 = y$, а в іншому – $y = x + 9$?

Якщо звертати увагу на всі несуттєві деталі, то основні моменти доведення загубляться в такому хаосі. Звичайно передбачається, що всі деталі читачеві зрозумілі і в разі необхідності він може сам їх відтворити.

Не існує точних правил, які б говорили, про що треба згадати, а що можна опустити. Витончений виклад доведення теореми – мистецтво. Надалі ми будемо припускати, що більшість аксіом, перелічених в цьому розділі, відомі і можуть використовуватися без грунтовних роз'яснень. Для початку приймемо наступні аксіоми рівності. Вони поширюються на елементи будь-якої множини, у тому числі і множини $\mathbb{Z}$ цілих чисел.

(E1) Для будь-якого a, $a = a$.

(E2) Для будь-якого a і b, якщо $a = b$, то $b = a$.

(E3) Для будь-яких a, b і c, якщо $a = b$ і $b = c$, то $a = c$.

Аксіоми (El), (E2) і (E3) говорять про те, що рівність на будь-якій множині має властивості відношення еквівалентності. Ці аксіоми поширюються на всі математичні форми, а не тільки на теорію чисел. Приймемо також наступні властивості додавання, віднімання та множення на множині $\mathbb{Z}$ цілих чисел.

I1 Якщо a та b — цілі числа, то $a + b$ і $a \cdot b$ — цілі числа, тобто множина цілих чисел замкнена відносно операцій додавання та множення.

I2 Якщо $a = b$ і $c = d$, то $a + c = b + d$ і $ac = bd$.

I3 Для будь-яких цілих чисел a і b справедливі рівності $a + b = b + a$ і $a \cdot b = b \cdot a$, тобто множина цілих чисел комутативна відносно операцій додавання та множення.

I4 Для будь-яких цілих чисел a, b, c справедливі рівності $(a + b) + c = a + (b + c)$ і $(ab)c = a(bc)$, тобто множина цілих чисел асоціативна відносно операцій додавання та множення.

I5 Для будь-яких цілих чисел a, b, c справедливі рівності $a(b + c) = (ab) + (ac)$, тобто множення цілих чисел дистрибутивно відносно додавання.

I6 Існують єдині цілі числа 0 і 1 такі, що $a - 0 = a + 0 = a$, $a \cdot 1 = 1 \cdot a = a$ для довільного цілого числа a. Ціле число 0 називається нейтральним елементом додавання, або нулем множини цілих чисел, ціле число 1 називається нейтральним елементом множення.

I7 Для кожного цілого числа a існує єдине ціле число $-a$, яке називають його оберненим елементом відносно додавання, таке, що $a + (-a) = (-a) + a = 0$.

I8 Якщо b та c — цілі числа і для деякого ненульового числа a маємо $ab = ac$, то $b = c$. Це твердження називається мультиплікативною властивістю скорочення.

Теорема 1.1. *Якщо n – парне, то n^2 також парне.*

Доведення. Допустимо, що n – (довільне) парне ціле число. За означенням парного цілого числа існує ціле число L таке, що

$$n = 2L.$$

Якщо цілі числа рівні, то рівні квадрати цих чисел, так що

$$n^2 = (2L)^2.$$

Але $(2L)^2 = 2L \cdot 2L = 2(2L^2)$, тому $n^2 = 2(2L^2)$ і $n^2 = 2J$ для деякого цілого числа J (а саме $J = 2L^2$). За означенням парного цілого числа n^2 – парне число. □

Теорема 1.2. *Якщо n^2 – парне, то n також парне.*

Доведення. Доведення цієї теореми буде прикладом доведення методом контрапозиції замість прямого доведення самої теореми. ОПИСАТЬ!!!

Цей метод доведення можливий, так як

$$(p \to q) \equiv (\widetilde{q} \to \widetilde{p}).$$

Це означає, що доведення $\widetilde{q} \to \widetilde{p}$ еквівалентно доведенню $p \to q$.

Твердження означає наступне: Якщо n не є парним, то n^2 також не є парним. Нехай n — ціле число, яке не є парним (нагадаємо, что парні цілі числа мають вид $2K$, а непарні цілі числа мають вид $2L+1$, і ціле число є або парним, або непарним, але не може бути і тим, і іншим одночасно). Необхідно показати, що число n^2 – непарне. Оскільки n непарне, існує ціле число L таке, що $n = 2L+1$. Піднесемо в квадрат обидві частини співвідношення, отримаємо

$$n^2 = (2L+1)^2 = 4L^2 + 4L + 1 = 2(2L^2 + 2L) + 1.$$

Так що, якщо

$$J = 2L^2 + 2L,$$

маємо

$$n^2 = 2J + 1.$$

За означення непарного числа, число n^2 непарне, і теорема доведена. □

Доведення наступної теореми залишаємо читачеві.

Теорема 1.3. *Нехай a, b і c — цілі числа.*

1. *Якщо $b + a = c + a$, то $b = c$.*
2. *Для довільного цілого числа a має місце рівність $a \cdot 0 = 0$.*
3. *Для довільного цілого числа a має місце рівність $-(-a) = a$.*
4. $a \cdot (-b) = -(a \cdot b)$.
5. $(-a) \cdot (-b) = a \cdot b$.
6. $-(a + b) = (-a) + (-b)$.

Множина цілих чисел $\mathbb{Z}$ містить підмножину $\mathbb{N}$ додатних цілих чисел. Останню прийнято називать множиною натуральних чисел $\mathbb{N}$. Приймемо в якості аксіом наступні твердження відносно множини $\mathbb{N}$.

N1 Ціле число 1 є натуральним числом.

N2 Множина натуральних чисел замкнена відносно додавання і множення, тобто якщо a, b – натуральні числа, то $a + b$, $a \cdot b$ – натуральні числа.

N3(Аксіоми трихотомії) Для кожного цілого числа a істинним є одне і лише одне з перелічених нижче тверджень

a) a – натуральне число;

b) $a = 0$;

c) $-a$ – натуральне число.

Далі наведемо часткове (ПРОВЕРИТЬ!) впорядкування цілих чисел, в якому цілі числа розташовані за принципом "більше за меншим". Звичайно цілі числа "впорядковані"таким чином:

$$..., -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, ...,$$

де всі додатні числа "йдуть за"нулем, а нуль "йде за"або "більше, ніж"будь-яке від'ємне число. Трихотомія дозволяє встановити, чи є число додатнім, тому відношення $>$ на множині $\mathbb{Z} \times \mathbb{Z}$ можна визначити так: $a > b$ тоді і тільки тоді, коли $a - b$ – додатнє. В силу трихотомії, $a - b$ або додатнє, або нуль, або від'ємне. Тому можна об'єднати дві з цих можливостей в одну і казати, що $a \geq b$ тоді і тільки тоді, коли $a > b$ або $a = b$. Сказане вище формалізуємо у вигляді такого означення.

Означення 1.1. Для цілих чисел a і b маємо: $a > b$ тоді і тільки тоді, коли $a - b$ додатнє; $a \geq b$ тоді і тільки тоді, коли $a > b$ або $a = b$. Крім того, $b < a$ рівносильно $a > b$ і $b \leq a$ рівносильно $a \geq b$.

Вочевидь, $a > 0$ рівносильно твердженню, що a – додатнє, тому що $a > 0$ тоді і тільки тоді, коли $a - 0 = a$ додатнє. Аналогічно, $a < 0$ рівносильне твердженню, що a – від'ємне. Хоча наведені нижче твердження добре відомі й можуть розглядатися як припущння, вони наведені для практики доведення теорем.

Теорема 1.4. *Для цілих чисел a і b: (СЛОВАМИ)*

a) $(a \geq b) \to (b > a) \Rightarrow a = b$;

b) $(a \geq b) \to (b > c) \Rightarrow a > c$;

Доведення. **a)** Тут ми використаємо принцип зведення до абсурду. Якщо, допустивши, що твердження в частині (a) є хибним, ми отримаємо протиріччя, то истинність цього твердження будет доведена. Допустимо, що твердження в частині (a) є хибним. Тоді, якщо $a \geq b$, $b \geq a$ і $a \neq b$, то $a > b$ і $b > a$. Але в цьому випадку $a - b$ додатнє і $b - a = -(a - b)$ додатнє, що суперечить аксіомі трихотомії $N3$. Так як ми прийшли до протиріччя, повинен мати місце випадок $a = b$.

b) Якщо $a > b$ і $b > c$, то $(a - b)$ і $(b - c)$ додатнє. Тому згідно з аксіомою $N2$ число $(a - b) + (b - c) = a - c$ додатнє, і $a > c$.

□

Теорема 1.5. *Нехай a, b, c, d – цілі числа. Тоді (СЛОВАМИ)*

a) $(a > b) \wedge (c > d) \Rightarrow a + c > b + d$;

b) $(a > 0) \wedge (c > d) \Rightarrow ac > ad$;

c) $(a > b > 0) \wedge (c > d > 0) \Rightarrow ac > bd$;

d) $(a \geq b \geq 0) \wedge (c \geq d \geq 0) \Rightarrow ac \geq bd$;

Доведення. **a)** Якщо $(a > b)$ і $(c > d)$, то числа $a - b$, $c - d$ – додатні. Тому, $(a - b) + (c - d)$ додатнє. Але $(a - b) + (c - d) = (a + c) - (b + d)$, і тому $a + c > b + d$;

b) Якщо $c > d$, то різниця $c - d$ додатня. Оскільки a додатнє, $a(c - d) = ac - ad$ також додатнє, і $ac > ad$.

c) Якщо $a > b > 0$ і $c > d > 0$, то $ac > bc$. Тому ac > bd.

d) Самостійно.

□

Далі ілюструємо застосування доведення перебором.

Теорема 1.6. *Нехай n – ціле число. Тоді $n^2 \geq 0$.*

Доведення. Так як n — ціле число, то згідно з аксіомою трихотомії воно або натуральне, або від'ємне, або дорівнює 0. Якщо n натуральне, то $n * n$ натуральне за аксіомою $N2$, і $n^2 \geq 0$. Якщо n від'ємне, то $n = -m$ для деякого натурального числа m. Тому $n^2 = (-m)(-m) = m^2$ знову є натуральним, і $n^2 \geq 0$. Якщо $n = 0$, то $n^2 = 0$, так що $n^2 \geq 0$. Тому, $n^2 \geq 0$. □

Вправи

1 Нехай a, b і c — цілі числа. Доведіть, що

a) якщо $b + a = c + a$, то $b = c$;

b) $a \cdot 0 = 0$ для довільного цілого числа a;

c) $-(-a) = a$ для довільного цілого числа a;

d) $a \cdot (-b) = -(a \cdot b)$;

e) $-a \cdot (-b) = a \cdot b$;

f) $-(a + b) = (-a) + (-b)$.

2 Доведіть, якщо $a + b = a$, то $b = 0$.

3 Доведіть, якщо $a > b > 0$ і $c > d > 0$, то $ac > bd$.

4 Доведіть нерівність $a^2 > a$ для довільного цілого числа a.

5 Доведіть нерівність $a^2 + b^2 > 2ab$ для цілих чисел a і b.

1.2. Математична індукція

Одна з найбільш складних проблем теорії чисел полягає в доведенні істинності тверджень для всіх натуральних чисел. Якщо твердження істинне для перших десяти натуральних чисел або навіть для перших десяти більйонів натуральних чисел, то з цього ще не випливає, що твердження істинне для всіх натуральних чисел.

Зазвичай легко довести, що твердження не є правдивим для всіх натуральних чисел. Насправді, використовуючи той факт, що запереченням $(\forall x P(x))$ є $(\exists x)\widetilde{P}(x)$, необхідно знайти тільки одне натуральне число, для якого твердження $P(x)$ не є істинним. Ця процедура відома як знаходження контрприкладу. Інструментом для доказу істинності тверджень щодо всіх натуральних чисел є принцип індукції, який буде нашою останньою аксіомою для множини натуральних чисел $\mathbb{N}$. Це зовсім не означає, що доказ будь-якого твердження щодо натуральних чисел вимагає індукції. Багато теорем можуть бути доведені на основі інших теорем і аксіом. Тим не менш, в основі доведення багатьох розглянутих нижче теорем лежить принцип індукції. Надалі принцип індукції буде сформульований в інший, еквівалентній формі.

N4(Принцип математичної індукції) Нехай $P(k)$ є таке твердження, що

a) $P(1)$ – істинне, і

b) для кожного k, якщо $P(k)$ істинне, то $P(k + 1)$ істинне.

Тоді $P(n)$ істинне для будь-якого натурального n.

В символічному записі принцип математичної індукції має вид (ОПИСАТЬ!)

$$(P(1) \wedge (\forall k)P(k) \to P(k + 1)) \to (\forall n)P(n).$$

Математичну індукцію можна порівняти з нескінченним рядом кісточок доміно. Властивість побудованого у ряд доміно полягає в тому, що якщо кинути одну кісточку, падає наступна. Нехай твердження $P(n)$ полягає в тому, що падає n-а кісточка. Падіння першої кісточки доміно позначимо $P(1)$, тобто істинність $P(1)$ полягає в тому, що перша кісточка падає. Оскільки кожна кісточка перекидає наступну, то з істинності $P(k)$ слідує істинність $P(k+1)$. Оскільки падають всі кісточки, $P(n)$ істинно для кожного натурального n. Надалі, проводячи доведення за допомогою описаного вище принципу математичної індукції, ми будемо просто говорити, що доводимо твердження по індукції.

Приклад 1.1. Допустимо, необхідно знайти формулу для обчислення суми перших n натуральних чисел, $1+2+3+...+n$. Така формула була б корисна, якщо потрібно було б, наприклад, знайти сумму перших 100000 натуральних чисел, не виконуючи для цього 99 999 операцій додавання. Припустимо, що сума перших n натуральних чисел дорівнює $\dfrac{n(n+1)}{2}$. Доведемо це твердження за індукцією.

Нехай S_n є твердження

$$1+2+3+...+n=\frac{n(n+1)}{2}. \tag{1.1}$$

Спочатку доведемо, що S_1 істинне. При $n=1$ ліва частина рівності (1.1) дорівнює 1. В правій частині рівності (1.1) отримаємо

$$\frac{n(n+1)}{2}=\frac{1+1}{2}=1,$$

так що S_1 істинне. Потім припустимо, що для довільного натурального k S_k істинне, тобто рівність (1.1) істинна для $n=k$. Це означає, що

$$1+2+3+...+k=\frac{k(k+1)}{2}. \tag{1.2}$$

Тепер необхідно довести, що S_{k+1} істинне, тобто рівність S_n істинна для $n=k+1$. Іншими словами, необхідно довести, що

$$1+2+3+...+k+(k+1)=\frac{(k+1)(k+1)+1)}{2}. \tag{1.3}$$

Використаємо припущення (1.2): порівнюючи цю рівність з рівністю (1.3), ми помічаємо, що, додавши $k+1$ до обох частин рівності (1.2), отримаємо ліву часть рівності (1.3):

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

Отже, доведено рівність (1.3), яка означає, що співвідношення (1.2) справедливе для $n = k + 1$. Цей результат забезпечує істинність S_{k+1}. Отже, в силу аксіоми $N4$, твердження S_n істинне для довільного натурального n.

Приклад 1.2. Необхідно довести, що

$$1^2 + 2^2 + 3^2 + ... + n^2 = \frac{n(n+1)(2n+1)}{6}. \tag{1.4}$$

Через S_n позначимо твердження, для якого справедлива рівність (1.4). Спочатку доведемо, що твердження S_n істинне для $n = 1$. Підставивши 1 в обидві частини рівності, отримаємо

$$1^2 = \frac{1(1+1)(2*1+1)}{6} = 1.$$

що забезпечує істинність твердження S_n при $n = 1$. Потім ми допускаємо, що рівність S_n істинна для $n = k$. Тобто,

$$1^2 + 2^2 + 3^2 + ... + k^2 = \frac{k(k+1)(2k+1)}{6}. \tag{1.5}$$

Тепер необхідно довести, що рівність S_n істинна для $n = k + 1$. Іншими словами, необхідно довести, що

$$1^2+2^2+3^2+...+k^2+(k+1)^2 = \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6} = \tag{1.6}$$

$$= \frac{(k+1)(k+2)(2k+3)}{6}.$$

Використаємо припущення (1.5), помітимо, що, додавши до обох частин рівності (1.5) доданок $(k+1)^2$, ми отримаємо ліву частину шуканої рівності (1.6). Таким чином,

$$1^2 + 2^2 + 3^2 + ... + k^2 + (k+1)^2 = \frac{k(k+1)(2k+1)}{6} + (k+1)^2 =$$

$$= \frac{k(k+1)(2k+1)}{6} + \frac{6(k+1)^2}{6} = \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} =$$

$$= \frac{(k+1)(k(2k+1) + 6(k+1))}{6} = \frac{(k+1)(2k^2+7k+6)}{6} =$$

$$= \frac{(k+1)(2k+3)(k+2)}{6}.$$

Отже, доведена рівність (1.6), яка означає, що рівність S_n виконується для $n = k + 1$. Тобто, S_n істинне для кожного натурального числа n.

Приклад 1.3. Необхідно довести, що для будь-якого натурального числа n, число n^3-n ділиться на 3 (Зауважимо, что натуральне число t ділиться на 3 при умові, що існує натуральне число m таке, що $t = 3m$).

Доведення будемо проводити за індукцією. Нехай S_n – твердження "n^3-n ділиться на 3". Доведемо, що S_1 істинно. Для $n = 1$ маємо $n^3-n = 1-1 = 0$, тому $n^3 - n$ при $n = 2$ ділиться на 3, так як $0 = 3 * 0$. Таким чином, S_1 істинно.

Тепер покажемо, що для довільного натуральноо числа k, якщо S_k істинне, то S_{k+1} істинне. Припустимо, що S_k істинне. Іншими словами, $k^3 - k$ ділиться на 3, тому $k^3-k = 3m$ для деякого натурального числа m. Необхідно довести, що S_{k+1} істинне. Останнє означає, що $(k+1)^3-(k+1)$ ділиться на 3, тобто існує натуральне число ω таке, що $(k+1)^3-(k+1) = 3\omega$. Звернемо увагу на натуральне число $(k+1)^3-(k+1)$. У даному випадку стратегія полягає в тому, щоб перетворити $(k + 1)^3 - (k + 1)$ таким чином, щоб була можливість використати наші знання про k (а саме, що $k^3 - k$=3m).

Отже,

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

$$= 3m + 3(k^2 + k) = 3\omega$$

де $\omega = m + (k^2 + k)$. Таким чином, $(k + 1)^3 - (k + 1)$ ділиться на 3, і, твердження S_{k+1} істинне. Тому, за індукцією, S_n істинне для всіх n.

Приклад 1.4. Потрібно довести, що площина, розділена на області будь-яким числом різних прямих ліній, може бути розфарбована чорною і білою фарбою таким чином, що будь-які дві області, які мають спільну межу, будуть пофарбовані в різні кольори, як зображено на мал. 1.2.

Оскільки у формулюванні задачі запитується про всі можливі випадки розташування областей і ліній, це призводить до нескінченно великого числа можливостей. Принцип індукції є найбільш підходящим для вирішення завдань зазначеного типу.

У нас є вибір: або довести, що будь-які m таких областей можна розфарбувати зазначеним чином, або довести, що будь-яке число областей, утворених за допомогою m прямих ліній, можна розфарбувати потрібним чином. У кожному з цих випадків покажемо, що рисунок може бути розфарбований потрібним чином. У першому випадку покажемо, що доведення за індукцією проводиться по числу областей. У другому випадку ми скажемо, що доведення за індукцією проводиться по числу прямих ліній. Далі будемо використовувати число ліній, вказаних на рисунку.

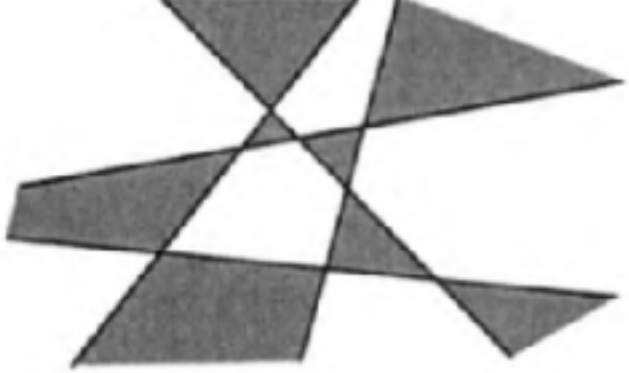

Рис. 1.1:
Зафарбовані області

Нехай $P(m)$ – твердження, що рисунок, виконаний з використанням m ліній, може бути розфарбований необхідним чином (тобто за допомогою чорного і білого кольорів, і при цьому ніякі сусідні області, які мають спільну частину межі, не будуть пофарбовані в один і той же колір).

Таким чином, якщо $M = N$, то рисунок, утворений будь-яким числом ліній, може бути потрібним чином розфарбованим. $M \subseteq N$ за означенням.

(а) Покажемо, що $1 \in M$. Це рівносильно тому, що $P(1)$ істинно, тобто рисунок, зроблений за допомогою тільки однієї лінії, може бути розфарбований. З геометрії відомо, що лінія, проведена в площині, ділить її на дві області. Зафарбуємо одну з них в чорний колір, а іншу – в білий, як показано на рис. 1.2.. Таким чином, доведено, що $1 \in M$.

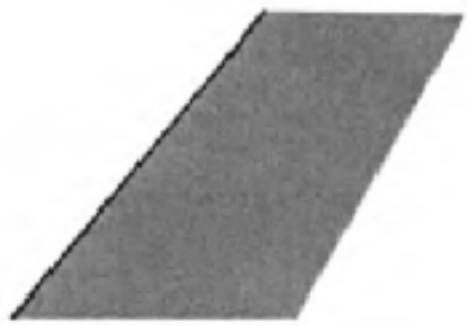

Рис. 1.2:
Зафарбовано у відповідності з наявністю однієї лінії у площині

(б) Покажемо, що з $m \in M$ слідує $m + 1 \in M$. Припустимо, що m – натуральне число з M. Це означає, що $P(m)$ істинно, і будь-який рисунок, виконаний за допомогою m ліній, може бути потрібним чином розфарбований. Розглянемо натурально число $m+1$. Необхідно показати, що $P(m+1)$ істинно, або, що еквівалентно, рисунок, виконаний з використанням $m+1$ лінії, може бути потрібним чином розфарбований. Для цього можна використати "індуктивну гіпотезу а саме: припущення про те, що будь-який рисунок, виконаний з використанням m ліній, може бути потрібним чином розфарбований.

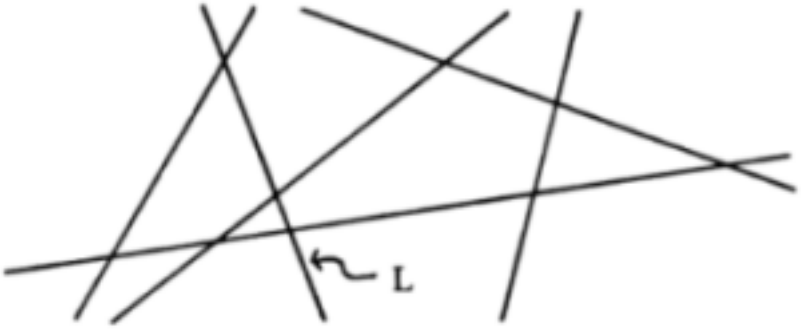

Рис. 1.3:
ліній

Розглянемо рисунок, виконаний з використанням $m+1$ лінії, як зображено на рис. 1.2.

Тепер нам потрібно створити ситуацію, в якій ми зможемо використати той факт, що $m \in M$, або що будь-який рисунок, виконаний з використанням m ліній, може бути розфарбований потрібним чином. Для цього виберемо одну з ліній, наприклад, лінію L, і видалимо її. Отриманий в результаті рисунок містить тільки m ліній, тому в силу індуктивного припущення (будь-який рисунок, який складається з m ліній, може бути необхідним чином розфарбований), можна потрібним чином розфарбувати рисунок на рис. 1.2.

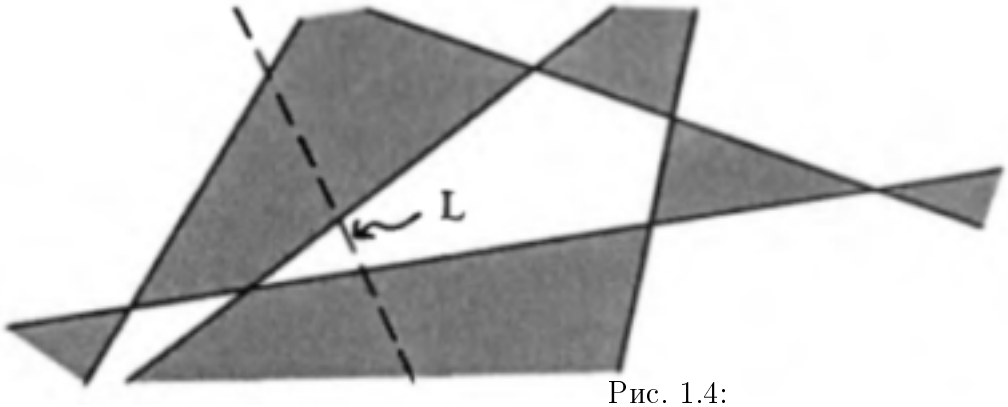

Рис. 1.4:
Зафарбовано у відповідності з наявністю m ліній.

Тепер повернемо лінію L на колишнє місце і змінимо колір кожної області з одного боку лінії L на протилежний (чорні області стануть білими, а білі – чорними), як показано на рис. 1.2. Цей рисунок розфарбований необхідним чином, тому кожні дві сусідні області, які перебували по той бік від L, де кольори були змінені, мали різні кольори по різні сторони лінії, оскільки кольори були змінені на протилежні, то кольори по різні боки будь-якої такої межі залишилися різними. Зміни вносять тільки ті межі, які знаходяться вздовж лінії L, але якщо L ділила область, то колір був змінений по обидві сторони від L, роблячи кольори різними по обидві сторони від такої межі. Таким чином, цей рисунок, виконаний з використа-

нням $m+1$ лінії, може бути необхідним чином розфарбований. Отриманий результат означає, що $P(m+1)$ істинно, тобто $m+1 \in M$.

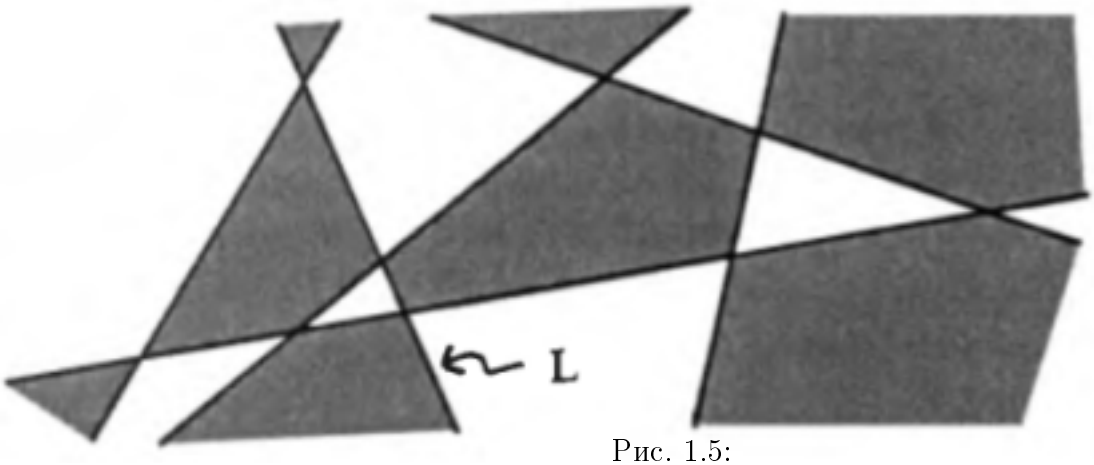

Рис. 1.5:
Зафарбовано у відповідності з наявністю $m+1$ ліній.

Отже, ми довели частини (а) і (б) принципу індукції. Таким чином, $M = N$. У таких випадках, як правило, говорять, що індукцією встановлено рівність M і N. Маємо, що рисунок, виконаний з використанням будь-якого (скінченного) числа ліній, може бути розфарбований потрібним чином.

Існує два інших еквівалентних визначення принципу математичної індукції. Вони еквівалентні вихідному визначенню в тому сенсі, що будь-яка з трьох форм може бути використана для доказу двох інших.

Розглянемо множину $A = \{3, 7, 8\}$. Ціле число 3 володіє відносно множини A унікальною властивістю, а саме: число 3 належить A і воно менше або дорівнює кожному елементу множини A. При цьому говорять, що 3 – найменше ціле число множини A. Не кожна множина цілих чисел має найменше ціле число. Порожня множина $\varnothing$ не має найменшого цілого числа, оскільки вона не містить цілих чисел взагалі. Множина

$$C = \{n : n \in \mathbb{Z}, n = 5k, k = \in \mathbb{N}\} = \{... - 15, -10, -5, 0, 5, 10, 15...\}.$$

не має найменшого цілого числа, тому, якщо m – найменше ціле число множини C, то $m = 5 \cdot k$ для деякого цілого числа k. Але ціле число $s = 5k - 1$ також належить C і, природно, $s = 5k - 1 < 5k < m$, так що $s < m$, і це суперечить припущенню про те, що m – найменше ціле число множини C.

Означення 1.2. Нехай A – множина цілих чисел. Ціле число a є найменшим цілим числом множини A тоді і тільки тоді, коли

a) a належить A $(a \in A)$,

b) якщо b належить A $(b \in A)$, то $a < b$.

Теорема 1.7. *Якщо множина цілих чисел має майменше ціле число, то таке число єдине.*

Доведення. Доведення методом від супротивного. Нехай, обидва числа a і b є найменшими елементами множини A. За означенням найменшого елемента, $a < b$ і $b < a$. Отже, $a = b$. □

Тепер сформулюємо два твердження, еквівалентних принципу індукції (ПРОВЕРИТЬ).

N5 (Принцип повного впорядкування) Кожна непорожня множина натуральних чисел містить найменший елемент.

N6 (Другий принцип індукції) Нехай $P(n)$ – твердження, яке володіє такими властивостями.

a) Якщо $P(1)$ – істинне, і

b) для довільного k з істинності $P(m)$ для всіх $m < k$ слідує істинність $P(k)$,

то $P(n)$ істинне для всіх натуральних n.

В символічній формі принцип індукції має вигляд

$$(P(1) \wedge (\forall k)(\forall m < k)P(m)) \to P(k)) \to (\forall n)P(n).$$

Приклад використання другого принципу індукції $N6$ буде наведено нижче при доведенні того, що кожне ціле число являє собою добуток простих чисел. Наступна теорема – приклад твердження, яке може здаватися занадто очевидним для проведення його доведення, але оскільки розглянута модель цілих чисел визначена сукупністю правил, для наших "цілих чисел" ці твердження можуть не виявитися настільки очевидними або навіть істинними. Ми можемо встановити це, доводячи відповідну теорему з використанням наявних правил. Доведення є хорошим прикладом використання принципу повного упорядкування $N5$. Воно є також прикладом використання принципу зведення до абсурду.

Теорема 1.8. *Не існує такого натурального a, що $0 < a < 1$.*

Доведення. Доведення методом від супротивного. Нехай таке число існує, і нехай S – множина всіх натуральних чисел між 0 і 1. Оскільки S непорожня множина, за аксіомою $N5$ множина S має найменше натуральне число, наприклад, a. Домноживши нерівність $0 < a < 1$ на a, отримаємо $0 < a^2 < a$. Тепер, оскільки $a < 1$, маємо $a^2 < 1$. Але це суперечить тому факту, що a – найменше натуральне число менше за 1. Тобто, S – порожня множина, і не існує натурального числа між 0 і 1. □

Наслідок 1.1. *Якщо b – ціле число, то не існує цілого числа a, що володіє властивістю $b < a < b + 1$.*

Аксіоми $N4$ і $N6$ сформульовані для цілих чисел, починаючи з 1, з продовженням умов на цілі числа, що більші за 1. Аналогічні теореми індукції справедливі для цілих чисел, не менших деякого цілого j, яке може не співпадати з 1. Наступна теорема є обгрунтуванням індукції для підмножини цілих, не обов'язково натуральних, чисел.

Теорема 1.9 (Принцип індукції для цілих чисел)**.** *Нехай $P(n)$ – твердження, яке володіє такими властивостями*

a) *$P(j)$ – істинне і*

b) *для довільного $k \geq j$, якщо $P(k)$ – істинно, то $P(k+1)$ істинне.*

Тоді $P(n)$ істинно для кожного $n \geq j$

Доведення. Доведення випливає з аксіоми $N4$. Для цього достатньо покласти $n = t - j + 1$. □

Далі в прикладі доводиться твердження, що включає нерівність. Часто в такій ситуації доводиться використовувати наступну властивість, сформульовану в теоремі 1.5:

$$(a > b > 0) \wedge (c > d > 0) \Rightarrow ac > bd$$

Приклад 1.5. За допомогою принципу індукції для цілих чисел, необхідно довести, що для будь-якого цілого числа $n \geq 4$ має місце нерівність $n! > 2^n$.

При використанні індукції за n, у даному випадку, не можна починати з $n = 1$, оскільки твердження для $n = 1$ невірне. Початковою точкой повинно бути $n = 4$, так як твердження невірне також для $n = 2$ і $n = 3$.

Згідно з означенням, прийнятими для принципу індукції для цілих чисел, маємо: $j = 4$, $P(n)$ – твердження "$n! > 2^n$". Спочатку доведемо твердження для $n = 4$. При $n = 4$ маємо $4! = 24$ і $2^4 = 16$, так що $4! > 24$.

За індуктивним припущенням маємо

$$k! > 2^k. \tag{1.7}$$

Нам необхідно довести, що

$$(k+1)! > 2^{k+1}. \tag{1.8}$$

Зауважимо, що результат (1.8) можна отримати, якщо домножити ліву частину нерівності (1.7) на $k + 1$, а праву – на 2. Тому, якщо ми покажемо,

що $k+1 > 2$, то отримаємо $k! > 2^k$ і $k+1 > 2$, та зможемо зробити висновок щодо справедливості нерівності (1.8). Оскільки $k \geq 4$, то $k > 2$. Отже, $(k+1) * k! = 2 * 2^k$ і $(k+1)! > 2^{k+1}$. Таким чином, $n! > 2n$ для кожного $n \geq 4$.

Вправи

1 Довести, що $1 + 4 + 7 + 10 + \ldots + (3n-2) = \frac{n(3n-1)}{2}$.

2 Довести, що $\frac{1}{1\cdot 3} + \frac{1}{3\cdot 5} + \frac{1}{5\cdot 7} + \frac{1}{7\cdot 9} + \ldots + \frac{1}{2n-1\cdot 2n+1} = \frac{n}{2n+1}$.

3 Довести, що $1 + 2 + 2^2 + 2^3 + \ldots + 2^{n-1} = 2^n - 1$.

4 Довести, що $1 + r + r^2 + r^3 + \ldots + r^{n-1} = \frac{1-r^n}{1-r}$.

5 Довести, що $1 + 3 + 5 + 7 + \ldots + (2n-1) = n^2$.

6 Довести, що $\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}$.

7 Довести, що $\sum_{i=1}^{n} i(i+1) = \frac{n(n+1)(n+2)}{3}$.

8 Для натурального числа n визначимо a^n як $a^1 = 0$ і $a^{k+1} = a^k \cdot a$. Доведіть, що $a^{m+n} = a^m \cdot a^n$.

9 Використайте математичну індукцію для доведення $(ab)^k = a^k \cdot b^k$.

10 Використайте математичну індукцію для доведення $n^2 > 2n + 1$ при $n \geq 3$.

11 Використайте математичну індукцію для доведення $2^n > n^2$ при $n \geq 5$.

12 Знайдіть найбільшу множину натуральних чисел, для якої $2n > n!$ істинно. Доведіть істинність твердження.

13 Доведіть, що кожне ціле число $n \geq 8$ може бути записаним як $3m + 5k$ для деяких невід'ємних чисел k, m.

14 Доведіть, що для кожного натурального числа $\frac{4^n}{n+1} < \frac{(2n)!}{(n!)^2}$ при $n \geq 2$.

15 Доведіть, що для будь-якого цілого числа a і натуральних чисел m, n має місце рівність $a^{mn} = a^m \cdot a^n$.

16 Використайте математичну індукцію для доведення $n! > n^3$ для всіх $n \geq 6$.

17 Використайте математичну індукцію для доведення

$$\left(1-\frac{1}{4}\right)\cdot\left(1-\frac{1}{9}\right)\cdot\left(1-\frac{1}{16}\right)\cdot\ldots\cdot\left(1-\frac{1}{n^2}\right)=\frac{n+1}{2n}$$

при $n \geq 2$.

18 Доведіть, якщо W – непорожня підмножина множини $\mathbb{Z}$ та існує ціле число x таке, що $x < w$ для всіх w з W, то W має найменший елемент.

19 Визначимо $\bigcup\limits_{i=1}^{n} A_i$ таким чином $\bigcup\limits_{i=1}^{1} A_i = A_1$ та $\bigcup\limits_{i=1}^{k+1} A_i = \left(\bigcup\limits_{i=1}^{k} A_i\right) \bigcup A_{k+1}$. Визначимо $\bigcap\limits_{i=1}^{n} A_i$ як $\bigcap\limits_{i=1}^{1} A_i = A_1$ та $\bigcap\limits_{i=1}^{k+1} A_i = \left(\bigcap\limits_{i=1}^{k} A_i\right) \bigcap A_{k+1}$. Доведіть, що

a) $\left(\bigcup\limits_{i=1}^{n} A_i\right) \bigcap A = \bigcup\limits_{i=1}^{n} (A_i \bigcap A)$;

b) $\left(\bigcup\limits_{i=1}^{n} A_i\right)' = \bigcap\limits_{i=1}^{n} A_i'$.

20 Використовуючи вище наведені означення, доведіть, що

a) $\left(\bigcap\limits_{i=1}^{n} A_i\right) \bigcap A = \bigcap\limits_{i=1}^{n} (A_i \bigcap A)$;

b) $\left(\bigcap\limits_{i=1}^{n} A_i\right)' = \bigcup\limits_{i=1}^{n} A_i'$.

1.3. Подільність

Багато цілих чисел можна представити як добуток менших чисел. Важливі характеристики й відношення цілих чисел можуть бути отримані на основі аналізу їхньої структури з погляду їх множників.

Означення 1.3. Ціле число a є кратне числа b, якщо $a = bm$ для деякого цілого числа m. Ненульове ціле число b ділить ціле число a, що позначається як $b|a$, якщо a є кратне b. Ціле число b, що ділить ціле число a, називається дільником числа a.

За означенням, $9|27$, оскільки $27 = 9 \cdot 3$, але 5 не ділить 12, тому що не існує цілого числа m такого, що $12 = 5m$. Цілі числа 1, 2, 3, 4, 6 і 12, і тільки вони, є додатніми дільниками числа 12. Цілі числа -1, -2, -3, -4, -6 і -12 також є дільниками числа 12.

Теорема 1.10. *Нехай a, b і c - цілі числа. Тоді*

1. *$a|a$ для будь-якого a.*

2. *Для будь-яких a, b і c з $a|b$ і $b|c$ слідує $a|c$.*

3. *Для будь-яких a, b і c маємо: $b|a$ і $b|c$ тоді й тільки тоді, коли $(b|m \cdot a + n \cdot c)$ для всіх цілих чисел m і n.*

Доведення. 1. $a = a \cdot 1$.

2. Якщо $a|b$ і $b|c$, то $b = a \cdot m$ і $c = b \cdot n$. Отже, $c = b \cdot n = (a \cdot m) \cdot n = a \cdot (m \cdot n)$ і $a|c$.

3. Припустимо, що $b|a$ й $b|c$. Тоді $a = b \cdot p$ і $c = b \cdot q$ для деяких цілих чисел p і q. Отже, $m \cdot a + n \cdot c = m(b \cdot p) + n(b \cdot q) = b \cdot (m \cdot p + n \cdot q)$. Обернено, припустимо, що $b|(m \cdot a + n \cdot c)$ для всіх цілих чисел m і n. Тоді, якщо $m = 1$, $n = 0$, маємо $b|a$. Якщо $m = 0$ і $n = 1$, маємо $b|c$.

□

Теорема 1.11. *Якщо a і b – натуральні числа й $a|b$, то $a \leq b$.*

Доведення. Для доведення теореми необхідно використати пункт г) теореми 1.5. □

Наслідок 1.2. *Якщо для натуральних чисел a і b виконується $a|b$ і $b|a$, то $a = b$.*

Теорема 1.12. *Якщо a і b – цілі числа і $a|b$ та $b|a$, то $a = b$ або $a = -b$.*

Доведення. Якщо $a > 0$ і $b > 0$, то в силу наслідку 1.2 маємо $a = b$. Якщо $a < 0$ і $b > 0$, то $-a > 0$ і $(-a)|b$, і $b|(-a)$, так що $b = -a$ або $a = -b$. Справедливість твердження теореми у випадку $a > 0$ і $b < 0$ є наслідком симетрії. Доведення випадку $a < 0$ і $b < 0$ надається читачеві. □

З наведених вище теорем слідує, що для натуральних чисел відношення "ділить"є рефлексивним, антисиметричним і транзитивним, тому воно є частковим порядком на множині натуральних чисел. Зверніть увагу, що відношення подільності не є відношенням часткового порядку на множині цілих чисел, тому що "ділить"не є на множині цілих чисел антисиметричним відношенням. Наступна теорема пояснює дію, що зустрічається в елементарній арифметиці. Натуральне число a можна розділити на натуральне число b і одержати остачу r, що менше, ніж b. Наприклад, якщо 31 розділити на 9, одержимо частку 3 і остачу 4. Наприклад, $31 = 3 \cdot 9 + 4$, де $4 < 9$. Доведення наступної теореми також є ілюстрацією принципу повного впорядкування (ПРОВЕРИТЬ).

Теорема 1.13 (Алгоритм ділення). *Для натуральних чисел a і b існують єдині невід'ємні цілі числа q і r, де $0 \leq r < b$ такі, що $a = bq + r$. Такі цілі числа r і q називаються, відповідно, остачею й часткою від ділення a на b.*

Доведення. (ПРОВЕРИТЬ по конспекту) Нехай a і b - натуральні числа. Розглянемо множину S всіх невід'ємних цілих чисел, що мають вид $a - bq'$ для не цілого числа q', тобто

$$S = \{x : x = a - bq', x \geq 0, q' \geq 0\}.$$

Множина S не порожня, оскільки для $q' = 0$ маємо $a - bq' = a - b \cdot 0 = a > 0$, так що $a \in S$. Множина S має найменший елемент. Дійсно, якщо $0 \in S$, він і є найменшим елементом. У противному випадку S містить тільки натуральні числа і, відповідно до принципу повного упорядкування N5 має найменший елемент. Оскільки r' належить S, нехай q' - невід'ємне ціле число таке, що $r' = a - bq'$. Якщо $r' \geq b$, то $r'' = r' - b \geq 0$ і

$$a - bq' = r',$$

$$a - bq' - b = r' - b,$$

$$a - b(q' + 1) = r'',$$

так що r'' належить S. Крім того, $r'' < r'$, тому що

$$b > 0,$$

$$-b < 0,$$

$$r' - b < r' + 0 = r'.$$

Але $r'' < r'$ і те, що $r'' \in S$, суперечить припущенню, що r' є найменшим елементом множини S. Таким чином, $0 \leq r' < b$. Щоб довести єдиність, припустимо, що $a = bq + r = bq + s$, де $0 \leq r \leq s < b$. Оскільки $r \geq 0$, то $-r \leq 0$. Отже, $s - r < b + 0 = b$. Але $s - r = b(q - p)$, і за теоремою 1.11, якщо $q - p$ не дорівнює 0, то $s - r \geq b$. Отже, $q - p = 0$, $q = p$ і $r = s$. □

Якщо $a < b$, то q повинно дорівнювати 0, щоб виконувалося $a = bq + r$, де $0 \leq r < b$ і $q \geq 0$. Наприклад, для $a = 4$ і $b = 7$ алгоритм ділення дає $q = 0$ і $r = a = 4$, так що $4 = 7 \cdot 0 + 4$. У силу єдиності q і r, якщо можна одержати q і r яким-небудь іншим способом, причому $a = bq + r$, $0 \leq r \leq s < b$ і $q \geq 0$, то ці q і r повинні збігатися з тими, які існують відповідно до теореми. Оскільки будь-який додатній дільник натурального числа n не може бути більше самого цього числа, всі додатні

дільники числа n можна знайти, перебираючи всі цілі числа від 1 до n і перевіряючи, чи не ділять вони n. Так, наприклад, ми визначили, що додатніми дільниками числа 12 є числа 1, 2, 3, 4, 6 і 12. Саме так можна показати, що додатніми дільниками числа 90 є 1, 2, 3, 5, 6, 9, 10, 15, 18, 30, 45 і 90. Перевірка показує, що числа 1, 2, 3 і 6 є дільниками як 12, так і 90. Числа 1, 2, 3 і 6 називаються спільними дільниками чисел 12 і 90. Більше того, 6 є найбільший із цих спільних дільників. Звернемо увагу, що загальні дільники 1, 2, 3 і 6 є також дільниками найбільшого спільного дільника 6. У контексті найбільших спільних дільників розглядаються тільки додатні дільники.

Означення 1.4. Натуральне число d називається спільним дільником чисел a і b, якщо $d|a$ і $d|b$.

Означення 1.5. Натуральне число d називають найбільшим спільним дільником цілих чисел a і b, якщо

a) $d|a$ і $d|b$, та

b) із $c|a$ і $c|b$ слідує $c|d$.

Найбільший спільний дільник чисел a і b позначається через НСД (a, b). Алгоритм знаходження найбільшого спільного дільника наведений у розділі 2.3.

Теорема 1.14. *Якщо d і c – найбільші спільні дільники цілих чисел a й b, то $= d$; інакше кажучи, існує єдиний спільник дільник для натуральних чисел a і b.*

Доведення. За означенням найбільшого спільного дільника $d|c$ і $c|d$. Отже, $= d$ або $= -d$. Оскільки і d – обоє додатні, то $= d$. □

Теорема 1.15. *Найбільший спільний дільник натуральних чисел a і b існує. Такий найбільший спільний дільник може бути записаний у вигляді*

$$u \cdot a + v \cdot b$$

для деяких цілих чисел u і v. Крім того, найбільший спільний дільник – це найменше натуральне число такого виду.

Доведення. Нехай S – множина всіх натуральних чисел, що мають форму $na + mb$. Нехай $d = ua + vb$ – найменший елемент множини S. Тоді $d \leq a$, тому що $= 1 \cdot a + 0 \cdot b$ належить S. Крім того, $a = qd + r$ для деяких q і r, де $q > 0$ і $0 \leq r < d$. Отже, $a = q(ua + vb) + r$. Вирішуючи відносно r,

одержуємо, $r = (1 - qu)a + (-v)qb$, так що r належить S або $r = 0$. Але r менше, ніж d, що, у свою чергу, є найменшим елементом множини S, так що $r = 0$. Тому $d|a$. Аналогічно, $d|b$. Якщо c – довільний дільник чисел a і b, то за теоремою 1.10 частина (в) $c|d$, оскільки $d = ua + vb$. Отже, d – найбільший спільний дільник чисел a і b. □

Алгоритм знаходження u і v наведений у розділі 2. Властивості найбільшого спільного дільника, які сформульовані в наступній теоремі, будуть використані надалі.

Теорема 1.16. . *Якщо $a = bq + c$, то НСД(a,b) = НСД (b, c); інакше кажучи, кожний дільник a і b є дільником b і c, і обернено.*

Доведення. Нехай e= НСД (a ,b) і f= НСД (b,c). Оскільки $e|a$ і $e|b$, то по теоремі 1.10 (в) маємо $e|c$, тому що $c = a - bq$. Тоді, за означенняя найбільшого спільного дільника $e|f$. Обернено, оскільки $f|b$ і $f|c$, то по теоремі 1.10 (в) $f|a$. За означенням найбільшого спільного дільника $f|e$. Отже, $e = f$. □

Теорема 1.17. *Якщо a, b і c – цілі числа, НСД(a, b) = 1 і $a|bc$, то $a|c$.*

Доведення. Оскільки НСД(a, b) = 1, то існують цілі числа u і v такі, що $au + bv = 1$. Помножимо кожний доданок на c, одержимо $cau + cbv = c$. Тоді $a|cau$ і $a|cbv$, тому що $a|bc$. Отже, $a|c$. □

Означення 1.6. Якщо найбільший спільний дільник a і b є 1, то числа a і b називаються взаємно простими.

Безпосередньо з означення слідує, що якщо a і b – взаємно прості числа, то існують цілі числа u і v такі, що $au + bv = 1$. Помітимо, що якщо a і b – натуральні числа, то ab кратно і a, і b. Якщо розглядати множину всіх чисел, кратних a і b, то відповідно до принципу повного впорядкування N5 існує найменше кратне чисел a і b. Якщо c - найменше кратне чисел a і b, а d – інше кратне чисел a і b, то $c|d$. Інакше говорячи, існують q і r такі, що $d = qc + r$, де $r < c$. Оскільки і a, і b ділять числа d і c, вони також ділять r. Але тоді r було б кратним a і b, що менше, ніж c, що приводить до протиріччя. Таким чином, ми приходимо до наступних означень.

Означення 1.7. Натуральне число m називається спільним кратним цілих чисел a і b, якщо $a|m$ і $b|m$.

Означення 1.8. Натуральне число m називається найменшим спільним кратним цілих чисел a і b, якщо

а) $a|b$ і $b|m$, і

b) якщо $a|n$ і $b|n$, то $m|n$.

Найменше спільне кратне чисел a і b будемо позначати НСК(a, b).

Використання найбільшого спільного дільника є корисним при знаходженні розв'язків рівнянь виду $ax + by = c$ або для доведення, що такі розв'язки не існують. Це випливає з наведеної нижче теореми.

Теорема 1.18. *Рівняння $ax + by = c$, де a, b і c – цілі числа, має цілий розв'язок (тобто існують цілі числа x і y такі, що $ax + by = c$) тоді й тільки тоді, коли c ділиться на N =НСД(a, b). Якщо c ділиться на N, то розв'язок $ax + by = c$ має вигляд*

$$x_0 = \frac{u \cdot c}{N}$$

$$y_0 = \frac{v \cdot c}{N}$$

де u і v – будь-який розв'язок рівняння $N = au + bv$.

Доведення. Відомо, що існують цілі числа u і v такі, що $au + bv =$ НСД(a, b). Якщо c ділиться на НСД (a, b), то $c = e\cdot$ НСД(a, b) для деякого цілого числа e. Отже, $aue + bve = e\cdot$НСД(a, b) $= c$, так що $x = ue$ і $y = ve$ – розв'язок рівняння. Обернено, якщо існують x і y такі, що $a + by = c$, то, оскільки НСД(a, b) ділить як a, так і b, він ділить $a + by$, отже, ділить c. □

Вправи

1 Знайдіть додатні дільники кожного з наступних цілих чисел: а) 54; б) 63; в) 72; г) 73; д) 74.

2 Для натуральних чисел a й b знайдіть невід'ємне цілі числа q і r, де $0 \leq r < b$ такі, що $a = bq + r$. а) a = 54, b = 27; б) a = 47, b = 47; в) a = 93, b = 17; г) a = 43, b= 8; д) a = 33, b = 1.

3 Для додатних цілих чисел a і b знайдіть НСД(a, b), НСК(a,b) і НСД(a,b)$\cdot$ НСК(a, b), якщо вони визначені. а) a = 54, b = 27; б) a = 17, b = 0; в) a = 6, b = 15; г) a = 12, b = 16; д) a = 33, b = 1.

4 Доведіть або спростуйте твердження: для натуральних чисел a і b НСД(a, b)$\leq$НСК(a, b).

5 Якщо $a = 0$ або $b = 0$, то що можна було б прийняти в якості НСК(a, b)? Відповідь обґрунтуйте.

6 Доведіть, що для взаємно простих чисел a й b і заданого цілого числа n існують цілі числа x і y такі, що $ax + by = n$.

7 Доведіть, що для натуральних чисел a і b, якщо $> b$, то НСД(a,b) = НСД(a-b,b).

8 Розглянемо теорему: якщо цілі числа a і b такі, що $a|b$ і $b|$, то $a = b$ або $a = -b$. Доведіть, що ця теорема також справедлива у випадку, коли $a < 0$ і $b < 0$.

1.4. Прості числа

Очевидно, що кожне ціле число a ділиться саме на себе і на 1, тому що $a = 1 \cdot a$. Кожне ціле число ділить 0, але 0 не ділить ніяке ціле число. Для деяких задач теорії чисел необхідно знати, чи має деяке конкретне ціле число дільники, відмінні від нього самого і 1. Деякі цілі числа не можуть бути розкладені в добуток цілих чисел, крім тривіального способу. Такі цілі числа називаються простими.

Означення 1.9. Ціле число, більше 1, називається простим, якщо воно не має додатних дільників, крім 1 і самого себе. Натуральне число, більше 1, називається складеним якщо воно не є простим.

Серед перших 10 натуральних чисел є чотири простих числа: 2, 3, 5 і 7. Цілі числа $4 = 2 \cdot 2$, $6 = 2 \cdot 3$, $8 = 2 \cdot 4$, $9 = 3 \cdot 3$ і $10 = 2 \cdot 5$ є складеним. Отже, якщо $n = r \cdot s$, де $1 < r < n$ і $1 < s < n$, то n – складене число. За означенням, ціле число 1 не є ні простим, ні складеним. Число 2 – єдине парне просте число. Визначити, чи є невелике ціле число простим, намагаючись розділити його на менші прості числа, порівняно легко, тому що кількість можливих варіантів невелика. Однак, питання про те, чи є простим велике ціле число, може виявитися досить складним. Наступна теорема показує, що існує нескінченно багато простих чисел. Доведення теореми являє класичний приклад використання принципу зведення до абсурду.

Теорема 1.19. *[Евклід] Існує нескінченно багато простих чисел.*

Доведення. Допустимо, що існує лише скінчена кількість простих чисел, наприклад, p_1, p_2, .., p_k. Розглянемо ціле число $(p_1, p_2, .., p_k) + 1$. Припустимо, що p_r - деяке просте число, і $p_r|((p_1, p_2, .., p_k) + 1)$. Але тоді $p_r|(p_1, p_2, .., p_k)$, звідки слідує, що $p_r|1$, а це приводить до протиріччя, тому що $p_r > 1$. Отже, $(p_1, p_2, .., p_k) + 1$ – просте число, що, у свою чергу, також є протиріччям, тому що цього числа немає серед зазначеної кінцевої сукупності простих чисел. Таким чином, наше припущення про те, що існує

скінчена кількість простих чисел, невірне, тому простих чисел повинно бути нескінченно багато. □

Оскільки розклад цілих чисел на прості множники є важливою задачею, необхідно мати швидкий і простий спосіб визначення, чи є дане натуральне число простим або складеним. Наступна теорема показує, що для перевірки простоти числа необхідно визначити тільки деякі з його можливих дільників.

Теорема 1.20. *Якщо натуральне число n є складеним, то n має простий дільник p такий, що $p^2 < n$.*

Доведення. Нехай p - найменший простий дільник числа n. Якщо n розкладається на множники p і s, то $p|r$ і $p|s$. Отже, $p^2 \leq rs = n$. Наприклад, щоб визначити, чи є $n = 521$ простим, необхідно розглянути тільки прості числа, які менше або рівні 22, тому що $22^2 = 484$, а $23^2 = 529$. Прості числа, менші або рівні 22, - це 2, 3, 5, 7, 11, 13, 17 і 19. Перевіряючи кожне з них, знаходимо, що жодне з них не ділить 521. Тому 521 є простим числом у силу попередньої теореми. Як покаже наступна теорема, прості числа утворять множину свого роду будівельних блоків для цілих чисел. □

Теорема 1.21. *[Основна теорема арифметики] Кожне натуральне число або дорівнює* 1*, або просте, або може бути записане як добуток простих чисел.*

Доведення. Припустимо, що $q_1q_2...q_n$ і $p_1p_2...p_s$ – два способи запису натурального числа m як добутку простих чисел. У доведенні теореми буде використана індукція по n, числу простих співмножників в першому добутку. Якщо $n = 1$, твердження теореми справедливе. Сформулюємо індуктивне припущення: нехай тверження теореми справедливе, коли $q_1q_2...q_k = p_1p_2...p_s$; якщо $m = q_1q_2...q_k = p_1p_2...p_s$, то $k = s$ і добуток єдиний, але з точністю до порядку простих співмножників. Припустимо тепер, що $m = q_1q_2...q_{k+1} = p_1p_2...p'_s$ Оскільки q_{k+1} ділить $p_1p_2...p'_s$, звідси слідує, що q_{k+1} ділить $p_1p_2...p'_s$ для деякого $1 \leq i \leq s'$. Розділимо обидва добутки на q_{k+1} або використаємо властивість скорочення (аксіому 18). Тоді $q_1q_2...q_k = p_1p_2...p_{i-1}p_{i+1}...p'_s$. Але по індукції до $k = s' - 1$, і добуток єдиний з точністю до порядку простих співмножників. Отже, до $k+1 = s'$, і розклад на множники числа m єдиний з точністю до порядку простих співмножників. □

Наприклад,

$$n = 39616304 = 2 \cdot 13 \cdot 7 \cdot 2 \cdot 23 \cdot 13 \cdot 2 \cdot 13 \cdot 2 \cdot 7 =$$

$$= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 7 \cdot 7 \cdot 13 \cdot 13 \cdot 13 \cdot 23$$

являють собою два розклади на множники числа n; однак, у кожному з добутків одно і теж саме просте число використане однакове число раз. Різниться тільки порядок запису простих чисел. Фактично є 12, 600 різних способів розкладу на множники числа n з використанням 10 простих співмножників, однак, кожний такий розклад містить рівно чотири двійки, дві сімки, три множники, рівних 13, і один, рівний 23. Звичайно прості множники групують, використовуючи експоненціальний запис. Наприклад, $n = 2^4 \cdot 7^2 \cdot 13^3 \cdot 23^1$.

Наслідок 1.3. *Кожне натуральне число, більше 1, може бути записано єдиним чином з точністю до порядку у вигляді* $q^{k(1)}q^{k(2)}...q^{k(n)}$ *, де* $k(1)$, $k(2)$, ..., $k(n)$ *– натуральні числа.*

Тепер зрозуміло, чому 1 не входить у множину простих чисел. У протилежному випадку теорема про єдиничність розкладу на прості множники була б невірна. При вивченні розкладу різних цілих чисел, використовуючи їх передставленя, дане в попередньому наслідку, найчастіше для зручності позначення допускається нульовий ступінь простого співмножника. Звичайно така практика не приводить до плутанини, тому що при $q_i^0 = i$ завжди $q_i \geq 1$. Якщо розклад на прості множники відомий, то прості числа, що формують розклад на прості множники будь-якого дільника цього числа, утворять підмножину, що відповідає множині для діленого. Доведення двох наступних теорем надається читачеві.

Теорема 1.22. *Якщо* $a = p_1^{a(1)}p_2^{a(2)}...p_k^{a(k)}$ *і* $b|a$, *то* $b = p_1^{b(1)}p_2^{b(2)}...p_k^{b(k)}$, *де* $0 \leq b(i) \leq a(i)$ *для всіх* i; *і навпаки.*

Теорема 1.23. *Нехай* $a = p_1^{a(1)}p_2^{a(2)}p_3^{a(3)}\ldots p_k^{a(k)}$ *і* $b = p_1^{b(1)}p_2^{b(2)}p_3^{b(3)}...p_k^{b(k)}$, *де* p_i *- прості числа, які ділять або* a, *або* b, *і деякі показники степеня можуть бути рівні 0. Нехай* $m(i) = min\{a(i), b(i)\}$ *і* $M(i) = max\{a(i), b(i)\}$ *для* $1 \leq i \leq k$. *Тоді НСД(*a, b*)=*$p_1^{m(1)}p_2^{m(2)}p_3^{m(3)}...p_k^{m(k)}$ *і НСК(*a, b*)=*$p_1^{M(1)}p_2^{M(2)}p_3^{M(3)}...p_k^{M(k)}$.

Застосуємо теорему 1.23 у випадку, коли $a = 195000$ і $B = 10435750$. Розклад на прості множники чисел a і b мають вигляд $a = 2^3 3^1 5^4 13^1$ і $b = 2^1 5^3 13^3 19^1$. Таким чином,

НСД(195000,10435750)$=2^{min(3,1)}3^{min(1,0)}5^{min(4,3)}13^{min(1,3)}19^{min(0,1)} = 2^1 3^0 5^3 13^1 19^0 = 2 \cdot 5^3 \cdot 13 = 3250$,

НСК(195000,10435750)$=2^{max(3,1)}3^{max(1,0)}5^{max(4,3)}13^{max(1,3)}19^{max(0,1)} = 2^3 3^1 5^4 13^3 19^1 = 626145000$.

Наступна теорема випливає з теореми 1.23. Доведення залишаємо читачу.

Теорема 1.24. *Якщо a й b – натуральні числа, то НСД(a,b)·НСК(a, b) = ab.*

Вправи

1. Розкладіть кожне з наступних цілих чисел на прості множники а) 728, б) 1599 (використовуйте рівність 1599 = 1600 - 1), в) 4899, г) 131, д)523.

2. Використовуйте теореми даного розділу для знаходження НСД і НСК наступних пар чисел: а) 162 і 12, б) 71 і 23, в) 72 і 30, г) n! і (n + 2)!, д) 75 і 99.

3. Два простих числа a й b називаються числами-близнюками, якщо різниця між ними дорівнює 2, тобто якщо $a + 2 = b$. Наприклад, 3 і 5 є числами-близнюками. Знайдіть три інші пари чисел-близнюків.

4. Чи є середнє арифметичне двох простих чисел-близнюків простим числом?

5. Якщо a і b – прості числа, звідси слідує, що $a^2 + b^2$ - просте число?

6. Поясніть, чому для будь-якого натурального числа n всі числа $n! + 1$, $n! + 2$, $n! + 3$, $n! + 4$, ... ,$n! + n$ є складеними. Що даний факт говорить про відстань між простими числами?

7. Покажіть, що числа 479001603 і 479001607 не є простими, використовуючи попередні вправи і калькулятор.

8. Якщо p_1, p_2, p_3, ...,p_n – перші n послідовних простих чисел, то чи слідує звідси, що $p_1 \cdot p_2 \cdot p_3 \cdot, ..., \cdot_n + 1$ (добуток перших n простих чисел плюс одиниця) є просте число. Обґрунтуйте свою відповідь.

9. Покажіть, що не існує трійок послідовних непарних чисел, кожне з яких є простим, за винятком трійки (3,5,7).

10. Доведіть, що якщо p і q – прості числа, більші або рівні 5, то $p + q$ або $p - q$ ділиться на 3 і, отже, $p^2 - q^2$ ділиться на 24. (Вказівка: $p + 2$ або $p - 2$ ділиться на 3 і $q - 2$ або $q + 2$ ділиться на 3.)

Означення 1.10. Нехай n – натуральне число. Ціле число a порівнянно із цілим числом b по модулю n, що позначається $a \equiv b(modn)$, якщо n ділить $(a - b)$.

Теорема 1.25. *Відношення $\equiv$ для фіксованого n є відношенням еквівалентності на множині цілих чисел. Це означає, що*

1. $a \equiv a(mod\ n)$ *для кожного цілого числа* a;
2. *якщо* $a \equiv b(modn)$, *то* $b \equiv a(modn)$ *для цілих чисел* a *і* b;
3. *якщо* $a \equiv b(modn)$ *і* $b \equiv c(modn)$, *то* $a \equiv c(modn)$.

Означення 1.11. Нехай n – натуральне число. Множина всіх класів еквівалентності по модулю n позначається Z_n і називається множиною класів лишків по модулю n.

Класи лишків по модулю n являють собою нові об'єкти. Вони є класами еквівалентності. Елементи кожного класу еквівалентності порівнянні між собою за модулем n. Наприклад, нехай $n = 3$. Маємо три класи еквівалентності по модулю 3, так що множина $Z_3 = \{[0], [1], [2]\}$ містить три елементи. Елементи Z_3 – класи еквівалентності, тобто множини. Ці три множини містять 0, 1 і 2, відповідно, як свої імена. У кожному із цих класів еквівалентності всі елементи порівнянні між собою по модулю 3, так що $a = b(mod3)$ тоді й тільки тоді, коли a і b належать тому самому класу еквівалентності – класу лишків. Таким чином,

$$[0] = ... - 6, -3, 0, 3, 6, 9...;$$

$$[1] = ... - 8, -5, -2, 1, 4, 7...;$$

$$[2] = ... - 7, -4, -1, 2, 5, 8....$$

Тепер нам потрібно визначити операції між класами лишків по модулю n. Відношення порівнянності $\equiv$, як підказує саме позначення, має багато спільного з загальним відношенням рівності. Але з відношенням рівності по модулю n зв'язано більше обмежень, чим з аналогічним йому відношенням рівності.

Теорема 1.26. *Відношення порівнянності має наступні властивості:*

а) *якщо* $a \equiv b(modn)$ *і* $c \equiv d(modn)$, *то* $a + c \equiv b + d(modn)$ *і* $ac = bd(modn)$;

b) *якщо* $a \equiv b(modmn)$, *то* $a \equiv b(modm)$ *і* $a \equiv b(modn)$.

Доведення. Ми доведемо пункт (а); частину (б) пропонуємо довести читачу. За означенням, якщо $a \equiv b(modn)$ і $c \equiv d(modn)$, то $a - b = un$ і $c - d = vn$ для деяких цілих чисел u і v. Таким чином, $(a + c) - (b + d) = (a - b) + (c - d) = u \cdot n + v \cdot n = (u + v) \cdot n$ для деяких цілих чисел u і v, і $a + c \equiv b + d(modn)$. Крім того, $a = b + un$ і $c = d + vn$, так що

$$ac = (b+(un))(d+(vn)) = bd+b(vn)+d(un)+uvn^2 = bd+(bv+ud+uvn)n.$$

Таким чином, $ac - bd = (bv + ud + vun)n$ і $ac = bd(modn)$. □

Приклад 1.6. Нехай $n = 3$.

$$1 \equiv 7(mod3),$$

$$2 \equiv -4(mod3).$$

З теореми 1.26 (а) слідує, що $1 + 2 \equiv 7 + (-4)(mod3)$, а також, що $(1)(2) \equiv (7)(-4)(mod3)$, що вірно, оскільки $2 - (-28) = 30 = 3 \cdot 10 = 3 \cdot k$

Теорема 1.27. *Для довільного натурального числа* n,

a) *якщо* $r = r'(modn)$, $0 \leq r < n$ *і* $0 \leq r' < n$, *то* $r = r'$;

b) *якщо* a *– будь-яке ціле число і* n *- натуральне число, то існує ціле число* r, *де* $0 \leq r < n$ *таке, що* $a \equiv r(modn)$. *Ціле число* r *– остача від ділення* a *на* n, *тому* $a = nq + r$.

Доведення. Твердження теореми випливають безпосередньо з алгоритму ділення.

Частина (а) твердження теореми гарантує, що класи лишків по модулю n володіють тією властивістю, що класи лишків, породжені невід'ємними цілими числами, меншими, ніж n, різні. Таким чином, [0], [1], [2], ..., $[n-2]$, $[n-1]$ – різні множини щодо порівнянності по модулю n.

Частина (б) показує, що кожне ціле число a порівнянне по модулю n з одним із цілих чисел 0, 1, 2, ... , $n-1$. Отже, будь-яке ціле число a належить одному з n різних класів еквівалентності [0], [1], ..., $[n-1]$. □

Проведене доведення служить поясненням до наступної теореми.

Теорема 1.28. *Нехай* n *– довільне натуральне число. Тоді* Z_n, *множина класів лишків по модулю* n, *складається точно з* n *різних класів лишків* [0], [1], [2], ..., $[n-1]$, *представлених різними лишками, які можуть бути отримані при діленні на* n. *Крім того, для* $0 \leq r < n$, *клас лишків* $[r]$ *складається точно з тих цілих чисел* a, *для яких* $a \equiv r(modn)$.

Наступна теорема є простим наслідком попередніх теорем, які, проте, часто виявляються корисними.

Теорема 1.29. *Якщо* $a = nq + r$ *і* $b = nq' + r'$ *для* $0 \leq r < n$ *і* $0 \leq r' < n$, *то* $r = r'$ *тоді й тільки тоді, коли* $a \equiv b(modn)$.

У цілому, при роботі із класами лишків по модулю n бажано для його подання вибрати в класі найменше невід'ємне ціле число. Це особливо важливо для додавання й множення класів лишків в Z_n, оскільки необхідно, щоб сума і добуток усе ще представлялися цілими числами, які перебувають між 0 і n-1. Це призводить до наступного означення.

Означення 1.12. . Нехай Z_n – множина класів лишків по модулю n. Для будь-якого заданого цілого числа m існує ціле число r таке, що $0 \leq r \leq n-1$ і $[m] = [r]$ або $m \equiv r(modn)$. При цьому говорять, що $[[m]]_n = r$.

Приклад 1.7. Для $n = 5$ одержуємо $Z_5 = \{[0], [2], [3], [4]\} = \{[r] : 0 \leq r < 5\}$.

На множині Z_n можна визначити операції додавання й множення. Якщо [] – клас лишків по модулю n, що містить a, і $[b]$ – клас лишків по модулю n, що містить b, то додавання й множення визначимо співвідношеннями

$$[a] \oplus [b] = [a + b] = [[a + b]]_n,$$

$$[a] \odot [b] = [a \cdot b] = [[a \cdot b]]_n,$$

де додавання й множення в центрі й праворуч здійснюється між цілими числами, а додавання й множення ліворуч виконується між класами еквівалентності. Використання попередньої теореми показує, що операції додавання й множення таких класів еквівалентності – класів лишків - визначені правильно; тобто визначення не залежить від представників класів лишків. Наприклад, якщо $[a] = [c]$, то результат додавання не повинен залежати від того, використовуємо ми $[a]$ або $[c]$. Інакше кажучи, якщо $[a] = [c]$ і $[b] = [d]$, то $[a] \oplus [b] = [c] \oplus [d]$ і $[a] \odot [b] = [c] \odot [d]$.

Приклад 1.8. Для $n = 5$ і $Z_5 = \{[0], [1], [2], [3], [4]\}$ знаходимо, що $[2] \oplus [4] = [2 + 4] = [6] = [1]$, оскільки $6 \equiv 1(mod5)$; $[2] \odot [4] = [2 \cdot 4] = [8] = [3]$, оскільки $8 \equiv 3(mod5)$.

Обчислюючи всі можливі суми й добутки, можна створити таблиці "додавання"і "множення"для класів лишків по модулю 5.

$[a] \oplus [b]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[2]$	$[0]$	$[2]$	$[4]$	$[1]$	$[3]$
$[3]$	$[0]$	$[3]$	$[1]$	$[4]$	$[2]$
$[4]$	$[0]$	$[4]$	$[3]$	$[2]$	$[1]$

Рис. 1.6:
Таблиці "додавання"і "множення"для класів лишків по модулю 5

Теорема 1.28 показує, що для довільного натурального числа n множина цілих чисел може бути розбита на n непересічних множин, або класів еквівалентності. Надалі ми часто будемо вертатися до цих множин, цікавлячись їхніми представниками.

Означення 1.13. . Якщо $b \equiv r(modn)$ для натурального числа n, то говорять, що r є лишком числа b по модулю n. Повна система лишків по модулю n є множина $S = \{r_1, r_2, ..., r_n\}$, де переріз множини S з кожним класом лишків по модулю n містить точно одне ціле число, тобто S містить одного й тільки одного представника з кожного такого класу лишків. Повна система лишків $0, 1, 2, ..., (n-1)$ називається первинною системою лишків. Якщо b – ціле число, $b \equiv r(modn)$ і $0 \leq r \leq n-1$, то цей єдиний первинний лишок по модулю n позначається через $r = [[b]]_n$. Зведена система лишків по модулю n є підмножиною повної системи лишків, що складається тільки з тих цілих чисел, які є взаємно простими з n, НОД$(r, n) = N$ тобто $\{r : r \in S,\ N = 1\}$.

Повна система лишків виходить шляхом вибору одного цілого числа з кожного класу лишків $[0], [1], ..., [n-1]$ множини Z_n. Отже, для $n = 6$, $\{24, 7, -58, 40, 113\}$ – повна система лишків по модулю 6, тому що $24 \equiv 0(mod6)$, тому $24 \in [0]$;
$7 \equiv 1(mod6)$, тому $7 \in [1]$;
$-58 \equiv 2(mod6)$, тому $-58 \in [2]$;
$15 \equiv 3(mod6)$, тому $15 \in [3]$;
$40 \equiv 4(mod6)$, тому $40 \in [4]$;
$113 \equiv 5(mod6)$, тому $113 \in [5]$.

Очевидно, що $\{0, 1, 2, 3, 4, 5\}$ є повною (і при тому первинною) системою лишків по модулю 6. За означенням, $[[24]]_6 = 0$ і $[[-58]]_6 = 2$.

Оскільки всі елементи будь-якого класу лишків по модулю n порівнянні один з іншим, але не є такими стосовно елементів іншого класу лишків, кожне ціле число порівнянне рівно з одним елементом повної системи лишків. Проведені міркування приводять до наступної теореми.

Теорема 1.30. *Якщо n – натуральне число, $\{r_1, r_2, ..., r_n\}$ – повна система лишків по модулю n і a - деяке ціле число, то $a \equiv r_k (mod n)$ для одного й тільки одного k, $1 \leq k \leq n$.*

Елементи повної системи лишків $\{24, 7, -58, 15, 40, 113\}$ і первинної (повної) системи лишків $\{0, 1, 2, 3, 4, 5\}$ по модулю 6, які є взаємно простими з $n = 6$, містять у собі, відповідно, множини $\{7, 113\}$ і $\{1, 5\}$. Тому обидві останні множини є зведеними системами лишків по модулю 6. При цьому говорять, що $\{1, 5\}$ є первинною зведеною системою лишків по модулю 6.

Наступна теорема показує, що зведена система лишків містить більше істотної інформації про цілі числа з $\mathbb{Z}$, ніж система чисел, взаємно простих з n. Доведення теореми надається читачеві.

Теорема 1.31. *Нехай n – натуральне число і $r_1, r_2, ..., r_k$ – зведена система лишків по модулю n. Якщо a – ціле число, взаємно просте з n, то $a \equiv r_j (mod n)$ для одного і тільки одного j, $1 \leq j \leq k$.*

Якщо дана одна система лишків, є кілька способів відтворити інші системи лишків. Один зі способів складається з додавання одного і того ж цілого числа до кожного з лишків в повній системі лишків. Інший спосіб демонструє наступна теорема. Доведення надається читачеві.

Теорема 1.32. *Нехай n – натуральне число і $\{r_1, r_2, ..., r_k\}$ – повна [зведена] система лишків по модулю n. Якщо a – ціле число, взаємно просте з n, то $\{ar_1, ar_2, ..., ar_k\}$ – також повна [зведена] система лишків.*

Оскільки НСД (6 ,35) = 1, маючи повну систему лишків $\{0, 1, 2, 3, 4, 5\}$ і зведену систему лишків $\{1, 5\}$ по модулю 6, одержуємо, що $\{35 \cdot 0, 35 \cdot 1, 35 \cdot 2, 35 \cdot 3, 35 \cdot 4, 35 \cdot 5\}$ і $\{35 \cdot 1, 35 \cdot 5\}$ є, відповідно, повною і зведеною системами лишків. Але

$$[[0]]_6 = 0,\ [[35 \cdot 0]]_6 = [[0]]_6 = 0;$$

$$[[1]]_6 = 1,\ [[35 \cdot 1]]_6 = [[35]]_6 = 5;$$

$$[[2]]_6 = 2,\ [[35 \cdot 2]]_6 = [[70]]_6 = 4;$$

$$[[3]]_6 = 3,\ [[35 \cdot 3]]_6 = [[107]]_6 = 3;$$

$$[[4]]_6 = 4,\ [[35 \cdot 4]]_6 = [[140]]_6 = 2;$$

$$[[5]]_6 = 5,\ [[35 \cdot 5]]_6 = [[175]]_6 = 1;$$

Таким чином, у результаті множення кожного елемента r_i повної або зведенної системи лишків по модулю n на ціле число a, взаємно просте з n,

одержуємо представників тих же класів лишків, можливо, в іншому порядку.

Вправи

1. Обчисліть а) $[[37]]_4$; б) $[[93]]_5$; в) $[[48]]_{23}$; г) $[[149]]_{27}$;
2. Обчисліть а) $[[33]]_4$; б) $[[47]]_9$; в) $[[49]]_{17}$; г) $[[146]]_{23}$;
3. Обчисліть а) $[[8!]]_6$; б) $[[1+2+3+4+5+6+7+8+9+10]]_3$; в) $[[1^2+2^2+3^2+...25^2]]_2$; г) $[[146^2]]_{21}$.
4. Покажіть, що з $a^2 \equiv b^2(modn)$ не слідує $\equiv b(modn)$.
5. Покажіть, що якщо a – непарне ціле число, то $a^2 \equiv 1(mod8)$.
6. Побудуйте таблицю додавання для класів лишків по модулю 4.
7. Побудуйте таблицю множення для класів лишків по модулю 4.
8. Побудуйте таблицю додавання для класів лишків по модулю 7.
9. Побудуйте таблицю множення для класів лишків по модулю 7.
10. Використовуючи таблиці додавання і множення для класів лишків по модулю 5, наведені раніше, знайдіть в Z_5 розв'язки наступних рівнянь: а)$x+[3]=[5]$; б) $[3]\cdot x=[2]$; в)$[4]\cdot x=[3]$; г)$[2]\cdot x=[1]$.
11. Використовуючи таблиці додавання й множення для класів лишків по модулю 4 з наведених вище вправ, знайдіть в Z_4 рішення наступних рівнянь: а) $X+[3]=[2]$; б) $[3]\cdot x=[2]$; в) $[2]\cdot x=[2]$; г) $[2]\cdot x=[0]$.
12. Використовуючи таблиці додавання і множення для класів лишків по модулю 7 з наведених вище вправ, знайдіть в Z_7 рішення наступних рівнянь: а) $x+[5]=[2]$; б) $[3]\cdot x=[4]$; в) $[2]\cdot x=[5]$; г) $[4]\cdot x=[6]$.
13. Доведіть, що якщо $a \equiv b(modmn)$, то $a \equiv b(modm)$ і $a \equiv b(modn)$.
14. Доведіть, що якщо $a \equiv bc(modn)$ і цілі числа c та n – взаємно прості, то $a \equiv b(modn)$.
15. Доведіть теорему 1.31.
16. Доведіть теорему 1.32.

ЧАСТИНА 2
Теорія чисел

2.1. Решето Ератосфена

Як відомо, алгоритм являє собою кінцеву множину правил для чисто механічного рішення задач. Першим прикладом алгоритму в теорії чисел буде древній метод знаходження простих чисел, названий "решетом Ератосфена що являє собою алгоритм визначення простих чисел, менших заданого цілого числа. Проілюструємо цей метод, визначаючи прості числа в інтервалі від 1 до 100. Насамперед, перелічимо цілі числа від 1 до 100:
1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20,
21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40,
41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60,
61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80,
81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100.
Починаючи з 2, що є першим простим числом, виділимо жирним шрифтом всі числа, кратні 2. Ця процедура дуже проста, тому що відзначеним повинне бути кожне друге ціле число, більше 2.
1, **2**, 3, **4**, 5, **6**, 7, **8**, 9, **10**, 11 **12**, 13, **14**, 15, **16**, 17, **18**, 19, **20**,
21, **22**, 23, **24**, 25, **26**, 27, **28**, 29, **30**, 31, **32**, 33, **34**, 35, **36**, 37, **38**, 39, **40**,
41, **42**, 43, **44**, 45, **46**, 47, **48**, 49, **50**, 51, **52**, 53, **54**, 55, **56**, 57, **58**, 59, **60**,
61, **62**, 63, **64**, 65, **66**, 67, **68**, 69, **70**, 71, **72**, 73, **74**, 75, **76**, 11, **78**, 79, **80**,
81, **82**, 83, **84**, 85, **86**, 87, **88**, 89, **90**, 91, **92**, 93, **94**, 95, **96**, 97, **98**, 99, **100**

Наступне просте число дорівнює 3. Продовжуючи процедуру, відзначимо всі числа, кратні 3. Ця процедура також є простою, тому що повинне бути відзначено кожне третє ціле число, більше 3.
1, **2**, **3**, **4**, 5, **6**, 7, **8**, **9**, **10**, 11 **12**, 13, **14**, **15**, **16**, 17, **18**, 19, **20**,
21, **22**, 23, **24**, 25, **26**, **27**, **28**, 29, **30**, 31, **32**, **33**, **34**, 35, **36**, 37, **38**, **39**, **40**,
41, **42**, 43, **44**, **45**, **46**, 47, **48**, 49, **50**, **51**, **52**, 53, **54**, 55, **56**, **57**, **58**, 59, **60**,
61, **62**, **63**, **64**, 65, **66**, 67, **68**, **69**, **70**, 71, **72**, 73, **74**, **75**, **76**, 77, **78**, 79, **80**,
81, **82**, 83, **84**, 85, **86**, **87**, **88**, 89, **90**, 91, **92**, **93**, **94**, 95, **96**, 97, **98**, **99**, **100**.

Тепер відзначаємо всі числа, кратні простому числу 5.
1, **2**, **3**, **4**, **5**, **6**, 7, **8**, **9**, **10**, 11 **12**, 13, **14**, **15**, **16**, 17, **18**, 19, **20**,
21, **22**, 23, **24**, **25**, **26**, **27**, **28**, 29, **30**, 31, **32**, **33**, **34**, **35**, **36**, 37, **38**, **39**, **40**,
41, **42**, 43, **44**, **45**, **46**, 47, **48**, 49, **50**, **51**, **52**, 53, **54**, **55**, **56**, **57**, **58**, 59, **60**,
61, **62**, **63**, **64**, **65**, **66**, 67, **68**, **69**, **70**, 71, **72**, 73, **74**, **75**, **76**, 77, **78**, 79, **80**,
81, **82**, 83, **84**, **85**, **86**, **87**, **88**, 89, **90**, 91, **92**, **93**, **94**, 95, **96**, 97, **98**, **99**, **100**.

Далі відзначаємо всі числа, кратні простому числу 7.

1, **2**, **3**, **4**, **5**, **6**, 7, **8**, **9**, **10**, 11 **12**, 13, **14**, **15**, **16**, 17, **18**, 19, **20**, **21**, **22**, 23, **24**, **25**, **26**, **27**, **28**, 29, **30**, 31, **32**, **33**, **34**, **35**, **36**, 37, **38**, **39**, **40**, 41, **42**, 43, **44**, **45**, **46**, 47, **48**, **49**, **50**, **51**, **52**, 53, **54**, **55**, **56**, **57**, **58**, 59, **60**, 61, **62**, **63**, **64**, **65**, **66**, 67, **68**, **69**, **70**, 71, **72**, 73, **74**, **75**, **76**, 77, **78**, 79, **80**, **81**, **82**, 83, **84**, **85**, **86**, **87**, **88**, 89, **90**, **91**, **92**, **93**, **94**, 95, **96**, 97, **98**, **99**, **100**.

Оскільки 7 – найбільше просте число, квадрат якого менше або дорівнює 100, по теоремі 1.20 продовжувати процес немає необхідності. Числа, більші 1 і не відзначені жирним шрифтом, являють собою прості числа, які не перевищують 100.

Вправи

1. Побудуйте решето Ератосфена для натуральних чисел, менших 200.
2. Використовуйте решето Ератосфена й калькулятор для розкладання на прості множники числа 1726.
3. Використовуйте решето Ератосфена й калькулятор для розкладання на прості множники числа 481.
4. Використовуйте решето Ератосфена й калькулятор для розкладання на прості множники числа 2502.
5. Використовуйте решето Ератосфена й калькулятор для розкладання на прості множники числа 1739.
6. Використовуйте решето Ератосфена й калькулятор для розкладання на прості множники числа 391.
7. Використовуйте решето Ератосфена й калькулятор для розкладання на прості множники числа 3901.

2.2. Метод виділення множників Ферма

Наступна теорема є основою алгоритму розкладання на прості множники, названого методом виділення множників Ферма. Метод використовується для визначення того, чи є число простим.

Теорема 2.1. *Ціле непарне число $n > 1$ не є простим тоді й тільки тоді, коли існують невід'ємні цілі числа p і q такі, що $n = p^2 - q^2$, і при цьому $p - q > 1$.*

Доведення. Очевидно, якщо n можна представити як різницю квадратів двох невід'ємних цілих чисел, скажемо, $n = p^2 - q^2$, тоді $n = (p-q)(p+q)$. Оскільки $-q > 1$, то також $+q > 1$; і n не є простим числом.

Обернено, якщо $n = rs$, де $r \geq s > 1$, тоді n можна представити як $((r+s)/2)^2 - ((r-s)/2)^2$. Оскільки n непарне, r і s також є непарними і, отже, $r+s$ і $r-s$ – парні числа. Поклавши $p = (r+s)/2$ і $q = (r-s)/2$, знаходимо, що і q - цілі невід'ємні числа і $-q = s > 1$. При $n = 1$ покладемо $= 1$, а $q = 0$. □

Застосування цього методу грунтується на спробі знайти цілі числа і q такі, що $n = p^2 - q^2$ або, що еквівалентно, $n + q^2 = p^2$, або $q^2 = p^2 - n$. Якщо використовується перше рівняння, отримаємо $q = 1, 2, ...$ доти, поки $n + q^2$ не стане повним квадратом. Якщо значення $q = (n-1)/2$ повний квадрат не досягнуть, розглянемо ситуацію, коли $q = (n-1)/2$, що дає $n + q^2 = ((n+1)/2)^2$ і приводить до розкладання n на множники $n \cdot 1$. Оскільки q має вигляд $(r-s)/2$, де r і s – дільники n, то очевидно, що q не може перевищити $(n-1)/2$. Отже, якщо до значення $q = (n-1)/2$ повний квадрат не досягнуть, число n є простим.

При використанні другого рівняння, тобто $q^2 = p^2 - n$, беремо в якості m найменше ціле число таке, що $m^2 \geq n$, і послідовно маємо, $p = m$, $m+1$, ... доти, поки $p^2 - n$ не стане повним квадратом. Як і колись, q не може перевищити $(n-1)/2$, тому якщо до значення $p = (n+1)/2$ повний квадрат не отриманий, число n є простим. Перевага використання другого співвідношення полягає в тому, що перевірці на повний квадрат підлягає менша кількість чисел.

Наприклад, розглянемо застосування запису $p^2 = n + q^2$ для перевірки, є чи простим число $n = 527$. Розглянемо $q = 1, 2, ..., (n-1)/2$.

q	$n + q^2$
1	$527 + 1 = 528$
2	$527 + 4 = 531$
3	$527 + 9 = 536$
4	$527 + 16 = 543$
5	$527 + 25 = 552$
6	$527 + 36 = 563$
7	$527 + 49 = 576 = (24)^2$

Рис. 2.1:
Таблиці "додавання"і "множення"для класів лишків по модулю 5

Отже, $n = 527$ є складеним, і його дільники легко обчислюються: $527 \stackrel{37}{=} (24)^2 - 7^2 = (24-7)(24+7) = 17 \cdot 31$. Рішення питання про те, чи є число n простим, не завжди вимагає перевірки для всіх значень q від 1 до $(n-1)/2$.

Вправи

Скориставшись методом виділення множників Ферма, визначте, чи є наступні числа простими. a)1001; b)1349; c)4851; d)1079; e)8051; f)567; g)7931.

2.3. Алгоритм ділення і алгоритм Евкліда

Раніше була доведена теорема, названа алгоритмом ділення. Теорема говорила, що для додатніх цілих чисел a і b існують єдині невід'ємні числа q і r такі, що $0 \leq r < b$ і $a = bq + r$. Це твердження не є алгоритмом, але алгоритми для знаходження q і r існують. Якщо числа a і b великі, число q можна "вгадати". Якщо помножити b на q і результат занадто великий, треба q замінити на $q-1$ і повторювати процес, поки не одержимо $bq \leq a$, після чого покласти $r = -bq$. Однак, якщо $bq < a$, але $a - bq \geq b$, то треба замінити q на $q+1$ і повторювати процес, поки не одержимо $a - bq < b$, після чого покласти $r = a - bq$. Більш системно метод описується наступним чином:

1. Покласти $q = 1$ і $r = a - bq$.
2. Якщо $r \geq b$, покласти $q = q + 1$ і $r = a - bq$.
3. Продовжувати процес, доки $r < b$.

Викладене являє собою алгоритм знаходження найбільшого спільного дільника великих чисел, названий алгоритмом Евкліда. Знаходження найбільшого спільного дільника необхідно при додаванні дробів, а також при розв'язанні рівнянь у цілих числах.

Теорема 2.2. *Допустимо, що a і b – додатні цілі числа, і послідовне застосування алгоритму ділення приводить до послідовності наступного виду:*

$$\begin{aligned} a &= bq_0 + r_0 \quad 0 \leq r_0 < b \\ b &= r_0 q_1 + r_1 \quad 0 \leq r_1 < r_0 \\ r_0 &= r_1 q_2 + r_2 \quad 0 \leq r_2 < r_1 3 \\ r_1 &= r_2 q_3 + r_3 \quad 0 \leq r_3 < r_2 \\ r_2 &= r_3 q_3 + r_3 \quad 0 \leq r_4 < r_3 \end{aligned}$$

$$\vdots$$

$$r_k = r_{k+1}q_{k+2} + r_{k+2} \quad 0 \le r_{k+2} < r_{k+1}$$

$$\vdots$$

Існує $r_k = 0$. Нехай s – перше ціле число таке, що $r_s = 0$. Тоді r_{s-1} = НСД(a, b), якщо $s > 0$, і b = НСД(a, b), якщо $s = 0$.

Доведення. Нехай $S = \{r_1, r_2, \ldots\}$. Якщо $r_1 = 0$, тоді результат очевидний, тому припустимо, що $r_0 > 0$. Відповідно до принципу повного впорядкування множина S містить найменше додатнє ціле число, скажемо, r_i. Але $0 \le r_{i+1} < r_i$, і тому $r_{i+1} = 0$. Покладемо $s = i + 1$. По теоремі 1.16 НСД(a, b) = НСД(b,r_0) = НСД(r_0,r_1) = ... = НСД(r_{s-1},r_s) але оскільки $r_s = 0$, НСД(r_{s-1}, r_s) = r_{s-1}, так що НСД (a, b) = r_{s-1}. □

Приклад 2.1. Використовуючи алгоритм Евкліда для знаходження НСД(203,91), діємо у такий спосіб. Спочатку ділимо 203 на 91 націло й одержуємо

$$203 = 91 \cdot 2 + 21;$$

$$a = b \cdot q_0 + r_0.$$

Тепер ділимо 91 на остачу 21 націло:

$$91 = 21 \cdot 4 + 7;$$

$$b = r_0 \cdot q_1 + r_1.$$

Розділяючи 21 на 7 націло, одержуємо

$$21 = 7 \cdot 3 + 0;$$

$$r_0 = r_1 \cdot q_2 + r_2.$$

Отже, $s = 2$ і НСД(203,91)=НСД(91,21)=НСД(21,7)=7=$r_{s-1} = r_1$.

Приклад 2.2. Знайти НСД(99,205). Діючи вищевказаним образом, ділимо 205 на 99 націло, одержимо

$$205 = 99 \cdot 2 + 7.$$

Тепер ділимо 99 націло на остачу 7, одержимо

$$99 = 7 \cdot 14 + 1.$$

Далі ділимо 7 на 1 і одержуємо

$$7 = 1 \cdot 7 + 0.$$

Таким чином, НСД(99,205)=1.

Алгоритм Евкліда дозволяє знаходити такі значення u і v, що НСД(a, b)$=r_t$, $av + vb$=НСД(a,b). Використовуючи позначення теореми 2.2, запишемо $r_{t-2} = r_{t-1} \cdot q_t + r_t$. Звідси $r_t = r_{t-2} - r_{t-1} \cdot q_t$. Аналогічно, $r_{t-1} = r_{t-3} - r_{t-2} \cdot q_{t-1}$. Підстановка в попереднє рівняння дає

$$r_t = r_{t-2} - (r_{t-3} - r_{t-2} \cdot q_{t-1}) \cdot q_t.$$

Аналогічним чином можна виразити r_{t-2} через r_{t-3} і r_{t-4} і, підставивши в попереднє рівняння, виключити r_{t-2}. Продовжуючи в тому ж дусі, можна виключити усі r_i і повернутися назад до a і b, одержавши НСД(a, b) у вигляді $ua + vb$.

Приклад 2.3. Виразити НСД(85,34) у вигляді 85u + 34v;. Для використання алгоритму Евкліда спочатку розділимо 85 на 34 націло: $85 = 34 \cdot 2 + 17$. Розділяючи 34 на 17 націло, одержуємо $34 = 17 \cdot 1 + 0$. Таким чином, НСД(85,34) = 17 і НСД(85,34) = 17 = (85)(1) + (34)(-2).

Приклад 2.4. Виразити НСД (252,580) у вигляді $252u + 580v$. Ділимо 580 на 252 націло, одержимо

$$580 = 252 \cdot 2 + 76;$$

$$a = b \cdot q_0 + r_0.$$

Зараз ділимо 252 націло на 76:

$$252 = 76 \cdot 3 + 24;$$

$$b = r_0 \cdot q_1 + r_1.$$

Продовжуючи процес, одержимо

$$76 = 24 \cdot 3 + 4;$$

$$r_0 = r_1 \cdot q_2 + r_2$$

і

$$24 = 4 \cdot 6 + 0;$$

$$r_1 = r_2 q_3 + r_3.$$

Зворотна підстановка дає

$$4 = \mathbf{76} - \mathbf{24} \cdot 3 = \mathbf{76} - [\mathbf{252} - \mathbf{76} \ \cdot 3] \cdot 3 = \mathbf{76} \cdot 10 + \mathbf{252} \cdot (-3) =$$

$$= [\mathbf{580} - \mathbf{252} \cdot 2]10 + \mathbf{252} \cdot (-3) = \mathbf{580} \cdot 104 - \mathbf{252} \cdot (-23),$$

де r_i виділені підкресленням.

Приклад 2.5. Виразити НСД(252,576) у вигляді $252u - 576v$. Спочатку розділимо 576 на 252 націло:

$$576 = 252 \cdot 2 + 72.$$

Зараз розділимо 252 націло на 72:

$$252 = 72 \cdot 3 + 36.$$

Після зворотної підстановки одержуємо

$$36 = 252 - 72 \cdot 3 = 252 - [576 - 252 \cdot 2] \cdot 3 = (7)(252) + (-3)(576).$$

У прикладі 2.1 показано, що НСД(91,203)=7. Якщо розділити числа 91 і 203 на їх найбільший загальний дільник 7, одержимо 91/7=13 і 203/7= 29. Легко бачити, що цілі числа 13 і 29 - взаємно прості; тобто НСД(13,29) = 1. Таким чином, виявилося, що результати ділення двох цілих чисел на їх найбільший спільний дільник не мають спільних дільників, за винятком 1. Доведення наступної теореми надаємо читачу.

Теорема 2.3. *Нехай задані цілі числа a і b, не рівні нулю, тоді числа a/НСД(a,b) і b/НСД(a,b) є взаємно простими, тобто НСД (a/НСД(a,b), b/НСД(a,b))=1.*

Було визначено раніше, що натуральне число m являє собою найменше спільне кратне цілих чисел a і b за умови, що (а) $a|m$ і $b|m$, і (б) якщо n – будь-яке спільне кратне чисел a і b, то $m|n$. Найменше спільне кратне чисел a і b позначимо НСК(a,b). Необхідно побудувати алгоритм знаходження найменшого спільного кратного двох цілих чисел. Ціль досягається визначенням найбільшого спільного дільника цих чисел (алгоритм знаходження якого вже є) і використанням у теоремі 1.24. Зазначена теорема затверджує, що длянатуральних чисел a і b НСД(a,b·НСК(a,b)=ab. Для знаходження НСК(91,203) спочатку визначимо НСД(91,203), скориставшись алгоритмом Евкліда, як це було зроблено раніше, а потім розділимо на його добуток чисел 91 і 203. Оскільки НСД(91,203)=7, знаходимо НСК(91,203) = (91)(203)/7 = 2639.

Вправи

1. Задано алгоритм ділення $a = bq + r$. Знайдіть q і r для зазначених нижче значень a і b: а) a = 75, b = 8; б) a = 102, b = 5; в) a = 81, b = 9; г) a = 16, b= 25.

2. Знайдіть найбільший спільний дільник для наступних пар чисел: а) 75, 25; б) 27, 18; в) 621, 437; г) 289, 377; д) 822, 436.

3. Знайдіть найменше спільне кратне для пар чисел із вправи 2.

4. Для наведених нижче пар чисел a і b знайдіть u, v і d такі, що $au+bv = d$, де d – найбільший спільний дільник чисел a і b: а) 83,17; б) 361,418; в) 25,15; г) 81,9; д) 216,324.

5. Доведіть, що якщо НСД(a,b) виражений як $ax + by$, то x і y - взаємно прості числа.

6. Доведіть, що для цілих чисел a і b, не рівних нулю, a/НСД(a,b) і b/НСД(a,b) – взаємно прості, тобто НСД(a/НСД(a,b),b/НСД(a,b))=1 (теорема 2.3).

7. Задано ціле число a і натуральне число b. Доведіть, що цілі числа, добуток яких дорівнює b і найбільший спільний дільник яких дорівнює b, існують тоді й тільки тоді, коли $b^2|a$.

8. Припускаючи, що $F(k) = 2^{2^k} + 1$ при $k \geq 0$,

   a) доведіть, що $F(m+1) = F(0)F(1)F(3)\ldots F(m) + 2$ для кожного $m \geq 0$;

   b) доведіть, що $F(m)$ і $F(n)$ – взаємно прості числа, якщо $m \neq n$

9. Покажіть, що якщо НСД(a,b) виражений як $ax + by$, то x і y не визначаються єдиним образом.

10. Доведіть, що якщо НСД(a,b) = 1, то НСД(a+nb,b)=1.

11. Доведіть, що n·НСД(a,b) = НСД(na,nb).

12. Нехай S – множина всіх цілих чисел виду $ax + by$. Покажіть, що НСД(a,b) ділить всі елементи множини S.

2.4. Ланцюгові дроби

У даній главі алгоритм ділення і алгоритм Евкліда будуть застосовуватися достатньо часто. Розглянемо спочатку раціональні числа $\frac{a}{b}$, де a і b – цілі числа і $b > 0$. Якщо алгоритм ділення застосований до цілих чисел a і b, де $b > 0$, то існують єдині цілі числа t (частка) і r (остача) такі, що

$$a = bt + r$$

при

$$0 \leq r < b.$$

Для a = -124 і b = 35 маємо -124=(35)(-4)+16. Переписавши останні дві рівності й перейшовши до раціональних чисел, одержуємо

$$\frac{a}{b} = t + \frac{r}{b}$$

і

$$-\frac{124}{35} = -4 + \frac{16}{35}.$$

Скориставшись функцією цілої частини числа, відношення можемо переписати в такому вигляді $\frac{a}{b} = t$ і $\left[-\frac{124}{35}\right] = -4$, при цьому дробова остача $\frac{r}{b}$ має властивість $0 \leq \frac{r}{b} < 1$.

Якщо $r \neq 0$, рівності можна переписати наступним чином:

$$\frac{a}{b} = t + \frac{1}{b/r}$$

і

$$-\frac{124}{35} = -4 + \frac{1}{35/16},$$

де $b/r > 1$. Алгоритм ділення можна застосувати знову і одержати $b = rt' + r'$ і $35 = (16)(2) + 3$. Таким чином, обертаючи дробову остачу й застосовуючи алгоритм ділення знову й знову зазначеним способом, одержуємо вираз раціонального числа $--\frac{124}{35}$:

$$-\frac{124}{35} = -4 + \frac{16}{35} = -4 + \frac{1}{35/16} = -4 + \frac{1}{2 + \frac{3}{16}} =$$

$$= -4 + \frac{1}{2 + \frac{1}{\left(\frac{16}{3}\right)}} = -4 + \frac{1}{2 + \frac{1}{\left(5 + \frac{1}{3}\right)}}.$$

Оскільки дріб $\frac{1}{3}$ має чисельником 1, не можна далі скорочувати $\frac{3}{1}$, використовуючи алгоритм ділення. Вираз

$$-4 + \frac{1}{2 + \frac{1}{\left(5 + \frac{1}{3}\right)}}$$

називається ланцюговим дробом і являє собою альтернативний спосіб запису раціонального числа $-\frac{124}{35}$. У зв'язку з тим, що ланцюговий дріб має регулярну структуру й чисельники завжди рівні 1, для точного завдання ланцюгового дробу необхідно згадати тільки числа -4, 2, 5 і 3, тому запишемо

$$-\frac{124}{35} = [-4; 2, 5, 3].$$

Числа -4, 2, 5 і 3 називаються елементами ланцюгового дробу або неповних часток, оскільки вони породжені алгоритмом ділення. Крапкою з комою відзначають особливу природу першого члена -4. Наприклад,

$$[3; 7] = 3 + \frac{1}{7} = \frac{22}{7},$$

але

$$[0; 3, 7] = 0 + \frac{1}{3} + \frac{1}{7} = \frac{7}{22}.$$

Вертаючись до ланцюгового дробу $- - \frac{124}{35} = [-4; 2, 5, 3]$, зауважуємо, що $-3 = (3-3)+1 = (3-1)+\frac{1}{1}$. Таким чином, можна записати

$$-\frac{124}{35} = -4 + \cfrac{1}{2 + \cfrac{1}{5 + \cfrac{1}{2 + \cfrac{1}{1}}}}$$

так що запис $- - \frac{124}{35} = [-4; 2, 5, 2, 1]$ теж має місце, однак у ній на останньому кроці алгоритм ділення не використаний. Приклад підказує, що кожне раціональне число має два різних представлення у вигляді ланцюгового дробу з цілими числами як елементи: в одному представленні останній елемент більше 1, а в іншому – дорівнює 1.

Якщо x – дійсне, але не раціональне число, алгоритм ділення не застосуємо; однак, використовуючи функцію цілої частини, можна одержати подане x у вигляді ланцюгового дробу довжини n способом, аналогічним раціональному випадку. Таким чином, для дійсного, але не раціонального числа x, існує єдине число t_0, де $t_0 \leq x < t_0 + 1$ таке, що $t_0 = [x]$. Тоді

$$1 > y_1 = x - [x] = -t_0 > 0$$

є так званою дробовою частиною x. Якщо $x_1 = \frac{1}{y_1}$, тоді

$$x = [x] + y_1 = t_0 + y_1 = t_0 + \frac{1}{x_1}$$

і $x_1 > 1$. Нехай $t_1 = [x_1]$, $y_2 = x_1 - [x_1]$ і $x_2 = 1/y_2$, так що $y_2 > 0$. Тоді $x_1 = t_1 + 1/x_2$, де $x_2 > 0$. Сполучення цих рівностей дає:

$$x = t_0 + \frac{1}{x_1} = t_0 + \frac{1}{t_1 + \frac{1}{x_2}}.$$

Продовжуючи в тому ж напрямі, одержуємо

$$x = t_0 + \cfrac{1}{t_1 + \cfrac{1}{t_2 + \cfrac{1}{t_3 + \ldots + \cfrac{1}{t_{k-1} + \cfrac{1}{x_k}}}}}.$$

де t_i - ціле число для кожного i, $t_i > 0$ для $i \geq 1$, x_k - ірраціональне дійсне число і $x_k > 1$. Можна також записати

$$x = [t_0; t_1, t_2, t_3, \ldots, t_{k-1}, x_k].$$

Наприклад, нехай $x\sqrt{3} = 1.7320508\ldots$. Побудуємо подання числа x у вигляді ланцюгового дробу наступним чином:

$$t_0 = [x] = [\sqrt{3}] = 1$$

де

$$y_1 = x - [x] = x - t_0 = \sqrt{3} - 1;$$
$$x_1 = 1/y_1 = 1/(\sqrt{3} - 1) = (\sqrt{3} + 1)/2;$$
$$t_1 = [x_1] = 1,$$

де

$$y_2 = x_1 - [x_1] = x1 - t_1 = (\sqrt{3} + 1)/2 - 1 = (\sqrt{3} - 1)/2;$$
$$x_2 = 1/y_2 = 2/(\sqrt{3} - 1) = \sqrt{3} + 1;$$
$$t_2 = [x_2] = 2,$$

де

$$y_3 = x_2 - [x_2] = x_2 - t_2 = (\sqrt{3} + 1) - 2 = \sqrt{3} - 1;$$
$$x_3 = 1/y_3 = 1/(\sqrt{3} - 1) = (\sqrt{3} + 1)/2,$$

таким чином,

$$\sqrt{3} = [t_0; x_1] = [1; (\sqrt{3} + 1)/2] = [t_0; t_1, x_1] = [t_0; [t_1, x_1]] = [1; 1, (\sqrt{3} + 1)] =$$

$$= [t_0; t_1, t_2, x_2] = [t_0; t_1, [t_2, x_2]] = [1; 1, 2, (\sqrt{3}+1)/2].$$

Але оскільки $x_3 = x_1$ структура повторюється, тому

$$\sqrt{3} = [1; 1, 2, 1, 2, 1, 2, (\sqrt{3}+1)/2].$$

і т.д.

Звідси виводимо наступне рекурсивне визначення ланцюгового дробу.

Означення 2.1. Для скіняенної послідовності $t_0, t_1, t_2, t_3, \ldots, t_n$ дійсних чисел, де $n \geq 0$ і $t_i > 0$ для $i \geq 1$, визначимо скінченний ланцюгову дріб $[t_0; t_1, t_2, t_3, \ldots, t_n]$ наступним чином:

$$[t_0;] = t_0;$$

$$[t_0; t_1] = \left[t_0 + \frac{1}{t_1}\right];$$

$$[t_0; t_1, t_2, t_3., .., t_k]; = [t_0; [t_1, t_2, t_3, \ldots, t_k]$$

для $1 < k \leq n$. Числа t_0, t_1, t_2, t_3, $\ldots$, t_n називаються неповними частками, або елементами ланцюгового дробу. Ланцюговий дріб $[t_0;\ t_1,\ t_2,\ t_3,\ \ldots,\ t_n]$ називається простим, якщо t_i – ціле число для кожного i, тобто кожний елемент ланцюгового дробу є ціле число. Числа $[t_0;]$, $[t_0; t_1]$, $[t_0; t_1, t_2]$, $\ldots$, $[t_0; t_1, t_2, t_3, \ldots, t_k]$, $\ldots$ $[t_0; t_1, t_2, t_3, \ldots, t_n]$ називаються підхідними дробами ланцюгового дробу $[t_0; t_1, t_2, t_3, \ldots, t_n]$. $[t_0; t_1, t_2, t_3, \ldots, t_k]$, де є k-тий підхідний дріб при $0 \leq k \leq n$. Для зручності позначення запис $[t_0; t_1, t_2, t_3, \ldots, t_k]$, використаний при $k = 0$, буде означати $[t_0;]$. Будемо говорити, що два ланцюгові дроби $[t_0; t_1, t_2, t_3, \ldots, t_n]$ і $[b_0; b_1, b_2, b_3, \ldots, b_n]$ рівні почленно, якщо $n = m$ і $t_i = b_i$ при $0 \leq i \leq n$. Якщо x – дійсне число і $x = [t_0; t_1, t_2, t_3, \ldots, t_n]$ і тоді будемо говорити, що $[t_0; t_1, t_2, t_3, \ldots, t_n]$ є подання ланцюговим дробом числа x. Два подання називаються співпадаючими, або рівними, якщо вони рівні почленно.

Наступна теорема дає інший спосіб розкладання ланцюгового дробу на відповідні дроби.

Теорема 2.4. *Якщо n – натуральне число і* $[t_0; t_1, t_2, t_3, \ldots, t_n]$ *– ланцюговий дріб, тоді для кожного* k, $1 \leq k \leq n$,

$$[t_0; t_1, t_2, t_3, \ldots, t_n] = [t_0; t_1, t_2, t_3, \ldots t_{k-1}, [t_k, t_{k+1}, t_{k+2}, \ldots, t_n]].$$

Доведення. Рівність доведемо методом математичної індукції. Якщо n = 1, за означенням, $[t_0; t_1] = [t_0; [t_1;]]$. Припустимо, що твердження теореми виконується при $n = m$, тобто для будь-якого ланцюгового дробу $[b_0; b_1, \ldots, b_m]$,

$$[b_0; b_1, \ldots, b_m] = [b_0; b_1, b_2, , .., b_{j-1}, [b_j; b_{j+1}, \ldots, b_m]]$$

для $1 \leq j \leq m$. Розглянемо $n = m + 1$. Нехай $[t_0; t_1, t_2, t_3, \ldots, t_{m+1}]$[46] ланцюговий дріб і $1 \leq k \leq m + 1$. Тоді

$$[t_0; t_1, t_2, t_3, \ldots, t_{m+1}] = [t_0; [t_1, t_2, t_3, \ldots, t_{m+1}]]$$

(за означенням)

$$= [t_0; [t_1, t_2, t_3, \ldots t_{k-1}, [t_k, t_{k+1}, t_{k+2}, \ldots, t_{m+1}]]],$$

маємо за індуктивним припущенням $b_i = t_{i+1}$ і $j = k - 1$. Таким чином,

$$[t_0; t_1, \ldots, t_{m+1}] = [t_0; t_1, t_2, t_3, \ldots t_{k-1}, [t_k, t_{k+1}, t_{k+2}, \ldots, t_{m+1}]]$$

відповідно до визначення ланцюгового дробу. Отже, згідно з методом індукції теорема справедлива. □

Вправи

1. Знайдіть два подання ланцюговим дробом $[t_0; t_1, t_2, t_3, \ldots, t_n]$ для кожного з наведених нижче раціональних чисел: а) 37/11; б) 48/1003; в) -257/2003; г) 11/37; д) -5/44; е) 5.

2. Обчислить наведені раціональні числа і виразите їх у вигляді p/q, де і q – цілі числа: а) [3;5,2]; б) [0;3,5,2]; в) [-10; 1,4,3]; г) [6; 4, 7, 3,5]; д) [2; 5,3]; е) [5; 3,7,4,6].

3. Знайдіть подання числа x скінченним ланцюговим дробом у вигляді

   $$[t_0; t_1, t_2, t_3, t_4, t_5, x_6]$$

   для а) x =$\sqrt{5}$; б) x = $\sqrt{2}$; в) x = π; г) x = $(1 + \sqrt{5})/2$.

4. Нехай $[t_0; t_1, t_2, t_3, \ldots, t_n]$ – скінченний ланцюговий дріб, де $t_i > 0$ для $1 \leq i \leq n$. Доведіть, якщо $b > 0$, то

   a) $[t_0; t_1, t_2, t_3, \ldots, t_n] > [t_0; t_1, t_2, t_3, \ldots, t_n + b]$, якщо n – парне;

   b) $[t_0; t_1, t_2, t_3, \ldots, t_n] < [t_0; t_1, t_2, t_3, \ldots, t_n + b]$, якщо n – непарне.

2.5. Підхідні дроби

Цілком очевидно, що $[t_0; t_1, t_2, .., t_k]$ для кожного k являє собою дійсне число. Запишемо перші чотири підхідні дроби й спростимо їх, виразивши кожний як відношення двох дійсних чисел, де як чисельник, так і знаменник виражені через t_i. Особливий інтерес будуть представляти чисельники і знаменник кожного з підхідних дробів.

$$[t_0;] = t_0 = \frac{t_0}{1} = \frac{p_0}{q_0}.$$

де ми поклали $p_0 = t_0$ і $q_0 = 1$.

$$[t_0; t_1] = t_0 + \frac{1}{t_1} = \frac{t_0 t_1 + 1}{t_1} = \frac{p_1}{q_1},$$

де $p_1 = t_0 t_1 + 1$ і $q_1 = t_1$.

$$[t_0; t_1, t_2] = [t_0; [t_1, t_2]] = t_0 + \frac{1}{[t_1, t_2]} = t_0 + \frac{1}{t_1 + \dfrac{1}{t_2}} = t_0 + \frac{t_2}{t_1 t_2 + 1} =$$

$$= \frac{t_0 t_1 t_2 + t_0 + t_2}{t_1 t_2 + 1} = \frac{(t_0 t_1 + 1) t_2 + t_0}{t_1 t_2 + 1} = \frac{p_1 t_2 + p_0}{q_1 t_2 + q_0} = \frac{p_2}{q_2},$$

де $p_2 = p_1 t_2 + p_0$ і $q_2 = q_1 t_2 + q_0$.

Подібним чином обчислюємо

$$[t_0; t_1, t_2, t_3] = \frac{t_0 t_1 t_2 t_3 + t_0 t_1 + t_2 t_3 + t_0 t_3 + 1}{t_1 t_2 t_3 + t_1 + t_3} =$$

$$= (t_0 t_1 t_2 + t_0 + t_2) t_3 + (t_0 t_1 + 1)/(t_1 t_2 + 1) t_3 + t_1 = \frac{p_2 t_3 + p_1}{q_2 t_3 + q_1} = \frac{p_3}{q_3},$$

де $p_3 = p_2 t_3 + p_1$ і $q_2 = q_2 t_3 + q_1$. У кожному випадку число $[t_0; t_1, t_2, .., t_k]$ "переформовується"з подання ланцюгового дробу без якого-небудь "скорочення"і утворює відношення двох поліномів P і Q у змінних t_0, t_1, t_2, ..., t_k, тобто

$$[t_0; t_1, t_2, .., t_k] = \frac{P(t_0; t_1, \ldots, tk)}{Q(t_0; t_1, \ldots, t_k)}.$$

Справедливим є й те, що q_0, q_1, q_2 і q_3 додатні, оскільки одержані шляхом множення й додавання додатніх чисел. Розглянуті приклади дають підставу сформулювати наступну теорему.

Теорема 2.5. *Нехай n – невід'ємне ціле число і $[t_0; t_1, t_2, .., t_n]$ – скінченний ланцюговий дріб, що рекурсивно визначає скінчені послідовності $p_1, p_2, \ldots, p_n$ і $q_1, q_2, \ldots, q_n$ наступним чином:*

a) $p_0 = t_0$, $q_0 = 1$.

b) $p_1 = t_0 t_1 + 1$, $q_1 = t_1$.

c) $\begin{matrix} p_k = p_{k-1} t_k + p_{k-2}, \\ q_k = q_{k-1} t_k + q_{k-2} \end{matrix}$ *при* $2 \le k \le n$.

Тоді $q_k > 0$ *і* $[t_0; t_1, t_2, .., t_k] = \dfrac{p_k}{q_k}$ *при* $0 \le k \le n$.

Доведення. Неважко методом математичної індукції довести, що $q_k > 0$ при $0 \le k \le n$. Цю частину теореми залишаємо довести читачеві. Вище було показано, що теорема справедлива при k=0,1 і 2, тобто $[t_0;] = \dfrac{p_0}{q_0}$, $[t_0;t_1] = \dfrac{p_1}{q_1}$ і $[t_0;t_1,t_2] = \dfrac{p_3}{q_3}$.

Припустимо, що $2 \le k < n$, і для будь-якого ланцюгового дробу $[b_0;b_1,\ldots,b_k]$ і будь-якого j: $0 \le j \le k$ справедливо твердження про те, що $[b_0;b_1,\ldots,b_k] = p'_j/q'_j$, де p'_j і q'_j визначені способом, аналогічним (a)-(c), але для ланцюгового дробу $[b_0;b_1,\ldots,b_k]$. Тоді $[t_0;t_1,\ldots,t_k,t_{k+1}] = [t_0;t_1,\ldots,t_{k-1}[t_k;t_{k+1}]] =$ (по теоремі 2.4) $= = [b_0;b_1,...,b_{k-1},b_k]$, де $b_i = t_i$ при $0 \le i \le k-1$ і $b_k = [t_k;t_{k+1}] = \dfrac{t_{k+1}}{t_{k+1}}$. Таким чином, у силу індуктивного припущення

$$[t_0;t_1,\ldots,t_k,t_{k+1}] = \frac{p'_{k-1}b_k + p'_{k-2}}{q'_{k-1}b_k + q'_{k-2}}.$$

Оскільки $b_i = t_i$ при $0 \le i \le k-1$, маємо, що для таких i $p_i = p'_i$ і $q_i = q'i$. Підставляючи відповідні вираження для b_k, p'_i і $q'i$ одержуємо

$$[t_0;t_1,\ldots,t_k,t_{k+1}] = \frac{p_{k-1}\left(t_k + \frac{1}{t_{k+1}}\right) + p_{k-2}}{q_{k-1}\left(t_{k+1} + \frac{1}{t_{k+1}}\right) + q_{k-2}} =$$

$$= \frac{(p_{k-1}t_{k-1} + p_{k-2}) + \frac{p_{k-1}}{t_{k+1}}}{(q_{k-1}t_k + q_{k-2}) + \frac{q_{k-1}}{t_{k+1}}} = \frac{p_kt_{k+1} + p_{k-1}}{q_kt_{k+1} + q_{k-1}} = \frac{p_{k+1}}{q_{k+1}}.$$

Отже, за індукцією, $[t_0;t_1,\ldots,t_k,t_{k+1}] = \dfrac{p_k}{q_k}$ при $0 \le k \le n$. □

Числа p_k і q_k (теорема 2.5) визначені поза залежністю від того, що вони можуть бути використані як чисельник і знаменник виразу, рівного k-ому підхідному дробу. Рекурсивне відношення, задане теоремою **??**, забезпечує швидкий спосіб обчислення підхідних дробів для заданого ланцюгового дробу, оскільки чисельник p_i і знаменник q_i можна обчислити одночасно й достатньо просто. Наприклад, для $x = [-4;2,5,2,1] = [t_0;t_1,t_2,t_3,t_4]$ підхідні дроби можна обчислити відповідно до наведеної нижче таблиці:

Так що $x = -124/35$, тобто числу, що породило ланцюговий дріб [-4; 2, 5,2,1] (див. розділ 5.1). Завдяки рекурсивному способу завдання ланцюгових дробів, є значна кількість співвідношень, що зв'язують підхідний дріб через чисельник і знаменники, p_k і q_k, уведені теоремою 2.5. Щоб запис цих відношень зробити справедливим при $k = 0$, найчастіше зручно визначати p_k і q_k при $k = -1$, поклавши

$$p_{-1} = 1,$$

k	t_k	p_k	q_k	p_k/q_k
0	-4	-4	1	$-4/1$
1	2	$(-4)(2)+1=-7$	2	$-7/2$
2	5	$(-7)(5)+(-4)=-39$	$(2)(5)+1=11$	$-39/11$
3	2	$-39)(2)+(-7)=-85$	$(11)(2)+2=24$	$-85/24$
4	1	$(-85)(1)+(-39)=-124$	$(24)(1)+11=35$	$-124/35$

$$q_{-1}=0.$$

Таким чином,

$$p_1=p_0t_1+p_{-1}=t_0t_1+1$$

і

$$q_1=q_0t_1+q_{-1}=1\cdot t_1+0=t_1,$$

як в теоремі 2.5.

Теорема 2.6. *Якщо $[t_0;t_1,\dots,t_n]$ – скінчений ланцюговий дріб, де t_i - дійсні числа, p_k і q_k - задані теоремою 2.5, тоді*

а) $p_kq_{k-1}-p_{k-1}q_k=(-1)^k$ *при* $0\le k\le n$;

б) $\frac{p_k}{q_k}-\frac{p_{k-1}}{q_{k-1}}=\frac{(-1)^{k-1}}{q_kq_{k-1}}$, *при* $1\le k\le n$;

в) $\dfrac{p_k}{q_k}-\dfrac{p_{k-2}}{q_{k-2}}=\dfrac{(-1)^kt_k}{q_kq_{k-2}}$, *при* $2\le k\le n$;

г) *Підхідні дроби парного порядку утворюють зростаючу послідовність, тобто*

$$\frac{p_0}{q_0}<\frac{p_1}{q_1}<\frac{p_2}{q_2}\dots,$$

Підхідні дроби непарного порядку утворюють спадну послідовність, тобто

$$\frac{p_0}{q_0}>\frac{p_1}{q_1}>\frac{p_2}{q_2}\dots.$$

Крім того,

$$\frac{p_{2j}}{q_{2j}}\le[t_0;t_1,t_2,..,t_n]\le\frac{p_{2i+1}}{q_{2i+1}}$$

при $0\le j\le[n/2]$ *і* $0\le i\le[(n-1)/2]$, *де зліва рівність має місце, коли* n *парне, а справа рівність має місце, коли* n *непарне.*

д) *Якщо дріб $[t_0;t_1,\dots,t_n]$ – простий, то* $q_k\ge k$ *при* $0\le k\le n$

є) *Якщо дріб $[t_0;t_1,\dots,t_n]$ – простий, то* $q_k\le q_{k+1}$ *при* $1\le k\le n-1$ *і* $q_0<q_1$.

Доведення. **а)** При к = 1 маємо $p_1q_0 - p_0q_1 = (t_0t_1+1) - t_0t_1 = 1 = (-1)^{1-1}$ за теоремою 2.5. Нехай $2 \leq m < n$ і припустимо, що формула в пункті (а) справедлива при $k = n$. Доведено, що формула має місце при $k = n+1$. Знову, використовуючи теорему 2.5, маємо

$$p_{m+1}q_m - p_mq_{m+1} = (p_mt_{m-1} + p_{m-1})\,q_m - p_m\,(q_mt_{m+1} + q_{m-q}) =$$

$$= q_mp_{m-1} - p_mq_{m-1} = (-1)\,(p_mq_{m-1} - q_mp_{m-1}) = (-1)(-1)^{m-1} = (-1)^{(m+1)-1}.$$

Таким чином, формула в пункті (а) має місце при $1 \leq k \leq n$. Також $p_0q_{-1} - p_{-1}q_0 = t_0 \cdot 0 - 1 \cdot 1 = -1$ і формула справедлива при $k = 0$.

б) Твердження теореми слідує з частини (а), якщо в відповідній рівності при $k \geq 1$ виконати ділення на q_kq_{k-1}.

в) Якщо $k \geq 2$, то за теоремою 2.5

$$p_k = p_{-l}t_k + p_{-2},$$

$$q_k = q_{k-1}t_k + q_{k-2}.$$

Домножимо першу з рівностей на q_{k-2}, другу – на p_{k-2}

$$p_kq_{k-2} = p_{-l}q_{k-2}t_k + p_{-2}q_{k-2},$$

$$q_kp_{k-2} = q_{k-1}p_{k-2}t_k + p_{k-2}q_{k-2}.$$

Віднімимо від першої рівності другу рівність, отримаємо

$$p_kq_{k-2} - q_kp_{k-2} = (p_{k-1}q_{k-2} - q_{k-1}p_{k-2})\,t_k.$$

Тепер, враховуючи твердження в частині (а), отримаємо

$$p_kq_{k-2} - q_kp_{k-2} = (-1)^{(k-1)-1}(-1)^2t_k = (-1)^kt_k.$$

Раозділимо на $q_kq_{k-2} > 0$, отримаємо бажаний результат:

$$\frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} = \frac{(-1)^kt_k}{q_kq_{k-2}}.$$

г) Якщо $2 \leq k \leq n$ и k – парне, то $k-2$ також парне і $k-2 \geq 0$. Тому $-1^k = 1$ і з тверждення в частині (в) слідує, що

$$\frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} = \frac{t_k}{q_kq_{k-2}} > 0.$$

оскільки t_k и $q_k q_{k-2}$ додатні при $k \geq 1$. Якщо $3 \leq k \leq n$ і k — непарне, то $k-2$ також непарне і $k-2 \geq 1$. В цьому випадку $(-1)^k = 1$, так що з твердження в частині (в) слідує, що

$$\frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} = \frac{(-1)^k t_k}{q_k q_{k-2}} < 0$$

так як t_k і $q_k q_{k-2}$ додатні при $k \geq 3$. Якщо n непарне, то згідно з (б) $\frac{p_n}{q_n} > \frac{p_{n-1}}{q_{n-1}}$, так що $[t_0; t_1, \ldots, t_n] = \frac{p_n}{q_n}$ більше, ніж найбільший підхідний дріб парного порядку $\frac{p_{n-1}}{q_{n-1}}$. Якщо n парне, то $\frac{p_n}{q_n} < \frac{p_{n-1}}{q_{n-1}}$, так що $[t_0; t_1, \ldots, t_n] = \frac{p_n}{q_n}$ менше, ніж найменший підхідний дріб непарного порядку, $\frac{p_{n-1}}{q_{n-1}}$. Доведення пунктів (д) і (є) залишаємо за читачем.

□

Список позначень

ЛОГІКА

1 $p \wedge q$ p і q стр. 16

2 $p \vee q$ p або q стр. 16

3 $\widetilde{p}$ не p стр. 16

4 $p \rightarrow q$ якщо p, то q стр. 23

5 $p \leftrightarrow q$ p тоді і тільки тоді, коли q стр. 25 и 32

6 $p \equiv q$ p логічно еквівалентно q стр. 28

7 $\forall$ для всіх стр. 114

8 $\exists$ існує стр. 115

МНОЖИНИ

9 $\{a_1, a_2, a_3, ..., a_n\}$ множина елементів $a_1, a_2, a_3, ..., a_n$ стр. 67

10 $\{x : P\}$ множина елементів, що володіє властивістю P стр. 68

11 $a \in A$ a є елемент множини A стр. 68

12 $A \subseteq B$ множина A є підмножина множини A стр. 68

13 $\oslash$ порожня множина, или нуль-множина стр. 69

14 $\mathbf{U}$ універсальна множина U стр. 69

15 $A \bigcap B$ перетин множин A и B стр. 71

16 $A \bigcup B$ об'єднання множин A и B стр. 71

17 $A - B$ різниця множин A и B стр. 72

18 $A \Delta B$ симетрична різниця множин A и стр. 72

19 A' доповнення множини A стр. 72

20 $\bigcap\limits_{i=1}^{n} A_i$ переріз множин $A_1, A_2, ..., A_n$ стр. 138

21 $\bigcup\limits_{i=1}^{n} A_i$ об'єднання множин $A_1, A_2, ..., A_n$

22 $\mathbb{Z}$ множина цілих чисел

23 $\mathbb{N}$ або $\mathbb{Z}+$ множина натуральних чисел

24 $a|b$ a ділить b

25 НСД(a,b) найбільший спільний дільник чисел a і b

26 НСК(a,b) наименше спільне кратне

27 $a \equiv b(modn)$ a порівняно з b за модулем n

28 $[a]$ клас еквівалентності, що містить a

29 $[a] \oplus [b]$ сума класів еквівалентності

30 $[a] \odot [b]$ добуток класів еквівалентності

31 $[[m]]_n$ найменше натуральне число, порівняне з m за модулем n

Список використаних джерел

[1] Андерсон, Джеймс А. Дискретная математика и комбинаторика. : Пер. с англ. — М. : Издательский дом "Вильямс 2004. — 960 с. : ил. — Парал. тит. англ. Фельдман, Л. П.

[2] Горбатов В.А. Фундаментальные основы дискретной математики. Информационная математика. – М.: Наука. Физматлит, 2000. – 544с.

[3] Карпов В.Г., Мощенский В.А. Математическая лигика и дискретная математика. – Минск.: Вышейшая школа, 1977. - 561 с.

[4] Кук Д., Бейз Г. Компьютерная математика. – М.: Наука., 1990 - 457 с.

[5] Фельдман, Л. П. Чисельні методи в інформатиці [Текст] : підруч. для студ. ВНЗ. - К. : BHV, 2006. - 480 с.

[6] Яблонский С.В. Введение в дискретную математику. – М.: Наука, 1986. - 453 с.