

# 1. Арифметика натуральних і цілих чисел

## 1.1. Принцип математичної індукції

Теорія чисел вивчає властивості натуральних чисел. Місце останніх у математиці дуже влучно й яскраво охарактеризував німецький математик Кронекер:

**“Натуральні числа створив Бог, все інше – справа рук людських”.**

Вважаємо, що читач добре уявляє множину  $\mathbb{N} = \{1, 2, 3, \dots\}$  натуральних чисел, знайомий з основними властивостями їх додавання і множення, а також з відношенням лінійного порядку  $\leq$  на цій множині. Серед властивостей, пов'язаних із відношенням порядку, звернемо увагу на так званий *принцип найменшого числа*, який ми вважатимемо аксіомою:

**у кожній непорожній підмножині множини  $\mathbb{N}$   
є найменше число.**

Чи не найважливішим наслідком цього принципу є

**Принцип математичної індукції.** *Нехай  $A$  – множина тих натуральних чисел, які мають певну властивість  $P$ . Якщо відомо, що*

*(a) число 1 має властивість  $P$  і*

*(b) із припущення, що натуральне число  $n$  має властивість  $P$ , випливає, що цю властивість має і число  $n+1$ ,*

*то множина  $A$  збігається із множиною  $\mathbb{N}$  усіх натуральних чисел.*

**Доведення.** Якщо множина  $A$  не збігається з  $\mathbb{N}$ , то існують натуральні числа, які не мають властивості  $P$ . Згідно з принципом найменшого числа серед таких чисел є найменше. Позначимо його  $m$ . Із умови a) випливає, що  $m \neq 1$ , тому число  $k = m - 1$  – натуральне. Оскільки  $k < m$  і  $m$  – найменше серед чисел, що не мають властивості  $P$ , то  $k$  цю властивість має. Але тоді із умови b) випливає, що число  $m = k + 1$  також має властивість  $P$ . Отже, припущення  $A \neq \mathbb{N}$  приводить до суперечності.  $\square$

Якщо позначити через  $P(n)$  той факт, що натуральне число  $n$  має властивість  $P$ , то принцип математичної індукції можна переформулювати дуже коротко:

*Якщо  $P(1)$  і для будь-якого натурального  $n$  із припущення  $P(n)$  випливає*

$$P(n+1), \text{ то } \{n \in \mathbb{N} | P(n)\} = \mathbb{N}.$$

Принцип математичної індукції інколи називають “**Принципом до-міно**”. Якщо кісточки доміно виставити в ряд так, щоб кожна кісточка при падінні збивала сусідню, а потім штовхнути першу, то впадуть усі кісточки.

Існують різні модифікації принципу математичної індукції. Так, нас може цікавити наявність властивості  $P$  лише в чисел певного вигляду (наприклад, в усіх  $n \geq 2000$  або в усіх парних чисел). У багатьох випадках зручним є варіант, коли в  $b$ ) припускається, що властивість  $P$  має не тільки число  $n$ , а й усі числа, менші за  $n$ . Відповідні точні формулювання читач легко наведе сам.

## 1.2. Теорема про ділення з остачею

Відносно операцій додавання й множення множина  $\mathbb{N}$  є замкненою. Але обернена до додавання операція віднімання для натуральних чисел виконлива не завжди. Тому часто буває зручно замість множини  $\mathbb{N}$  розглядати більшу множину  $\mathbb{Z}$  цілих чисел, яка є замкненою також і відносно віднімання. Стосовно ділення множина  $\mathbb{Z}$  залишається незамкненою, але має місце дуже важлива

**Теорема 1.1 (про ділення з остачею).** *Для кожної пари цілих чисел  $a$  і  $b$ ,  $b \neq 0$ , можна знайти такі цілі числа  $q$  і  $r$ , що*

$$a = qb + r \quad i \quad 0 \leq r < |b|. \quad (1.1)$$

*Числа  $q$  і  $r$  цими умовами визначаються однозначно.*

**Доведення.** Спочатку доведемо існування чисел  $q$  і  $r$ . Якщо  $a = 0$ , то можна взяти  $q = r = 0$ . Тому далі вважатимемо, що  $a \neq 0$ . Найперше розглянемо випадок, коли  $a > 0$  і  $b > 0$ . Позначимо через  $A$  множину  $A = \{a - nb \mid n \in \mathbb{Z}\}$ . Серед її елементів є додатні числа (таким буде, наприклад, число  $a - (-1)b = a + b$ ). Тому, згідно з принципом найменшого числа, серед невід'ємних чисел із множини  $A$  є найменше. Позначимо його через  $r$  і нехай  $r = a - qb$  – зображення  $r$  як елемента множини

*A.* Легко бачити, що  $r < b$ , бо в противному разі множина  $A$  містила б невід'ємне число  $r - b = a - (q + 1)b$ , яке менше від  $r$ . Оскільки  $r \geq 0$  і  $a = qb + r$ , то числа  $q$  і  $r$  – шукані.

Інші випадки легко зводяться до розглянутого. Справді, нехай числа  $p$  і  $s$  задовольняють умови  $|a| = p \cdot |b| + s$  і  $0 \leq s < |b|$ . Якщо  $s = 0$ , то можна взяти  $q = p \cdot \frac{ab}{|ab|}$  і  $r = 0$ . Якщо ж  $s \neq 0$ , то у випадку  $a > 0$ ,  $b < 0$  шуканими є числа  $q = -p$ ,  $r = s$ , у випадку  $a < 0$ ,  $b > 0$  – числа  $q = -p - 1$ ,  $r = b - s$ , а у випадку  $a < 0$ ,  $b < 0$  – числа  $q = p + 1$  і  $r = -b - s$ .

Для доведення однозначності чисел  $q$  і  $r$  припустимо, що пара  $(q_1; r_1)$  також задовольняє умовам  $a = q_1b + r_1$  і  $0 \leq r_1 < |b|$ . Тоді із  $q_1b + r_1 = qb + r$  випливає  $|q_1 - q| \cdot |b| = |r - r_1|$ . Очевидно, що  $|r - r_1| < |b|$ , бо числа  $r$  і  $r_1$  лежать в інтервалі  $[0, |b|]$ . Звідси  $|q_1 - q| \cdot |b| < |b|$  і  $|q_1 - q| < 1$ . Оскільки число  $q_1 - q$  – ціле, то  $|q_1 - q| = 0$  і  $q_1 = q$ . Але тоді  $r_1 = (q - q_1)b + r = r$ , що й треба було довести.  $\square$

У співвідношеннях (1.1) число  $q$  називають (*неповною*) *часткою*, а число  $r$  – *остачею від ділення*  $a$  на  $b$ .

**Вправа 1.1.** Як знаки чисел  $a$  і  $b$  впливають на знак частки  $q$  від ділення  $a$  на  $b$ ?

**Задача 1.1.** Обчислити частку  $q$  й остаточу  $r$  від ділення числа  $-187$  на число  $-13$ .

*Розв’язання.* Оскільки  $\frac{187}{13} = 14\frac{5}{13}$ , то  $-187 = 14\frac{5}{13} \cdot (-13) = (15 - \frac{8}{13}) \cdot (-13) = 15 \cdot (-13) + 8$ . Отже,  $q = 15$  і  $r = 8$ .  $\square$

**Задача 1.2.** Обчислити натуральне число  $b$  й остаточу  $r$  від ділення числа  $a = 19178$  на  $b$ , якщо частка від ділення  $a$  на  $b$  дорівнює 129.

*Розв’язання.* Із рівності  $19178 = 129 \cdot b + r$  маємо  $b = \frac{19178 - r}{129} = 148 + \frac{86 - r}{129}$ . Оскільки число  $b$  – ціле, то  $b \leq 148$ . Із нерівності  $0 \leq r < b$  тепер отримуємо  $\frac{86}{129} = \frac{86 - 0}{129} \geq \frac{86 - r}{129} > \frac{86 - 148}{129} = -\frac{62}{129}$ . Але число  $\frac{86 - r}{129}$  має бути цілим. Тому  $\frac{86 - r}{129} = 0$ , звідки  $r = 86$  і  $b = 148$ .  $\square$

**Задача 1.3.** Обчислити натуральне число  $b$  і частку  $q$  від ділення числа  $a = 3616$  на  $b$ , якщо  $q > 1$  й остатча від ділення  $a$  на  $b$  дорівнює 305.

*Розв’язання.* Із рівності  $3616 = qb + 305$  маємо  $qb = 3311 = 7 \cdot 11 \cdot 43$ . За умовою задачі  $b > 305$  і  $b < 3311$ , бо  $q > 1$ . Серед дільників числа 3311

є лише один, який задовольняє ці нерівності, а саме  $11 \cdot 43 = 473$ . Тому  $b = 473$  і  $q = 7$ .  $\square$

### 1.3. Подільність чисел

Якщо остатча від ділення  $a$  на  $b$  дорівнює 0, то кажуть, що  $a$  *ділиться* на  $b$  (або що  $b$  *ділить*  $a$ ), і позначають цей факт символом  $b|a$ . Замість позначення  $b|a$  інколи вживають символ  $a:b$ . Число  $a$  ще називають *кратним* числа  $b$ , а  $b$  – *дільником* числа  $a$ , бо умова  $b|a$  рівносильна існуванню такого  $q$ , що  $a = bq$ . Останнє зауваження дає змогу переформулювати означення подільності чисел лише в термінах дії множення. Такий підхід є кращим, оскільки він дозволяє визначити поняття подільності елементів у довільних кільцях (і навіть просто множинах із множенням), для яких теорема про ділення з остаточею може й не виконуватись.

Факт, що  $a$  не ділиться на  $b$ , позначатимемо через  $b \nmid a$ .

Безпосередньо із означення подільності чисел випливає

**Теорема 1.2 (про найпростіші властивості відношення подільності).**

- (a)  $a|a$  (рефлексивність відношення подільності);
- (b) якщо  $a|b$  і  $b|c$ , то  $a|c$  (транзитивність відношення подільності);
- (c) якщо  $a|b$ , то  $a|bc$ ;
- (d) якщо  $a|b$  і  $a|c$ , то  $a|(b \pm c)$ ;
- (e) 0 ділиться на кожне число, і немає інших чисел з такою властивістю;
- (f) кожне число ділиться на  $\pm 1$ , і немає інших чисел з такою властивістю;
- (g) якщо  $a|b$  і  $c|d$ , то  $ac|bd$ .

**Вправа 1.2.** Довести строго всі твердження попередньої теореми.

**Вправа 1.3.** Довести рівносильність таких умов: (a)  $a|b$ ; (b)  $(-a)|b$ ; (c)  $a|(-b)$ ; (d)  $|a| \parallel |b|$ .

**Задача 1.4.** Знайти всі натуральні числа  $n$ , для яких  $(n+2)|(n^2 + 2)$ .

*Розв'язання.* Із рівності  $n^2+2 = (n+2)(n-2)+6$  випливає, що  $n+2|n^2+4$  тоді і лише тоді, коли  $n+2|6$ . Оскільки  $n$  – натуральне, то  $n+2 = 3$  або  $n+2 = 6$ . Отже,  $n = 1$  або  $n = 4$ .  $\square$

**Задача 1.5.** Довести, що для кожного натурального числа  $n$

$$13|(4^{2n-1} + 3^{n+1}).$$

*Розв'язання.* Скористаємось принципом математичної індукції. Для  $n = 1$  твердження виконується. Із рівності  $4^{2(n+1)-1} + 3^{(n+1)+1} = 4^{2n+1} + 3^{n+2} = 16 \cdot 4^{2n-1} + 3 \cdot 3^{n+1} = 13 \cdot 4^{2n-1} + 3 \cdot (4^{2n-1} + 3^{n+1})$  тепер випливає, що коли твердження задачі виконується для числа  $n$ , то воно виконується і для числа  $n+1$ . А тому воно виконується для всіх натуральних  $n$ .  $\square$

**Задача 1.6.** Довести, що для кожного цілого числа  $k \geq 0$

$$7|(2^{2^{2k}} + 5).$$

*Розв'язання.*  $2^{2^{2k}} + 5 = 2^{4^k} + 5 = 2^{(3+1)^k} + 5$ . У правій частині рівності  $(3+1)^k = C_k^0 \cdot 3^k + C_k^1 \cdot 3^{k-1} + \dots + C_k^{k-1} \cdot 3 + 1$  всі доданки, крім останнього, діляться на 3. Тому число  $(3+1)^k$  можна записати у вигляді  $(3+1)^k = 3m+1$ . Звідси  $2^{(3+1)^k} + 5 = 2^{3m+1} + 5 = 2 \cdot 8^m + 5 = 2 \cdot (7+1)^m + 5$ . Аналогічно попередньому, число  $(7+1)^m$  можна записати у вигляді  $(7+1)^m = 7t+1$ . Користуючись цим, отримуємо  $2 \cdot (7+1)^m + 5 = 2 \cdot (7t+1) + 5 = 7 \cdot (2t+1)$ .  $\square$

Якщо  $a|b$  і  $b|a$ , то числа  $a$  і  $b$  називають *асоційованими*. Ненульові асоційовані числа можуть відрізнятись щонаїбільше знаком. Справді, із  $a|b$  випливає існування такого числа  $q_1$ , що  $aq_1 = b$ , а із  $b|a$  – такого числа  $q_2$ , що  $bq_2 = a$ . Звідси отримуємо рівність  $(aq_1)q_2 = a$ , або  $q_1q_2 = 1$ . Оскільки серед цілих чисел оборотними є лише  $\pm 1$ , то  $q_1 = \pm 1$  і  $b = \pm a$ .

З іншого боку, протилежні числа є асоційовані. Тому ненульові цілі числа розбиваються на пари асоційованих. Зокрема, кожна така пара містить рівно одне натуральне число. Із вирави 1.3 випливає, що асоційовані числа будуть або не будуть дільниками даного числа одночасно. Тому дільники числа інколи вивчають з точністю до асоційованості й обмежуються лише натуральними дільниками.

## 1.4. Прості і складені числа

До дільників числа  $a$  завжди належать числа  $\pm 1$  і  $\pm a$ . Такі дільники числа  $a$  називаються *невласними*, а всі інші – *власними*. Зауважимо, що дільник  $b$  числа  $a \neq 0$  буде власним тоді й лише тоді, коли він задовольняє нерівності  $1 < |b| < |a|$ .

Число, яке має власні дільники, називається *складеним*. Якщо число не є складеним і відмінне від  $\pm 1$ , то воно називається *простим*. Причина, чому числа  $\pm 1$  не відносять ні до простих, ні до складених, стане зрозуміло дещо пізніше. Очевидно, що відмінне від  $\pm 1$  число  $p$  буде простим тоді й лише тоді, коли для будь-якого розкладу  $p$  у добуток двох множників  $p = ab$  один із них дорівнює  $\pm 1$ .

**Вправа 1.4.** Довести, що кожне натуральне складене число  $n$  має власний натуральний дільник, який не перевищує  $\sqrt{n}$ .

**Вправа 1.5.** Виписати 10 перших натуральних простих чисел.

Зупинимось детальніше на властивостях простих чисел.

**Твердження 1.1.** Кожне відмінне від  $\pm 1$  ціле число ділиться на деяке просте число.

*Доведення.* Скористаємося індукцією за модулем числа  $n$ . Для чисел 0 і  $\pm 2$  твердження очевидне. Розглянемо довільне  $n$ ,  $|n| > 2$ , і припустимо, що для всіх чисел, модуль яких менший від  $|n|$ , твердження вже доведене. Якщо  $n$  – просте, то воно має власний натуральний дільник саме. Якщо ж  $n$  – складене, то воно має власний натуральний дільник  $m$ . Оскільки  $1 < m < |n|$ , то, за припущенням індукції,  $m$  має простий дільник  $p$ . Із транзитивності відношення подільності тепер випливає, що  $p|n$ .  $\square$

Коли ми говоримо про добуток  $m_1 \cdot m_2 \cdot \dots \cdot m_k$   $k$  множників, то до розгляду включено і випадок  $k = 1$ . Більше того, число 1 зручно вважати добутком нульової кількості множників. Це спрощує формулювання багатьох тверджень. Прикладом може слугувати

**Теорема 1.3.** Кожне натуральне число розкладається в добуток простих чисел.

*Доведення.* Для числа 1 твердження теореми випливає з нашої домовленості. Розглянемо тепер довільне  $n > 1$  і припустимо, що для всіх чисел, менших від  $n$ , теорему вже доведено. Якщо  $n$  – просте, то шуканий

розклад для  $n$  складається з одного множника  $n$ . Якщо ж  $n$  складене, то за попереднім твердженням  $n$  можна розкласти в добуток  $n = p_1m$ , де  $p_1$  – просте і  $m < n$ . За припущенням індукції для  $m$  є розклад  $m = p_2p_3 \dots p_k$  у добуток простих чисел. Тоді  $n = p_1p_2 \dots p_k$  буде шуканим розкладом для числа  $n$ .  $\square$

**Теорема 1.4 (Евклід).** Існує нескінченно багато простих чисел.

*Доведення* цієї теореми є класичним зразком доведення від супротивного. Справді, припустимо, що множина простих чисел скінчена, і нехай  $p_1, p_2, \dots, p_k$  – їх повний список. Розглянемо число  $n = p_1p_2 \dots p_k + 1$ . За доведеним твердженням  $n$  має простий дільник  $p$ . Цей дільник не може збігатися з жодним із чисел  $p_1, \dots, p_k$ , бо  $n$  на ці числа не ділиться. Отже, просте число  $p$  не зустрічається в списку  $p_1, \dots, p_k$ , що суперечить припущенню про його повноту. Теорему доведено.  $\square$

**Задача 1.7.** Знайти всі такі натуральні прості числа  $p$ , для яких кожне із чисел  $p+4$  і  $p+14$  також буде простим.

*Розв'язання.* Розглянемо остаті від ділення цих чисел на 3. Із рівностей  $p+4 = 3 + (p+1)$  і  $p+14 = 12 + (p+2)$  випливає, що числа  $p$ ,  $p+4$  і  $p+14$  при діленні на 3 дають різні остаті. Отже, одна із цих остаті дорівнює 0, тобто одне із цих чисел ділиться на 3. Але числа  $p+4$  і  $p+14$  прості й більші, ніж 3, тому вони на 3 не діляться. Звідси  $3|p$  і  $p = 3$ , бо  $p$  – просте. Оскільки числа  $3+4 = 7$  і  $3+14 = 17$  – прості, то  $p = 3$  справді задовільняє умову задачі.  $\square$

**Задача 1.8.** Якою буде відповідь у попередній задачі, якщо не вимагати, щоб число  $p$  було натуральним?

*Розв'язання.* Як і в попередній задачі, доводимо, що одне із простих чисел  $p$ ,  $p+4$  і  $p+14$  ділиться на 3. Це дає нам 6 випадків: 1)  $p = 3$ ; 2)  $p = -3$ ; 3)  $p+4 = 3$ ; 4)  $p+4 = -3$ ; 5)  $p+14 = 3$ ; 6)  $p+14 = -3$ . Перевірка показує, що у 2-му і 3-му випадках не будуть простими відповідно числа  $p+4$  і  $p$ , а в решті випадків всі числа  $p$ ,  $p+4$  і  $p+14$  будуть простими. Це дає 4 розв'язки:  $p = 3$ ,  $p = -7$ ,  $p = -11$ ,  $p = -17$ .  $\square$

**Задача 1.9.** Довести, що існує нескінченно багато простих чисел виду  $4k+3$ .

*Розв'язання.* Зауважимо, що кожне непарне число має вигляд  $4k+1$  або  $4k+3$ , і що добуток чисел вигляду  $4k+1$  знову буде числом такого

ж вигляду:  $(4m+1) \cdot (4n+1) = 4 \cdot (4mn+m+n) + 1$ . Тому не може бути, щоб у розкладі числа вигляду  $4k+3$  у добуток простих всі множники були вигляду  $4k+1$ . Отже, кожне число вигляду  $4k+3$  має хоча б один простий дільник такого ж вигляду. Далі хід міркувань подібний до доведення теореми Евкліда. Справді, припустимо, що простих чисел вигляду  $4k+3$  – скінчена кількість, і нехай  $p_1, \dots, p_t$  – їх повний список. Число  $n = 4p_1 \cdots p_t - 1 = 4 \cdot (p_1 \cdots p_t - 1) + 3$  є числом вигляду  $4k+3$  і не ділиться на жодне із чисел  $p_1, \dots, p_t$ . Тому той простий дільник числа  $n$ , який має вигляд  $4k+3$ , не зустрічається у списку  $p_1, \dots, p_t$ . Отже, припущення про скінченність простих чисел вигляду  $4k+3$  приводить до суперечності.  $\square$

У багатьох книгах з теорії чисел наводяться таблиці натуральних простих чисел, що не перевищують даного числа  $N$ . Простий метод побудови таких таблиць запропонував близько 200 р. до н.е. грецький математик із Александрії Ератостен. Цей метод, відомий під назвою “решета Ератостена”, виглядає так.

Випишемо підряд всі натуральні числа від 2 до  $N$ . Число 2 як просто залишимо, а всі інші парні числа викреслимо. Перше незакреслене число після 2 – це просте число 3. Після цього викреслимо кожне третє число після 3 (при цьому треба рахувати також і ті числа, що їх викреслено раніше). Першим незакресленим числом після 3 буде число 5. Воно знову просте. Тепер викреслимо кожне п’яте число після 5, і т.д. Якщо в такий спосіб знайдено всі прості числа до числа  $p$  включно, а потім викреслено всі числа, які більші  $p$  і кратні  $p$ , то перше незакреслене після  $p$  число знову буде простим (бо воно не ділиться на жодне менше просте число). Продовжуючи таке викреслювання, доки це можливо, врешті-решт одержимо всі прості числа, які не перевищують  $N$ .

**Зауваження.** Як випливає із вправи 1.4, досить викреслювати кратні лише тих простих чисел, які не перевищують  $\sqrt{N}$ . Це значно зменшує об’єм обчислень.

**Задача 1.10.** За допомогою “решета Ератостена” знайти всі прості числа з проміжку [1230; 1250].

**Розв’язання.** Оскільки  $\sqrt{1250} < 36$ , то з проміжку [1230; 1250] досить викреслити кратні лише тих простих чисел, що не перевищують 35, тобто кратні чисел 2, 3, 5, 7, 11, 13, 17, 19, 23, 29 і 31. Після викреслювання чисел, кратних 2, 3 і 5, невикресленими залишаться тільки числа 1231, 1237, 1241, 1243, 1247 і 1249. Остачі від ділення 1230 на прості числа 7,

11, 13, 17, 19, 23, 29 і 31 дорівнюють відповідно 5, 9, 8, 6, 14, 11, 12 і 21. Тому на проміжку [1230; 1250] кратними цих простих чисел будуть:

число р	його кратні	число р	його кратні
7	1232, 1239, 1246	19	1235
11	1232, 1243	23	1242
13	1235, 1248	29	1247
17	1241	31	1240.

Якщо викреслити її кратні, то невикресленими залишаться числа 1231, 1237 і 1249. Вони і є шуканими.  $\square$

Занумеруємо натуральні прості числа у порядку їх зростання:  $p_1 = 2$ ,  $p_2 = 3$ ,  $p_3 = 5$ , .... Коли продовжити цей ряд досить далеко, то кидається у вічі нерегулярність, з якою прості числа розподілені серед натуральних. Є проміжки, на яких прості числа зустрічаються часто, і не тільки на початку натурального ряду. Наприклад, по 4 простих числа містить кожен із проміжків [5651; 5659] і [299471; 299479]. Нерідко трапляються пари простих чисел, які відрізняються одне від одного лише на 2, як, скажімо, 17 і 19 або 4091 і 4093 (такі пари простих чисел називають “близнятами”, в межах першого мільйона їх 8164. Досі невідомо, чи таких пар скінчена кількість).

З іншого боку, зустрічаються досить довгі проміжки натуральних чисел, які не містять жодного простого. Так, зовсім нема простих серед 13 чисел із проміжку [114; 126] і серед 33 чисел із проміжку [1328; 1360]. Навіть більше, існують як завгодно довгі проміжки натуральних чисел, що не містять жодного простого.

**Вправа 1.6.** *Довести, що проміжок  $[n!+2; n!+n]$  не містить жодного простого числа.*

Видима хаотичність, з якою розміщені прості числа в натуральному ряді, з давніх давен спонукала багатьох математиків до виявлення закономірностей в чергуванні простих і складених чисел. Зокрема, величезні зусилля були затрачені на пошуки так званої “формули  $n$ -го простого числа” (особливо це стосується математиків–любителів). Напевне не менш часу та зусиль забрала й інша задача, на перший погляд значно простіша: вказати яку-небудь функцію  $f(n)$  натурального аргументу, яка б “легко” обчислювалась, набувала лише простих значень, і цих значень було б нескінченно багато.

**Вправа 1.7.** Перевірте, що значення многочлена  $g(x) = x^2 - x + 41$  у точках  $x = 0, 1, 2, \dots, 39, 40$  будуть простими числами.

Однак  $g(41) = 41^2$  вже не є простим числом. Поява серед значень многочлена складеного числа є закономірною.

**Задача 1.11.** Довести, що не існує такого многочлена  $f(x)$  ненульового степеня з цілими коефіцієнтами, щоб для всіх натуральних  $n$  значення многочлена  $f(n)$  були простими числами.

*Розв'язання.* Нехай  $f(x) = a_0x^n + \dots + a_n$ . Оскільки  $n > 0$ , то існує таке натуральне число  $k$ , що  $|f(k)| > 1$ . Нехай  $p$  – якийсь простий дільник числа  $f(k)$ . Із формулі  $a^m - b^m = (a - b)(a^{m-1} + a^{m-2}b + \dots + b^{m-1})$  випливає, що для кожного цілого  $t$  число  $f(k + tp) - f(k) =$

$$= \sum_{i=1}^n a_{n-i}((k + tp)^i - k^i) = \sum_{i=1}^n a_{n-i}(k + tp - k)((k + tp)^{i-1} + \dots + k^{i-1})$$

ділиться на  $p$ . Але тоді для кожного  $t$  число  $f(k + tp)$  також ділиться на  $p$ . Оскільки чисел вигляду  $k + tp$  нескінченно багато, а кожне з рівнянь  $f(x) = p$  і  $f(x) = -p$  має не більше  $n$  коренів, то для всіх достатньо великих чисел  $t$  значення многочлена  $f(k + tp)$  будуть складеними числами.  $\square$

У 1970 р. незалежно один від одного ленінградський математик Матіясевич Ю.В. і київський математик Чудновський Г.В. (на той час – студент 1-го курсу Київського університету) довели існування многочлена  $f(x_1, \dots, x_n)$  від багатьох змінних із цілими коефіцієнтами, множина додатних значень якого (при натуральних значеннях змінних  $x_1, \dots, x_n$ ) збігається з множиною простих чисел. Згодом різними авторами побудовано кілька прикладів таких многочленів. Найвідоміший з них має 26 змінних, і для його запису використовують усі букви латинського алфавіту. Однак для побудови конкретних простих чисел ці многочлени мало придатні, бо дуже важко вказати хоча б один набір значень  $x_1, \dots, x_n$ , для якого  $f(x_1, \dots, x_n) > 0$ .

## 1.5. Найбільший спільний дільник і найменше спільне кратне

Число  $d$  називають *найбільшим спільним дільником* чисел  $a$  і  $b$ , якщо воно задовільняє 2 умови:

- (a)  $d|a$  і  $d|b$ ;
- (b) якщо  $c|a$  і  $c|b$ , то  $c|d$ .

Найбільший спільний дільник чисел  $a$  і  $b$  позначають НСД( $a, b$ ) або  $(a, b)$ .

У словосполученні “найбільший спільний дільник” слово “найбільший” означає не найбільший за величиною, а те, що цей дільник є кратним будь-якого іншого спільного дільника чисел  $a$  і  $b$ . Наприклад, спільними дільниками чисел 12 і 18 будуть  $\pm 1$ ,  $\pm 2$ ,  $\pm 3$ ,  $\pm 6$ , а найбільшими спільними дільниками цих чисел є 6 і  $-6$  (зауважимо, що за величиною  $-6$  є найменшим серед спільніх дільників чисел 12 і 18).

Означення найбільшого спільного дільника двох чисел з використанням лише поняття подільності є зручним для теоретичних міркувань. До того ж воно легко переноситься на інші математичні структури, де можна говорити про подільність, але де не можна змістово визначити величину елементів. Трохи пізніше ми побачимо, що для натуральних чисел наше поняття найбільшого спільного дільника насправді збігається з прийнятим у школі.

Однак тепер зовсім не очевидно, що визначений таким чином найбільший спільний дільник існує для довільної пари чисел  $a$  і  $b$ . Ми доведемо його існування методом, який, попри свою прозорість, є вихідною точкою деяких глибоких понять сучасної алгебри.

**Теорема 1.5 (про існування найбільшого спільного дільника).**  
Для будь-яких цілих чисел  $a$  і  $b$  існує їх найбільший спільний дільник  $(a, b)$ .

**Доведення.** Безпосередньо перевіряється, що  $0 = (0, 0)$ . Тому далі можна вважати, що серед чисел  $a$  і  $b$  є ненульове. Розглянемо множину  $I = \{ma + nb : m, n \in \mathbb{Z}\}$ . Вона, зокрема, містить числа  $a = 1 \cdot a + 0 \cdot b$ ,  $b = 0 \cdot a + 1 \cdot b$ , і разом із числом  $ma + nb$  містить протилежне число  $(-m)a + (-n)b$ . Тому серед елементів множини  $I$  є натуральні числа. Позначимо через  $d$  найменше з них і доведемо, що  $d$  є найбільшим спільним дільником чисел  $a$  і  $b$ . Справді, нехай  $d = m_0a + n_0b$ . Припустимо, що  $a$  не ділить  $b$ . Тоді розділимо  $a$  на  $d$  з остачею:  $a = qd + r$ ,  $0 < r < d$ , і матимемо:  $r = a - qd = (1 - qm_0)a + (-qn_0)b \in I$ , що суперечить вибору числа  $d$ .

Аналогічно доводиться, що  $d|b$ . Отже, першу умову з означення найбільшого спільного дільника число  $d$  задоволяє.

Припустимо тепер, що  $c|a$  і  $c|b$ . Тоді існують розклади  $a = ca_0$  і  $b = cb_0$ , звідки  $d = m_0 \cdot ca_0 + n_0 \cdot cb_0 = c(m_0a_0 + n_0b_0)$ . Таким чином,  $c|d$ .  $\square$

Очевидно, що разом із  $d$  найбільшим спільним дільником чисел  $a$  і  $b$  буде і число  $-d$ . Навпаки, якщо  $d_1$  і  $d_2$  – найбільші спільні дільники чисел  $a$  і  $b$ , то має бути  $d_1|d_2$  і  $d_2|d_1$ , тобто  $d_1$  і  $d_2$  – асоційовані і відрізняються щонайбільше знаком. Щоб досягти однозначності, можна домовитись розглядати лише додатне значення найбільшого спільного дільника.

Із доведення останньої теореми одразу випливає такий важливий

**Наслідок 1.** Якщо  $d = \text{НСД}(a, b)$ , то можна підібрати такі цілі числа  $m$  і  $n$ , що  $d = ma + nb$ .

**Вправа 1.8.** Якщо  $p$  – просте число, то для довільного числа  $a$  або  $\text{НСД}(a, p) = 1$ , або  $\text{НСД}(a, p) = p$ .

Поняття найбільшого спільного дільника легко узагальнюється на довільну скінченну кількість чисел, а саме:  $d$  називається найбільшим спільним дільником чисел  $a_1, a_2, \dots, a_n$ , якщо  $d$  задовольняє такі умови:

- (a)  $d|a_1, d|a_2, \dots, d|a_n$ ;
- (b) якщо  $c|a_1, c|a_2, \dots, c|a_n$ , то  $c|d$ .

Цілком аналогічно випадку двох чисел доводиться, що найбільший спільний дільник довільного набору чисел  $a_1, a_2, \dots, a_n$  існує і визначений з точністю до знаку. Він позначається  $\text{НСД}(a_1, a_2, \dots, a_n)$  або просто  $(a_1, a_2, \dots, a_n)$ . І в загальному випадку для однозначності братимемо лише додатне значення найбільшого спільного дільника.

**Задача 1.12.** Довести, що  $(a, b, c) = ((a, b), c) = ((a, c), b) = ((b, c), a)$ .

*Розв'язання.* Досить довести лише першу рівність. Позначимо  $d_1 = (a, b, c)$ ,  $d_2 = ((a, b), c)$ ,  $d = (a, b)$ . Із  $d_1|a$  і  $d_1|b$  випливає, що  $d_1|d$ , а з  $d_1|d$  і  $d_1|c$  – що  $d_1|d_2$ . З іншого боку, із  $d_2|d$  випливає, що  $d_2|a$  і  $d_2|b$ . Крім того,  $d_2|c$ . Тому  $d_2|d_1$ . Позаяк  $d_1$  і  $d_2$  – асоційовані і додатні, то  $d_1 = d_2$ .  $\square$

**Задача 1.13.** Знайти довжину найкоротшої арифметичної прогресії, членами якої будуть числа 15, 69, 105 і 189.

*Розв'язання.* У найкоротшій прогресії числа 15 і 189 повинні бути крайніми членами. Можна вважати, що 15 – перший член, а 189 – останній. Різниця  $a_n - a_m$  двох довільних членів арифметичної прогресії завжди ділиться на різницю  $d$  цієї прогресії. Тому  $d$  ділить кожне з чисел  $69 - 15 = 54$ ,  $105 - 69 = 36$ ,  $189 - 105 = 84$ . Щоб прогресія була найкоротшою, її різниця має бути найбільшою. Отже,  $d = \text{НСД}(54, 36, 84) = 6$ . Тепер із рівності  $189 = 15 + 6 \cdot (k-1)$  знаходимо  $k = 30$ , тобто найкоротша прогресія містить 30 членів.  $\square$

Числа  $a$  і  $b$  називаються *взаємно простими*, якщо  $\text{НСД}(a, b) = 1$ . Наприклад, взаємно простими будуть числа 15 і 28, 100 і 243, 1001 і 1110.

**Вправа 1.9.** Довести, що числа  $n$  і  $n+1$  завжди взаємно прості.

**Теорема 1.6 (критерій взаємної простоти двох чисел).** Числа  $a$  і  $b$  взаємно прості тоді й лише тоді, коли можна підібрати такі цілі числа  $m$  і  $n$ , що  $ma + nb = 1$ .

*Доведення.* Необхідність умови випливає з наслідку 1 теореми 1.5, а достатність – із того, що будь-який спільний дільник чисел  $a$  і  $b$  буде і дільником суми  $ma + nb$ . Тому коли  $ma + nb = 1$ , то  $a$  і  $b$  не мають відмінних від 1 спільних дільників.  $\square$

Питання про взаємну простоту двох чисел виникає, наприклад, при записі раціональних чисел у вигляді дробів: якщо  $a$  і  $b$  не взаємно прості, то ми можемо скоротити чисельник і знаменник дробу  $\frac{a}{b}$  на їх спільний дільник і тим самим перейти до дробу, який у певному сенсі є простішим від початкового.

**Твердження 1.2.** (a) Якщо  $(a, b) = 1$  і  $(a, c) = 1$ , то  $(a, bc) = 1$ .

(b) Якщо  $a|bc$  і  $(a, b) = 1$ , то  $a|c$ .

(c) Якщо  $a|c$ ,  $b|c$  і  $(a, b) = 1$ , то  $ab|c$ .

*Доведення.* (a) За критерієм взаємної простоти чисел умови  $(a, b) = 1$  і  $(a, c) = 1$  рівносильні існуванню таких цілих чисел  $m$ ,  $n$ ,  $k$ ,  $l$ , що  $ma + nb = 1$ ,  $ka + lc = 1$ . Перемноживши ці рівності, одержимо:  $(mka + mlc + nkb) \cdot c + nl \cdot bc = 1$ . За тим же критерієм звідси випливає, що  $(a, bc) = 1$ .

(b) Помноживши обидві частини рівності  $ma + nb = 1$  на  $c$ , одержимо:  $mac + nbc = c$ . Оскільки  $a|mac$  і  $a|nbc$ , то  $a|c$ .

(c) За умовою існують такі  $a_0, b_0, m$  і  $n$ , що  $c = aa_0 = bb_0$  і  $ma + nb = 1$ .  
Тоді  $c = mac + nbc = ma \cdot bb_0 + nb \cdot aa_0 = (mb_0 + na_0)ab$ . Отже,  $ab|c$ .  $\square$

**Твердження 1.3.** Якщо  $(a, b) = d$  і  $a = a_0d$ ,  $b = b_0d$ , то числа  $a_0$  і  $b_0$  взаємно прості.

**Доведення.** Зобразимо  $d$  у вигляді  $d = ma + nb = ma_0d + nb_0d$ . Тоді після скорочення на  $d$  матимемо:  $1 = ma_0 + nb_0$ . Отже, за критерієм взаємної простоти чисел,  $(a_0, b_0) = 1$ .  $\square$

Число  $m$  називається *найменшим спільним кратним* чисел  $a$  і  $b$ , якщо воно задовільняє дві умови:

- (a)  $a|m$  і  $b|m$ ;
- (b) якщо  $a|n$  і  $b|n$ , то  $m|n$ .

Найменше спільне кратне чисел  $a$  і  $b$  позначають НСК( $a, b$ ) або  $[a, b]$ .

Як і для двоїстого поняття найбільшого спільного дільника, слово “найменше” у словосполученні “найменше спільне кратне” розуміється в сенсі подільності, а не величини: це кратне мусить бути дільником будь-якого іншого кратного чисел  $a$  і  $b$ .

**Вправа 1.10.** Довести, що найменше спільне кратне чисел  $a$  і  $b$  (у разі його існування) визначене з точністю до знаку.

Далі для однозначності ми будемо розглядати лише додатне значення найменшого спільного кратного.

**Вправа 1.11.** Довести, що коли  $(a, b) = 1$ , то  $[a, b] = ab$ .

Існування найменшого спільного кратного, а заразом і спосіб його обчислення, випливають із наступної теореми.

**Теорема 1.7.** Для натуральних чисел  $a$  і  $b$   $[a, b] = \frac{ab}{(a, b)}$ .

**Доведення.** Нехай  $(a, b) = d$ . Тоді  $a = a_0d$ ,  $b = b_0d$  і  $\frac{ab}{(a, b)} = a_0b_0d$ . Очевидно, що  $m = a_0b_0d = b_0a = a_0b$  є спільним кратним чисел  $a$  і  $b$ .  
Нехай тепер  $M$  – якесь спільне кратне чисел  $a$  і  $b$ . Тоді  $M = aa_1 = bb_1$ .  
За твердженням 1.3  $(a_0, b_0) = 1$ , а тому існують такі числа  $k$  і  $l$ , що  $1 = ka_0 + lb_0$ . Помножимо обидві частини цієї рівності на  $M$ , матимемо:  
 $M = ka_0M + lb_0M = ka_0bb_1 + lb_0aa_1 = kmb_1 + lma_1 = m(kb_1 + la_1)$ .  
Отже,  $m|M$ .  $\square$

Поняття найменшого спільного кратного легко узагальнюється на довільну скінченну кількість чисел:  $m$  називається *найменшим спільним кратним* чисел  $a_1, a_2, \dots, a_k$ , якщо  $m$  задовольняє такі умови:

- (a)  $a_1|m, a_2|m, \dots, a_k|m;$
- (b) якщо  $a_1|n, a_2|n, \dots, a_k|n$ , то  $m|n$ .

Зауважимо, що задача знаходження найменшого спільного знаменника кількох дробів, яка постійно виникає при додаванні чи відніманні дробів, є не що інше як обчислення найменшого спільного кратного знаменників цих дробів.

## 1.6. Основна теорема арифметики

Узагалі кажучи, розклади число в добуток простих можна багатьма способами. Наприклад,  $30 = 2 \cdot 3 \cdot 5 = 3 \cdot (-2) \cdot (-5) = 5 \cdot (-3) \cdot (-2)$ . Однак наведені розклади числа 30 розрізняються лише порядком і знаками множників. Твердження, що так буде для кожного числа, заслужено називають основною теоремою арифметики. У нас вже є все необхідне для її доведення.

**Теорема 1.8 (основна теорема арифметики).** *Кожне натуральне число розкладається в добуток простих чисел, причому такий розклад є однозначним з точністю до порядку і знаків множників.*

*Доведення.* Існування розкладу вже доведене (теорема 1.3), тому обґрутування вимагає лише однозначності розкладу. Скористаємося індукцією за довжиною  $k$  найкоротшого розкладу числа (тобто розкладу, який містить найменшу кількість простих множників). Якщо  $k = 0$  (число 1) або  $k = 1$  (прості числа), то однозначність розкладу очевидна.

Нехай для всіх чисел, для яких існує розклад на менше ніж  $k$  простих множників, однозначність розкладу вже доведена, і нехай

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m \quad (m \geq k) \quad (1.2)$$

— два розклади числа  $n$  на прості множники. Якщо  $(p_1, q_1) = 1, (p_1, q_2) = 1, \dots, (p_1, q_m) = 1$ , то з твердження 1.2(a) випливає, що  $(p_1, q_1 q_2 \cdots q_m) = 1$ . Але це суперечить рівності (1.2). Тому існує таке  $i$ , що  $(p_1, q_i) \neq 1$ . Оскільки  $p_1$  і  $q_i$  — прості числа, то вони відрізняються щонайбільше знаком. Змінивши, у разі потреби, в добутку  $q_1 q_2 \cdots q_m$  порядок множників

і знаки двох множників, можемо вважати, що  $i = 1$  та  $p_1 = q_1$ . Тоді рівність (1.2) набуває вигляду  $p_1 p_2 \dots p_k = p_1 q_2 \dots q_m$ . Після скорочення на  $p_1$  отримаємо:  $p_2 \dots p_k = q_2 \dots q_m$ . Але добуток у лівій частині цієї рівності містить уже менше, ніж  $k$  множників. Тому за припущенням індукції кількість множників в обох частинах рівності однакова (тобто  $k - 1 = m - 1$  і  $k = m$ ), а добутки  $p_2 \dots p_k$  і  $q_2 \dots q_m$  розрізняються щонайбільше порядком і знаками множників. Якщо згадати, що  $p_1 = q_1$ , то однозначність розкладу числа  $n$  доведена.  $\square$

**Зауваження.** (a) Оскільки від'ємне число  $n$  можна записати у вигляді  $n = -|n|$ , то з теореми 1.8 одразу випливає існування та однозначність розкладу в добуток простих множників і для від'ємних цілих чисел.

(b) Тепер стає зрозумілим, чому число 1 не вважають простим: якби 1 відносили до простих чисел, то зникла б однозначність розкладу в добуток простих, бо до кожного розкладу можна було б приєднати довільну кількість множників 1.

(c) Існування та однозначність розкладу натурального числа в добуток простих підтверджується такою величезною кількістю прикладів, що дуже довго основна теорема арифметики вважалась очевидним фактом, і математики навіть не відчували потреби в її явному формулюванні. Ситуація змінилась на межі XVIII – XIX ст., коли з'явились перші приклади математичних структур, де ще можна говорити про розклад у добуток простих елементів, але однозначності розкладу вже нема. Свого часу відкриття таких структур стало для математиків великою несподіванкою. Уперше явно сформулював і довів основну теорему арифметики у 1801 р. Гаус.

Щоб показати нетривіальність цієї теореми, розглянемо множину  $2\mathbb{Z}$  парних чисел. Як і  $\mathbb{Z}$ , ця множина замкнена відносно додавання і множення, і в ній можна виділити прості елементи (назовемо їх парно-простими числами), які не розкладаються в добуток двох парних чисел. Очевидно, що парно-простими будуть усі числа вигляду  $2m$ , де  $m$  – непарне, і тільки такі числа. З основної теореми арифметики випливає, що кожне парне число  $n$  можна записати у вигляді  $n = 2^k m$ , де  $k \geq 1$  і  $m$  – непарне. Тому кожне парне число легко розкладається в добуток парно-простих:  $2^k m = 2 \cdot 2 \cdots 2 \cdot 2m$ . Але тепер розклад перестає бути однозначним. Наприклад, 840 можна розкласти в добуток парно-простих чисел п'ятьма суттєво різними способами:  $840 = 2 \cdot 2 \cdot 210 = 2 \cdot 6 \cdot 70 = 2 \cdot 10 \cdot 42 = 2 \cdot 14 \cdot 30 = 6 \cdot 10 \cdot 14$ .

**Задача 1.14.** Розкладти на прості множники число  $3^{18} - 2^{18}$ .

*Розв'язання.* Користуючись формулами скороченого множення, отримуємо:  $3^{18} - 2^{18} = (3^9 - 2^9)(3^9 + 2^9) = (3^3 - 2^3)(3^6 + 3^3 \cdot 2^3 + 2^6)(3^3 + 2^3)(3^6 - 3^3 \cdot 2^3 + 2^6) = (3 - 2)(3^2 + 3 \cdot 2 + 2^2)(3^6 + 3^3 \cdot 2^3 + 2^6)(3 + 2)(3^2 - 3 \cdot 2 + 2^2)(3^6 - 3^3 \cdot 2^3 + 2^6) = 1 \cdot 19 \cdot 1009 \cdot 5 \cdot 7 \cdot 577 = 5 \cdot 7 \cdot 19 \cdot 577 \cdot 1009$ .  $\square$

У розкладі натурального числа  $n$  у добуток простих усі множники можна взяти додатними. Якщо ще впорядкувати ці множники за зростанням, то число  $n$  можна записати у вигляді

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m},$$

де  $p_1, p_2, \dots, p_m$  – прості числа і  $p_1 < p_2 < \cdots < p_m$ . Такий розклад числа  $n$  називається *канонічним*. Основна теорема арифметики гарантує однозначність канонічного розкладу.

Інколи, особливо при одночасному розгляді канонічних розкладів кількох чисел, зручно вважати, що деякі прості числа можуть зустрічатися в канонічних розкладах із нульовими показниками. Наприклад, для числа 20, окрім розкладу  $20 = 2^2 \cdot 5^1$ , вважатимемо канонічними і розклади  $20 = 2^2 \cdot 3^0 \cdot 5^1 = 2^2 \cdot 3^0 \cdot 5^1 \cdot 7^0 = \dots$ .

**Твердження 1.4.** Якщо канонічний розклад числа  $n$  має вигляд  $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ , то кожний натуральний дільник  $d$  числа  $n$  має вигляд

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_m^{\beta_m}, \text{ де } 0 \leq \beta_1 \leq \alpha_1, 0 \leq \beta_2 \leq \alpha_2, \dots, 0 \leq \beta_m \leq \alpha_m.$$

*Доведення* випливає із простого зауваження, що коли  $n = d \cdot f$  і канонічні розклади множників  $d$  і  $f$  мають вигляд

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_m^{\beta_m}, \quad f = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_m^{\gamma_m},$$

то канонічний розклад числа  $n$  має вигляд  $n = p_1^{\beta_1 + \gamma_1} p_2^{\beta_2 + \gamma_2} \cdots p_m^{\beta_m + \gamma_m}$ .  $\square$

**Наслідок 1.** Якщо для чисел  $a$  і  $b$  відомі їх канонічні розклади  $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ ,  $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_m^{\beta_m}$ , то

$$HC\mathcal{D}(a, b) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \cdots p_m^{\min(\alpha_m, \beta_m)},$$

$$HCK(a, b) = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \cdots p_m^{\max(\alpha_m, \beta_m)}.$$

**Наслідок 2.** Числа  $a$  і  $b$  є взаємно простими тоді і лише тоді, коли кожне просте число входить із додатним показником у канонічний розклад не більше ніж одного з чисел  $a$  і  $b$ .

*Доведення.* Із наслідку 1 твердження 1.4 випливає, що числа

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} \text{ і } b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_m^{\beta_m}$$

взаємно прості тоді й лише тоді, коли  $\min(\alpha_1, \beta_1) = \min(\alpha_2, \beta_2) = \dots = \min(\alpha_m, \beta_m) = 0$ . Останнє рівносильне тому, що в кожній парі показників  $\alpha_i, \beta_i$  принаймні один із показників дорівнює 0.  $\square$

Наслідок 1 твердження 1.4 легко узагальнюється на довільну кількість чисел. Лишаємо це читачеві як вправу.

**Задача 1.15.** Довести, що коли добуток двох взаємно простих множників є точним квадратом, то кожен із множників також є точним квадратом.

*Розв'язання.* Нехай числа  $a$  і  $b$  взаємно прості,  $ab = c^2$  і

$$a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \quad b = q_1^{\beta_1} \cdots q_l^{\beta_l}, \quad c = r_1^{\gamma_1} \cdots r_m^{\gamma_m}$$

— канонічні розклади чисел  $a, b, c$  з додатними показниками  $\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_l, \gamma_1, \dots, \gamma_m$ . За наслідком 2 твердження 1.4 жодне з чисел  $p_i$  не дорівнює жодному  $q_j$ . Тому з однозначності канонічного розкладу і рівності

$$p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{\beta_1} \cdots q_l^{\beta_l} = r_1^{2\gamma_1} \cdots r_m^{2\gamma_m}$$

випливає, що  $m = k + l$  і кожен із показників  $\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_l$  дорівнює якомусь із показників  $2\gamma_1, \dots, 2\gamma_m$ . Звідси матимемо, що всі показники в лівій частині — парні:  $\alpha_1 = 2\alpha'_1, \dots, \alpha_k = 2\alpha'_k, \beta_1 = 2\beta'_1, \dots, \beta_l = 2\beta'_l$ . Але тоді  $a = (p_1^{\alpha'_1} \cdots p_k^{\alpha'_k})^2, b = (q_1^{\beta'_1} \cdots q_l^{\beta'_l})^2$ .  $\square$

**Задача 1.16.** Спираючись на основну теорему арифметики, довести ірраціональність числа  $\sqrt{2}$ .

*Розв'язання.* Припустимо, що  $\sqrt{2}$  — раціональне число. Тоді його можна записати у вигляді дробу  $\sqrt{2} = \frac{a}{b}$ . Після піднесення обох частин рівності до квадрату одержимо:  $2b^2 = a^2$ . Але в канонічному розкладі числа  $2b^2$  число 2 зустрічається з непарним показником, а в канонічному розкладі числа  $a^2$  — із парним. Отже, припущення про раціональність числа  $\sqrt{2}$  приводить до суперечності з однозначністю канонічного розкладу.  $\square$

**Задача 1.17.** Нехай  $P = \{p_1, p_2, \dots, p_k\}$  – скінчена множина простих чисел, а  $M(P)$  – множина тих натуральних чисел, які є простими дільниками яких належать до  $P$ . Довести, що ряд

$$\sum_{n \in M(P)} \frac{1}{n}$$

збігається й обчислити його суму.

**Розв'язання.** Кожне число  $n \in M(P)$  має вигляд  $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ , де  $\alpha_1, \alpha_2, \dots, \alpha_k \geq 0$ . З іншого боку, після розкриття дужок у формальному добутку нескінчених геометричних прогресій

$$S = \left(1 + \frac{1}{p_1} + \frac{1}{p_1^2} + \frac{1}{p_1^3} + \cdots\right) \cdots \left(1 + \frac{1}{p_k} + \frac{1}{p_k^2} + \frac{1}{p_k^3} + \cdots\right) \quad (1.3)$$

одержимо суму одночленів вигляду  $1/(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k})$  із показниками  $\alpha_1, \alpha_2, \dots, \alpha_k \geq 0$ , причому кожний набір  $(\alpha_1, \alpha_2, \dots, \alpha_k)$  невід'ємних показників буде зустрічатись рівно один раз. Але це означає, що

$$S = \sum_{n \in M(P)} \frac{1}{n}.$$

Застосовуючи до (1.3) формулу для суми нескінченної геометричної прогресії, остаточно одержуємо, що

$$\sum_{n \in M(P)} \frac{1}{n} = \frac{1}{1 - \frac{1}{p_1}} \cdots \frac{1}{1 - \frac{1}{p_k}} = \frac{p_1 \cdots p_k}{(p_1 - 1) \cdots (p_k - 1)}.$$

□

**Зауваження.** Із задачі 1.17 і того, що ряд  $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} + \cdots$  обернених до натуральних чисел розбігається, випливає ще одне доведення нескінченості множини простих чисел.

**Задача 1.18.** Довести, що

$$[a, b, c] = \frac{abc \cdot (a, b, c)}{(a, b) \cdot (a, c) \cdot (b, c)}. \quad (1.4)$$

*Розв'язання.* Нехай просте число  $p$  зустрічається в канонічних розкладах чисел  $a$ ,  $b$  і  $c$  відповідно з показниками  $\alpha$ ,  $\beta$  і  $\gamma$ . Без обмежень загальності можна вважати, що  $0 \leq \alpha \leq \beta \leq \gamma$ . Тоді в канонічних розкладах чисел  $(a, b, c)$ ,  $(a, b)$ ,  $(a, c)$ ,  $(b, c)$  число  $p$  зустрічається відповідно з показниками  $\alpha$ ,  $\alpha$ ,  $\alpha$ ,  $\beta$ . Тому показник, з яким  $p$  зустрічається в канонічному розкладі правої частини рівності (1.4) дорівнює  $\alpha + \beta + \gamma + \alpha - \alpha - \alpha - \beta = \gamma$  і збігається з показником  $p$  у канонічному розкладі лівої частини. Оскільки просте число  $p$  довільне, то канонічні розклади лівої і правої частин з (1.4) збігаються, що й доводить рівність.  $\square$

## 1.7. Алгоритм Евкліда

Хоча формули для НСД( $a, b$ ) і НСК( $a, b$ ) з наслідку 1 твердження 1.4 виглядають дуже симпатично, вони мало придатні для практичних обчислень. Їх головним недоліком є необхідність знати канонічний розклад чисел  $a$  і  $b$ . Для дво-цифрових чисел знайти такий розклад неважко. Але для великих чисел, які мають десятки або й сотні цифр, задача знаходження канонічного розкладу (її ще називають *задачею факторизації*) стає з обчислювального погляду дуже громіздкою (особливо коли прості множники числа також є великими).

Ще древні греки знали ефективний метод обчислення найбільшого спільного дільника двох чисел, який не вимагає розкладу цих чисел на множники. Він ґрунтуються на простій лемі.

**Лема 1.1.** Якщо  $a = qb + r$ , то  $(a, b) = (b, r)$ .

*Доведення.* Нехай  $(a, b) = d_1$ ,  $(b, r) = d_2$ . Із рівності  $a = qb + r$  випливає, що  $d_2|a$ . Крім того,  $d_2|b$ . Тому  $d_2|d_1$ . З іншого боку,  $d_1|a$ , а з рівності  $r = a - qb$  маємо, що  $d_1|r$ . Тому  $d_1|d_2$ . Отже,  $d_1$  і  $d_2$  – асоційовані. Позаяк вони додатні, то  $d_1 = d_2$ .  $\square$

Нехай тепер  $a$  і  $b$  – натуральні числа і  $a > b$ . Розділимо  $a$  на  $b$  з остачею:  $a = q_1b + r_1$ ,  $0 < r_1 < b$ . Потім розділимо  $b$  на  $r_1$ :  $b = q_2r_1 + r_2$ ,  $0 < r_2 < r_1$ . Потім розділимо  $r_1$  на  $r_2$ :  $r_1 = q_3r_2 + r_3$ ,  $0 < r_3 < r_2$ . І т.д. У нас виникає монотонно спадний ряд чисел

$$a > b > r_1 > r_2 > r_3 > \dots, \quad (1.5)$$

члени якого визначаються послідовно за допомогою ділення з остачею:

$$r_{i-1} = q_{i+1}r_i + r_{i+1}, \quad 0 < r_{i+1} < r_i.$$

Оскільки усі члени ряду (1.5) є натуральними числами, то цей ряд не може продовжуватись як завгодно довго. На якомусь кроці відбудеться ділення націло:  $r_{k-2} = q_k r_{k-1} + r_k$ ,  $r_{k-1} = q_{k+1} r_k$ .

**Теорема 1.9.** *Остання ненульова остача  $r_k$  з послідовності остач  $(1.5)$  є найбільшим спільним дільником чисел  $a$  і  $b$ .*

*Доведення.* Використовуючи лему і правило побудови послідовності (1.5), отримуємо ланцюжок рівностей  $(a, b) = (b, r_1) = (r_1, r_2) = (r_2, r_3) = \dots = (r_{k-1}, r_k) = r_k$ .  $\square$

Метод обчислення НСД( $a, b$ ), який випливає з теореми 1.9, називається *алгоритмом Евкліда*.

**Задача 1.19.** *Обчислити найбільший спільний дільник і найменше спільне кратне чисел 9367 і 4318.*

*Розв'язання.* Застосуємо алгоритм Евкліда:  $9367 = 2 \cdot 4318 + 731$ ,  $4318 = 5 \cdot 731 + 663$ ,  $731 = 1 \cdot 663 + 68$ ,  $663 = 9 \cdot 68 + 51$ ,  $68 = 1 \cdot 51 + 17$ ,  $51 = 3 \cdot 17$ . Остання ненульова остача дорівнює 17, тому  $(9367, 4318) = 17$ . Для знаходження найменшого спільного кратного скористаємося теоремою 1.7:

$$[9367, 4318] = \frac{9367 \cdot 4318}{(9367, 4318)} = 2379218. \quad \square$$

Алгоритм Евкліда можна використовувати і для знаходження зображення  $d = ma + nb$  найбільшого спільного дільника  $d$  чисел  $a$  і  $b$ . Справді, з рівності  $r_{k-2} = q_k r_{k-1} + r_k$  можна одержати зображення  $d = r_k = r_{k-2} - q_k r_{k-1}$  найбільшого спільного дільника як лінійної комбінації остач  $r_{k-1}$  та  $r_{k-2}$ . Використовуючи попередню рівність  $r_{k-3} = q_{k-1} r_{k-2} + r_{k-1}$ , одержимо зображення  $d = r_{k-2} - q_k(r_{k-3} - q_{k-1} r_{k-2}) = (1 + q_k q_{k-1}) r_{k-2} - q_k r_{k-3}$  як лінійної комбінації остач  $r_{k-2}$  та  $r_{k-3}$ . Піднімаючись ланцюжком рівностей з алгоритму Евкліда вгору, на наступному кроці одержимо зображення  $d$  як лінійної комбінації остач  $r_{k-3}$  і  $r_{k-4}$ , потім – як лінійної комбінації остач  $r_{k-4}$  та  $r_{k-5}$ , і т.д., доки за допомогою першої рівності  $a = q_1 b + r_1$  не одержимо зображення  $d$  як лінійної комбінації  $a$  і  $b$ .

**Задача 1.20.** *Зобразити найбільший спільний дільник чисел 9367 і 4318 у вигляді лінійної комбінації цих чисел.*

*Розв'язання.* Скористаємося ланцюжком рівностей із розв'язання задачі 1.19. Будемо мати:  $17 = 1 \cdot 68 - 1 \cdot 51 = 1 \cdot 68 - 1 \cdot (1 \cdot 663 - 9 \cdot 68) = 10 \cdot 68 - 1 \cdot 663 = 10 \cdot (1 \cdot 731 - 1 \cdot 663) - 1 \cdot 663 = 10 \cdot 731 - 11 \cdot 663 = 10 \cdot 731 - 11 \cdot (1 \cdot 4318 - 5 \cdot 731) = 65 \cdot 731 - 11 \cdot 4318 = 65 \cdot (9367 - 2 \cdot 4318) - 11 \cdot 4318 = 65 \cdot 9367 - 141 \cdot 4318$ .  $\square$

**Задача 1.21.** Довести, що для довільних натуральних чисел  $a, b$  і  $c$  з рівностей  $a = q_1c + r_1$  і  $b = q_2c + r_2$  випливає рівність  $(a, b, c) = (r_1, r_2, c)$ .

*Розв'язання.* Можна дати доведення, цілком аналогічне доведенню леми 1.1. А можна скористатись цією лемою і задачею 1.12. Тоді одержимо такий ланцюжок рівностей:  $(a, b, c) \stackrel{\text{зад.1.12}}{=} ((a, c), b) \stackrel{\text{лема1.1}}{=} ((r_1, c), b) \stackrel{\text{зад.1.12}}{=} (r_1, (c, b)) \stackrel{\text{лема1.1}}{=} (r_1, (r_2, c)) \stackrel{\text{зад.1.12}}{=} (r_1, r_2, c)$ .  $\square$

**Вправа 1.12.** Сформулювати й обґрунтувати алгоритм відшукання найбільшого спільного дільника трьох натуральних чисел, який базується б на твердженні задачі 1.21.

На завершення оцінимо обчислювальну складність алгоритму Евкліда, тобто кількість кроків, необхідних для знаходження останньої ненульової остачі (під кроком ми розуміємо обчислення чергового члена послідовності  $a, b, r_1, r_2, r_3, \dots$ ). Бачимо, що для великих чисел кількість кроків може бути як завгодно великою. Справді, якщо для обчислення НСД( $a, b$ ),  $a > b$ , потрібно  $k$  кроків, то обчислення за допомогою алгоритму Евкліда НСД вимагатиме вже на 1 крок більше.

**Теорема 1.10.** Обчислення за допомогою алгоритму Евкліда найбільшого спільного дільника чисел  $a$  і  $b$ ,  $a > b > 0$ , вимагає менше ніж  $2 \log_2 a$  кроків.

*Доведення.* Для зручності позначимо  $r_{-1} = a$ ,  $r_0 = b$  і нехай  $r_k$  – остання ненульова остача при обчисленні НСД( $a, b$ ). Покажемо, що в послідовності остач  $(r_{-1}, r_0, r_1, r_2, \dots, r_{k-1}, r_k)$  за будь-які два кроки остача зменшується принаймні вдвічі, точніше, що для всіх  $i$   $r_{i+2} < \frac{1}{2}r_i$ . Справді, якщо  $r_{i+1} \leq \frac{1}{2}r_i$ , то це твердження одразу випливає з нерівності  $r_{i+2} \leq r_{i+1}$ . Якщо ж  $r_{i+1} > \frac{1}{2}r_i$ , то  $r_i - r_{i+1} < r_i - \frac{1}{2}r_i = \frac{1}{2}r_i < r_{i+1}$ . Але з рівності  $r_i = r_{i+1} + (r_i - r_{i+1})$  тепер випливає, що остача  $r_{i+2}$  від ділення  $r_i$  на  $r_{i+1}$  дорівнює  $r_i - r_{i+1}$ . Тому  $r_{i+2} = r_i - r_{i+1} < \frac{1}{2}r_i$ .

Нехай тепер  $2m - 1$  – найбільше непарне число, яке не перевищує  $k$ . Тоді  $k \leq 2m$ . Крім того, з нерівності  $r_{i+2} < \frac{1}{2}r_i$  випливає, що  $r_{2m-1} < \frac{a}{2^m}$ .

Оскільки  $r_{2m-1} \geq 1$ , то  $2^m < a$ , звідки  $m < \log_2 a$ . Отже,  $k \leq 2m < 2 \log_2 a$ , що й треба було довести.  $\square$

Трішки модифікувавши алгоритм Евкліда, можна досягти, щоб обчислення  $\text{НСД}(a, b)$  вимагало завжди не більше  $\log_2 a$  кроків.

**Вправа 1.13.** Довести, що коли остача від ділення  $a$  на  $b$  дорівнює  $r$ , то  $(a, b) = (b, b - r)$ .

Будемо називати число  $b - r$  доповненням остачі  $r$  до дільника  $b$ . Розглянемо тепер послідовність  $a, b, r'_1, r'_2, r'_3, \dots$ , де  $r'_1$  – остача від ділення  $a$  на  $b$ , якщо вона не перевищує  $\frac{1}{2}b$ , або в протилежному разі її доповнення до  $b$ ;  $r'_2$  – остача від ділення  $b$  на  $r'_1$ , якщо вона не перевищує  $\frac{1}{2}r'_1$ , або в протилежному разі її доповнення до  $r'_1$ , і т.д. Як і для звичайного алгоритму Евкліда, доводиться, що останній ненульовий член цієї послідовності збігається з найбільшим спільним дільником чисел  $a$  і  $b$ . Оскільки кожний наступний член цієї послідовності приналежить вдвічі менший за попередній, то кількість кроків не перевищує  $\log_2 a$ .

**Задача 1.22.** За допомогою модифікованого алгоритму Евкліда обчислити найбільший спільний дільник чисел 9367 і 4318.

*Розв'язання.*  $9367 = 2 \cdot 4318 + 731$ ,  $4318 = 6 \cdot 731 - 68$ ,  $731 = 11 \cdot 68 - 17$ ,  $68 = 4 \cdot 17$ . Отже,  $(9367, 4318) = 17$ .  $\square$

Порівнюючи з обчисленнями в розв'язанні задачі 1.19, бачимо, що для обчислення  $(9367, 4318)$  модифікований алгоритм Евкліда вимагає на 2 кроки менше.

**Вправа 1.14.** З'ясувати, чи можна за допомогою модифікованого алгоритму Евкліда знайти зображення  $d = ta + pb$  найбільшого спільного дільника  $d$  чисел  $a$  і  $b$  у вигляді їх лінійної комбінації.

## 1.8. Розв'язування лінійних діофантових рівнянь від двох змінних

Алгоритм Евкліда можна використати для розв'язування лінійних діофантових рівнянь, тобто рівнянь вигляду  $ax + by + \dots + cz = d$  з цілими коефіцієнтами, розв'язки яких шукають у множині цілих чисел (Увага! Вимога ціличисельності розв'язку входить в означення діофантового рівняння). Ми розглянемо лише лінійні діофантові рівняння від двох змінних.

**Теорема 1.11.** Лінійне діофантове рівняння  $ax + by = c$  має розв'язки тоді й лише тоді, коли їого права частина  $c$  ділиться на найбільший спільний дільник чисел  $a$  і  $b$ .

*Доведення.* Необхідність умови очевидна, бо сума  $ax + by$  завжди ділиться на найбільший спільний дільник  $d$  чисел  $a$  і  $b$ .

Достатність. Нехай  $c = c_0d$ . За наслідком 1 теореми 1.5 існують такі цілі числа  $m$  і  $n$ , що  $ma + nb = d$ . Тоді з рівності  $mc_0a + nc_0b = c_0d$  випливає, що цілі числа  $x = mc_0$  і  $y = nc_0$  є розв'язком рівняння  $ax + by = c$ .  $\square$

**Теорема 1.12.** Якщо лінійне діофантове рівняння

$$ax + by = c \quad (1.6)$$

має цілий розв'язок  $x_0, y_0$ , то воно має нескінченно багато цілих розв'язків, і всіх їх можна знайти за формулами

$$x = x_0 - \frac{b}{d}k, \quad y = y_0 + \frac{a}{d}k, \quad (1.7)$$

де  $d = HCD(a, b)$ , а  $k$  – довільне ціле число.

*Доведення.* За умовою

$$ax_0 + by_0 = c. \quad (1.8)$$

Тому  $a(x_0 + \frac{b}{d}k) + b(y_0 - \frac{a}{d}k) = ax_0 + \frac{ab}{d}k + by_0 - \frac{ba}{d}k = ax_0 + by_0 = c$ . Крім того, числа  $\frac{b}{d}k$  і  $\frac{a}{d}k$  – цілі. Отже, формули (1.7) справді визначають розв'язок рівняння (1.6).

Нехай тепер  $x, y$  – довільний розв'язок рівняння (1.6). Позначимо  $\frac{a}{d} = a_0$ ,  $\frac{b}{d} = b_0$ . Віднімаючи (1.6) від рівності (1.8), одержимо  $a(x_0 - x) + b(y_0 - y) = 0$  або, після ділення на  $d$ ,

$$a_0(x_0 - x) + b_0(y_0 - y) = 0. \quad (1.9)$$

Звідси випливає, що  $a_0|b_0(y - y_0)$ . Оскільки, за твердженням 1.2, числа  $a_0$  і  $b_0$  взаємно прості, то  $a_0|y - y_0$ . Тому існує таке ціле число  $k$ , що  $y - y_0 = a_0k$  і  $y = y_0 + a_0k$ . Рівність (1.9) тепер набуває вигляду  $a_0(x_0 - x) = b_0a_0k$ , звідки  $x_0 - x = b_0k$  і  $x = x_0 - b_0k$ . Таким чином, кожен розв'язок рівняння (1.6) має вигляд (1.7), що й треба було довести.  $\square$

Із теорем 1.11 і 1.12 випливає наступний метод розв'язання лінійного діофантового рівняння  $ax + by = c$ :

- (a) за допомогою алгоритму Евкліда знаходимо найбільший спільний дільник  $d = (a, b)$  і перевіряємо, чи  $d|c$ . Якщо  $d \nmid c$ , то рівняння розв'язків не має.
- (b) Якщо  $d|c$ , то за допомогою алгоритму Евкліда знаходимо зображення  $d = ma + nb$  і частковий розв'язок  $x_0 = m\frac{c}{d}$ ,  $y_0 = n\frac{c}{d}$ .
- (c) Знаходимо загальний розв'язок

$$x = m\frac{c}{d} - \frac{b}{d}k, \quad y = n\frac{c}{d} + \frac{a}{d}k, \quad k \in \mathbb{Z}.$$

**Задача 1.23.** Знайти загальний розв'язок лінійного діофантового рівняння  $15x - 39y = 55$ .

*Розв'язання.*  $(15, 39) = 3$ , але  $3 \nmid 55$ . Тому дане рівняння розв'язків не має.  $\square$

**Задача 1.24.** Знайти загальний розв'язок лінійного діофантового рівняння  $187x - 143y = 77$ .

*Розв'язання.* (a) Шукаємо найбільший спільний дільник чисел 187 і 143:  $187 = 1 \cdot 143 + 44$ ,  $143 = 3 \cdot 44 + 11$ ,  $44 = 4 \cdot 11$ . Отже,  $(187, 143) = 11$ . Оскільки  $11|77$ , то розв'язки існують.

(b) Шукаємо зображення 11 як лінійної комбінації чисел 187 і 143:  $11 = 143 - 3 \cdot 44 = 143 - 3 \cdot (187 - 1 \cdot 143) = 4 \cdot 143 - 3 \cdot 187$ . Тоді  $7 \cdot (-3) \cdot 187 + 7 \cdot 4 \cdot 143 = 7 \cdot 11 = 77$  і пара  $(7 \cdot (-3), -7 \cdot 4) = (-21, -28)$  є частковим розв'язком рівняння.

(c) Загальний розв'язок має вигляд

$$x = -21 - \frac{-143}{11}k = -21 + 13k, \quad y = -28 + \frac{187}{11}k = -28 + 17k, \quad k \in \mathbb{Z}. \quad \square$$

Інколи на розв'язки лінійного діофантового рівняння накладають додаткові обмеження. Наприклад, задача про видачу касиром суми  $c$ , якщо в касі є лише банкноти номіналів  $a$  і  $b$ , зводиться до розв'язування лінійного діофантового рівняння  $ax + by = c$  за природного обмеження  $x \geq 0$ ,  $y \geq 0$  (Питання: як у цій задачі можна трактувати розв'язок, одна з компонент якого – від'ємна?).

**Задача 1.25.** Знайти всі натуральні розв'язки рівняння  $5x + 7y = 116$ .

*Розв'язання.* Оскільки  $(5, 7) = 1$  і  $3 \cdot 5 - 2 \cdot 7 = 1$ , то частковим розв'язком рівняння буде, наприклад, пара  $(3 \cdot 116, -2 \cdot 116) = (348, -232)$ , а загальний розв'язок матиме вигляд  $x = 348 - 7k$ ,  $y = -232 + 5k$ ,  $k \in \mathbb{Z}$ . Щоб розв'язки були натуральними, мають виконуватись нерівності  $348 - 7k > 0$  і  $-232 + 5k > 0$ . Звідси  $\frac{348}{7} > k > \frac{232}{5}$ . Позаяк  $k$  – ціле, то  $k \in \{47, 48, 49\}$ , а натуральні розв'язки рівняння вичерпуються парами  $(19, 3)$ ,  $(12, 8)$ ,  $(5, 13)$ .  $\square$

### 1.9. Задачі для самостійного розв'язування

1. Обчислити частку  $q$  й остачу  $r$  від ділення  $a$  на  $b$ , якщо:
  - (a)  $a = -249$ ,  $b = 21$ ; (b)  $a = 387$ ,  $b = -12$ ; (c)  $a = -314$ ,  $b = -8$ .
2. Обчислити натуральне число  $b$  й остачу  $r$  від ділення числа  $a$  на  $b$ , якщо число  $a$  і частка  $q$  від ділення  $a$  на  $b$  дорівнюють:
  - (a)  $a = 13307$ ,  $q = 97$ ; (b)  $a = 17000$ ,  $q = 89$ .
3. Обчислити натуральне число  $b$  і частку  $q$  від ділення числа  $a$  на  $b$ , якщо  $q > 1$ , а число  $a$  і остача  $r$  від ділення  $a$  на  $b$  дорівнюють:
  - (a)  $a = 4500$ ,  $r = 139$ ; (b)  $a = 4600$ ,  $r = 123$ .
4. Довести, що для кожного натурального числа  $n$ :
  - (a)  $169|3^{3n} - 26n - 1$ ; (b)  $3^n|2^{3^n} + 1$ .
5. Довести, що для кожного цілого числа  $k \geq 0$ :
  - (a)  $7|2^{2^{2k+1}} + 3$ ; (b)  $13|2^{2^{2k+2}} - 3$ .
6. Довести, що кожне із чисел  $48, 4488, 444888, 44448888, \dots$  розкладається в добуток двох послідовних парних чисел.
7. Знайти всі такі натуральні прості числа  $p$ , для яких кожне із чисел  $p + 8$ ,  $p + 14$ ,  $p + 26$ ,  $p + 32$  також буде простим. Як зміниться відповідь, якщо не вимагати, щоб число  $p$  було натуральним?
8. Довести, що існує нескінченно багато простих чисел вигляду  $6k - 1$ .
9. За допомогою “решета Ератостена” знайти всі прості числа з проміжку:
  - (a)  $[1070, 1090]$ ; (b)  $[1480, 1490]$ ; (c)  $[1330, 1360]$ .

10. Довести, що  $[a, b, c] = [[a, b], c] = [[a, c], b] = [[b, c], a]$ .
11. Знайти довжину найкоротшої арифметичної прогресії, членами якої будуть числа:  
 (a) 20, 152, 236, 404; (b) 30, 90, 2095, 3085, 3253.
12. Довести, що коли  $b|a$  і  $c|a$ , то  $[b, c]|a$ .
13. Описати всі парні числа, для яких розклад у добуток парно-простих чисел є однозначним.
14. Скількома суттєво різними способами можна розкласти в добуток парно-простих чисел  
 число  $2^m p_1 p_2 \dots p_k$ , де  $m \geq 1$ , а  $p_1, p_2, \dots, p_k$  – попарно різні непарні прості числа?
15. Довести, що коли добуток двох взаємно простих множників є точним  $n$ -м степенем, то кожен із множників також є точним  $n$ -м степенем.
16. Довести, що для кожного простого числа  $p$  і натурального числа  $k$ ,  $k < p$ ,  $p|\binom{p}{q}$ , де  $\binom{p}{q}$  – біноміальний коефіцієнт.
17. Розкласти на прості множники число:  
 (a)  $2^9 + 3^9$ ; (b)  $5^{12} - 3^{12}$ ; (c)  $3^{20} - 2^{20}$ .
18. Нехай натуральні числа  $k, l, m, n$  задовольняють умову  $kl = mn$ .  
 Довести, що число  $k + l + m + n$  є складеним.
19. Довести, що для будь-яких непарних чисел  $m, n, k$   $(m, n, k) = (\frac{m+n}{2}, \frac{m+k}{2}, \frac{n+k}{2})$ .
20. Довести, що  $(a, b)(a, c)(b, c)[a, b][a, c][b, c] = a^2 b^2 c^2$ .
21. Обчислити найбільший спільний дільник і найменше спільне кратне чисел:  
 (a) 993 і 3961; (b) 2533 і 4023; (c) 17385 і 6283; (d) 8385 і 14921.
22. Обчислити найбільший спільний дільник  $d$  чисел  $a$  і  $b$  і знайти його лінійне зображення  $d = ma + nb$ :  
 (a)  $a = 105, b = 154$ ; (b)  $a = 756, b = 855$ ; (c)  $a = 966, b = 3289$ ;  
 (d)  $a = 1997, b = 613$ .

23. Обчислити найбільший спільний дільник чисел  
(a) 1287, 1001 і 1518; (b) 1305, 1827 і 1015.
24. Знайти загальний розв'язок лінійного діофантового рівняння:  
(a)  $5x + 7y = 2$ ; (b)  $12x + 5y = 19$ ; (c)  $41x + 37y = 21$ ; (d)  $27x - 51y = 21$ .
25. Нехай натуральні числа  $m$  і  $n$  взаємно прості і  $m > n$ . Довести, що:  
(a) будь-яке натуральне число  $k > mn$  можна записати у вигляді  $k = mx + ny$  із натуральними  $x$  та  $y$ ;  
(b) будь-яке натуральне число  $k \geq m(n - 1)$  можна записати у вигляді  $k = mx + ny$  із невід'ємними цілими  $x$  та  $y$ .
26. Знайти всі натуральні розв'язки діофантового рівняння:  
(a)  $12x + 5y = 203$ ; (b)  $15x + 21y = 321$ .
27. Знайти загальний розв'язок лінійного діофантового рівняння  $35x + 55y + 77z = 1$ .