Глава 4

АЛГОРИТМИ ЕВКЛІДА

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

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

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

Алгоритм 1. Знаходження частки та остачі від ділення

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

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

покласти $v_1 = n - a$;

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

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

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

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

якщо $v_3 < a$, то .....

.....

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

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

1. Алгоритм Евкліда знаходження найбільшого спільного дільника

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

Алгоритм 2. Знаходження найбільшого спільного дільника

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

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

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

якщо $r_1 = 0$, то $d = a$ STOP.

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

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

якщо $r_2 = 0$, то $d = r_1$ STOP.

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

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

якщо $r_3 = 0$, то $d = r_2$ STOP.

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

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

якщо $r_4 = 0$, то .....

.....

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

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

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

нює нулеві нова остача. Якщо позначити

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

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

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

③ Дія алгоритму завершується, якщо на певному кроці

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

де ϕ — це *золотий перетин*.

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

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

2. Знаходження оберненого числа в арифметиці за модулем

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

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

для деякого j. Це означає, що рівняння

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(8)

			q_3	q_2	q_1
0	1				

$=$

			2	1	4
0	1				

Ми будемо виконувати для фрагментів

		i_3
i_1	i_2	

таблиці (8) таке перетворення:

(9)

		i_3
i_1	i_2	

$\longrightarrow$

		i_3
i_1	i_2	i_4

, де $i_4 = i_3 i_2 + i_1$.

Починаємо з фрагменту

		q_3
0	1	

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

		2	1	4
0	1			

$\to$

		2	1	4
0	1	2		

$\to$

		2	1	4
0	1	2	3	

$\to$

		2	1	4
0	1	2	3	14

Тепер таблиця є заповненою. Нескладно перевірити, що

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

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

Загальний випадок розглянуто у наступному результаті.

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

(10)

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

,

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

(11)

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

.

Тоді

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

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

Крім того,

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3. Розширений алгоритм Евкліда

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

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

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

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

Алгоритм 3. Розширений алгоритм Евкліда

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

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

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

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

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

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

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

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

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

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

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

.....

В алгоритмі 3 покроково обчислюються послідовності

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

Зауваження 3. Якщо не обчислювати послідовності

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

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

Умовою завершення алгоритму 3 на кроці k є

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

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

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

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

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

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

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

Тому за припущенням індукції

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

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

Крім того,

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

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

Теорема 4. *Нехай для певного k виконано умову* (17), *тобто алгоритм* 3 *закінчується на кроці k. Тоді*

$$u_k a + v_k n = (n, a).$$

Таким чином, якщо a та n є взаємно простими, то

$$u_k a + v_k n = 1.$$

Доведення. З другої умови в (18) випливає, що $u_k a + v_k n = t_k$. Оскільки t_k — це остача від ділення на попередньому кроці, то $t_k = (n, a)$ на підставі теореми 1. $\square$

4. Контрольні питання

1. Перевірити, що $n = ka + r$ (стор. 94).

2. Чому на певному кроці v_k стане меншим за n? (стор. 94).

3. Впевнитись, що на k-ому кроці алгоритм 2 обчислює формулу (2) (стор. 96).

4. Чому остачі в алгоритмі 2 зменшуються на кожному кроці? (стор. 96).

5. Чому r повинно ділитися на k? (стор. 96).

6. Пояснити, чому (j, r) ділиться на (i, j)? (стор. 96).

7. Чому ми доведемо, що $(a, n) = r_k$, якщо діятимо, як у доведенні теореми 1? (стор. 97).

8. Чому y_0 є цілим числом? (стор. 98).

9. Пояснити, чому $x = c + \lambda n$ для деякого $\lambda \in \mathbf{Z}$? (стор. 98).

10. Чому $y = y_0 - a\lambda$? (стор. 99).

11. Як знайти c, якщо знати тільки один з розв'язків рівняння (4)? (стор. 99).

12. Перевірити рівність $16^{-1} \pmod{75} = 61$. (стор. 100).

13. Впевнитись, що алгоритм 3 є цілком ідентичним до алгоритму 2, якщо не обчислювати послідовності (16). (стор. 104).

14. Перевірити, що умови (18) стають тривіальними при $k = 1$, а саме $n = n$ та $a = a$. (стор. 105).

5. Задачі для самостійної роботи

Задача 1. *Використовуючи алгоритм Евкліда (алгоритм 2), знайти найбільший спільний дільник (a, b) чисел a та b:*

a) $a = 4076$ *та* $b = 1024$; b) $a = 4076$ *та* $b = 1706$;
c) $a = 1769$ *та* $b = 2378$; d) $a = 1331$ *та* $b = 5005$.

Задача 2. *За допомогою алгоритма Евкліда (алгоритм 2) знайти найбільший спільний дільник чисел*

a) 1024 *та* 1000; b) 2024 *та* 1024;
c) 5040 *та* 7700; d) 3777 *та* 5565.

Задача 3. *За допомогою алгоритма Евкліда знайти*

(a) $(252, 198)$; (b) $(34, 55)$; (c) $(20785, 44350)$.

Задача 4. *За допомогою алгоритма Евкліда (алгоритм 2) знайти*

(a) $(45, 75)$; (b) $(102, 222)$; (c) $(666, 1414)$.

Задача 5. *За допомогою алгоритма Евкліда (алгоритм 2)знайти найбільший спільний дільник чисел*

a) 2076 *та* 1076; b) 2076 *та* 1776;
c) 1976 *та* 1776; d) 3076 *та* 1776.

Задача 6. *Довести, що теорему 3 можна використовувати навіть у випадку* $(a,n) \neq 1$. *Які зміни необхідно внести у формулювання теореми, якщо* $(a,n) \neq 1$?

Задача 7. *Використовуючи обчислення, зроблені при розв'язанні задачі* 1, *та задачу* 6 *записати* $(4076, 1024)$ *у вигляді лінійної комбінації* 4076 *та* 1024. *Цю ж задачу розв'язати для пар чисел* (b)–(d) *з задачі* 1.

Задача 8. *Записати* (a,b) *у вигляді лінійної комбінації* a *та* b *для чисел з задачі* 2.

Задача 9. *Записати* (a,b) *у вигляді лінійної комбінації* a *та* b *для чисел з задачі* 3.

Задача 10. *Записати* (a,b) *у вигляді лінійної комбінації* a *та* b *для чисел з задачі* 4.

Задача 11. *Записати* (a,b) *у вигляді лінійної комбінації* a *та* b *для чисел з задачі* 5.

Задача 12. *Використовуючи розширений алгоритм Евкліда (алгоритм* 3), *записати* (a,b) *у вигляді лінійної комбінації* a *та* b *для чисел з задачі* 2.

Задача 13. *Використовуючи розширений алгоритм Евкліда (алгоритм* 3), *записати* (a,b) *у вигляді лінійної комбінації* a *та* b *для чисел з задачі* 5.

Задача 14. *Нехай* $(a,n) = d$. *Довести, що* $(a/d, n/d) = 1$.

Задача 15. *Нехай* a, b, c — *три натуральні числа. Довести, що* $(ac, bc) = c(a,b)$.

Задача 16. *Спростувати наступне твердження: якщо* $(a,b) = 1 = (b,c)$, *то* $(a,c) = 1$.

Задача 17. *Спростувати наступне твердження: якщо* $(a,b) = 2 = (b,c)$, *то* $(a,c) = 2$.

Задача 18. *Нехай* $p_1, \ldots, p_n$ — *різні прості числа,* $a = p_1^{\alpha_1} \ldots p_n^{\alpha_n}$, $b = p_1^{\beta_1} \ldots p_n^{\beta_n}$. *Довести, що* $(a,b) = p_1^{\min\{\alpha_1,\beta_1\}} \ldots p_n^{\min\{\alpha_n,\beta_n\}}$.

Задача 19. *Найменшим спільним кратним двох натуральних чисел a та b називається найменше натуральне число, яке ділиться і на a, і на b. Це число позначається $[a, b]$. Довести, що*

a) *якщо p — просте число, $a = p^\alpha$, $b = p^\beta$, то $[a, b] = p^{\max\{\alpha,\beta\}}$;*
b) *якщо p_1, p_2 — два різних простих числа, $a = p_1^{\alpha_1} p_2^{\alpha_2}$, $b = p_1^{\beta_1} p_2^{\beta_2}$, то $[a, b] = p_1^{\max\{\alpha_1,\beta_1\}} p_2^{\max\{\alpha_2,\beta_2\}}$;*
c) *якщо $p_1, \ldots, p_n$ — різні прості числа, $a = p_1^{\alpha_1} \ldots p_n^{\alpha_n}$, $b = p_1^{\beta_1} \ldots p_n^{\beta_n}$, то $[a, b] = p_1^{\max\{\alpha_1,\beta_1\}} \ldots p_n^{\max\{\alpha_n,\beta_n\}}$.*

Задача 20. *Знайти $[a, b]$ для всіх пар чисел a та b з задачі 1.*

Задача 21. *Знайти $[a, b]$ для всіх пар чисел a та b з задачі 2.*

Задача 22. *Знайти $[a, b]$ для всіх пар чисел a та b з задачі 3.*

Задача 23. *Знайти $[a, b]$ для всіх пар чисел a та b з задачі 4.*

Задача 24. *Знайти $[a, b]$ для всіх пар чисел a та b з задачі 5.*

Задача 25. *Довести, що $[a, b] \cdot (a, b) = ab$.*

Задача 26. *Довести, що $(a, b) \mid [a, b]$.*

Задача 27. *Довести, що $[ca, cb] = c[a, b]$.*

Задача 28. *Чи є вірними наступні твердження?*

a) *Найменше спільне кратне двох простих чисел дорівнює їхньому добутку.*
b) *Найменше спільне кратне двох послідовних натуральних чисел дорівнює їхньому добутку.*
c) *Найменше спільне кратне двох різних простих чисел дорівнює їхньому добутку.*
d) *Якщо $(a, b) = 1$, то $[a, b] = ab$.*
e) *Якщо $p \nmid a$, то $[p, a] = pa$.*

Задача 29. *Чи є вірними наступні твердження?*

a) *Якщо $[a, b] = 1$, то $a = 1 = b$.*
b) *Якщо $[a, b] = b$, то $a = 1$.*
c) *Якщо $[a, b] = b$, то $a \mid b$.*
d) *Якщо $[a, b] = ab$, то $a = b$.*
e) *Якщо $[a, b] = ab$ and $[b, c] = bc$, то $[a, c] = ac$.*

Задача 30. *Розглянемо прямокутник розміру* 23×13*, який позначимо* P_1 *(див. рис. 1). Найбільший квадрат* K_1*, який можна в нього вписати, має розмір* 13×13*. Найбільший квадрат* K_2*, який можна вписати в* $P_2 = P_1 \setminus K_1$*, має розмір* 10×10*. В* $P_3 = P_2 \setminus K_2$ *можна вписати три квадрати розміру* 3×3*. Після цього залишаються три квадрати розміру* 1×1 *(див. рис. 2).*

Рис. 1. *Прямокутник* P_1

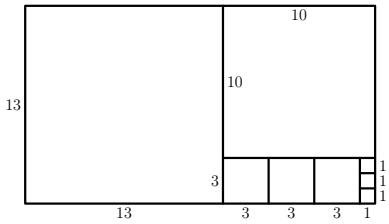

Рис. 2. *Вписані квадрати*

Запишемо тепер дії алгоритму Евкліда для знаходження $(23, 13)$:

$$\begin{aligned} 23 &= 1 \cdot 13 + 10 \\ 13 &= 1 \cdot 10 + 3 \\ 10 &= 3 \cdot 3 + 1 \\ 3 &= 3 \cdot 1. \end{aligned} \tag{19}$$

a) *Чи бачите ви зв'язок між обчисленнями в алгоритмі Евкліда та заповненням прямокутника квадратами?*
b) *Чи є цей зв'язок універсальним?*

Задача 31. *Два гравці починають гру, маючи пару додатних чисел. По черзі вони роблять кроки наступного типу. Гравець може спочатку переставити числа у порядку зростання, а потім замінити нову пару* $\langle x, y\rangle$*,* $x \geq y$*, на будь-яку іншу вигляду* $\langle x - ty, y\rangle$*, де* t *— таке натуральне число, що* $x - ty \geq 0$*. Виграє той, хто першим отримає пару з нульовою координатою. Доведіть, що якщо гра починається з парою* $\langle a, b\rangle$*, то вона закінчується парою* $\langle 0, (a, b)\rangle$*.*

Задача 32. *Нехай* $a \in \mathbf{N}$. *Розглянемо всі такі числа* n, *що алгоритм Евкліда закінчується за* n *кроків при обчисленні* (a, b) *для деякого* $b < a$ (*тобто*, $(a, b) = r_{n-1}$). *Найбільше з таких* n *назвемо висотою числа* a *і позначимо* $h(a)$.

a) *Довести, що* $h(a) = 1$ *тобі і тільки тоді, коли* $a = 2$;
b) *Підрахувати* $h(a)$ *для* $a \leq 8$.

6. БІОГРАФІЇ

Евклід, *грец.* $Ενκλειδης$ (близько 365–близько 300 до Р. Х.), старогрецький математик і визнаний основоположник математики.

Евклід

Наукова діяльність Евкліда проходила в Александрійській бібліотеці — суспільній інституції, що являла собою бібліотечний, науковий, навчальний, інформаційно-аналітичний, і культурологічний комплекс.*

Основна праця Евкліда "*Начала*" (латинізована назва "*Елементи*") включає в себе 13 книжок, у яких міститься систематизований виклад геометрії, а також деяких питань теорії чисел.

Книги з такою ж назвою, в яких послідовно викладалися всі основні факти геометрії і теоретичної арифметики, складалися раніше Гіппократом Хіосським, Леонтом і Февдієм. Проте "*Начала*" Евкліда витіснили всі ці твори з ужитку і протягом більш ніж двох тисячоліть

* Місто Александрія знаходиться зараз у Єгипті. Александрійська бібліотека заснована, як вважається, Птолемеєм I на початку третього століття до Р. Х. Значення цієї величезної бібліотеки важко переоцінити для елінського світу: у ній зберігалися сотні тисяч папірусних сувій, які використовувались вченими для розвитку науки.

залишалися базовим підручником геометрії. Створюючи свій підручник, Евклід включив в нього багато з того, що було створене його попередниками, обробивши цей матеріал і звівши його воєдино.

У рукописах, що дійшли до нас, до тринадцяти книг Евкліда додані ще дві: XIV книга належить александрійцу Гипсиклу (біля 200 р. до Р. Х.), а XV книгу створено під час життя Ісідора Мілетського, будівельника храму св. Софії в Константинополі (початок VI ст. Р. Х.).

Коментарі до "*Начал*" в античності складали Герон, Порфирій, Папп, Прокл, Симплікій. Зберігся коментар Прокла до I книги, а також коментар Паппа до X книги (у арабському перекладі).

У створенні і розвитку науки нового часу "*Начала*" зіграли важливу ідейну роль; вони залишаються і донині зразком математичного строгості.

Алгоритм знаходження найбільшого спільного дільника двох чисел (алгоритм 2) в "*Началах*" описано двічи, спочатку у книзі VII (для знаходження найбільшого спільного дільника двох натуральних чисел), а потім у книзі X (для знаходження найбільшої загальної міри двох однорідних величин). В обох випадках Евклід надав геометричний опис алгоритму.

Цей алгоритм не було відкрито Евклидом, оскільки згадка про нього є вже в "*Топіках*" Аристотеля. Давньогрецькі математики називали цей алгоритм $\alpha\nu\theta\nu\phi\alpha\iota\rho\varepsilon\sigma\iota\zeta$, тобто "взаємне віднімання".

Про життя Евкліда мало що відомо, крім того, що він жив і викладав в Александрії. Тим не менш, існує багато фольклорних цитат, приписуваних Евкліду. Наприклад, він нібито був учителем правителя Птолемея I, який царював з 306 р. до Р. Х. Якось Птолемей запитав у Евкліда, чи є простіший спосіб вивчити геометрію. Евклід нібито відповів, що у геометрії не існує царської дороги.**

** Про це написав Прокл у коментарях до книги I Евклідівських "*Начал*". Вираз "царська дорога" став крилатим ще в античні часи; так називали найбільш швидкий, легкий й розумний спосіб досягнути своєї мети. Вираз з'явився після того, як Геродот у своїй "*Історії*" із захопленням описав спосіб доставки пошти у V сторіччі до Р. Х. під час правління персидського царя Дарія, який побудував для цього спеціальну дорогу.

Ламе, *Габриель* (1795–1870), французький математик, механік, фізик та інженер. Вніс вагомий вклад в розвиток математичної фізики та теорії пружності.

Габриель Ламе

Ламе вважається провідним французький математик свого часу. Про це писали багато хто, зокрема Гаусс, який не був людиною, яка так просто поширювала схвальні відгуки про інших. Дивно, але за межами Франції йому давали більш високі оцінки, ніж усередині країни. Можливо французам, здавалося, що його дослідження є занадто прикладними для математика і водночас занадто теоретичними для інженера.

Одним з найбільших його внесків в математику є використання криволінійних координат, але відомими є також *параметри* (у теорії пружності) та *функції* (у рівняннях математичної фізики) Ламе.

Ламе намагався слідувати новим ідеям Коші про строгість математичних доведень. Відомою є критична стаття Ламе про стиль викладання та непослідовне доведення теореми Тейлора в університеті Санкт-Петербурга, де Ламе провів певний час.