

## Дискретна математика - 2

### Змістовий модуль 7. Теорія чисел і криптографія

#### Тема 7. Алгоритм Евкліда. Лінійні конгруенції

##### План лекції

- Алгоритм Евкліда
- Лінійні конгруенції
- Первісні корені й дискретні логарифми

##### Алгоритм Евкліда.

Нехай  $a$  та  $b$  – цілі числа, які одночасно не дорівнюють нулю. Найбільше ціле  $d$  таке, що  $d \mid a$  і  $d \mid b$  називають *найбільшим спільним дільником*  $a$  та  $b$  і позначають як  $\gcd(a, b)$ .

Для знаходження  $\gcd(a, b)$  можна використати факторизацію. Нехай

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, \quad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n},$$

тут  $p_1, p_2, \dots, p_n$  – прості множники (деякі степені можуть дорівнювати нулю). Тоді

$$\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}.$$

**Приклад.** Оскільки  $120 = 2^3 \cdot 3 \cdot 5$ ,  $500 = 2^2 \cdot 5^3$ , то

$$\gcd(120, 500) = 2^{\min(3, 2)} \cdot 3^{\min(1, 0)} \cdot 5^{\min(1, 3)} = 2^2 \cdot 3^0 \cdot 5^1 = 20.$$

Числа  $a$  та  $b$  називають *взаємно простими*, якщо  $\gcd(a,b)=1$ .

Числа  $a_1, a_2, \dots, a_n$  називають *попарно взаємно простими*, якщо  $\gcd(a_i, a_j)=1$  для всіх  $1 \leq i < j \leq n$ . Наприклад, числа 10, 17 і 21 – попарно взаємно прості, а числа 10, 19 і 24 – ні.

Функцією Ейлера називають функцію  $\varphi$ , визначену на множині додатних цілих чисел, значення якої дорівнює кількості додатних цілих чисел, не більших  $n$ , які є взаємно простими з  $n$ .

Можна довести, що число  $n$  є простим тоді й тільки тоді, коли  $\varphi(n) = n - 1$ .

Обчислювати найбільший спільний дільник двох цілих чисел виходячи з їхньої факторизації нерационально. Ефективніше це робити за допомогою алгоритму Евкліда. Цей алгоритм зручно пояснити на прикладі. Знайдемо  $\gcd(91, 287)$ . Спочатку поділимо більше з цих двох чисел на менше:

$$287 = 91 \cdot 3 + 14 \text{ (перше ділення).}$$

Кожен дільник 91 і 287 є також дільником  $287 - 91 \cdot 3 = 14$ . Отже, кожний дільник 91 і 14 також є дільником  $287 = 91 \cdot 3 + 14$ . Отже, найбільший спільний дільник 91 і 287 той самий, що й найбільший спільний дільник 91 і 14. Із цих міркувань випливає, що задачу знаходження  $\gcd(91, 287)$  можна спростити до задачі знаходження  $\gcd(91, 14)$ .

Далі, поділимо 91 на 14:

$$91 = 14 \cdot 6 + 7 \text{ (друге ділення).}$$

Аналогічні міркування приводять до висновку, що  $\gcd(91, 14) = \gcd(14, 7)$ .

Поділивши 14 на 7, одержимо

$$14 = 7 \cdot 2 \text{ (третє ділення).}$$

Із того, що 7 ділить 14 випливає, що  $\gcd(14,7)=7$ . Оскільки  $\gcd(91,287) = \gcd(91,14) = \gcd(14,7) = 7$ , то задачу знаходження  $\gcd(91,287)$  розв'язано, бо 7 є останньою ненульовою остачею.

Нижче подано алгоритм Евкліда у вигляді псевдокоду.

Алгоритм 4.2. Алгоритм Евкліда.

**procedure**  $\gcd(a,b : \text{positive integers})$

$x := a$

$y := b$

**while**  $y \neq 0$

**begin**

$r := x \bmod y$

$x := y$

$y := r$

**end**

**return**  $x \{ \gcd(a,b) \text{ is } x \}$

В алгоритмі початкові значення для змінних  $x$  та  $y$  – це  $a$  та  $b$  відповідно, причому  $a \geq b$ . На кожній ітерації алгоритму  $x$  замінюється на  $y$ , а  $y$  замінюється на  $x \bmod y$ , що являє собою остачу від ділення  $x$  на  $y$ . Ітерації продовжуються допоки виконується умова  $y \neq 0$ . Алгоритм зупиняється коли  $y=0$ , і значення  $x$  у цій точці, яке є останньою ненульовою остачею в цій процедурі, є найбільшим спільним дільником  $a$  та  $b$ . Кількість операцій ділення в цьому алгоритмі складає  $O(\log b)$ .

### ***Найбільші спільні дільники як лінійні комбінації.***

Важливою властивістю найбільшого спільного дільника двох додатних цілих чисел  $a$  та  $b$  є те, що його можна подати як лінійну комбінацію

$$sa + tb,$$

де  $s$  та  $t$  – цілі. Наприклад,  $\gcd(6, 14) = 2$ , і  $2 = (-2) \cdot 6 + 1 \cdot 14$ . Цей факт констатується в наступній теоремі.

**Теорема 3.8 (теорема Безу).** Якщо  $a$  та  $b$  – додатні цілі числа, то існують такі цілі числа  $s$  і  $t$ , що  $\gcd(a, b) = sa + tb$ .

Опишемо на прикладі метод, який дає змогу знайти фактичне подання  $\gcd(a, b)$  як лінійної комбінації  $sa + tb$ . Цей метод ґрунтується на зворотному проходженні кроків алгоритму Евкліда, отже, спочатку потрібно виконати сам алгоритм.

**Приклад.** Виразити  $\gcd(252, 198) = 18$  як лінійну комбінацію 252 і 198 з цілими коефіцієнтами.

Спочатку покажемо, що  $\gcd(252, 198) = 18$ . Застосуємо алгоритм Евкліда.

$$252 = 1 \cdot 198 + 54 \text{ (перше ділення),}$$

$$198 = 3 \cdot 54 + 36 \text{ (друге ділення),}$$

$$54 = 1 \cdot 36 + 18 \text{ (третє ділення),}$$

$$36 = 2 \cdot 18 \text{ (четверте ділення).}$$

Остання ненульова остача 18, отже,  $\gcd(252, 198) = 18$ . Використовуючи передостаннє (третє ділення) ми можемо записати 18 як лінійну комбінацію 54 та 36. Маємо

$$18 = 54 - 1 \cdot 36.$$

Друге ділення показує, що

$$36 = 198 - 3 \cdot 54.$$

Підставимо цей вираз для 36 у попередню рівність, тоді подамо 18 як лінійну комбінацію 54 і 198:

$$18 = 54 - 1 \cdot 36 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198$$

Перше ділення показує, що  $54 = 252 - 1 \cdot 198$ . Підставляючи цей вираз у попередню рівність дістанемо вираз для  $\gcd(252, 198) = 18$  у вигляді лінійної комбінації 252 і 198. Остаточо матимемо:

$$18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198.$$

Отже, ми дістали вираз для  $\gcd(252, 198) = 18$  у вигляді лінійної комбінації  $s \cdot 252 + t \cdot 198$ , де  $s = 4$ ,  $t = -5$ .

Наведений спосіб визначення коефіцієнтів  $s$  і  $t$  є наочним, але не оптимальним, бо вимагає збереження в пам'яті проміжних обчислень алгоритму Евкліда. Розглянемо кращий спосіб, так званий *розширений алгоритм Евкліда*. Цей алгоритм дає змогу отримати вираз для  $\gcd(a, b)$  у вигляді лінійної комбінації  $a$  та  $b$  за один прохід, без використання зворотних кроків.

### ***Розширений алгоритм Евкліда.***

Покладемо  $s_0 = 1$ ,  $s_1 = 0$ ,  $t_0 = 0$ ,  $t_1 = 1$ . Нехай  $s_j = s_{j-2} - q_{j-1}s_{j-1}$  і  $t_j = t_{j-2} - q_{j-1}t_{j-1}$  для  $j = 2, 3, \dots, n$ , де  $q_j$  – частки від ділення, яке використовується, коли алгоритм Евкліда обчислює  $\gcd(a, b)$ . Можна довести, що  $\gcd(a, b) = s_n a + t_n b$ .

**Приклад.** Використаємо розширений алгоритм Евкліда для подання  $\gcd(252, 198)$  як лінійної комбінації 252 і 198. Коли застосуємо алгоритм Евкліда, то одержимо такі частки та залишки:  $q_1 = 1$ ,  $r_2 = 54$ ,  $q_2 = 3$ ,  $r_3 = 36$ ,  $q_3 = 1$ ,  $r_4 = 18$ ,  $q_4 = 2$ . Зазначимо, що в цьому прикладі  $n = 4$ . Тепер ми обчислимо значення  $s_i$  і  $t_i$ , використовуючи рекурентні вирази, наведені вище.

$$\begin{aligned} s_2 &= s_0 - q_1 s_1 = 1 - 1 \cdot 0 = 1 & t_2 &= t_0 - q_1 t_1 = 0 - 1 \cdot 1 = -1 \\ s_3 &= s_1 - q_2 s_2 = 0 - 3 \cdot 1 = -3 & t_3 &= t_1 - q_2 t_2 = 1 - 3 \cdot (-1) = 4 \\ s_4 &= s_2 - q_3 s_3 = 1 - 1 \cdot (-3) = 4 & t_4 &= t_2 - q_3 t_3 = -1 - 1 \cdot 4 = -5 \end{aligned}$$

Отже,  $\gcd(252, 198) = 18$ , і  $18 = 4 \cdot 252 - 5 \cdot 198$ .

Подамо розширений алгоритм Евкліда у вигляді псевдокоду. Ми виходимо з алгоритму Евкліда (алгоритму 1) і додаємо змінні для зберігання значень  $s$  і  $t$ . Нам потрібно три з них, бо нове значення  $s$  залежить від попередніх двох значень  $s$  і те саме щодо  $t$ . Нам також потрібно пам'ятати значення  $q$  – результат чергового ділення.

#### Алгоритм 4.3. Розширений алгоритм Евкліда.

**procedure** *extended \_ Euclidean*(*a, b* : *positive integers*)

*x* := *a*

*y* := *b*

*oldolds* := 1

*olds* := 0

*oldoldt* := 0

*oldt* := 1

**while** *y* ≠ 0

**begin**

*q* := *x* **div** *y*

*r* := *x* **mod** *y*

*x* := *y*

*y* := *r*

*s* := *oldolds* − *q* · *olds*

*t* := *oldoldt* − *q* · *oldt*

*oldolds* := *olds*

*oldoldt* := *oldt*

*olds* := *s*

*oldt* := *t*

**end**

{gcd(*a, b*) is *x*, and (*oldolds*) · *a* + (*oldoldt*) · *b* = *x*}

## Лінійні конгруенції.

Конгруенцію  $ax \equiv b \pmod{m}$ , де  $m$  – додатне ціле число,  $a$  та  $b$  – цілі,  $x$  – змінна, називають *лінійною конгруенцією*. Такі конгруенції виникають у теорії чисел та її застосуваннях.

Як розв'язати лінійну конгруенцію  $ax \equiv b \pmod{m}$ , тобто як знайти всі цілі числа  $x$ , які задовольняють цю конгруенцію? Метод, що ми його тут розглянемо, використовує ціле число  $a^{-1}$  таке, що  $a^{-1}a \equiv 1 \pmod{m}$ , якщо таке число існує. Таке ціле  $a^{-1}$  називають *оберненим* до  $a$  за модулем  $m$ . Теорема 3.9 гарантує, що обернене до  $a$  за модулем  $m$  існує, якщо  $a$  та  $m$  взаємно прості.

**Теорема 3.9.** Якщо  $a$  та  $m$  взаємно прості цілі числа і  $m > 1$ , то обернене до  $a$  за модулем  $m$  існує. Більше того, воно єдине обернене до  $a$  за модулем  $m$ . (Це означає, що існує єдине додатне ціле  $a^{-1} < m$ , обернене до  $a$  за модулем  $m$ , а кожне інше число, обернене до  $a$  за модулем  $m$ , буде конгруентним до  $a^{-1}$  за модулем  $m$ .)

**Доведення.** Доведемо лише існування. За теоремою 3.8 (Безу) із  $\gcd(a, m) = 1$  випливає існування таких цілих  $s$  і  $t$ , що  $sa + tm = 1$ . Звідси випливає, що  $sa + tm \equiv 1 \pmod{m}$ . Оскільки  $tm \equiv 0 \pmod{m}$ , то  $sa \equiv 1 \pmod{m}$ .



Для практичного знаходження  $a^{-1}$  можна скористатись розширеним алгоритмом Евкліда.

**Приклад.** Знайдемо обернене до 3 за модулем 7. Оскільки  $\gcd(3, 7) = 1$ , то теоремою 3.9 таке обернене існує. У цьому простому прикладі звичайний алгоритм Евкліда одразу приводить до результату:

$$7 = 2 \cdot 3 + 1;$$

із останньої рівності маємо

$$1 = -2 \cdot 3 + 1 \cdot 7.$$

Із цього випливає, що коефіцієнти Безу для 3 і 7 становлять  $-2$  і  $1$  відповідно. Отже,  $-2$  є оберненим до 3 за модулем 7. Зазначимо, що кожне ціле, конгруентне до  $-2$  за модулем 7, є також оберненим до 3: це числа  $-9, 5, 12$  тощо. Єдиним цілим, оберненим до 3 за модулем 7, про яке йдеться в теоремі 3.9, є 5.

**Приклад.** Знайдемо обернене до 17 за модулем 3432. За розширеним алгоритмом Евкліда знайдемо  $\gcd(3432, 17)$  як лінійну комбінацію 17 і 3432. Під час використання алгоритму Евкліда одержимо такі частки й остачі:  $q_1 = 201, r_2 = 15, q_2 = 1, r_3 = 2, q_3 = 7, r_4 = 1, q_4 = 2$ , тобто  $\gcd(3432, 17) = 1$  (остання ненульова остача), і  $17^{-1} \bmod 3432$  існує. Для його знаходження скористаємося рекурентними рівностями розширеного алгоритму Евкліда:

$$\begin{aligned} s_2 &= s_0 - q_1 s_1 = 1 - 201 \cdot 0 = 1 & t_2 &= t_0 - q_1 t_1 = 0 - 201 \cdot 1 = -201 \\ s_3 &= s_1 - q_2 s_2 = 0 - 1 \cdot 1 = -1 & t_3 &= t_1 - q_2 t_2 = 1 - 1 \cdot (-201) = 202 \\ s_4 &= s_2 - q_3 s_3 = 1 - 7 \cdot (-1) = 8 & t_4 &= t_2 - q_3 t_3 = -201 - 7 \cdot 202 = -1615 \end{aligned}$$

Отже,  $\gcd(3432, 17) = 1 = 8 \cdot 3432 + (-1615) \cdot 17$ . Коефіцієнт Безу при 17 є шуканою відповіддю, він дорівнює  $(-1615)$ , що є тим самим, що й 1817 за модулем 3432. (В обчисленнях використовують найменше додатне значення оберненого до  $a$  за модулем  $m$ ; таке  $a^{-1} < m$ , за теоремою 3.9, єдине. Запам'ятаємо таку, як у цьому прикладі, можливу ситуацію для подальших застосувань.)

Як тільки ми отримали  $a^{-1}$ , обернене до  $a$ , ми можемо розв'язати конгруенцію  $ax \equiv b \pmod{m}$ , помноживши обидві її частини на  $a^{-1}$ . Наступний приклад ілюструє ці дії.

**Приклад.** Знайдемо розв'язки конгруенції  $3x \equiv 4 \pmod{7}$ . Із одного з попередніх прикладів випливає, що 5 є оберненим до 3 за модулем 7. Помноживши обидві частини конгруенції на 5 дістанемо

$$5 \cdot 3x \equiv 5 \cdot 4 \pmod{7}.$$

Оскільки  $15 \equiv 1 \pmod{7}$  і  $20 \equiv 6 \pmod{7}$ , то  $x \equiv 6 \pmod{7}$ . Це такі числа: 6, 13, 20, ... і  $-1$ ,  $-8$ ,  $-15$ , ...

### **Китайська теорема про остачі.**

Системи лінійних конгруенцій досить широко використовують. Пропонована теорема, яка супроводжується конструктивним доведенням, дає змогу ефективно розв'язувати такі системи.

**Теорема 3.10 (китайська теорема про остачі).** Нехай  $m_1, m_2, \dots, m_n$  – попарно взаємно прості додатні цілі числа, більші від 1, і  $a_1, a_2, \dots, a_n$  – довільні цілі. Тоді система

$$\begin{aligned}x &\equiv a_1 \pmod{m_1}, \\x &\equiv a_2 \pmod{m_2}, \\&\dots\dots\dots \\x &\equiv a_n \pmod{m_n}\end{aligned}$$

має єдиний розв'язок за модулем  $m = m_1 m_2 \cdots m_n$ . (Це слід розуміти так, що існує розв'язок  $x$ ,  $0 \leq x < m$ , а всі інші розв'язки конгруентні до цього розв'язку за модулем  $m$ .)

**Доведення.** Тут ми доведемо лише існування розв'язку, причому доведення конструктивне: побудуємо алгоритм конструювання цього розв'язку.

Нехай  $\mu_k = m/m_k$  для  $k = 1, 2, \dots, n$ . Отже,  $\mu_k$  – добуток усіх модулів за виключенням  $m_k$ . Оскільки  $m_i$  та  $m_k$  не мають спільних множників більших від 1, для  $i \neq k$ , то  $\gcd(m_k, \mu_k) = 1$ . Отже, за теоремою 3.9 існує ціле  $y_k$ , яке є оберненим до  $\mu_k$  за модулем  $m_k$  тобто  $y_k = \mu_k^{-1}$ , і, отже

$$\mu_k y_k \equiv 1 \pmod{m_k}.$$

Сумісний розв'язок побудуємо як суму

$$x = a_1 \mu_1 y_1 + a_2 \mu_2 y_2 + \cdots + a_n \mu_n y_n.$$

Тепер покажемо, що  $x$  справді є таким розв'язком. Передусім зазначимо, що  $\mu_j \equiv 0 \pmod{m_k}$  коли  $j \neq k$ , бо тоді  $\mu_j$  містить  $m_k$  як співмножник. Тому всі доданки окрім  $k$ -го конгруентні до 0 за модулем  $m_k$ . У той же час  $\mu_k y_k \equiv 1 \pmod{m_k}$ , бо  $y_k = \mu_k^{-1}$  за модулем  $m_k$ . Остаточно

$$x \equiv a_k \mu_k y_k \equiv a_k \pmod{m_k}$$

для  $k = 1, 2, \dots, n$ . Отже, доведено, що  $x$  – сумісний розв'язок  $n$  конгруенцій.

Доведення існування розв'язку в теоремі 3.10 дає загальний метод розв'язування систем лінійних конгруенцій із попарно взаємно простими модулями.

**Приклад.** Розв'яжемо систему лінійних конгруенцій  $x \equiv 1 \pmod{5}$ ,  $x \equiv 2 \pmod{6}$  і  $x \equiv 3 \pmod{7}$ . Передусім обчислимо  $m = 5 \cdot 6 \cdot 7 = 210$ ,  $\mu_1 = m/5 = 42$ ,  $\mu_2 = m/6 = 35$ ,  $\mu_3 = m/7 = 30$ . Далі знаходимо обернене до  $\mu_1$  за модулем 5:  $y_1 = 3$ , обернене до  $\mu_2$  за модулем 6:  $y_2 = 5$  і обернене до  $\mu_3$  за модулем 7:  $y_3 = 4$ . Розв'язок системи

$$x \equiv a_1 \mu_1 y_1 + a_2 \mu_2 y_2 + a_3 \mu_3 y_3 = 1 \cdot 42 \cdot 3 + 2 \cdot 35 \cdot 5 + 3 \cdot 30 \cdot 4 = 836 \equiv 206 \pmod{210}.$$

## Мала теорема Ферма

Мала теорема Ферма надзвичайно корисна для обчислення остач за модулем  $p$  від великих степенів цілих чисел,

**Теорема 3.11 (мала теорема Ферма).** Якщо  $p$  – просте число,  $a$  – ціле, неподільне на  $p$ , то

$$a^{p-1} \equiv 1 \pmod{p}.$$

Більше того, для будь-якого цілого  $a$  ми маємо

$$a^p \equiv a \pmod{p}.$$

**Приклад.** Знайдемо  $7^{222} \bmod 11$ . Ми можемо використати малу теорему Ферма для швидшого обчислення ніж за алгоритмом 4.1 модулярного піднесення до степеня. За малою теоремою Ферма  $7^{10} \equiv 1 \pmod{11}$ , отже,  $(7^{10})^k \equiv 1 \pmod{11}$  для кожного додатного цілого  $k$ . Для того, щоб скористатись виграшем від останньої конгруенції, поділимо показник 222 на 10, тоді  $222 = 22 \cdot 10 + 2$ . Тоді

$$7^{222} = 7^{22 \cdot 10 + 2} = (7^{10})^{22} 7^2 \equiv (1)^{22} \cdot 49 \equiv 5 \pmod{11}.$$

Отже,  $7^{222} \bmod 11 = 5$ .

Цей приклад показує, як можна використати малу теорему Ферма для обчислення  $a^n \bmod p$ , якщо  $p$  – просте число й  $p \nmid a$ . Поділимо  $n$  на  $(p-1)$ , тоді дістанемо частку  $q$  і остачу  $r$ , звідки  $n = q \cdot (p-1) + r$ , де  $0 \leq r < p-1$ . Звідси

$$a^n = a^{q(p-1)+r} = (a^{p-1})^q a^r \equiv 1^q a^r \equiv a^r \pmod{p}.$$

## Первісні корені й дискретні логарифми

Нехай  $p$  – просте число. *Первісним коренем за модулем  $p$  називають ціле  $r$  із множини  $\mathbf{Z}_p = \{0, 1, 2, \dots, p-1\}$  таке, що кожний ненульовий елемент  $\mathbf{Z}_p$  являє собою степінь  $r$ .*

**Приклад.** Якщо ми обчислимо степені  $2 \in \mathbf{Z}_{11}$  за модулем 11, то дістанемо:  $2^1 = 2$ ,  $2^2 = 4$ ,  $2^3 = 8$ ,  $2^4 = 5$ ,  $2^5 = 10$ ,  $2^6 = 9$ ,  $2^7 = 7$ ,  $2^8 = 3$ ,  $2^9 = 6$ ,  $2^{10} = 1$ . Легко побачити, що кожний ненульовий елемент множини  $\mathbf{Z}_{11}$  є степенем 2. Отже, 2 є первісним коренем 11. Якщо ж ми будемо обчислювати степені 3 за модулем 11, то матимемо  $3^1 = 3$ ,  $3^2 = 9$ ,  $3^3 = 5$ ,  $3^4 = 4$ ,  $3^5 = 1$ ; при подальших піднесеннях до степеня ця послідовність буде повторюватись. Тому що не всі елементи  $\mathbf{Z}_{11}$  є степенями 3, то доходимо висновку, що 3 не є первісним коренем 11.

Важливий результат теорії чисел полягає в тому, що для кожного простого  $p$  існує первісний корінь за модулем  $p$ .

Нехай  $p$  – просте число,  $r$  – первісний корінь за модулем  $p$  і  $a$  – ціле число в межах від 1 до  $p-1$  включно, тобто  $a$  – ненульовий елемент  $\mathbf{Z}_p$ . Відомо, що існує єдиний показник  $e$  такий, що  $r^e = a$  в  $\mathbf{Z}_p$ , тобто  $r^e \bmod p = a$ .

Нехай  $p$  – просте число,  $r$  – первісний корінь за модулем  $p$  і  $a$  – ціле число в межах від 1 до  $p-1$  включно. Якщо  $r^e \bmod p = a$  та  $0 \leq e \leq p-1$ , то  $e$  називають *дискретним логарифмом числа  $a$  за модулем  $p$  при основі  $r$*  і пишуть  $\log_r a = e$  (тут просте число  $p$  мається на увазі).

**Приклад.** Щойно ми обчислили степені 2 за модулем  $p=11$ , зокрема,  $2^8=3$  і  $2^4=5$  в  $\mathbf{Z}_{11}$ . Отже, дискретні логарифми 3 і 5 за модулем 11 при основі 2 є, відповідно, 8 та 4. (Це степені 2, які дорівнюють, відповідно, 3 і 5 в  $\mathbf{Z}_{11}$ .) Ми пишемо  $\log_2 3=8$  і  $\log_2 5=4$  (тут модуль 11 мається на увазі і явно не записується).

*Задача обчислення дискретного логарифму як вхід має просте число  $p$ , первісний корінь  $r$  за модулем  $p$  і додатне ціле  $a \in \mathbf{Z}_p$ . Її вихід – дискретний логарифм числа  $a$  за модулем  $p$  при основі  $r$ . Для розв’язування цієї задачі невідомий жодний поліноміальний алгоритм. Тому що ця задача складна для розв’язування, вона відіграє важливу роль у криптографії.*