Київський національний університет імені Тараса Шевченка

Н.С. Головащук, Є.А. Кочубінська, С.А. Овсієнко

ПРАКТИКУМ З ПРИКЛАДНОЇ АЛГЕБРИ

для студентів механіко – математичного факультету

Київ
2015

Н.С. Головащук, Є.А. Кочубінська, С.А. Овсієнко. Практикум з прикладної алгебри.: для студентів механіко – математичного факультету. – К.:2015. – 59 с.

Рецензенти: д-р фіз.-мат. наук, М.Ф.Городній
д-р фіз.-мат. наук, проф. А.П.Петравчук

Наведено теоретичні відомості та задачі з курсу прикладної алгебри, що читається у шостому семестрі на механіко – математичного факультету.

Рекомендовано до друку вченою радою механіко – математичного факультету Київського національного університету імені Тараса Шевченка (протокол № 12 від 15 червня 2015 року)

Зміст

Передмова

У посібнику висвітлено деякі аспекти прикладної алгебри. Зрозуміло, що застосування алгебри не вичерпуються наведеними у посібнику. Вибір зумовлений курсом, який один з авторів, Сергій Адамович Овсієнко, читав на механіко–математичному факультеті протягом багатьох років. Увагу приділено модулярній арифметиці, обчисленням в скінченних полях та теорії кодування. Виклад матеріалу супроводжується прикладами, які ілюструють наведені поняття та конструкції. Кожний розділ доповнений задачами для самостійного опрацювання, які допоможуть читачеві краще оволодіти матеріалом. Припускається, що читач знайомий з базовими положеннями лінійної алгебри, теорії груп, теорії кілець та теорії Галуа.

1 Елементи теорії чисел

1.1 Подільність в кільці цілих чисел

У цьому підрозділі зібрано відомі факти про подільність цілих чисел. Позначимо через $\mathbb{Z}$ множину усіх цілих чисел, через $\mathbb{N}$ — множину натуральних чисел.

Означення 1.1. Нехай a та $b \neq 0$ — цілі числа. Говорять, що b *ділить* a, або що a *ділиться на* b, якщо існує таке ціле число c, що $a = bc$.

Запис $b \mid a$ позначає, що b ділить a. Якщо b не ділить a, то писатимемо $b \nmid a$.

Твердження 1.1 (Властивості подільності)**.** *Нехай* $a, b, c \in \mathbb{Z}$.

1. *Якщо* $a \mid b$, $b \mid c$, *то* $a \mid c$.
2. *Якщо* $a \mid b$, $a \mid c$, *то* $a \mid b \pm c$.
3. *Якщо* $a \mid b$, $b \mid a$, *то* $a = \pm b$. (*У цьому випадку числа* a *та* b *називаються асоційованими.*)

Доведення залишаємо читачеві у якості вправи. □

Ціле число $u \in \mathbb{Z}$ називається *оборотним* в $\mathbb{Z}$, якщо існує таке $v \in \mathbb{Z}$, для якого $uv = 1$. Множину усіх оборотних елементів в $\mathbb{Z}$ позначимо через $\mathbb{Z}^*$. Легко зрозуміти, що $\mathbb{Z}^* = \{1, -1\}$. Множина $\mathbb{Z}^*$ є групою відносно множення. Неважко бачити, що два цілих числа $a, b \in \mathbb{Z}$ є асоційованими, якщо існує таке $u \in \mathbb{Z}^*$, що $a = b \cdot u$.

Означення 1.2. *Спільним дільником* цілих чисел a та b називається таке ціле число d, що $d \mid a$ та $d \mid b$.

Найбільшим спільним дільником цілих чисел a та b називається такий спільний дільник d чисел a та b, який ділиться на будь–який інший спільний дільник чисел a та b. Найбільший спільний дільник чисел a та b позначається НСД(a, b) або (a, b).

Зауважимо, що НСД двох цілих чисел визначений не однозначно, а з точністю до асоційованості. У кільці цілих чисел це означає, що НСД визначений з точністю до знака. Домовимося на наступне, що НСД є додатним цілим числом.

Теорема 1.1 (Теорема про ділення з остачею)**.** *Нехай* a, $b \neq 0$ — *натуральні числа. Тоді існують такі цілі числа* q *та* r, *що*

$$a = bq + r, \ \text{де } 0 \leqslant r < n. \tag{1}$$

Числа q та r визначаються однозначно.

Доведення. Доведемо спершу існування зображення (1). Розглянемо числа, кратні b: b, $2b$, $3b$, ... Ясно, що врешті–решт ми досягнемо числа, яке більше за . Нехай q — це найбільше таке число $x \in \mathbb{N}$, для якого $xb \leqslant a$, тобто $qb \leqslant a$, але $b(q+1) > a$. Покладемо $a - bq$. Тоді $r \geqslant 0$, але $r < b$, та $m = bq + r$.

Вираз $a = bq + r$, де $0 \leqslant r < b$, назвемо *зображенням* a за модулем b, $a, b \in \mathbb{N}$. Покажемо тепер, що таке зображення єдине. Припустимо, що існує два різних зображення:

$$a = bq + r = bq' + r', \text{ де } r < a, r' < a'.$$

Якщо $r = r'$, то $bq = bq'$, а тому $q = q'$. Припустимо, що $r \neq r'$, будемо вважати, що $r > r'$. Тоді

$$r - r' = b(q' - q),$$

але число зліва строго менше за b, а число справа ділиться на b, що неможливо. □

Теорема 1.2 (Алгоритм Евкліда)**.** *Нехай $a, b \in \mathbb{N}$, $a \geqslant b$.*

Наступний алгоритм обчислює НСД(a, b) за скінченну кількість кроків.

(1) *Нехай $r_0 = a$ та $r_1 = b$.*

(2) *Покладемо $i = 1$.*

(3) *Розділимо r_{i-1} на r_i з остачею, одержимо в результаті частку q_i та остачу r_{i+1}:*

$$r_{i-1} = r_i q_i + r_{i+1} \text{ де } 0 \leqslant r_{i+1} < r_i.$$

(4) *Якщо остача $r_{i+1} = 0$, то r_i = НСД(a, b), і алгоритм завершує роботу.*

(5) *В іншому разі, $r_{i+1} > 0$, тому покладемо $i = i + 1$ та повернемося до кроку 3.*

Доведення. Алгоритм Евкліда складається з послідовності ділень з остачею, яку запишемо у таблицю:

$$
\begin{array}{|cc|}
\hline
a = bq_1 + r_1, & \text{де } 0 \leqslant r_2 < b, \\
b = r_2q_2 + r_3, & \text{де } 0 \leqslant r_3 < r_2, \\
r_2 = r_3q_3 + r_4, & \text{де } 0 \leqslant r_4 < r_3, \\
r_3 = r_4q_4 + r_5, & \text{де } 0 \leqslant r_5 < r_4, \\
\vdots & \vdots \\
r_{k-2} = r_{k-1}q_{k-1} + r_k, & \text{де } 0 \leqslant r_k < r_{k-1}, \\
r_{k+1} = r_kq_k & \\
\hline
\multicolumn{2}{|l|}{\text{Тоді } r_k = \text{НСД}(a, b).} \\
\hline
\end{array}
$$

Оскільки на кожному кроці остачі r_i строго спадають, то в певний момент ми одержимо остачу, яка дорівнює 0, і алгоритм припинить свою роботу. Отже, алгоритм закінчить свою роботу за скінченну кількість кроків.

При кожній ітерації кроку 3 маємо рівність вигляду

$$r_{i-1} = r_iq_i + r_{i+1}.$$

З цієї рівності випливає, що будь–який спільний дільник чисел r_{i-1} та r_i є дільником і числа r_{i+1}, а також, що спільний дільник чисел r_i та r_{i+1} є дільником числа r_{i-1}. Отже,

$$\text{НСД}(r_{i-1}, r_i) = \text{НСД}(r_i, r_{i+1}), \text{ для } i = 1, 2, 3, \ldots \tag{2}$$

Але, як було зауважено вище, в деякий момент ми прийдемо до нульової остачі, нехай це буде $r_{k+1} = 0$. Тоді $r_{k-1} = r_kq_k$. Отже,

$$\text{НСД}(r_{k-1}, r_k) = \text{НСД}(r_kq_k, r_k) = r_k.$$

З рівності 2 випливає, що це значення буде дорівнювати $\text{НСД}(r_0, r_1)$, тобто $\text{НСД}(a, b)$. Отже, остання ненульова остача в алгоритмі Евкліда дійсно дає найбільший спільний дільник. □

Приклад 1.1. Знайдемо найбільший спільний дільник чисел $a = 1634$ та $b = 252$.

Виконаємо послідовність ділень з остачею, ділитимемо до тих пір, поки не одержимо нульову остачу:

$$
\begin{aligned}
1634 &= 252 \cdot 6 + 122; \\
252 &= 122 \cdot 2 + 8; \\
122 &= 15 \cdot 8 + 2; \\
8 &= 2 \cdot 4.
\end{aligned}
$$

Отже, НСД$(1634, 252) = 2$.

Теорема 1.3 (Розширений алгоритм Евкліда)**.** *Нехай a та b — натуральні числа. Тоді рівняння*

$$au + bv = НСД(a, b) \tag{3}$$

завжди має цілочисельний розв'язок.

Доведення. Звернемось до таблиці, яка наведена в доведенні теореми 1.2. З першої рівності знайдемо $r_2 = a - bq_1$ та підставимо в другу рівність, одержимо

$$b = (a - bq_1)q_2 + r_3, \qquad \text{отже, } r_3 = -aq_2 + b(1 + q_1q_2).$$

Підставимо вирази для r_2 та r_3 у третю рівність,одержимо

$$a - bq_1 = (-aq_2 + b(1 + q_1q_2))q_3 + r_4.$$

Перегрупувавши змінні, одержимо

$$r_4 = a(1 + q_2q_3) - b(q_1 + q_3 + q_1q_2q_3).$$

Тут основним є те, що $r_4 = au' + bv'$ для цілих чисел $u' = 1 + q_2q_3$, $v' = -(q_1 + q_3 + q_1q_2q_3)$. Неважливо, що вирази u' та v' через q_1, q_2, q_3 є доволі громіздким. Продовжуючи таким чином далі, одержимо, що кожну остачу r_i можна подати у вигляді суми чисел, одне з яких кратне a, а інше кратне b. Зрештою, ми одержимо зображення

$$r_k = \text{НСД}(a, b) = au + bv$$

для деяких цілих чисел u та v. □

Зображення найбільшого спільного дільника у вигляді (3) часто називають *лінійним зображенням* найбільшого спільного дільника.

Приклад 1.2. Знайдемо лінійне зображення найбільшого спільного дільника чисел $a = 1634$ та $b = 252$. Виконаємо ділення з остачею, як у прикладі 1.1, і на кожному кроці будемо записувати лінійні зображення для остач

$$\begin{aligned} 1634 &= 252 \cdot 6 + 122, & 122 &= 1634 - 252 \cdot 6; \\ 252 &= 122 \cdot 2 + 8, & 8 &= 252 - 122 \cdot 2; \\ 122 &= 15 \cdot 8 + 2, & 2 &= 122 - 15 \cdot 8; \\ 8 &= 2 \cdot 4. \end{aligned}$$

Отже, остаточно матимемо:

$$\begin{aligned}\text{НСД}(1634, 252) = 2 = 122 - 15 \cdot 8 = \\ = 122 - 15 \cdot (252 - 122 \cdot 2) = 122 \cdot 31 - 15 \cdot 252 = \\ = (1634 - 252 \cdot 6) \cdot 31 - 15 \cdot 252 = 1634 \cdot 31 - 252 \cdot 201.\end{aligned}$$

1.2 Модулярна арифметика

Означення 1.3. Нехай $n \in \mathbb{N}$. Цілі числа a та b називаються *конгруентними за модулем* n, якщо різниця $a - b$ ділиться на n. Позначається $a \equiv b \pmod{n}$.

Твердження 1.2 (Властивості конгруенцій)**.** *Нехай* $n \in \mathbb{N}$.

1. *Якщо* $a_1 \equiv a_2 \pmod{n}$ *та* $b_1 \equiv b_2 \pmod{n}$, *то*

$$a_1 \pm b_1 \equiv a_2 \pm b_2 \pmod{n} \text{ та } a_1 b_1 \equiv a_2 b_2 \pmod{n}.$$

2. *Нехай* $a \in \mathbb{Z}$. *Тоді* $ab \equiv 1 \pmod{n}$ *для деякого* $b \in \mathbb{Z}$ *тоді і лише тоді, коли* НСД$(a, n) = 1$. *Якщо таке число* b *існує, то воно називається (мультиплікативним) оберненим за модулем* n. *Позначатимемо* $b \equiv a^{-1} \pmod{n}$.

Доведення. 1. Вправа.

2. Припустимо спершу, що НСД$(a, n) = 1$. Тоді з теореми 1.3 випливає, що існують такі цілі числа u та v, що $au + nv = 1$. Це означає, що $au - 1 = -nv$ ділиться на n. Отже, $au \equiv 1 \pmod{n}$. Для доведення в інший бік, припустимо, що для $a \in \mathbb{Z}$ існує обернений за модулем n, тобто існує таке $b \in \mathbb{Z}$, що $ab \equiv 1 \pmod{n}$. Це означає, що $ab - 1 = kn$ для деякого $k \in \mathbb{Z}$. З цього випливає, що НСД(a, n) ділить $ab - kn = 1$, отже, НСД$(a, n) = 1$. □

Елемент, для якого існує обернений за модулем n, називається *оборотним* за модулем n.

Приклад 1.3. 1. Нехай $n = 7$, $a = 3$. Оскільки НСД$(7, 3) = 1$, то до елемента $a = 3$ існує обернений за модулем $n = 7$. Неважко переконатися, що $3^{-1} \equiv 5 \pmod{n}$.

2. Нехай $n = 353$, $a = 19$. Числа 353 та 19 взаємно прості, отже, існує 19^{-1} за модулем 353. Проте на відміну від попереднього прикладу легко вгадати обернений не вдається.

Для знаходження оберненого за модулем можна використати розширений алгоритм Евкліда. Дійсно, якщо НСД$(a, n) = 1$, то знайдуться

такі цілі числа u та v, що $au+nv=1$. Якщо в останній рівності перейти до конгруентності за модулем n, то одержимо $au \equiv 1 \pmod{n}$, що дасть $a^{-1} \equiv u \pmod{n}$.

Для $n = 353$ та $a = 19$ запишемо кроки розширеного алгоритму Евкліда:

$$\begin{aligned} 353 &= 19 \cdot 18 + 11, & 11 &= 353 - 19 \cdot 18; \\ 19 &= 11 \cdot 1 + 8, & 8 &= 19 - 11 \cdot 1; \\ 11 &= 8 \cdot 1 + 3, & 3 &= 11 - 8 \cdot 1; \\ 8 &= 3 \cdot 2 + 2, & 2 &= 8 - 3 \cdot 2; \\ 3 &= 2 \cdot 1 + 1, & 1 &= 3 - 2 \cdot 1; \\ 2 &= 2 \cdot 1. \end{aligned}$$

Звідси маємо таке зображення 1:

$$\begin{aligned} 1 = 3 - 2 \cdot 1 = 3 - (8 - 3 \cdot 2) \cdot 1 = 3 \cdot 3 - 8 \cdot 1 = \\ = (11 - 8 \cdot 1) \cdot 3 - 8 \cdot 1 = 11 \cdot 3 - 8 \cdot 4 = \\ = 11 \cdot 3 - (19 - 11 \cdot 1) \cdot 4 = 11 \cdot 7 - 19 \cdot 4 = \\ = (353 - 19 \cdot 18) \cdot 7 - 19 \cdot 4 = 353 \cdot 7 - 130 \cdot 19. \end{aligned}$$

Перейшовши до конгруентності за модулем 353, одержимо

$$19^{-1} \equiv 130 \equiv 223 \pmod{353}.$$

Згадавши властивості подільності, неважко переконатися, що різних остач від ділення на $n \in \mathbb{N}$ буде n. Розглянемо множину всіх різних остач від ділення на n

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}.$$

Ця множина є кільцем відносно додавання та множення за модулем n. Це кільце називається *кільцем лишків за модулем n*.

Позначимо через $\mathbb{Z}_n^*$ множину всіх оборотних за модулем n елементів кільця $\mathbb{Z}_n$. З твердження 1.2 маємо, що для цілого числа a існує обернений за модулем n тоді і лише тоді, коли $\text{НСД}(a, n) = 1$, тому матимемо

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \text{НСД}(a, n) = 1\}.$$

Множина $\mathbb{Z}_n^*$ є групою відносно операції множення за модулем n. Ця група називається *мультиплікативною групою* кільця $\mathbb{Z}_n$. Дійсно, з означення цієї множини випливає, що для кожного елемента з $\mathbb{Z}_n^*$ існує обернений. Візьмемо два довільні елементи $a, b \in \mathbb{Z}_n^*$. З розширеного

алгоритму Евкліда та твердження 1.2 випливає існування таких цілих чисел r, s, u та v, що

$$ar + ns = 1 \text{ та } bu + nv = 1.$$

Тоді

$$(ar + ns)(bu + nv) = abru + n(var + sbu + nsv) = 1.$$

Перейшовши до конгруенції за модулем n, одержимо

$$abru \equiv 1 \pmod{n},$$

тобто для елемента ab існує обернений за модулем n.

Приклад 1.4. Мультиплікативна група кільця $\mathbb{Z}_{24}$ складається з 8 елементів

$$\mathbb{Z}_{24}^* = \{1, 5, 7, 11, 13, 17, 19, 23\}.$$

Нагадаємо, що функція Ейлера $\varphi(n)$ — це функція на множині натуральних чисел, яка визначається правилом

$$\varphi(n) = |\{a \in \mathbb{N} \mid \text{НСД}(a, n) = 1\}|.$$

Очевидно, що $|\mathbb{Z}_n^*| = \varphi(n)$. З цієї рівності випливають такі твердження.

Теорема 1.1 (Мала теорема Ферма)**.** *Нехай p — просте число, a — ціле число, $(a, p) = 1$. Тоді*

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

Теорема 1.2 (Теорема Ейлера)**.** *Нехай a та m — цілі числа, $(a, m) = 1$. Тоді*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

1.2.1 Модулярна арифметика та шифри заміни

Шифр Цезаря. За легендою Юлій Цезар для таємного листування використовував шифр, при якому кожна літера зсувалася на 3 позиції, тобто

$$A \mapsto D, \quad B \mapsto E, \quad C \mapsto F, \quad \ldots, \quad Z \mapsto C.$$

Відомий вислів `ALEA JACTA EST` при такому зашифровуванні мав би вигляд `DOHD MDFWD HVW`.

Припишемо кожній літері номер як у таблиці

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Тоді математичною мовою шифр Цезаря можна описати наступним чином:

$$X \mapsto X + 3 \pmod{26}.$$

Шифр Цезаря є частковим випадком простого шифру заміни. Надалі під відкритим текстом розумітимемо повідомлення, яке потрібно зашифрувати, а під шифртекстом розумітимемо повідомлення, яке одержується після зашифровування.

Розглянемо випадок, коли алфавіти символів повідомлень та шифртекстів збігаються. Нехай $\mathcal{A}$ — це алфавіт, наприклад, $\mathcal{A} = \{A, B, \ldots, Z\}$. Нехай $m = m_1 m_2 m_3 \ldots$ — це повідомлення, яке потрібно зашифрувати і яке є конкатенацією символів $m_i \in \mathcal{A}$. Якщо використовується простий шифр заміни, то при шифруванні кожній літері m_i вихідного повідомлення зіставляється однозначно визначена літера $e(m_i) \in \mathcal{A}$, де відображення $e : \mathcal{A} \to \mathcal{A}$ — це підстановка на множині $\mathcal{A}$:

$$E_e(m) = e(m_1)e(m_2)e(m_3)\ldots\ .$$

Розглянемо простий шифр заміни, який полягає у зсуві кожної літери на k позицій. Припустимо, що використовується алфавіт, який складається з N літер. У розглядуваному шифрі число k виступає у якості ключа як зашифровування, так і розшифрування. Процес зашифровування можна схематично описати таким чином

$$(\text{Шифртекст}) \equiv (\text{Відкритий текст}) + (\text{Таємний ключ}) \pmod{N},$$

а процес розшифрування так

$$(\text{Відкритий текст}) \equiv (\text{Шифртекст}) - (\text{Таємний ключ}) \pmod{N}.$$

Зрозуміло, що при такому шифрування знання ключа зашифровування одразу дає інформацію про ключ розшифрування.

Вправа 1. Переконайтеся в тому, що при описаному вище шифруванні знання ключа зашифровування одразу дає інформацію про ключ розшифрування.

Розглянемо ще одне узагальнення шифру Цезаря — так званий *афінний шифр*. Якщо знов вважати, що алфавіт складається з N літер, а через $\mathcal{M}$ та $\mathcal{C}$ позначити відкритий та шифртекст відповідно, то процес зашифровування можна описати формулою

$$\mathcal{C} = a\mathcal{M} + b \pmod{N},$$

де $a, b \in \mathbb{N}$, причому НСД$(a, N) = 1$, і ключем зашифровування є пара чисел (a, b). Як і у попередньому прикладі знання ключа розшифрування дає змогу легко знайти ключ розшифрування. Неважко переконатися (зробіть це самостійно!), що правило розшифрування задається формулою

$$\mathcal{M} = a^{-1}\mathcal{C} - a^{-1}b \pmod{N}.$$

З цієї формули стає очевидною вимога НСД$(a, N) = 1$, бо у цьому випадку для a існує обернений за модулем N.

Варто відзначити, що прості шифри заміни є надзвичайно ненадійними. У кожній мові є літери, що зустрічаються дуже часто або дуже рідко. У відповідності до частоти появи літер у текстах для мови будується частотна таблиця, в якій вказується з якої частотою зустрічається та чи інша буква. Маючи текст належної довжини, можна підрахувати, який скільки разів зустрічається кожний символ, обчислити частотність його появи у тексті та на основі таблиць частотності зробити висновки щодо літери у відкритому тексті.

1.2.2 Швидке піднесення до степеня

У прикладних задачах часто виникає потреба знайти великий степінь натурального числа за модулем деякого натурального числа N.

Припустимо, що потрібно обчислити a^m. Можна діяти прямолінійно, послідовно множачи на a:

$$a_1 \equiv a \pmod{N}, a_2 = a_1 \cdot a \pmod{N}, a_3 = a_2 \cdot a \pmod{N}, \ldots,$$

Звісно, таким чином ми коли–небудь одержимо відповідь, але для достатньо великих m, скажімо $m = 2^{1024}$, час роботи може оцінюватися мільярдами років. Інша ідея полягає у зображенні показника степеня у бінарній системі числення та наступного обчислення порядку $\log_2 m$ квадратів числа a та приблизно такої самої кількості множень. Проілюструємо цю ідею прикладом.

Приклад 1.5. Для обчислення 3^{100} шляхом послідовного множення на 3 потрібно 99 дій. А можна діяти таким чином. Зобразимо спершу число 100 у вигляді суми степенів 2:

$$100 = 2^6 + 2^5 + 2^2.$$

Після цього обчислимо

$$3^2, \quad 3^4 = (3^2)^2, \quad 3^8 = (3^4)^2, \quad 3^{16} = (3^8), \quad 3^{32} = (3^{16})^2, \quad 3^{64} = (3^{32})^2,$$

остаточно підрахуємо

$$3^{100} = 3^{64} \cdot 3^{32} \cdot 3^4.$$

Отже, для обчислення 3^{100} нам знадобилося лише 8 множень.

Опишемо алгоритм швидкого піднесення до степеня формально.

Алгоритм швидкого піднесення до степеня.

Дано: $a \in \mathbb{N}$, $m \in \mathbb{N}$.
Обчислити: a^m.

Крок 1. Зобразити m у вигляді суми степенів 2:

$$m = m_0 + m_1 \cdot 2 + m_2 \cdot 2^2 + \ldots + m_k \cdot 2^k, \qquad m_0, \ldots, m_k \in \{0, 1\},$$

можемо припускати, що $m_k = 1$.

Крок 2. Обчислити a^{2^j} для $0 \leqslant j \leqslant k$ шляхом послідовного піднесення до квадрату:

$$\begin{gathered} b_0 = a \\ b_1 = b_0^2 = a^2 \\ b_2 = b_1^2 = a^{2^2} \\ b_3 = b_2^2 = a^{2^3} \\ \vdots \\ b_k = b_{k-1}^2 = a^{2^k}. \end{gathered}$$

Оскільки кожне число b_j є квадратом попереднього, то потрібно виконати k піднесень до квадрату.

Крок 3. Обчислити a^m за формулою

$$\begin{gathered} a^m = a^{m_0 + m_1 \cdot 2 + m_2 \cdot 2^2 + \ldots + m_k \cdot 2^k} \\ = a^{m_0} \cdot (a^2)^{m_1} \cdot (a^{2^2})^{m_2} \cdot (a^{2^3})^{m_3} \cdot \ldots (a^{2^k})^{m_k} \\ = b_0^{m_0} \cdot b_1^{m_1} \cdot b_2^{m_2} \cdot b_3^{m_3} \ldots b_k^{m_k}. \end{gathered}$$

Враховуючи, що $b_0, b_1, b_2, b_3, \ldots, b_k$ були обчислені на попередньому кроці, то цей крок вимагає щонайбільше k множень.

Таким чином, цей алгоритм потребую щонайбільше $2k$ множень для обчислення a^m. Оскільки $m \geqslant 2^k$, то нам потрібно не більше, ніж $\log_2 m$ дій множення.

1.3 Китайська теорема про остачі

У цьому розділі розглянемо спосіб розв'язання системи конгруенцій. Найпростіший випадок маємо, коли система складається з двох конгруенцій:

$$x \equiv a \pmod{m} \quad \text{та} \quad x \equiv b \pmod{n}, \tag{4}$$

де m та n — взаємно прості числа. Ця система має єдиний розв'язок за модулем mn. Це твердження випливає з китайської теореми про остачі, яка буде сформульована та доведена далі.

Почнемо з невеликого прикладу, в якому наведемо спосіб знаходження розв'язку.

Приклад 1.6. Знайдемо розв'язок системи конгруенцій:

$$x \equiv 1 \pmod{5} \quad \text{та} \quad x \equiv 2 \pmod{7}, \tag{5}$$

З першої конгруенції випливає, що множина її розв'язків — це набір цілих чисел вигляду

$$x = 1 + 5y, \qquad y \in \mathbb{Z} \tag{6}$$

Підставивши цей вираз у другу конгруенцію з (5), одержимо

$$1 + 5y \equiv 2 \pmod{7}, \quad \text{а тому} \quad 5y \equiv 1 \pmod{7}. \tag{7}$$

Домножимо обидві частини останньої конгруенції на обернений до 5 за модулем 7. Зауважимо, що цей обернений існує, бо $(5, 7) = 1$. Його можна знайти способом, описаним у прикладі 1.3, але у даному прикладі легко переконатися, що $5^{-1} \equiv 3 \pmod{7}$. В результаті одержимо

$$y \equiv 3 \pmod{7}.$$

Множина всіх розв'язків цієї конгруенції описується множиною

$$y = 3 + 7z, \qquad z \in \mathbb{Z}. \tag{8}$$

Для знаходження розв'язку системи конгруенцій (5) підставимо вираз цей в (6). Остаточно одержимо

$$x = 1 + 5y = 1 + 5(3 + 7z) = 16 + 35z, \qquad z \in \mathbb{Z},$$

або, що те саме,

$$x \equiv 16 \pmod{36}.$$

Цю саму ідею можна використати для доведення китайської теореми про остачі.

Теорема 1.3 (Китайська теорема про остачі)**.** *Якщо натуральні числа $n_1, n_2, \ldots, n_k$ — попарно взаємно прості, то система конгруенцій*

$$\begin{array}{rcll} x & \equiv & a_1 & \pmod{n_1} \\ x & \equiv & a_2 & \pmod{n_2} \\ & \vdots & & \\ x & \equiv & a_k & \pmod{n_k} \end{array}$$

має єдиний розв'язок за модулем $n = n_1 n_2 \ldots n_k$.

Доведення. Припустимо, що для деякого i ми вже знайшли спільний розв'зок

$$x = c_i$$

перших i конгруенцій

$$\begin{array}{rcll} x & \equiv & a_1 & \pmod{n_1} \\ x & \equiv & a_2 & \pmod{n_2} \\ & \vdots & & \\ x & \equiv & a_i & \pmod{n_i} \end{array} \tag{9}$$

Наприклад, якщо $i = 1$, то можна взяти $c_1 = a_1$. Покажемо, як знайти розв'язок системи, що складається з $i + 1$ конгруенцій:

$$\begin{array}{rcll} x & \equiv & a_1 & \pmod{n_1} \\ x & \equiv & a_2 & \pmod{n_2} \\ & \vdots & & \\ x & \equiv & a_{i+1} & \pmod{n_{i+1}} \end{array} \tag{10}$$

Ідея полягає у відшуканні розв'язку вигляду

$$x = c_i + m_1 m_2 \ldots m_i y$$

Зауважимо, що це значення x вже задовольняє всі конгруенції з системи (9), тому потрібно знайти таке y, яке б задовольняло також і рівність

$$x \equiv a_{i+1} \pmod{n_{i+1}}$$

Іншими словами, нам потрібно знайти y, яке було б розвязком конгруенції

$$c_i + m_1 m_2 \dots m_i y \equiv a_{i+1} \pmod{m_{i+1}}.$$

Оскільки НСД$(m_{i+1}, m_1 m_2 \dots m_i) = 1$, то таке y існує. □

Наведене доведення китайської теореми про остачі дає метод розв'язання системи когруенцій, проте це не єдиний алгоритм розв'язування системи конгруенцій.

Вправа 2. Покажіть, що розв'язок системи конгруенцій з теореми 1.3 можна знайти наступним чином:

$$x = \sum_{i=1}^{k} a_i N_i M_i,$$

де $N_i = n/n_i$, а $M_i = N_i^{-1} \pmod{n}_i$. Цей алгоритм називається *алгоритмом Гауса* розв'язування системи конгруенцій.

Приклад 1.7. Розв'яжемо систему конгруенцій:

$$\begin{array}{rcll} x & \equiv & 2 & \pmod 5 \\ x & \equiv & 3 & \pmod 7 \\ x & \equiv & 5 & \pmod{11}. \end{array} \tag{11}$$

Зауважимо спочатку, що числа 5, 7 та 11 попарно взаємно прості, тому за китайською теоремою про остачі ця система має єдиний розв'язок за модулем числа $n = 5 \cdot 7 \cdot 11 = 385$.

Розв'яжемо цю систему конгруенцій двома способами.

Перший спосіб повторить доведення теореми 1.3. Почнемо з розв'язку $x = 2$ першої конгруенції $x \equiv 2 \pmod 5$. Запишемо загальний розв'язок $x = 2 + 5y$, $y \in \mathbb{Z}$ та підставимо у другу конгруенцію $x \equiv 3 \pmod 7$:

$$2 + 5y \equiv 3 \pmod 7.$$

Цю конгруенцію можна спростити до

$$5y \equiv 1 \pmod 7.$$

Оскільки $(5, 7) = 1$, то можна домножити обидві частини на $5^{-1} \pmod 7$, після чого одержимо

$$y \equiv 3 \pmod 7.$$

Загальним розв'язком цієї конгруенції є $y = 3 + 7z$, $z \in \mathbb{Z}$. Це дасть загальний розв'язок перших двох конгруенцій:

$$x = 2 + 5y = 2 + 5(3 + 7z) = 17 + 35z, \quad z \in \mathbb{Z}.$$

Підставимо цей розв'язок у третю конгуенцію:

$$17 + 35z = 5 \pmod{11}.$$

Після перетворень, аналогічних попереднім, одержимо $z \equiv 5 \pmod{11}$. Її загальним розв'язком є $z = 5 + 11t$, $t \in \mathbb{Z}$. Знайдемо тепер розв'язок початкової системи конгруенцій:

$$x = 17 + 35z = 17 + 35(5 + 11t) = 192 + 385t, \quad t \in \mathbb{Z}.$$

Другий спосіб використовує алгоритм Гауса.

Покладемо $n_1 = 5$, $n_2 = 7$, $n_3 = 11$, $n = n_1 n_2 n_3 = 385$. Обчислимо спочатку

$$N_1 = n/n_1 = 77, \quad N_2 = n/n_2 = 55, \quad N_3 = 35.$$

Потім обчислимо

$$M_1 = N_1^{-1} \pmod{n_1} = 77^{-1} \equiv 2^{-1} \equiv 3 \pmod{5},$$

$$M_2 = N_2^{-1} \pmod{n_2} \equiv 55^{-1} \equiv (-1)^{-1} \equiv -1 \equiv 6 \pmod{7},$$

$$M_3 = N_3^{-1} \pmod{n_3} = 35^{-1} \equiv 2^{-1} \equiv 6 \pmod{11}.$$

Запишемо остаточний розв'язок

$$x \equiv 2 \cdot 77 \cdot 3 + 3 \cdot 55 \cdot 6 + 5 \cdot 35 \cdot 6 \equiv 192 \pmod{385}.$$

Китайська теорема про остачі та її узагальнення мають велику кількість застосувань в теорії чисел та різноманітних галузях математики, деякі з яких будуть наведені у наступних розділах.

Розглянемо задачу, яка, на перший погляд, не вимагає китайської теореми про остачі, але яка легко розв'язується з її використанням.

Приклад 1.8. Знайдіть остачу від ділення 444^{235} на 1001.

Розв'язок. Перейдемо від конгруенції $x \equiv 444^{235} \pmod{1001}$ до системи конгруенцій

$$x \equiv 444^{235} \pmod{7}; \; x \equiv 444^{235} \pmod{11}; \; x \equiv 444^{235} \pmod{13}.$$

До кожної конгруенції можна застосувати малу теорему Ферма та зменшити основу степеня за відповідним модулем. Наприклад, очевидно, що $444 \equiv 3 \pmod 7$. За малою теоремою Ферма $3^{7-1} \equiv 1 \pmod 7$, тому $3^{235} = 3^{39\cdot 6+1} \equiv 3 \pmod 7$. Аналогічно можна спростити інші конгруенції. Одержимо

$$\begin{array}{ll} 444 \equiv 3 \pmod 7, & 235 \equiv 1 \pmod 6, \\ 444 \equiv 4 \pmod{11}, & 235 \equiv 5 \pmod{10}, \\ 444 \equiv 2 \pmod{13}, & 235 \equiv 7 \pmod{12}. \end{array}$$

Одержимо еквівалентну початковій систему

$$x \equiv 3 \pmod 7; \quad x \equiv 4^5 \pmod{11}; \quad x \equiv 2^7 \pmod{13}.$$

Після подальших спрощень дістанемо

$$x \equiv 3 \pmod 7; \quad x \equiv 1 \pmod{11}; \quad x \equiv 11 \pmod{13}.$$

Числа 3, 7 та 11 попарно взаємно прості, тому за китайської теоремою про остачі ці система має єдиний розв'зок. Застосувавши один з алгоритмів розв'язання, знайдемо $x = 661$. □

Перша письмова згадка про задачу, яка у сучасній математичній термінології зводиться до розв'язання системи конгруенцій, відноситься до праці китайського математика Сунь Цзи межі 3–4 ст. н.е.

Приклад 1.9 (Задача Сунь Цзи)**.** У нас є певна кількість речей, проте ми не знаємо точно скільки. Якщо ми порахуємо їх по три, то лишиться дві речі. Якщо ми порахуємо їх по п'ять, то лишиться три речі. Якщо ми порахуємо їх по сім, то лишиться дві речі. Скільки у нас є речей?

Задачі

Задача 1.1. Використовуючи алгоритм Евкліда, знайдіть найбільший спільний дільник чисел a та b, записати всі кроки алгоритму, якщо

(a) $a = 292$, $b = 321$; (b) $a = 324$, $b = 675$; (c) $a = 717$, $b = 906$;
(d) $a = 1089$, $b = 1287$; (e) $a = 1572$, $b = 1789$; (f) $a = 3141$, $b = 2718$.

Задача 1.2. Використовуючи розширений алгоритм Евкліда, знайдіть лінійне зображення НСД(a, b), отриманих у задачі 1.1, записати всі кроки алгоритму.

Задача 1.3. Використовуючи алгоритм Евкліда, обчисліть

(a) 33^{-1} в $\mathbb{Z}_{101}$; (b) 31^{-1} в $\mathbb{Z}_{131}$; (c) 157^{-1} в $\mathbb{Z}_{1057}$;
(d) 123^{-1} в $\mathbb{Z}_{2030}$; (e) 131^{-1} в $\mathbb{Z}_{1031}$; (f) 147^{-1} в $\mathbb{Z}_{1093}$.

Задача 1.4. Нехай a та b — натуральні числа.

(a) Припустимо, що існують такі цілі числа u та v, що $au + bv = 1$. Доведіть, що НСД$(a, b) = 1$.

(b) Припустимо, що існують такі цілі числа u та v, що $au + bv = 6$. Чи випливає звідси, що НСД$(a, b) = 6$?

(c) Припустимо, що (u_1, v_1) та (u_2, v_2) — два розв'язки в цілих числах рівняння $au+bv = 1$. Доведіть, що a ділить v_2-v_1, а b ділить u_2-u_1.

Задача 1.5. Нехай $a_1, a_2, \ldots, a_k$ — цілі числа, для яких

$$\text{НСД}(a_1, a_2, \ldots, a_k) = 1.$$

Доведіть, що існують такі цілі числа $u_1, u_2, \ldots, u_k$, що

$$a_1u_1 + a_2u_2 + \cdots + a_ku_k = 1.$$

Задача 1.6. Нехай a та b — взаємно прості числа. Доведіть, що

$$a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{ab}.$$

Задача 1.7. Нехай a та b — цілі числа. Припустимо, що $g^a \equiv 1 \pmod{m}$ та $g^b \equiv 1 \pmod{m}$. Доведіть, що

$$g^{\text{НСД}(a,b)} \equiv 1 \pmod{m}.$$

Задача 1.8. Розглянемо конгруенцію

$$ax \equiv c \pmod{m}.$$

(a) Доведіть, що ця конгруенція має розв'язок тоді і лише тоді, коли НСД(a, m) ділить c.

(b) Доведіть, що коли ця конгруенція має розв'язок, то вона має НСД(a, m) різних розв'язків за модулем m.

Задача 1.9. Використовуючи алгоритм швидкого піднесення до степеня, обчисліть (a) $19^{199} \pmod{256}$; (b) $13^{477} \pmod{1001}$; (c) $7^{271} \pmod{314}$; (d) $14^{1789} \pmod{2046}$.

Задача 1.10. Розв'яжіть задачу Сунь-Цзи, за умови, що кількість речей менша за 100 (див. приклад 1.9).

Задача 1.11. Розв'яжіть системи конгруенцій в кільці $\mathbb{Z}$:

$$\text{a)}\ \begin{array}{l} x \equiv 1 \pmod 2, \\ x \equiv 1 \pmod 3, \\ x \equiv 9 \pmod{11}; \end{array} \qquad \text{b)}\ \begin{array}{l} x \equiv 2 \pmod 5, \\ x \equiv 3 \pmod 7, \\ x \equiv 5 \pmod{11}; \end{array} \qquad \text{c)}\ \begin{array}{l} x \equiv 5 \pmod 9, \\ x \equiv 7 \pmod 8, \\ x \equiv 3 \pmod 7; \end{array}$$

$$\text{d)}\ \begin{array}{l} x \equiv 1 \pmod 3, \\ 5x \equiv 5 \pmod 6, \\ 2x \equiv 10 \pmod 7; \end{array} \qquad \text{e)}\ \begin{array}{l} 4x \equiv 1 \pmod 7, \\ 4x \equiv 3 \pmod 9, \\ 4x \equiv 9 \pmod{11}; \end{array} \qquad \text{f)}\ \begin{array}{l} 3x \equiv 4 \pmod 5, \\ 7x \equiv 1 \pmod 8, \\ 10x \equiv 9 \pmod{13}. \end{array}$$

Задача 1.12. Знайдіть остачу від ділення (a) 123^{456} на 1001; (b) 271^{314} на 1001.

Задача 1.13. Знайдіть найменше трицифрове натуральне число N, таке, що $N - 3$ ділиться на 5 і 11, а $N - 5$ ділиться на 8.

Задача 1.14. Знайдіть таке найбільше трицифрове натуральне число, яке при діленні на 5 дає в остачі 7, при діленні на 7 дає в остачі 4, а при діленні на 11 дає в остачі 3.

Задача 1.15. Нехай N — це тризначне додатне число, яке при діленні на 9 і 10 дає в остачі 7, а при діленні на 11 дає в остачі 3. Про це число також відомо, що воно є дільником деякого 6-значного натурального числа M, яке при діленні на 9, 10 і 11 дає в остачі 8, 7 і 1 відповідно. Знайдіть частку від ділення M на N.

Задача 1.16. Використовуючи афінне перетворення шифрування

$$X \mapsto 7X + 17 \pmod{26},$$

зашифруйте повідомлення `WFAVP`.[1]

Задача 1.17. Використовуючи афінне перетворення шифрування

$$X \mapsto 11X + 13 \pmod{26},$$

зашифруйте повідомлення `ONWJKKAYTRL`

Задача 1.18. Використовуючи афінне перетворення шифрування

$$X \mapsto 7X + 17 \pmod{26},$$

зашифруйте повідомлення `ONJVNOYNWFAVP`

[1] В цій та інший задачах вважаємо, що літери занумеровано як у таблиці на стор. 12

Задача 1.19. Використовуючи афінне перетворення шифрування

$$X \mapsto 9X + 14 \pmod{26},$$

зашифруйте повідомлення `QFKXPRWNRSWM`

Задача 1.20. Використовуючи афінне перетворення шифрування

$$X \mapsto 17X + 12 \pmod{26},$$

зашифруйте повідомлення `FUAHYDYXYMSY`

Задача 1.21. Відомо, що при шифруванні використовувалося афінне перетворення шифрування $X \mapsto 17X + 13 \pmod{26}$. Було отримано повідомлення `CDSI`. Відновіть повідомлення. Знайдіть перетворення розшифровування.

Задача 1.22. Алекс надіслав Юстасу наступне повідомлення, зашифроване за допомогою афінного перетворення за модулем 26,

`KQQLJQDKOEMRCN`.

Відомо, що останні чотири літери — це підпис ALEX. Розшифруйте перехоплене повідомлення.

Задача 1.23. Найкраща шпигунка надіслала наступне повідомлення, зашифроване за допомогою афінного перетворення за модулем 26,

`YVOEYJJPKBY`.

Відомо, що перші три літери — це жіноче ім'я EVA. Розшифруйте це повідомлення. Знайдіть перетворення розшифровування.

Задача 1.24. Головним контррозвідником країни Оз було перехоплене наступне повідомлення, зашифроване за допомогою афінного перетворення за модулем 26,

`RLZPNUFXOINJT`.

Відомо, що останні чотири літери — це ім'я JACK. Розшифруйте повідомлення. Знайдіть перетворення розшифровування.

Задача 1.25. Найголовніший бос надіслав своїй заступниці повідомлення, зашифроване за допомогою афінного перетворення за модулем 26,

`FRGQRDLBMVMPTQQ`.

Відомо, що перші п'ять літер — це її ім'я CARLA. Розшифруйте повідомлення. Знайдіть перетворення розшифровування.

2 Елементи теорії скінчених полів

2.1 Характеризація скінченних полів

Нагадаємо, що поле — це непорожня множина, яку позначимо F, на якій визначено дві бінарні дії, які називаються *додаванням* та *множенням*, і яка містить два виділені елементи 1 та 0, причому $1 \neq 0$. Крім того, $(F, +)$ — абелева група з нейтральним елементом 0, $(F^*, \cdot)$ — абелева група з нейтральний елементом 1. Додавання та множення пов'язані дистрибутивними законами.

Означення 2.1. Найменше таке $k \in \mathbb{N}$, що

$$\underbrace{1 + 1 + \ldots + 1}_{k} = 0,$$

називається *характеристикою* поля. Позначається $\operatorname{char} F$. Якщо такого k не існує, то вважають, що $\operatorname{char} F = 0$.

Твердження 2.1. *Характеристика поля є або простим числом, або 0. Характеристика скінченного поля завжди є простим числом.*

Доведення. Припустимо, що F — поле, характеристикою якого є складене число, нехай це число $n = kl$, де $k, l < n$. Тоді

$$n \cdot 1 = (kl) \cdot 1 = (k \cdot 1)(l \cdot 1) = 0.$$

Оскільки в полі немає дільників нуля, то $k \cdot 1 = 0$ або $l \cdot 1 = 0$. Суперечність з означенням характеристики поля.

Припустимо, що F — скінченне поле. Тоді в послідовності

$$0,\ 1,\ 1+1,\ 1+1+1,\ \ldots$$

деякі члени повинні повторюватись. Нехай для деяких $r > s$

$$r \cdot 1 = s \cdot 1.$$

Тоді

$$(r - s) \cdot 1 = 0.$$

Отже, поле F має скінченну характеристику. □

Теорема 2.1. *1. Якщо характеристика поля F дорівнює простому числу p, то просте підполе поля F ізоморфне полю $\mathbb{Z}_p$.*

2. *Якщо характеристика поля F дорівнює 0, то просте підполе поля F ізоморфне полю раціональних чисел $\mathbb{Q}$.*

Доведення. 1. Нехай P — просте підполе поля F.

Нехай $\operatorname{char} F = p$. Тоді можемо визначити відображення

$$\Theta : \mathbb{Z}_p \to F$$

за правилом

$$\overline{r} \mapsto r \cdot 1, \quad (r = 0,\ 1,\ , \ldots, p-1).$$

Легко перевірити, що відображення Θ є ізоморфізмом між $\mathbb{Z}_p$ та $\operatorname{Im}\Theta$. Кожне підполе F містить елемент 1, а тому містить і $r \cdot 1 = \underbrace{1 + 1 + \ldots + 1}_{r}$.

Отже, поле $\operatorname{Im}\Theta$ міститься в кожному підполі поля F, а тому є його простим підполем:

$$P = \operatorname{Im}\Theta \simeq \mathbb{Z}_p.$$

Ізоморфізм Θ є єдиним, бо

$$\Theta(1) = 1 \Rightarrow \Theta(r) = \Theta(1 + \ldots + 1) = \Theta(1) + \ldots + \Theta(1) = r \cdot 1.$$

2. Вправа. □

Наслідок 2.1. *Поле $\mathbb{Z}_p$ є єдиним полем, що складається з p елементів.*

Надалі єдине поле з p елементів позначатимемо $\mathbb{F}_p$.

Лема 2.1. *Нехай F — скінченне поле, яке містить підполе K з q елементів. Тоді F складається з q^m елементів, де $m = [F : K]$.*

Доведення. Оскільки F — скінченне поле, то його можна розглядати як скінченновимірний векторний простір над K, позначимо $\dim_K F = m$. Нехай $b_1, b_2, \ldots, b_m$ — базис F над K. Тоді кожний елемент $b \in F$ єдиним чином зображується у вигляді

$$b = k_1 b_1 + k_2 b_2 + \ldots k_m b_m, \text{ де } k_1, k_2, \ldots, k_m \in K.$$

□

Теорема 2.2. *Нехай F — скінченне поле. Тоді воно складається з p^n елементів, де просте число p є характеристикою поля F, а $n \in \mathbb{N}$ є степенем поля F над його простим підполем.*

Доведення. Оскільки поле F скінченне, то $\operatorname{char} F = p$, де p — деяке просте число. Тому просте підполе поля F ізоморфне полю $\mathbb{F}_p$, а, отже, містить p елементів. З леми 2.1 випливає, що $|F| = p^n$. □

Лема 2.2. *Якщо F — скінченне поле з q елементів, то для кожного $a \in F$ виконується $a^q = a$.*

Доведення. Очевидно. □

Лема 2.3. *Якщо F — скінченне поле з q елементів та K — підполе поля F, то многочлен$x^q - x \in K[x]$ розкладається над F наступним чином*

$$x^q - x = \prod_{a \in F} (x - a),$$

а F є полем розкладу многочлена $x^q - x$ над полем K.

Доведення. Оскільки степінь многочлен $x^q - x$ дорівнює q, то він має щонайбільше q коренів в F. З леми 2.2 нам відомі ці корені — ними є всі елементи поля F. Таким чином, многочлен $x^q - x$ розкладається над F вказаним способом і не може розкладатися над жодним меншим полем. □

Теорема 2.3 (існування та єдиність скінченних полів)**.** *Для кожного простого числа p та кожного натурального числа n існує скінченне поле з p^n елементів. Кожне скінченне поле з $q = p^n$ елементів ізоморфне полю розкладу многочлена $x^q - x$ над полем $\mathbb{F}_p$.*

Доведення. Існування. Для $q = p^n$ розглянемо многочлен $x^q - x \in \mathbb{F}_p[x]$, нехай F — його поле розкладу над $\mathbb{F}_p$. Цей многочлен має q різних коренів в полі F, бо його похідна $qx^{q-1} - 1 = -1 \neq 0$ є сталим многочленом з $\mathbb{F}_p$, а тому не може мати спільних коренів з $x^q - x$.

Покладемо

$$S = \{a \in F \mid a^q - a = 0\}.$$

Множина S має властивості:

(i) S містить 0 та 1;

(ii) якщо $a, b \in S$, то $(a - b)^q = a^q - b^q = a - b$, звідки $a - b \in S$;

(iii) для $a, b \in S$, $b \neq 0$, маємо $(ab^{-1})^q = a^q b^{-q} = ab^{-1}$, отже, $ab^{-1} \in S$.

Отже, множина S є полем.

З іншого боку, многочлен $x^q - x$ повинен цілком розкладатися в S, оскільки S містить всі його корені. Таким чином, $S = F$, а оскільки S складається з q елементів, то F є скінченним полем з q елементів.

Єдиність. Нехай F — скінченне поле, яке складається з $q = p^n$ елементів. Тоді $\operatorname{char} F = p$, а тому F містить в якості підполя $\mathbb{F}_p$. З леми 2.3

випливає, що F є полем розкладу многочлена $x^q - x$ над полем $\mathbb{F}_p$. Твердження теореми випливає тепер з єдиності поля розкладу многочлена. □

Ця теорема дає змогу говорити про цілком визначене скінченне поле з q елементів (або полі Галуа з q елементів). Позначатимемо його надалі через $\mathbb{F}_q$. Скінченне поле з q елементів також позначається $GF(q)$.

Позначимо через $\mathbb{F}_q^*$ мультиплікативну групу поля $\mathbb{F}_q$.

Теорема 2.4. *Мультиплікативна група $\mathbb{F}_q^*$ довільного скінченного поля $\mathbb{F}_q$ є циклічною.*

Доведення. Нагадаємо, що експонентою групи G називається найменше таке $e \in \mathbb{N}$, що $g^e = 1$ для всіх $g \in G$. З означення випливає, що $e \leqslant |G|$ та $e \mid |G|$. Неважко показати (зробіть це!), що в довільній абелевій групі експоненти e існує елемент порядку e.

Припустимо, що мультиплікативна група $\mathbb{F}_q^*$ має експоненту e. Тоді кожний з $q-1$ елементів групи $\mathbb{F}_q^*$ задовольняє рівняння $x^e - 1 = 0$. Оскільки кількість коренів многочлена не перевищує його степінь, то $q - 1 \leqslant e$. Враховуючи, що $e \mid (q-1)$, одержимо $e = q - 1$. Отже, група $\mathbb{F}_q^*$ містить елемент, порядок якого дорівнює порядку групи G, а тому є циклічною. □

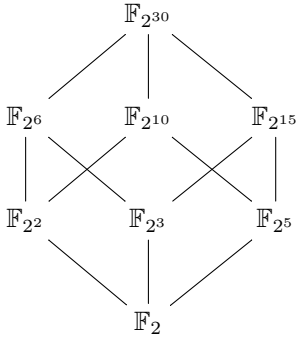
Означення 2.2. Твірний елемент циклічної групи $\mathbb{F}_q^*$ називається примітивним елементом поля $\mathbb{F}_q$.

Теорема 2.5 (критерій підполя)**.** *Нехай $\mathbb{F}_q$ — скінченне поле, яке складається з $q = p^n$ елементів, p — просте число. Тоді кожне підполе поля $\mathbb{F}_q$ має порядок p^m, де m — додатний дільник числа n. Навпаки, якщо m — додатний дільник числа n, то існує рівно одне підполе поля $\mathbb{F}_q$ з p^m елементів.*

Доведення. Ясно, що підполе K поля F повинен мати порядок p^m для деякого $m \in \mathbb{N}$, $m \leqslant n$. З леми 2.1 випливає, що число $q = p^n$ має бути степенем числа p^m, так що m обов'язко ділить число n.

Навпаки, якщо m — додатний дільник числа n, то $(p^m - 1) | (p^n - 1)$. Отже, многочлен $x^{p^m-1} - 1$ ділить многочлен $x^{p^n-1} - 1$ в $\mathbb{F}_p[x]$. Таким чином, $x^{p^m} - x$ ділить многочлен $x^{p^n} - x$ в $\mathbb{F}_p[x]$. Отже, кожний корінь многочлена $x^{p^m} - x$ є коренем многочлена $x^q - x$, а тому належить полю $\mathbb{F}_q$. Тому поле $\mathbb{F}_q$ повинно містити в якості підполя поле розкладу многочлена $x^{p^m} - x$ над $\mathbb{F}_p$. З доведення теореми 2.3 випливає, що таке поле розкладу має порядок p^m. Якби поле $\mathbb{F}_q$ містило два різних підполя порядку p^m, то ці два підполя містили б у сукупності більше, ніж p^m коренів многочлена $x^{p^m} - x$ в полі $\mathbb{F}_q$, що неможливо. □

Приклад 2.1. Всі підполя поля $\mathbb{F}_{2^{30}}$:



2.2 Корені з одиниці та кругові многочлени

Дослідимо поле розкладу многочлена $x^n - 1$ над довільним полем K, де $n \in \mathbb{N}$.

Означення 2.3. Для $n \in \mathbb{N}$ поле розкладу многочлена $x^n - 1$ над довільним полем K називається n–круговим (або n–циклотомічним) полем над K і позначається $K^{(n)}$. Корені многочлена $x^n - 1$ з поля K називаються коренями n-го степеня з одиниці над K, множину цих коренів позначимо $E^{(n)}$.

Теорема 2.6. *Нехай $n \in \mathbb{N}$, K — поле характеристики p (можливо $p = 0$). Тоді*

(i) *Якщо $p \nmid n$, то множина $E^{(n)}$ є циклічною підгрупою порядку n мультиплікативної групи поля $K^{(n)}$.*

(ii) *Якщо $p \mid n$ та $n = mp^e$, де $m, e \in \mathbb{N}$ і $p \nmid m$, то $K^{(n)} = K^{(m)}$, $E^{(n)} = E^{(m)}$ і коренями многочлена $x^n - 1$ в полі $K^{(n)}$ є m елементів множини $E^{(m)}$, кожний з яких має кратність p^e.*

Доведення. (i) Випадок $n = 1$ тривіальний.

Нехай $n \geqslant 2$. Многочлен $x^n - 1$ та його похідна nx^{n-1} не мають спільних коренів, бо nx^{n-1} має єдиний корінь 0 в полі $K^{(n)}$. Тому многочлен $x^n - 1$ не може мати кратних коренів, так що множина $E^{(n)}$ складається з n елементів.

Якщо $\zeta, \eta \in E^{(n)}$, то $(\zeta\eta^{-1})^n = \zeta^n(\eta^n)^{-1} = 1$, так що $\zeta\eta^{n-1} \in E^{(n)}$. Отже, $E^{(n)}$ — мультиплікативна група.

Нехай $n = p_1^{e_1} \dots p_t^{e_t}$ — розклад числа n у добуток простих співмножників. Застосувавши далі ті самі міркування, що й при доведенні теореми про циклічність мультиплікативної групи скінченного поля, прийдемо до того, що для кожного i, $1 \leqslant i \leqslant t$ існує елемент $\alpha_i \in E^{(n)}$, який не є коренем многочлена $x^{n/p_i} - 1$. Отже, порядок елемента $\beta_i = \alpha_i^{n/p_i^{e_i}}$ дорівнює $p_i^{e_i}$. Таким чином, $E^{(n)}$ — циклічна група з твірним $\beta = \beta_1 \dots \beta_t$.

(ii) Цей пункт випливає з пункту (i) та рівності $x^n - 1 = x^{mp^e} - 1 = (x^m - 1)^{p^e}$. □

Означення 2.4. Нехай K — поле характеристики p, n — натуральне число, яке не ділиться на p. Тоді твірний елемент циклічної групи $E^{(n)}$ називається первісним (або примітивним) коренем n-го степеня з одиниці над полем K.

Група $E^{(n)}$ має $\varphi(n)$ твірних елементів, тобто існує $\varphi(n)$ примітивних коренів з одиниці над полем K. Якщо ζ — один з них, тоді множина всіх примітивних коренів з одиниці над полем K описується таким чином

$$\{\zeta^s \mid 1 \leqslant s \leqslant n, (n, s) = 1\}.$$

Означення 2.5. Нехай K — поле характеристики p, n — натуральне число, яке не ділиться на p, і ζ — первісний корінь n-го степеня з одиниці над полем K. Тоді многочлен

$$Q_n(x) = \prod_{\substack{s=1 \\ (s,n)=1}}^{n} (x - \zeta^s)$$

називається *n–круговим* (або *n–циклотомічним*) многочленом над полем K.

Очевидно, що $\deg Q_n(x) = \varphi(n)$, а коефіцієнти належать n-круговому полю над K. Покажемо, що насправді вони належать простому підполю поля K.

Теорема 2.7. *Нехай K — поле характеристики p, n — натуральне число, яке не ділиться на p. Тоді*

(i) $x^n - 1 = \prod_{d|n} Q_d(x)$;

(ii) *коефіцієнти n-кругового многочлена $Q_n(x)$ належать простому підполю поля K, або кільцю $\mathbb{Z}$, якщо $p = 0$.*

Доведення. (i) Кожний корінь n-го степеня з одиниці над полем K є первісним коренем d-го степеня з одиниці рівно для одного натурального дільника d числа n. А саме: якщо ζ^s — довільний корінь n-го степеня з одиниці над K (де ζ — деякий первісний корінь n-го степеня над полем K), то вказане число d дорівнює $\frac{n}{(s,n)}$, тобто d — порядок елемента ζ^s в групі $E^{(n)}$. Оскільки

$$x^n - 1 = \prod_{s=1}^{n} (x - \zeta^s),$$

то формулу в пункті (i) можна одержати, зібравши ті множники $(x-\zeta^s)$, для яких ζ^s є первісним коренем з одиниці d-го степеня з одиниці над полем K (для кожного додатного дільника d числа n.)

(ii) Індукція по n. Твердження, очевидно, є справедливим для многочлена $Q_1(x) = x - 1$. Нехай $n > 1$, та припустимо, що твердження виконується для всіх $Q_d(x)$, де $1 \leqslant d < n$. За пунктом (i)

$$Q_n(x) = \frac{x^n - 1}{\prod_{d|n, d<n} Q_d(x)}.$$

За припущенням індукції коефіцієнта многочлена у знаменнику належать простому підполю поля K (або $\mathbb{Z}$, якщо $\operatorname{char} K = 0$). Розділивши чисельник на знаменник, одержимо твердження пункту (ii). □

Приклад 2.2. Нехай $n = 3$, K — довільне поле, для якого $\operatorname{char} K \neq 3$, нехай ζ — примітивний кубічний корінь над K. Тоді

$$Q_3(x) = (x - \zeta)(x - \zeta^2) = x^2 - (\zeta + \zeta^2)x + \zeta^3 = x^2 + x + 1.$$

Приклад 2.3. Нехай r — просте і $k \in \mathbb{N}$. Тоді

$$Q_{r^k} = 1 + x^{r^k k - 1} + x^{2r^{k-2}} + \ldots + ^{(r-1)r^{k-1}},$$

оскільки за теоремою 2.7

$$Q_{r^k} = \frac{x^{r^k} - 1}{Q_1(x) Q_r(x) \ldots Q_{r^{k-1}}} = \frac{x^{r^k} - 1}{x^{r^{k-1}} - 1}.$$

При $k = 1$ маємо

$$Q_r(x) = 1 + x + x^2 + \ldots + x^{r-1}.$$

Використовуючи формулу обертання Мьобіуса, можна одержати явну формулу для n-го кругового многочлена $Q_n(x)$ для довільного $n \in \mathbb{N}$. Зацікавлений читач може знайти це у [2].

Означення 2.6. Нехай b та n — взаємно прості натуральні числа. Найменше таке $k \in \mathbb{N}$, що $b^k \equiv 1 \pmod{n}$ називається *мультиплікативним порядком* b за модулем n, позначається $\mathrm{ord}_n(b)$.

Теорема 2.8. *Кругове поле $K^{(n)}$ є простим алгебраїчним розширенням поля K. Більше того, якщо $k = \mathbb{F}_q$ та $(q, n) = 1$, а $d = \mathrm{ord}_n(q)$, тоді*

- *Q_n розкладається у добуток $\varphi(n)/d$ різних унітарних незвідних многочленів з $K[x]$ одного і того самого степеня d;*
- *$K^{(n)}$ є полем розкладу довільного такого незвідного дільника над полем K;*
- *$[K^{(n)} : K] = d$.*

Доведення. Якщо існує примітивний корінь з одиниці n-го степеня ζ над K, то $K^{(n)} = K(\zeta)$. В іншому разі K — це поле, характеристика якого дорівнює простому числу p, яке ділить число n. У цьому випадку ми потрапляємо у ситуацію теореми 2.6 (ii), тоді $K^{(n)} = K^{(m)}$, де $n = mp^e$, $(m, p) = 1$. Отже, знов $K^{(n)} = K(\zeta)$, бо існує первісний корінь m-го степеня з одиниці ζ над K.

Нехай $K = \mathbb{F}_q$, припустимо, що $(q, n) = 1$. Отже, існує примітивний корінь з одиниці степеня n над полем $\mathbb{F}_q$. Нехай η — один з них. Тоді

$$\eta \in \mathbb{F}_{q^k} \Leftrightarrow \eta^{q^k} = \eta \Leftrightarrow q^k \equiv 1 \pmod{n}.$$

Найменше натуральне число, для якого це виконується, це $k = d$, отже, $\eta \in \mathbb{F}_{q^d}$, але не в довільному власному підполі. Таким чином, мінімальний многочлен для η має степінь d. Оскільки η — довільний корінь $Q_n(x)$, то твердження теореми має місце, бо ми можемо послідовно ділити на мінімальні многочлени коренів многочлена $Q_n(x)$. □

Приклад 2.4. Нехай $K = \mathbb{F}_{11}$, $n = 12$. З попереднього прикладу маємо, що $Q_{12}(x) = x^4 - x^2 + 1 \in \mathbb{F}_{11}[x]$. Нас цікавить $K^{(12)}$.

- Оскільки $12 \nmid (11 - 1)$, але $12 \mid (11^2 - 1)$, то $d = \mathrm{ord}_{12}(11) = 2$.
- Таким чином, $Q_{12}(x)$ розкладається в добуток $\varphi(12)/2 = 4/2 = 2$ унітарних квадратних незвідних над $\mathbb{F}_{11}$ многочленів. Круговим полем є $K^{(12)} = \mathbb{F}_{121}$.

- Неважко перевірити, що розклад $Q_{12}(x)$ на множники має вигляд

$$Q_{12} = (x^2 + 5 + 1)(x^2 - 5x + 1).$$

Теорема 2.9. *Скінченне поле $\mathbb{F}_q$ є $(q-1)$-круговим полем над будь-яким зі своїх підполів.*

Доведення. Многочлен $x^{q-1} - 1$ цілком розкладається на множники в полі $\mathbb{F}_q$, бо його коренями є як раз всі ненульові елементи поля $\mathbb{F}_q$. З іншого боку, зрозуміло, що цей многочлен не може цілком розкладатися на множники в жодному іншому власному підполі поля $\mathbb{F}_q$. Отже, $\mathbb{F}_q$ є полем розкладу многочлена $x^{q-1}-1$ над довільним зі своїх підполів. □

Зображення елементів скінченних полів

Якщо скінченне поле складається з p елементів, p — просте число, то його елементи можна ототожнити з елементами кільця лишків $\mathbb{Z}_p$. Якщо ж кількість елементів скінченного поля є степенем простого числа, то таке ототожнення неможливе, бо кільце лишків є полем лише за модулем простого числа. Отже, у такому випадку потрібні інші способи зображення елементів скінченного поля. Розглянемо два способи зображення елементів скінченного поля $\mathbb{F}_q = \mathbb{F}_{p^n}$.

Перший спосіб. Поле $\mathbb{F}_q$, де $q = p^n$, є простим алгебраїчним розширенням поля $\mathbb{F}_p$. Дійсно, якщо f — незвідний многочлен степеня n над полем $\mathbb{F}_p$, то кожний корінь цього α цього многочлена належить полю $\mathbb{F}_{p^n} = \mathbb{F}_q$, а тому $\mathbb{F}_q = \mathbb{F}_p(\alpha)$. Отже, кожний елемент поля $\mathbb{F}_q$ можна однозначно подати у вигляді значень деякого многочлена від x над $\mathbb{F}_p$ степеня, не більшого за $n-1$, при $x = \alpha$. Можна також розглядати поле $\mathbb{F}_q$ як факторкільце $\mathbb{F}_p[x]/(f)$.

Приклад 2.5. Побудуємо поле з дев'яти елементів. Візьмемо незвідний над $\mathbb{Z}_3$ многочлен $x^2 + 1$ та розглянемо факторкільце $\mathbb{Z}_3[x]/(x^2 + 1)$. Нехай $\alpha \in \mathbb{F}_9$ — корінь многочлена $f(x) = x^2 + 1$, тобто в полі $\mathbb{F}_9$ $\alpha^2 + 1 = 0$. Тоді елементи поля можна зобразити у вигляді $a_0 + a_1\alpha$, де $a_0, a_1 \in \mathbb{Z}_3$. Отже,

$$\mathbb{F}_9 = \{0, 1, 2, \alpha, 1 + \alpha, 2 + \alpha, 2\alpha, 1 + 2\alpha, 2 + 2\alpha\}.$$

Наведемо приклади додавання та множення у цьому полі. Нехай $f_1 = 2 + \alpha$, $f_2 = 2 + 2\alpha$. Тоді (обчислення відбуваються за модулем 3, також враховуємо, що $\alpha^2 + 1 = 0$)

$$f_1 + f_2 = 4 + 3\alpha = 1, \quad f_1 f_2 = 4 + 6\alpha + 2\alpha^2 = 2.$$

У *другому способі* використовується те, що мультиплікативна група скінченного $\mathbb{F}_q$ поля є циклічною. Тоді елементи поля подаються у вигляді степенів примітивного елемента поля $\mathbb{F}_q$. Для знаходження примітивних многочленів можна використовувати кругові многочлени, тут допоможуть теореми 2.8 та 2.9. Оскільки $\mathbb{F}_q = \mathbb{F}_{p^n}$ є $(q-1)$–круговим полем над $\mathbb{F}_p$, то можемо побудувати це поле наступним чином:

- Знайти розклад $(q-1)$-кругового многочлена $Q_{q-1} \in \mathbb{F}_p[x]$ в добуток незвідних многочленів в $\mathbb{F}_p[x]$, всі степені яких однакові.
- Корінь α кожного з цих дільників є первісним коренем $(q-1)$-го степеня з одиниці над $\mathbb{F}_p$, а тому є примітивним елементом поля $\mathbb{F}_q$.
- Для такого α ми маємо

$$\mathbb{F}_q = \left\{0, \alpha, \alpha^2, \ldots, \alpha^{q-2}, \alpha^{q-1} = 1\right\}.$$

Приклад 2.6. Розглянемо знов поле $\mathbb{F}_9$. Будемо діяти у відповідності з викладеним вище.

- Поле $\mathbb{F}_9$ є 8–круговим розширенням поля $\mathbb{F}_3$, тобто $\mathbb{F}_9 = \mathbb{F}_3^{(8)}$.
- Знайдемо 8–круговий многочлен $Q_8(x)$:

$$Q_8(x) = \frac{x^{2^3} - 1}{x^{2^2} - 1} = x^4 + 1 \in \mathbb{F}_3[x].$$

  Він розкладається в добуток незвідних в кільці $\mathbb{F}_3[x]$ наступним чином

$$Q_8(x) = (x^2 + x + 2)(x^2 + 2x + 2).$$

  Ми маємо $\varphi(8)/(\mathrm{ord}_8\, 3) = 4/2 = 2$ незвідних многочленів другого степеня.

- Нехай ζ — корінь $x^2 + x + 2$. Тоді ζ є первісним степенм з одиниці над полем $\mathbb{F}_3$. Отже,

$$\mathbb{F}_9 = \left\{0, \zeta, \zeta^2, \ldots, \zeta^7, \zeta^8 = 1\right\}.$$

Природним чином виникає питання, яким чином це зображення елементів поля $\mathbb{F}_9$ пов'язане з попереднім.

Приклад 2.7. Розглянемо многочлен $f(x) = x^2 + 1 \in \mathbb{F}_3[x]$, він є незвідним над полем $\mathbb{F}_3$. Отже, ми можемо побудувати поле $\mathbb{F}_9$ шляхом приєднання кореня α многочлена $f(x) = x^2+1$ до поля $\mathbb{F}_3$. Тоді $\alpha^2+1 = 0$ в $\mathbb{F}_9$ і

$$\mathbb{F}_9 = \{0, 1, 2, \alpha, 1+\alpha, 2+\alpha, 2\alpha, 1+2\alpha, 2+2\alpha\}.$$

Помітимо тепер, що $\zeta = \alpha + 1$ є коренем многочлена $x^2 + x + 2 \in \mathbb{F}_3[x]$. Отже, елементи в двох зображеннях поля $\mathbb{F}_9$ пов'язані наступним чином:

i	ζ^i
1	$1+\alpha$
2	2α
3	$1+2\alpha$
4	2
5	$2+2\alpha$
6	α
7	$2+\alpha$
8	1

Зображення елементів скінченного поля таким способом дає зручний спосіб знаходження добутку елементів. Дійсно,

$$\zeta^3 \cdot \zeta^6 = \zeta^9 = \zeta,$$

бо $\zeta^8 = 1$ у $\mathbb{F}_9^*$.

Проте цей спосіб не дуже зручний для виконання дії додавання. Для спрощення дії додавання будуються так звані таблиці додавання одиниці. Нас цікавить, чому дорівнюватиме показник j у рівності $\zeta^i + 1 = \zeta^j$ для всіх $i = 1, \ldots, 8 \cup \{-\infty\}$ (за домовленістю вважається, що $0 = \zeta^{-\infty}$). Складемо таблицю. Для її побудови використаємо вже знайдені зображення елементів поля $\mathbb{F}_9$:

i	1	2	3	4	5	6	7	8	$-\infty$
ζ^i	$1+\alpha$	2α	$1+2\alpha$	2	$2+2\alpha$	α	$2+\alpha$	1	0
ζ^i+1	$2+\alpha$	$1+2\alpha$	$2+2\alpha$	0	2α	$1+\alpha$	α	2	1
ζ^j	ζ^7	ζ^3	ζ^5	$\zeta^{-\infty}$	ζ^2	ζ	ζ^6	ζ^4	ζ^8
j	7	3	5	$-\infty$	2	1	6	4	8

Насправді нас цікавлять лише перший та останній рядки цієї таблиці, бо нам потрібно знати лише показники степенів.

Тепер цю таблицю зручно використовувати для "перетворення" дії додавання на дію множення. Наприклад,

$$\zeta^6 + \zeta^3 = \zeta^3(\zeta^3 + 1) = \zeta^3 \cdot \zeta^5 = \zeta^8 = 1.$$

2.3 Задача дискретного логарифмування та алгоритми її розв'язування

Задача дискретного логарифмування. Нехай дано просте число p, твірний елемент α групи $\mathbb{Z}_p^*$ та елемент $\beta \in \mathbb{Z}_p^*$. Знайти таке ціле число x, $0 \leqslant x \leqslant p-2$, що $\alpha^x \equiv \beta \pmod{p}$.

Узагальнена задача дискретного логарифмування. Нехай дано скінченну циклічну групу G порядку n, твірний елемент α групи G, елемент $\beta \in G$. Знайти таке ціле число x, $0 \leqslant x \leqslant n-1$, що $\alpha^x \equiv \beta$.

Число x називається *дискретним логарифмом* β з основою α.

Приклад 2.8. Візьмемо групу $G = \mathbb{Z}_{11}^* = \langle 2 \rangle$. Тоді дискретний логарифм числа 7 з основою 2 дорівнює 7.

Зауваження 1. Нехай α та γ — два різних твірних циклічної групи G порядку n, нехай $\beta \in G$. Нехай $x = \log_\alpha \beta$, $y = \log_\gamma \beta$, $z = \log_\alpha \gamma$. Тоді $\alpha^x = \beta = \alpha^y = (\alpha^z)^y$, звідки $x = zy \pmod{n}$ та

$$\log_\gamma \beta = (\log_\alpha \beta)(\log_\alpha \gamma)^{-1} \pmod{n}.$$

Це означає, що будь-який алгоритм, який обчислює логарифми з основою α, можна використати для обчислення логарифму з будь-якою іншою основою γ. Отже, *складність задачі дискретного логарифмування не залежить від вибору твірного групи G.*

Алгоритми розв'язування задачі дискретного логарифмування

Повний перебір. Найбільш очевидний алгоритм розв'язування узагальненої задачі дискретного логарифмування — це послідовно обчислювати

$$\alpha^0, \alpha^1, \alpha^2, \ldots,$$

доки не одержимо β. Цей метод вимагає $O(n)$ множень, де n — це порядок α, а тому неефективний, коли n велике (наприклад, у криптографічних інтересах).

Метод Шенкса (Baby-step giant-step). Це фундаментальний алгоритм розв'язування задачі дискретного логарфимування. Він застосовний до будь–якої скінченної циклічної групи.

Нехай $m = [\sqrt{n}] + 1$, де n — це порядок елемента α. Алгоритм Шенкса базується на наступному спостереженні. Якщо $\beta = \alpha^x$, тоді можна записати $x = im + j$, де $0 \leqslant i, j < m$. Отже, $\alpha^x = \alpha^{im}\alpha^j$, з чого випливає $\beta(\alpha^{-m})^i = \alpha^j$. Це передбачає наступний алгоритм обчислення x.

Алгоритм Шенкса.

Дано: твірний α циклічної групи G порядку n та елемент $\beta \in G$.

Знайти: дискретний логарифм $x = \log_\alpha \beta$.

1. Покласти $m = [\sqrt{n}] + 1$.
2. Побудувати таблицю зі входженнями (j, α^j) для $0 \leqslant j < m$. Впорядкувати цю таблицю за другою компонентою.
3. Обчислити α^{-m} та покласти $\gamma = \beta$.
4. Для i від 0 до $m - 1$ зробити наступне:
   (a) Перевірити, чи не є γ другою компонентою деякого елемента з таблиці.
   (b) Якщо $\gamma = \alpha^j$, то покласти $x = im + j$.
   (c) Покласти $\gamma = \gamma \cdot \alpha^{-m}$.

Оцінимо кількість дій, потрібних для роботи алгоритму Шенксак. Для побудови таблиці потрібно $O(\sqrt{n})$ множень та $O(\sqrt{n} \ln n)$ порівнянь для сортування. Маючи вже побудовану таблицю, для кроку 4 нам потрібно $O(\sqrt{n})$ множень та $O(\sqrt{n})$ переглядів таблиці. За припущення, що групове множення вимагає більше часу, ніж $\ln n$ порівнянь, то час роботи алгоритму можна оцінити наступним чином.

Факт. *Алгоритм Шенкса вимагає $O(\sqrt{n})$ групових множень.*

Приклад 2.9. Нехай $p = 113$, $\alpha = 3$ — твірний $\mathbb{Z}^*_{113}$. Обчислимо $\log_3 32$.

1. Покладемо $m = [\sqrt{112}] + 1 = 11$.
2. Побудуємо таблицю з елементів (j, α^j) для $j = 0, 1, 2, \ldots$.

j	0	1	2	3	4	5	6	7	8	9	10
$3^j \pmod{113}$	1	3	9	27	81	17	51	40	7	21	63

   та відсортуємо за другою компонентою:

j	0	1	8	2	5	9	3	7	6	10	4
$3^j \pmod{113}$	1	3	7	9	17	21	27	40	51	63	81

3. Обчислюємо в групі $\mathbb{Z}^*_{113}$ спочатку $\alpha^{-1} = 3^{-1} = 38$, а потім $\alpha^{-m} = 3^{-113} = 58$.

4. Далі обчислюємо $\gamma = \beta\alpha^{-mi} \pmod{113}$ для $i = 0, 1, 2, \ldots$ до тих пір, доки не одержимо значення з другого рядка таблиці:

i	0	1	2	3	4	5
$\gamma = 32 \cdot 58^i \pmod{113}$	32	48	72	108	49	17

Оскільки $\beta\alpha^{-5m} = \alpha^5$, то $\beta = \alpha^{60}$. Отже, $\log_3 32 = 60$.

Алгоритм обчислення спільного таємного значення (алгоритм Діффі–Хелмана)

Цей алгоритм дає змогу двом віддаленим абонентам мережі встановити спільне таємне значення шляхом обміну нетаємними повідомленнями. Це спільне таємне значення використовується для обчислення спільного сесійного таємного ключа в алгоритмах симетричного шифрування.

Процес встановлення спільного таємного значення.

Перед початком роботи абоненти A та B узгоджують скінченну циклічну групу G порядку n та її твірний елемент g. Після цього виконують наступні дії.

Абонент A

- обирає випадкове ціле число x, $0 \leqslant x < n$;
- обчислює в групі G елемент $X = g^x$;
- надсилає елемент $X = g^x$ групи G абоненту B.

Абонент B

- обирає випадкове ціле число y, $0 \leqslant y < n$;
- обчислює в групі G елемент $Y = g^y$;
- надсилає елемент $Y = g^y$ групи G абоненту A.

Після цього абонент A обчислює Y^x, а абонент B обчислює X^y. Таким чином абоненти A і B обчислили спільне таємне значення, бо

$$Y^x = g^{yx} = g^{xy} = X^y.$$

Задача Діффі–Хелмана. *Нехай g — твірний скінченної циклічної групи. Знаючи g, g^x та g^y, знайти g^{xy}.*

Припущення Діффі–Хелмана. *Складність обчислення g^{xy} за g, g^x та g^y надзвичайно висока.*

Складність розв'язання задачі Діффі–Хелмана забезпечує надійність алгоритму Діффі-Хелмана встановлення спільного таємного значення.

Припущення Діффі–Хелмана апріорі не слабше за припущення про надзвичайну складність задачі дискретного логарифмування в скінченній групі. Якби можна було легко обчислювати дискретні логарифми, то припущення Діффі–Хелмана було б невірним. Є думка, що справедливим є і обернене твердження, проте поки це питання лишається відкритим. Іншими словами, поки ще ніхто не запропонував алгоритм одержання g^{xy} з g^x та g^y без використання x та y. Проте цілком можливо, що такий спосіб існує.

Задачі

Задача 2.1. Випишіть всі незвідні поліноми над полем $\mathbb{F}_2$ степенів $1, 2, 3, 4$ та довести їх незвідність.

Задача 2.2. Доведіть, що натуральне число n ділить число $\varphi(p^n - 1)$, де φ — функція Ейлера, p — просте число.

Задача 2.3. Доведіть, що в полі $\mathbb{Z}_p$ виконуються рівності

(a) $\sum_{k=1}^{p-1} \frac{1}{k} = 0$, $p > 2$;

(b) $\sum_{k=1}^{(p-1)/2} \frac{1}{k^2} = 0$, $p > 3$.

Задача 2.4. Доведіть, що факторкільце $F = \mathbb{Z}_3[x]/(x^2 + 1)$ є полем. Позначимо $\overline{f(x)} = f(x) + \big(x^2 + 1\big)$. Покажіть, що $\overline{x + 1}$ є твірним мультиплікативної групи F^* поля F.

Задача 2.5. Розв'яжіть рівняння $x^3 + x^2 - 2x - 1$ у полі (a) $\mathbb{Z}_3$; (b) $\mathbb{Z}_5$; (c) $\mathbb{Z}_7$; (d) $\mathbb{Z}_{11}$.

Задача 2.6. Доведіть, що довільний квадратний многочлен з $\mathbb{F}_q[x]$ розкладається над полем $\mathbb{F}_{q^2}$ на лінійні множники.

Задача 2.7. Знайдіть всі незвідні над $\mathbb{F}_q$ многочлени, коренями яких є елементи $\mathbb{F}_{q^2}$.

Задача 2.8. Знайдіть кількість таких елементів $a \in \mathbb{F}_q$, які не є квадратами в $\mathbb{F}_{q^2}$.

Задача 2.9. Розкладіть многочлен $x^{16}+x \in \mathbb{F}_2[x]$ на незвідні множники над полем $\mathbb{F}_2$.

Задача 2.10. Знайдіть степені незвідних многочленів, в добуток яких розкладається многочлен $x^n - 1 \in \mathbb{F}_q[x]$ над полем $\mathbb{F}_q$, якщо $q = 2^4$, а $n = 5, 7, 22$. Відповідь обґрунтуватии.

Задача 2.11. Побудуйте скінченне поле з (a) 8; (b) 9; (c) 16; (d) 25 елементів.

Задача 2.12. Знайдіть всі примітивні елементи скінченних полів:

(a) $\mathbb{Z}_5$; (b) $\mathbb{Z}_7$; (c) $\mathbb{Z}_{11}$; (d) $\mathbb{Z}_{13}$; (e) $\mathbb{Z}_{17}$; (f) $\mathbb{Z}_{19}$.

Задача 2.13. Скільки примітивних елементів має поле $\mathbb{F}_8$? Вкажіть який–небудь примітивний елемент поля $\mathbb{F}_8$. Зобразіть решту примітивних елементів як його степені. Зобразіть елементи поля $\mathbb{F}_8$ двома способами.

Задача 2.14. Скільки примітивних елементів має поле $\mathbb{F}_9$? Вкажіть який–небудь примітивний елемент поля $\mathbb{F}_9$. Зобразіть решту примітивних елементів як його степені. Зобразіть елементи поля $\mathbb{F}_9$ двома способами.

Задача 2.15. Нехай $\alpha \in \mathbb{F}_{16}$ — корінь многочлена $x^4 + x + 1 \in \mathbb{F}_2[x]$. Зобразіть елементи поля $\mathbb{F}_{16}$ як многочлени від α степеня, меншого за 4.

Задача 2.16. Нехай $\alpha \in \mathbb{F}_{27}$ — корінь многочлена $x^3 + 2x + 1 \in \mathbb{F}_3[x]$. Зобразіть елементи поля $\mathbb{F}_{27}$ як многочлени від α степеня, меншого за 3.

Задача 2.17. Покажіть, що факторкільце $\mathbb{F}_2[x]/(x^4 + x + 1)$ є полем. Знайдіть мультиплікативні порядки елементів (тобто як елементів мультиплікативної групи)

(a) $x^2 + x + \big(x^4 + x + 1\big)$;

(b) $x^2 + 1 + \big(x^4 + x + 1\big)$;

(c) $x^2 + x + 1 + \big(x^4 + x^3 + 1\big)$;

(d) $x^3 + x + \big(x^4 + x + 1\big)$;

(e) $x^3 + 1 + \big(x^4 + x + 1\big)$;

(f) $x^3 + x + 1 + \big(x^4 + x + 1\big)$;

(g) $x^3 + x^2 + 1 + \big(x^4 + x + 1\big)$;

(h) $x^3 + x^2 + x + 1 + \big(x^4 + x + 1\big)$.

Задача 2.18. Покажіть, що факторкільце $F = \mathbb{Z}_2[x]/(x^3 + x + 1)$ є полем. Знайдіть всі твірні елементи мультиплікативної групи F^* цього поля. Для одного з твірних побудуйте таблицю додавання одиниці.

Задача 2.19. Покажіть, що факторкільце $F = \mathbb{Z}_2[x]/(x^3 + x^2 + 1)$ є полем. Знайдіть всі твірні елементи мультиплікативної групи F^* цього поля. Для одного з твірних побудуйте таблицю додавання одиниці.

Задача 2.20. Покажіть, що факторкільце $F = \mathbb{Z}_3[x]/(x^3 + 2x + 1)$ є полем. Знайдіть всі твірні елементи мультиплікативної групи F^* цього поля. Для одного з твірних побудуйте таблицю додавання одиниці.

Задача 2.21. Покажіть, що факторкільце $F = \mathbb{Z}_2[x]/(x^4 + x + 1)$ є полем. Знайдіть всі твірні елементи мультиплікативної групи F^* цього поля. Для одного з твірних побудуйте таблицю додавання одиниці.

Задача 2.22. Нехай α — примітивний елемент поля $\mathbb{F}_p$.

(a) Припустимо, що a та b — цілі розв'язки конгруенції $\alpha^x = \beta$. Доведіть, що $a \equiv b \pmod{p-1}$.

(b) Доведіть, що $\log_\alpha(\beta_1\beta_2) = \log_\alpha \beta_1 + \log_\alpha \beta_2$ для всіх $\beta_1, \beta_2 \in \mathbb{F}_p^*$.

(c) Доведіть, що $\log_\alpha(\beta^n) = n \log_\alpha \beta$ для всіх $\beta \in \mathbb{F}_p^*$, $n \in \mathbb{Z}$,

Задача 2.23. Нехай p — непарне просте число, нехай α — примітивний елемент поля $\mathbb{F}_p$. Доведіть, що $a \in \mathbb{F}_p$ є квадратом у полі $\mathbb{F}_p$ тоді і лише тоді, коли дискретний логарифм $\log_\alpha a$ — парне число.

Задача 2.24. За допомогою методу Шенкса обчисліть в мультиплікативній групі $\mathbb{F}_{113}^* = \langle 3 \rangle$

(a) $\log_3 80$; (b) $\log_3 14$; (c) $\log_3 91$; (d) $\log_3 24$; (e) $\log_3 23$; (f) $\log_3 12$.

Задача 2.25. За допомогою методу Шенкса обчисліть в мультиплікативній групі $\mathbb{F}_{229}^* = \langle 6 \rangle$

(a) $\log_6 74$; (b) $\log_6 200$; (c) $\log_6 47$; (d) $\log_6 182$; (e) $\log_6 31$; (f) $\log_6 150$.

Задача 2.26. Анна та Борис домовилися використовувати поле $\mathbb{F}_{1373}$ та в якості твірного його мультиплікативної групи обрали 2. Відомо, що таємним значенням Анни є 333, а таємним значенням Бориса є 515. Які числа повинні вони надіслати один одному? Чому дорівнює їхнє спільне таємне значення?

Задача 2.27. Анна та Борис домовилися використовувати поле $\mathbb{F}_{1373}$ та в якості твірного його мультиплікативної групи обрали 2. Анна надіслала Борису значення $X = 609$. Відомо, що таємним значенням Бориса є 271. Яке число повинен Борис надіслати Анні? Чому дорівнює їхнє спільне таємне значення? Чи можете ви знайти таємне число Анни?

Задача 2.28. Відомо, що Анна та Борис домовилися використовувати поле $\mathbb{F}_{1373}$ та в якості твірного його мультиплікативної групи обрали 2. Зловмисник слідкує за їхнім листуванням та знає, що Анна надіслала Борису число $X = 1118$, а Борис надіслав Анні число $Y = 514$. Чому дорівнює їхній спільний таємний ключ?

Задача 2.29. Нехай p — просте, α — натуральне число. Переформулюємо задачу Діффі–Хелмана як задачу прийняття рішення, тобто таку, відповіддю на яку є "так" або "ні". Припустимо, що дано три цілі числа A, B та C, для яких

$$A = \alpha^a \pmod p \text{ та } B = \alpha^b \pmod p,$$

але значення a та b невідомі. Потрібно з'ясувати, чи $C \equiv \alpha^{ab} \pmod p$.

(a) Доведіть, що алгоритм, який дозволяє розв'язати задачу Діффі–Хелмана, дозволяє також розв'зати і задачу Діффі–Хелмана як задачу прийняття рішення.

(b) На вашу думку, задача Діффі–Хелмана як задача прийняття рішення є складною чи простою з обчислювального погляду?

Задача 2.30. Запропонуйте аналог алгоритму Діффі–Хелмана, який дозволив би встановити спільне таємне значення для (a) трьох; (b) чотирьох; (c) n абонентів.

3 Елементи теорії кодування

3.1 Поняття коду

Нехай X — це скінченна множина символів ($|X| = q > 1$), яку називатимемо *алфавітом*, нехай n — натуральне число. *Словом* довжиною n над алфавітом X називається послідовність $a_1a_2\dots a_n$ з n символів, де $a_1, a_2, \dots, a_n \in X$. *Код* $\mathcal{C}$ довжиною n — це підмножина множини X^n всіх слів довжиною n, за умови, що $|\mathcal{C}| > 1$. Елементи множини $\mathcal{C}$ називаються *кодовими словами*.

Означення 3.1. Нехай $v = v_1 \dots v_n$, $w = w_1 \dots w_n$ — слова довжиною n. Відстанню Хеммінга $d(v, w)$ від слова v до слова w називається кількість координат, в яких словах v та w відрізняються:

$$d(v, w) = |\{i \mid 1 \leqslant i \leqslant n, v_i \neq w_i\}|.$$

При передачі повідомлення зашумленим каналом зв'язку деякі символи можуть бути змінені. Відстань Хеммінга між словом, що передавалося, та словом, що було одержане, вказує на кількість помилок.

Твердження 3.1. (a) *Для довільних слів v та w* $d(v, w) \geqslant 0$ *та* $d(v, w) = 0$ *тоді і лише тоді, коли $v = w$.*

(b) *Для довільних слів v та w* $d(v, w) = d(w, v)$.

(c) (*Нерівність трикутника.*) *Для довільних слів u, v, w*

$$d(u, w) \leqslant d(u, v) + d(v, w).$$

З твердження 3.1 випливає, що відстань Хеммінга задає метрику на множині слів над алфавітом X.

Означення 3.2. Нехай $e \in \mathbb{N}$. Кажуть, що код $\mathcal{C}$ довжиною n виправляє e помилок, якщо для довільного слова w довжиною n існує щонайбільше одне кодове слово c, таке, що $d(w, c) \leqslant e$.

Назва "коди, що виправляють помилки" пояснюється наступним чином. Припустимо, що код $\mathcal{C}$ — це код, що виправляє e помилок, і ми знаємо, що при передачі одного слова може трапитися не більше, ніж e помилок. Тоді ці помилки можуть бути виправлені. Якщо c — це слово, що передавалось, а w — це слово, яке було одержане, то за припущенням $d(c, w) \leqslant e$. Оскільки код $\mathcal{C}$ виправляє e помилок, то будь–яке інше кодове слово c' задовольняє нерівність $(c', w) > e$. Отже, c — це кодове слово, як найближче до передаваного слова, а тому декодування є правильним.

Означення 3.3. Найменшою відстанню коду $\mathcal{C}$ називається найменша відстань між двома різними словами цього коду.

Найменшу відстань коду $\mathcal{C}$ позначатимемо $d_{\min}\mathcal{C}$.

Теорема 3.1. *Код $\mathcal{C}$ виправляє e помилок тоді і лише тоді, коли*

$$d_{\min}\mathcal{C} \geqslant 2e + 1.$$

Доведення. Необхідність. Нехай код $\mathcal{C}$ виправляє e помилок. Припустимо, що $d_{\min}\mathcal{C} = d \leqslant 2e$. Покладемо $f = [d/2]$, тоді $f \leqslant e$ та $e - f \leqslant e$. З умови випливає, що знайдуться два кодові слова c_1 та c_2, відстань між якими дорівнює $d(c_1, c_2) = d$. Це означає, що перейти від слова c_1 до слова c_2 можна шляхом зміни d координат. Будемо змінювати координати по одній. Нехай w — це слово, яке одержане з c_1 після f замін. Тоді $d(c_1, w) = f \leqslant e$, $d(c_2, w) = d - f \leqslant e$. Отже, існують два кодові слова, які знаходяться на відстані не більшій за e від слова w. Таким чином, код $\mathcal{C}$ не є кодом, що виправляє e помилок.

Достатність. Припустимо, що код $\mathcal{C}$ не є кодом, що виправляє e помилок. Тоді існують слово w та два кодових слова c_1 та c_2, які знаходяться на відстані не більшій за e від слова w, тобто $d(c_1, w) \leqslant e$ та $d(c_2, w) \leqslant e$. З твердження 3.1 випливає, що $d(c_1, c_2) \leqslant e + e = 2e$. Отже, маємо суперечність з умовою $d_{\min}\mathcal{C} \geqslant 2e + 1$. □

Теорема 3.2. *Нехай $\mathcal{C}$ — код довжиною n над алфавітом з q символів, d — мінімальна відстань коду. Тоді*

(a) *(границя Хеммінга) якщо $d \geqslant 2e + 1$, то*

$$|\mathcal{C}| \leqslant q^n / \sum_{i=0}^{e} \binom{n}{i} (q-1)^i;$$

(b) *(границя Сінглтона)*

$$|\mathcal{C}| \leqslant q^{n-d+1}.$$

Доведення. (a) Нехай c — кодове слово. Лишаємо читачеві в якості вправи перевірити, шо кількість слів w, які задовольняють нерівність $d(c, w) \leqslant e$, дорівнює

$$\sum_{i=0}^{e} \binom{n}{i} (q-1)^i.$$

Можна дивитися на ці слова як на "сфери" радіуса e, центром яких є кодове слово c. Якщо ми зробимо це для всіх кодових слів, то знайдені слова не будуть накладатися, бо, за припущенням, код $\mathcal{C}$ виправляє e помилок, то немає жодного слова, яке б знаходилось на відстані, що не перевищує e, від двох або більше слів. Геометрично це означає, що сфери упаковані у просторі без накладань. Отже, загальна кількість шуканих слів дорівнює

$$|\mathcal{C}| \cdot \sum_{i=0}^{e} \binom{n}{i} (q-1)^i,$$

але це число не може перевищувати загальної кількості q^n слів довжиною n над алфавітом q.

(b) В усіх кодових словах візьмемо лише перші $n-d+1$ координат. Покажемо, що всі ці початки різні. Дійсно, припустимо, що перші $n-d+1$ координат деяких різних слів c_1 та c_2 однакові, але тоді вони можуть відрізнятися не більше ніж в останніх $n-(n-d+1)=d-1$ координатах. Отже, $d(c_1,c_2)\leqslant d-1$, що суперечить припущенню. Таким чином, кількість кодових слів не може перевищувати загальну кількість початків, яка дорівнює q^{n-d+1}. □

Коди, які досягають границю Хеммінга, називаються *досконалими*. Коди, які досягають границю Сінглтона, називаються *роздільними кодами з максимальною відстанню*.

Приклад 3.1. Кодом з повтореннями називається код, у якому всі кодові слова мають вигляд $aa\ldots a$, $a\in X$, $|X|=q$. Такий код складається з q слів, і його мінімальна відстань дорівнює довжині n. Якщо $d=n$, то за пунктом (b) теореми 3.2 $|\mathcal{C}|\leqslant q^{n-n+1}=q$, тобто код з повтореннями досягає границі Сінглтона. Якщо $q=2$, а $n=2e+1$, то цей код досягає також і границі Хеммінга.

3.2 Лінійні коди

Формалізуємо процеси кодування та декодування. Нехай S — це множина повідомлень, X — алфавіт, що складається з q символів, $\mathcal{C}$ — код довжиною n над алфавітом X. Тоді відображення кодування — це ін'єктивне відображення

$$\epsilon\colon S\to\mathcal{C}.$$

Відображення декодування — це відображення

$$\delta : X^n\to\mathcal{C}.$$

Хоча жодних формальних вимог не висувається, як правило, припускають, що кодове слово декодується в найближче слово, тобто $\delta(w)$ — це слово, яке якомога ближче до слова w.

Візьмемо в якості алфавіту X скінченне поле $\mathbb{F}_q$ і надалі всі кодові слова розглядатимемо над таким алфавітом. Доволі часто коди розглядають над полем $\mathbb{F}_2$, у таких випадках говорять про бінарний алфавіт, а коди над алфавітом $\mathbb{F}_2$ називають *бінарними* кодами.

Означення 3.4. Лінійним кодом довжиною n та розмірністю k, або скорочено лінійним (n,k) – кодом, називається k–вимірний підпростір векторного простору $\mathbb{F}_q^n$.

Означення 3.5. Вагою $\mathrm{wt}(w)$ слова w називається кількість ненульових координат слова w. Мінімальною вагою кода називається найменша вага серед усіх кодових слів.

Твердження 3.2. *Мінімальна вага та мінімальна відстань лінійного коду однакові.*

Доведення. Пропонуємо читачеві довести це твердження самостійно. □

З цього твердження вже випливають певні переваги лінійних кодів. Наприклад, замість того, щоб порівнювати усі пари кодових слів, щоб знайти мінімальну відстань, досить переглянути усі кодові слова та знайти мінімальну вагу. Якщо передавалося слово c, а одержане було слово w, то $c = w + x$, де вага слова x дорівнює кількості помилок, що трапилися при передачі повідомлення.

Природним чином виникає запитання, як описати лінійний код. Оскільки лінійний код $\mathcal{C}$ — це підпростір простору $\mathbb{F}_q^n$, то в ньому можна обрати базис, що складатиметься з k слів довжиною n. Утворимо матрицю G, рядками якої будуть слова, що відповідають цим базисним векторам. Ця матриця називається *твірною матрицею* коду $\mathcal{C}$.

Кожне кодове слово можна єдиним чином записати у вигляді

$$c = x_1 g_1 + \cdots + x_k g_k, \text{ де } g_1, \ldots, g_k \text{ — рядки матриці } G.$$

Якщо позначити $x = x_1 \ldots x_k \in \mathbb{F}_q^k$, то більш коротко можна записати $c = xG$. Таким чином, якщо множина S повідомлень, які мають бути передані, це множина $\mathbb{F}_q^k$ всіх слів довжиною k, тоді відображення ϵ кодування — це просто лінійне відображення

$$x \mapsto x\,G: \quad \mathbb{F}_q^k \to \mathbb{F}_q^n.$$

Це відображення є ін'єктивним, а його образом є код $\mathcal{C}$.

З курсу лінійної алгебри відомо, що коли до рядків матриці G застосувати елементарні перетворення, то векторний простір, що породжується рядками матриці, не зміниться. Таким чином, матриця, одержана в результаті елементарних перетворень, буде твірною матрицею лінійного коду $\mathcal{C}$. Зрозуміло, що за допомогою елементарних перетворень матрицю можна звести до вигляду

$$(I \quad A) = \begin{pmatrix} 1 & 0 & \ldots & 0 & a_{11} & \ldots & a_{1,n-k} \\ 0 & 1 & \ldots & 0 & a_{21} & \ldots & a_{2,n-k} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 & a_{k1} & \ldots & a_{k,n-k} \end{pmatrix},$$

де I позначає одиничну, а A деяку матрицю. Тому за потреби ми можемо вважати, що твірна матриця коду записана у вигляді $(I\ A)$. Цей вигляд називатимемо *стандартною* матрицею коду. Легко переконатися, що коли матриця G записана у стандартному вигляді, то відображення кодування задається правилом

$$x \mapsto x\,G = (x \quad xA).$$

У цьому випадку перші k символів кодового слова — це в точності повідомлення, яке передавалося. Ці перші k символів називаються *інформаційними символами*, а решта $n-k$ символів називаються *перевірочними символами*. Неважко зрозуміти, що коли код заданий стандартною матрицею, то процеси кодування та декодування стають надзвичайно простими.

Приклад 3.2. Розглянемо код над полем $\mathbb{F}_2$, який заданий твірною матрицею

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Як бачимо, матриця G — це записана у стандартній формі матриця бінарного коду розмірності 4 довжиною 7. Якщо виписати всі 16 кодових слів, то побачимо, що мінімальна вага коду дорівнює 3, тобто цей код може виправляти одну помилку. При кодуванні слова $x_1x_2x_3x_4$ одержимо кодове слово $x_1x_2\ldots x_7$, де

$$\begin{aligned} x_5 &= x_2 + x_3 + x_4, \\ x_6 &= x_1 + x_3 + x_4, \\ x_7 &= x_1 + x_2 + x_4. \end{aligned}$$

Зауважимо, що цей код досягає границі Хеммінга. Дійсно

$$|\mathcal{C}| = 16 = \frac{2^7}{(1 + 7(2-1))}.$$

Це означає, що кулі радіуса 1 покривають весь простір $\mathbb{F}_2^7$, отже, кожне слово знаходиться на відстані 0 або 1 рівно від одного кодового слова. Тому декодування ми можемо здійснити наступним чином: взяти одержане слово, передивитися всі 16 кодових слів, обрати серед них те, яке збігається з даним словом або відрізняється щонайбільше на один символ та взяти перші чотири символи цього кодового слова.

Зрозуміло, що описаний метод декодування важко назвати ефективним. Розглянемо далі більш ефективний спосіб, так зване *декодування за допомогою синдрому*.

Для цього дамо дещо інакше означення лінійного коду. Пригадаємо з курсу лінійної алгебри, що з кожним лінійним відображенням можна пов'язати образ та ядро. Попереднє означення прив'язувалося до образу лінійного відображення.

З боку теорії кодування є серйозні причини звернутися до ядра відображення кодування. Повідомлення приходить у вигляді

$$\text{кодове слово} + \text{помилка}.$$

Наша мета — прибрати помилку та відновити кодове слово. Нам невідомо, який символ був змінений у процесі передачі повідомлення, але ми знаємо, з якого простору обирається кодове слово. Тому розглянемо такий спосіб декодування. Спершу приберемо кодове слово, щоб віднайти помилку, а потім одержимо кодове слово, віднявши помилку від одержаного слова. Тому природно, що ми хочемо мати таке лінійне відображення f, яке відображає кожне кодове слово в нульове слово, але є ін'єктивним на множині всіх можливих помилок, тобто

$$f(\text{кодове слово}+\text{помилка}) = f(\text{кодове слово})+f(\text{помилка}) = f(\text{помилка}).$$

Пов'яжемо з кодом ще одну матрицю.

Означення 3.6. Нехай $\mathcal{C}$ — лінійний код довжиною n та розмірністю k над алфавітом X. *Перевірочною матрицею* коду називається матриця H розміру $(n-k)\times n$ з властивістю, що для слова $w \in X^n$ виконується

$$wH^T = 0 \Longleftrightarrow w \in \mathcal{C}.$$

Слово wH^T називається *синдромом* слова w.

Твердження 3.3. *Нехай H — перевірочна матриця лінійного коду, який виправляє e помилок. Нехай w_1, w_2 — довільні слова, вага яких не перевищує e. Тоді синдроми слів w_1 та w_2 однакові тоді і лише тоді, коли $w_1 = w_2$.*

Доведення. Якщо $w_1H = w_2H$, то $(w_1 - w_2)H = 0$, а тому $w_1 - w_2 \in \mathcal{C}$. Але вага слова $w_1 - w_2$ щонайбільше $2e$, в той час як мінімальна вага коду $\mathcal{C}$ щонайменше $2e+1$. Отже, $w_1 - w_2 = 0$. □

Приклад 3.3. Розглянемо матрицю

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Ця матриця є перевірочною матрицею для коду з прикладу 3.2. У цьому легко переконатися, обчисливши добуток GH^T. Зверніть увагу, що i–й стовпчик — це двійкове зображення i.

Оскільки цей код виправляє 1 помилку, то множина всіх помилок складається з нульового слова 0 та слів e_i, в яких на i–му місці стоїть 1, а решта 0, для $i = 1, \ldots, 7$. Синдромом нульового є 0, а синдромом помилки e_i є i–й стовпчик матриці H.

Процес декодування тепер виглядає наступним чином. Маючи слово w, потрібно обчислити його синдром wH. Якщо він дорівнює 0, то помилок не відбулося. Якщо синдром — це двійкове зображення i, то це означає, що помилка відбулася в i–й позиції.

Припустимо, що ми хочемо передати слово $w = \texttt{1001}$. Відповідне йому кодове слово — це $c = \texttt{1001100}$. Припустимо, що у другій позиції відбулася помилка та у процесі передачі було одержане слово $c' = \texttt{1101100}$. Його синдром дорівнює $c'H = \texttt{(001)}^T$, а це другий стовпчик матриці H. Тому ми виправляємо кодове слово c' на $\texttt{1001100}$ і одержуємо вихідне повідомлення $\texttt{1001}$.

Якщо ж трапилося дві помилки, то правильне декодування стає неможливим. Припустимо, що при передачі відбулося дві помилки, наприклад, у позиціях 2 та 3, і було одержане кодове слово $c'' = \texttt{1111100}$. Синдром цього слова дорівнює $\texttt{(001)}^T$, тобто помилка відбулася у першій позиції. Після виправлення одержимо кодове слово $\texttt{0111100}$, візьмемо перші чотири символи 0111, що дасть, на жаль, неправильне повідомлення.

Декодування за допомогою синдрому можна використовувати для довільного лінійного коду, хоча в деяких випадках це не найбільш ефективний спосіб. Мінімальну вагу коду можна знайти за його перевірочною матрицею.

Твердження 3.4. *Нехай $\mathcal{C}$ — лінійний код з перевірочною матрицею H. Тоді мінімальна вага коду $\mathcal{C}$ не менша за δ тоді і лише тоді, коли довільні $\delta - 1$ стовпців матриці H лінійно незалежні.*

Доведення. Нехай $h_1, \ldots, h_n$ — стовпці перевірочної матриці H. Тоді $c_1 \ldots c_n$ є кодовим словом тоді і лише тоді, коли

$$c_1 h_1 + \cdots + c_n h_n = 0.$$

З цього випливає, що кодові слова ваги f відповідають відношенню лінійної залежності на множині з f стовпців. Мінімальна вага дорівнює мінімальній кількості лінійно залежних стовпців. □

Використання поняття перевірочної матриці дає змогу легко ввести важливий клас кодів, а саме кодів Хеммінга. Нехай k — деяке фіксоване натуральне число, $F = \mathbb{F}_q$ — скінченна поле, F^k — k–вимірний векторний простір всіх стовпців вимірністю k. Позначимо $X = F^k \setminus \{0\}$. Тоді $|X| = q^k - 1$.

На множині X введемо відношення еквівалентності за правилом: два елементи множини X еквівалентні тоді і лише тоді, коли один з них пропорційний іншому. Зрозуміло, що кожний клас еквівалентності складається з $q - 1$ елементів, а кількість класів еквівалентності дорівнює

$$n = \frac{q^k - 1}{q - 1}.$$

Нехай Y — множина представників класів еквівалентності, тобто вона складається з ненульових векторів, взятих по одному з кожного класу суміжності. Нехай H — матриця розміру $k \times n$, стовпцями якої є елементи множини Y. Лінійний код (n, k)-код, перевірочною матрицею якого є матриця H, називається *q-арним кодом Хеммінга.* Код з прикладу 3.2 є бінарним $(7, 4)$ – кодом Хеммінга, це випливає з прикладу 3.3.

Твердження 3.5. *Коди Хеммінга є досконалими кодами, які виправляють одну помилку, тобто вони досягають границі Хеммінга.*

Доведення. За побудовою всі стовпці перевірочної матриці коду Хеммінга є ненульовими і жодні два непропорційні. Таким чином, довільні два стовпці цієї матриці лінійно незалежні. Отже, за твердженням 3.4 мінімальна вага цього коду щонайменше 3, а тому він є кодом, що виправляє одну помилку.

Оскільки

$$|C| = q^{n-k} = \frac{q^n}{1 + n(q-1)},$$

то цей код досягає границі Хеммінга. □

Природним чином виникає питання, як за твірною матрицею коду знайти його перевірочну матрицю.

Твердження 3.6. *Нехай G та H — це матриці розмірів $k \times n$ та $(n - k) \times n$ відповідно над скінченним полем F, рядки яких є лінійно незалежними. Тоді G та H є відповідно твірною та перевірочною матрицею одного й того самого коду тоді і лише тоді, коли $GH^\top = 0$.*

Якщо твірна матриця записана у стандартній формі $G = (I \quad A)$, *то перевірочна матриця має вигляд* $H = (-A \quad I)$.

Доведення. Розмірність коду $\mathcal{C}$ як векторного простору дорівнює k. Розмірність ортогонального доповнення $\mathcal{C}'$ до простору, породженого рядками матриці H, теж дорівнює k. Отже, умова $GH^\top = 0$ еквівалентна припущенню, що кожний рядок G належить $\mathcal{C}'$, тобто $\mathcal{C} \subset \mathcal{C}'$. Таким чином, $\mathcal{C} = \mathcal{C}'$.

Другу частину твердження залишаємо читачеві в якості вправи. □

Зауважимо наостанок, що твірна та перевірочна матриці коду $\mathcal{C}$ є відповідно перевірочною та твірною матрицями деякого коду $\mathcal{C}^\perp$. Такий код $\mathcal{C}^\perp$ називається *дуальним*, або *ортогональним*,кодом до коду $\mathcal{C}$. З погляду лінійної алгебри дуальний код $\mathcal{C}^\perp$ є ортогональним доповнення до коду $\mathcal{C}$.

3.3 Циклічні коди

Означення 3.7. Нехай $\mathcal{C}$ — лінійний код довжиною n над полем F. Код $\mathcal{C}$ називається *циклічним*, якщо для довільного слова

$$w = a_0 a_1 \dots a_{n-1} \in \mathcal{C}$$

його циклічний зсув $a_{n-1}a_0 \dots a_{n-2}$ теж належить коду $\mathcal{C}$.

З кожним словом $w = a_0 a_1 \dots a_{n-1} \in \mathcal{C}$ можна пов'язати многочлен $w(x) = a_0 + a_1 x + \dots + a_{n-1}x^{n-1} \in F[x]$.

Нехай I — це ідеал в кільці $F[x]$, породжений многочленом $x^n - 1$, та нехай R — це факторкільце $F[x]/R$. Кожний клас суміжності з R можна однозначно подати у вигляді $f(x) + I$, де $f(x)$ — це многочлен з $F[x]$ степеня не більшого за $n-1$. Отже, існує природна бієкція між множиною $R = F[x]/I$ та множиною F^n всіх слів довжиною n.

Твердження 3.7. *Код* $\mathcal{C}$ *довжиною* n *є циклічним кодом тоді і лише тоді, коли відповідні елементи кільця* R *утворюють ідеали.*

Доведення. Покажемо спершу, що множення на x у факторкільці R відповідає циклічному зсуву для коду $\mathcal{C}$. Розглянемо слово $w = a_0 a_1 \dots a_{n-1}$. Йому відповідає многочлен $a_0 + a_1 x + \dots a_{n-1}x^{n-1}$. Помноживши на x, матимемо $a_0 x + a_1 x^2 + \dots a_{n-1}x^n$. Оскільки x^n та 1 належать одному класу суміжності за ідеалом I, то маємо рівність класів суміжності

$$a_0 x + a_1 x^2 + \dots a_{n-1}x^n + I = a_{n-1} + a_0 x + \dots + a_{n-2}x^{n-1} + I,$$

а многочлен $a_{n-1} + a_0 x + \dots a_{n-2} x^{n-1}$ відповідає слову $a_{n-1} a_0 \dots a_{n-2}$, яке є циклічним зсувом слова w.

Таким чином, якщо множина $\mathcal{C}$ є ідеалом, то вона замкнена відносно додавання та множення на скаляр (тобто є лінійним кодом), а також відносно множення на x (тобто замкнена відносно циклічного зсуву, а тому є циклічним кодом).

Навпаки, припустимо, що код $\mathcal{C}$ — циклічний. Тоді він замкнений відносно додавання та множення на довільний скаляр або x. Поєднуючи ці дві дії, ми можемо побудувати довільний многочлен, тобто множина $\mathcal{C}$ замкнена відносно множення на довільний многочлен, а тому є ідеалом. □

Нагадаємо, що коли R — комутативне кільце з одиницею, в якому кожний ідеал є головним, то ця властивість зберігається для довільного факторкільця кільця R.

Твердження 3.8. *Кожний ідеал факторкільця $R = F[x]/(x^n - 1)$ породжується класом $g(x) + (x^n - 1)$, де $g(x)$ — унітарний дільник многочлена $x^n - 1$. Для кожного ідеалу існує єдиний такий многочлен.*

Доведення. Нехай ідеал I кільця $F[x]/(x^n - 1)$ породжується класом $f(x) + \big(x^n - 1\big)$. Нехай $g(x)$ — це унітарний найбільший спільний дільник многочленів $f(x)$ та $x^n - 1$. Тоді g ділить f, а тому (g) містить f. З іншого боку, з розширеного алгоритму Евкліда маємо рівність

$$g(x) = a(x) f(x) + b(x)(x^n - 1).$$

Перейшовши до факторкільця R матимемо рівність класів суміжності

$$g(x) + \big(x^n - 1\big) = a(x) f(x) + \big(x^n - 1\big).$$

Отже, f ділить g, а тому (f) містить (g). Таким чином, $I = (g)$, де многочлен g — унітарний дільник многочлена $x^n - 1$. Єдиність такого многочлена випливає з другої теореми про гомоморфізм для кілець. □

Многочлен $g(x)$ називається *твірним многочленом* циклічного коду, який відповідає ідеалу $(g(x))$.

З цього твердження випливає, що для побудови всіх циклічних кодів довжиною n, ми повинні розкласти многочлен $x^n - 1$ у добуток незвідних над полем F многочленів, перерахувати всі дільники $x^n - 1$ та для кожного дільника побудувати відповідний йому ідеал факторкільця R.

Наступна теорема дає спосіб за твірним многочленом циклічного коду виписати твірну та перевірочну матриці коду.

Теорема 3.3. *Нехай $g(x)$ — твірний многочлен циклічного коду $\mathcal{C}$ та*

$$g(x) = a_{n-k}x^{n-k} + a_{n-k-1}x^{n-k-1} + \cdots + a_0, \quad a_{n-k} = 1.$$

Нехай $x^n - 1 = g(x)h(x)$, де

$$h(x) = b_k x^k + b_{k-1}x^{k-1} + \cdots + b_0, \quad b_k = 1.$$

Тоді твірна матриця G та перевірочна матриця H мають вигляд

$$G = \begin{pmatrix} a_0 & a_1 & \dots & a_{n-k} & 0 & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_{n-k} & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & a_0 & a_1 & \dots & a_{n-k} \end{pmatrix},$$

$$H = \begin{pmatrix} b_k & b_{k-1} & \dots & a_0 & 0 & \dots & 0 \\ 0 & b_k & b_{k-1} & \dots & b_0 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & b_k & b_{k-1} & \dots & b_0 \end{pmatrix}.$$

Доведення. Рядки матриці G відповідають многочленам $g(x)$, $xg(x)$, …, $x^{k-1}g(x)$, отже, всі вони належать $\mathcal{C}$. Візьмемо деяке слово $w \in \mathcal{C}$, що відповідає многочлену $f(x)g(x) \pmod{x^n-1}$. Розділимо многочлен $f(x)$ на $h(x)$ з остачею:

$$f(x) = h(x)q(x) + r(x), \qquad \text{де } r = 0 \text{ або } \deg r(x) < \deg k.$$

Тоді

$$f(x)g(x) = (x^n - 1)q(x) + r(x)g(x).$$

Звідси випливає, що

$$f(x)g(x) \equiv r(x)g(x) \pmod{x^n - 1},$$

а добуток $r(x)g(x)$ є лінійною комбінацією многочленів $x^i g(x)$, де $i < k$. Отже, слово w є лінійною комбінацією рядків матриці G. Звідси випливає, що код $\mathcal{C}$ є векторним простором, натягнутим на систему векторів–рядків матриці G.

На місці (i, j) матриці G стоїть елемент a_{j-i}, причому $a_l = 0$, якщо l не належить відрізку $[0, n-k]$. З подібним обмеженням на місці (i, j) стоїть елемент b_{k-j+i}. З правила множення матриць випливає, що на місці (i, j) матриці $GH^\top$ стоїть елемент

$$\sum_l a_{l-i}b_{k-l+j} = \sum_m a_m b_{k-i+j-m}.$$

Цей елемент є $(k-i+j)$-м коефіцієнтом добутку gh. Для $1 \leqslant i \leqslant k$ та $1 \leqslant j \leqslant n-k$ виконується

$$k-k+1 = 1 \leqslant k-i+j \leqslant k-1+(n-k) = n-1.$$

Але $g(x)h(x) = x^n - 1$ і всі відповідні коефіцієнти дорівнюють 0. Отже, $GH^\top = 0$ і за твердженням 3.6 матриця H є перевірочною матрицею коду $\mathcal{C}$. □

З цієї теореми, зокрема, випливає, що $\dim \mathcal{C} = k = n - \deg g(x)$.

Приклад 3.4. Опишемо всі бінарні циклічні коди довжиною 7. Маємо розклад

$$x^7 - 1 = (x-1)(x^3+x+1)(x^3+x^2+1).$$

Отже, існує 8 різних циклічних кодів, що відповідають дільникам x^7-1. Опишемо декілька кодів, решту залишимо читачеві як вправу.

- $g(x) = 1$. Цей код породжується словом `1000000` та його циклічними зсувами, а, отже, збігається з усім простором $\mathbb{F}_2^7$.
- $g(x) = x - 1$. Цей код породжується словом `1100000` та його циклічними зсувами та складається з усіх слів з парними вагами. Розмірність цього коду дорівнює 6, а мінімальна вага дорівнює 2.
- $g(x) = x^6+x^5+x^4+x^3+x^2+x+1$. Цей код є кодом з повтореннями, який породжений словом `1111111`.
- $g(x) = x^7 + 1$. Це взагалі не є кодом, бо ця множина містить лише нульовий вектор, а код за означенням повинен містити принаймні два кодових слова.

3.4 Коди БЧХ

У попередніх розділах ми побачили, як можна будувати коди заданих довжини та розмірності. Ця задача є доволі простою, проте задача відшукання мінімальної відстані вже є набагато складнішою. Звісно, зручно було б мати конструкцію, яка б дозволяла за наперед заданими довжиною n та мінімальною відстанню d знайти код довжиною n та мінімальною відстанню щонайменше d.

Конструкція кодів з такими властивостями була запропонована незалежно Хоквінгемом у 1959 р. та Боузом і Чоудхурі у 1960 р. Коди з такою властивістю називаються *кодами БЧХ*. Властивості цих кодів залежать від властивостей скінченних полів.

Коди, які ми будемо будувати, — це циклічні коди довжиною n над полем $\mathbb{F}_q$, де n та q — взаємно прості. Також у нас є наперед задане число $\delta \in \mathbb{N}$. Нижче ми визначимо код БЧХ довжиною n та заданою мінімальною відстанню δ.

Нехай e — це мультиплікативний порядок q за модулем n. Нехай a — первісний корінь степеня n з одиниці в $\mathbb{F}_{q^e}$. Нехай $\mathbb{F}_{q^e} = \mathbb{F}_q(\alpha)$. Тоді кожний елемент поля $\mathbb{F}_{q^e}$ можна однозначно подати у вигляді

$$c_0 + c_1\alpha + \cdots + c_{e-1}\alpha^{e-1}.$$

Кожному такому многочлену можна зіставити набір

$$(c_0 c_1 \dots c_{e-1}).$$

З технічних міркувань будемо використовувати стовпцеве зображення $(c_0 c_1 \dots c_{e-1})^\top$. Вибір елемента α несуттєвий, тому можемо взяти $\alpha = a$.

Означення 3.8. *Кодом БЧХ довжиною n та конструктивною відстанню δ* називається код, перевірочна матриця якого має вигляд:

$$H = \begin{pmatrix} 1 & a & a^2 & \dots & a^{n-1} \\ 1 & a^2 & a^4 & \dots & a^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a^{\delta-1} & a^{2(\delta-1)} & \dots & a^{(\delta-1)(n-1)} \end{pmatrix}.$$

Кожний елемент матриці H належить полю $\mathbb{F}_{q^e}$, а тому вона є матрицею розміру $e \times 1$ над полем $\mathbb{F}_q$. Таким чином, матриця H є матрицею розміру $e(\delta-1) \times n$ над полем $\mathbb{F}_q$.

Теорема 3.4. *Мінімальна відстань коду БЧХ довжиною n та конструктивною відстанню δ дорівнює щонайменше δ, а його розмірність не менша за $n - e(\delta-1)$.*

Доведення. Щоб показати, що мінімальна відстань коду не менша за δ, необхідно і достатньо довести, що довільні $\delta - 1$ стовпців перевірочної матриці лінійно незалежні.

Розглянемо визначник матриці, складеної зі стовпців з номерами $m_1, m_2, \dots, m_{\delta-1}$ матриці H як матриці над полем $\mathbb{F}_{q^e}$:

$$\begin{pmatrix} a^{m_1} & \dots & a^{m_{\delta-1}} \\ \vdots & \ddots & \vdots \\ a^{m_1(\delta-1)} & \dots & a^{m_{\delta-1}(\delta-1)} \end{pmatrix}.$$

Винісши з i–го стовпця, $i = 1, \ldots, \delta - 1$, множник $a^{m_i} \neq 0$, одержимо визначник Вандермонда $V(a^{m_1}, \ldots, a^{m_{\delta-1}})$, який не дорівнює 0, бо всі $a^{m_1}, \ldots, a^{m_{\delta-1}}$ різні. Отже, обрані стовпці лінійно незалежні над полем $\mathbb{F}_{q^e}$, а тому лінійно незалежні і над меншим полем.

Розмірність коду дорівнює $n - \operatorname{rank} H$. А ранг перевірочної матриці H не більший за кількість стовпців, яка дорівнює $e(\delta - 1)$. □

Теорема 3.5. *Коди БЧХ є циклічними.*

Доведення. Будь–якому слову $w = c_0 c_1 \ldots c_{n-1}$ відповідає многочлен $f(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$. Умова належності слова w коду БЧХ може бути записана наступним чином

$$f(a^i) = c_0 + c_1 a^i + \cdots + c_{n-1} a^{i(n-1)} = 0,$$

для $i = 1, 2, \ldots, \delta - 1$.

Нехай $g(x)$ — це найменше спільне кратне мінімальних многочленів елементів $a, a^2, \ldots, a^{\delta-1}$ над полем $\mathbb{F}_q$. Тоді слово, що відповідає $f(x)$ належить коду БЧХ тоді і лише тоді, коли $f(x)$ ділиться на $g(x)$. Більше того, корені $g(x)$ є коренями n–го степеня з одиниці, отже, $g(x)$ ділить $x^n - 1$. Таким чином, коди БЧХ є циклічними кодами з твірним многочленом $g(x)$. □

Важливим частковим випадком кодів БЧХ є випадок, коли $n = q - 1$. Коди з такою властивістю називаються *кодами Ріда–Соломона*. У цьому випадку $\operatorname{ord}_n q = 1$, тому відповідно до теореми 3.4 для коду $\mathcal{C}$ Ріда–Соломона одержимо $\dim \mathcal{C} \geqslant n - \delta + 1$. З іншого боку, якщо справжня мінімальна відстань дорівнює d, то $\delta \leqslant d$ і границя Сінглтона дасть $|\mathcal{C}| \leqslant q^{n-d+1}$, звідки $\dim(\mathcal{C}) \leqslant n - d + 1$. Підсумувавши, одержимо

$$n - d + 1 \leqslant n - \delta + 1 \leqslant \dim(\mathcal{C}) \leqslant n - d + 1,$$

що дає $\dim(\mathcal{C}) = n - d + 1$. Отже, маємо таку властивість кодів Ріда–Соломона:

Твердження 3.9. *Мінімальна відстань коду Ріда–Соломона з конструктивною відстанню δ дорівнює δ, а розмірність дорівнює $n - \delta + 1$. Отже, коди Ріда–Соломона є роздільними кодами з максимальною відстанню.*

Задачі

Задача 3.1. Нехай кодовими словами коду $\mathcal{C}$ над алфавітом $\{0,1,2\}$ є `001122`, `112200`, `220011`, `012012`, `120120`, `201201`. Знайдіть мінімальну відстань цього коду.

Задача 3.2. *Ваговим многочленом* коду $\mathcal{C} \subset \mathbb{F}_q^n$ називається многочлен

$$W_{\mathcal{C}}(t) = \sum_{x \in \mathcal{C}} t^{w(t)} \in \mathbb{Z}[t],$$

де $w(x)$ — вага вектора x. Знайдіть ваговий многочлен коду Хеммінга.

Задача 3.3. Знайдіть ваговий многочлен коду $\mathcal{C} = \mathbb{F}_q^n$.

Задача 3.4. Знайдіть всі кодові слова, мінімальну відстань та перевірочну матрицю бінарного лінійного коду, заданого твірною матрицею

(a) $\begin{pmatrix} 0&1&0&0&1 \\ 0&0&1&0&1 \\ 1&0&0&1&1 \end{pmatrix}$; (b) $\begin{pmatrix} 1&1&0&0&1 \\ 0&0&0&0&1 \\ 0&0&1&1&1 \end{pmatrix}$; (c) $\begin{pmatrix} 1&1&0&0&1 \\ 0&1&1&0&1 \\ 0&1&0&1&0 \end{pmatrix}$; (d) $\begin{pmatrix} 1&0&0&1&0 \\ 0&1&1&1&0 \\ 0&1&0&1&1 \end{pmatrix}$.

Скільки помилок можуть виправляти ці коди?

Задача 3.5. Для кодів з задачі 3.4 знайдіть кодове слово, в яке кодується слово `101` та знайдіть синдром помилки слова `10101`. Якщо можливо, то виправте помилку та декодуйте одержане слово.

Задача 3.6. Нехай $\mathcal{C}$ — тернарний лінійний код, тобто визначений над полем $\mathbb{F}_3$, який заданий твірною матрицею

$$G = \begin{pmatrix} 1&1&0&1 \\ 0&2&2&1 \end{pmatrix}.$$

(a) Скільки кодових слів містить код $\mathcal{C}$?

(b) Яка мінімальна вага цього коду?

(c) Яка мінімальна відстань цього коду?

(d) Знайдіть перевірочну матрицю цього коду.

(e) Використовуючи код $\mathcal{C}$, закодуйте слово $a =$ `12` та розкодуйте слово $b =$ `1022`.

Задача 3.7. Нехай $\mathcal{C}$ — бінарний лінійний код, заданий твірною матрицею

$$G = \begin{pmatrix} 1&1&1&1&1&1&1&1 \\ 0&0&1&1&0&0&1&1 \\ 0&1&0&1&0&1&0&1 \\ 0&0&0&0&1&1&1&1 \end{pmatrix}.$$

(a) Чому дорівнює мінімальна вага цього коду?

(b) Покажіть, що цей код виправляє одну помилку.

(c) Знайдіть перевірочну матрицю цього коду.

(d) Припустимо, що пре передачі повідомлення відбулася одна помилка. Чому дорівнює відповідний синдром?

(e) Декодуйте слово $b = \texttt{10101101}$.

Задача 3.8. Нехай $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ — поле з чотирьох елементів, де елемент α задовольняє рівність $\alpha^2 = \alpha+1$. Нехай $\mathcal{C}$ — лінійний код над полем $\mathbb{F}_4$, який заданий твірною матрицею

$$G = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & \alpha & \alpha^2 \\ 0 & 0 & 1 & 1 & \alpha^2 & \alpha \end{pmatrix}.$$

Знайдіть перевірочну матрицю цього коду та його мінімальну вагу. Доведіть, що кількість кодових слів довільного іншого лінійного коду над алфавітом з чотирьох символів, який має таку саму довжину та мінімальну відстань як код $\mathcal{C}$, не перевищує кількість кодових слів коду $\mathcal{C}$.

Задача 3.9. Нехай $\mathcal{C} \subset \mathbb{F}_q^n$ — лінійний код. *Дуальним*, або *ортогональним*, кодом до коду $\mathcal{C}$ називається лінійний код

$$\mathcal{C}^\perp = \{x \in \mathbb{F}_q^n | \, (x, y) = 0 \text{ для всіх } y \in \mathcal{C}\}.$$

Переконайтеся, що це дійсно лінійний код. Доведіть, що коли G і H — це твірна та перевірочна матриці коду $\mathcal{C}$ відповідно, то H та G — це твірна та перевірочна матриці коду $\mathcal{C}^\perp$.

Задача 3.10. Знайдіть коди, дуальні до кодів з задачі 3.4.

Задача 3.11. Нехай $\mathcal{C}$ — лінійний (n, k)–код. Доведіть, що

$$\dim \mathcal{C}^\perp = n - k.$$

Задача 3.12. Доведіть, що для довільного лінійного коду має місце рівність $(\mathcal{C}^\perp)^\perp = \mathcal{C}$.

Задача 3.13. Доведіть, що для довільних лінійних кодів $\mathcal{C}_1$ та $\mathcal{C}_2$ над полем $\mathbb{F}_q$, які мають однакову довжину, має місце рівність $(\mathcal{C}_1 + \mathcal{C}_2)^\perp = \mathcal{C}_1 \cap \mathcal{C}_2$.

Задача 3.14. Знайдіть перевірочну матрицю бінарного $(7,4)$–коду Хеммінга.

Задача 3.15. Знайдіть твірну матрицю $(7,3)$–коду, дуального до бінарного коду Хеммінга.

Задача 3.16. Знайдіть перевірочну матрицю тернарного, тобто над полем $\mathbb{F}_3$, коду Хеммінга довжиною 3.

Задача 3.17. Нехай поле $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$, де $\alpha^2 = \alpha + 1$. Доведіть, що код, визначений над полем $\mathbb{F}_4$ за допомогою твірної матриці

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & \alpha & \alpha^2 \end{pmatrix}^T.$$

є роздільним кодом з максимальною відстанню 3.

Задача 3.18. Нехай $\mathcal{C}$ — це (n,k)–код над полем $\mathbb{F}_q$ з твірною матрицею G. Покажіть, що коли матриця G не має нульових стовпців, то сума ваг кодових слів з $\mathcal{C}$ дорівнює $n(q-1)q^{k-1}$.

Задача 3.19. Нехай $\mathcal{C}$ — бінарний (n,k)–код. Доведіть, що множина кодових слів парної довжини є лінійним підкодом, тобто підпростором векторного простору $\mathcal{C}$.

Задача 3.20. Нехай α — примітивний елемент поля $\mathbb{F}_9$ з мінімальним многочленом x^2+2x+2 над полем $\mathbb{F}_3$. Знайдіть твірних многочлен коду БЧХ над полем $\mathbb{F}_3$ довжиною 8 розмірністю 4. Знайдіть мінімальну відстань цього коду.

Задача 3.21. Знайдіть твірний многочлен коду БЧХ над полем $\mathbb{F}_3$ розмірністю 12 з конструктивною відстанню 5.

Задача 3.22. Нехай $\mathbb{F}_{16} = \mathbb{F}_2(\alpha)$, де $\alpha^4 = \alpha^3 + 1$. Знайдіть твірний многочлен бінарного коду БЧХ довжиною 15, який виправляє 3 помилки.

Задача 3.23. Опишіть всі бінарні циклічні коди довжиною 7.

Задача 3.24. Доведіть, що код з повторенням для $q = 2$ досягає границі Хеммінга.

Задача 3.25. Нехай $\mathcal{C}$ — лінійний код з перевірочною матрицею H. Доведіть, що код $\mathcal{C}$ є кодом, який виправляє 1 помилку, тоді і лише тоді, коли H не має нульових стовпці та жодні два стовпці не пропорційні.

Задача 3.26. Чому дорівнює розмірність бінарного коду БЧХ довжиною 31 та з конструктивною відстанню 5?

Задача 3.27. Знайдіть твірний многочлен коду БЧХ над полем $\mathbb{F}_2$ розмірності 12 з конструктивною відстанню 5.

Задача 3.28. Нехай многочлен $g(x) = x^3 + x^2 + 1$ породжує бінарний циклічний $(7, 4)$–код.

(a) Знайдіть перевірочний многочлен цього коду.

(b) Знайдіть твірну та перевірочну матриці цього коду.

Задача 3.29. Нехай многочлен $g(x) = x^3 + x + 1$ породжує бінарний циклічний $(7, 4)$–код.

(a) Знайдіть перевірочний многочлен цього коду.

(b) Знайдіть твірну та перевірочну матриці цього коду.

Задача 3.30. Нехай $\mathcal{C}$ — бінарний код БЧХ довжиною 15 з конструктивною відстанню 5.

(a) Покажіть, що многочлен $g(x) = x^4 + x + 1$ є незвідним над полем $\mathbb{F}_2$, а його корені є примітивними елементами поля $\mathbb{F}_{16}$.

(b) Нехай $\alpha \in \mathbb{F}_{16}$ — корінь многочлена $g(x)$. Покажіть, що α^2 та α^4 теж є коренями $g(x)$, а α^3 є коренем многочлена $x^4 + x^3 + x^2 + x + 1$.

(c) Знайдіть твірний многочлен коду $\mathcal{C}$.

(d) Покажіть, що цей код може виправляти дві помилки.

(e) Знайдіть розмірність коду $\mathcal{C}$.

Задача 3.31. Доведіть, що q–арний код Хеммінга є циклічним, коли числа $q - 1$ та n взаємно прості.

Задача 3.32. Опишіть $(15, 13)$–код Ріда–Соломона над полем $\mathbb{F}_{16}$, вказавши його твірний многочлен і кількість помилок, які цей код може виправляти.

Задача 3.33. Доведіть, що код, дуальний до коду Ріда–Соломона, є кодом Ріда–Соломона.

Задача 3.34. Два лінійних коди $\mathcal{C}_1$ та $\mathcal{C}_2$ над полем $\mathbb{F}_q$ називається *еквівалентними*, якщо кодові слова коду $\mathcal{C}_1$ можна одержати з кодових слів коду $\mathcal{C}_2$ за допомогою деякої фіксованої підстановки координат в кодових словах коду $\mathcal{C}_2$. Нехай G — твірна матриця лінійного коду $\mathcal{C}$. Покажіть, що довільна перестановка рядків або стовпців цієї матриці приводить до твірної матриці деякого лінійного коду, еквівалентного коду $\mathcal{C}$.

Задача 3.35. Переконайтеся, що бінарні коди, як задані твірними матрицями

$$G_1 = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix} \text{ та } G_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

є еквівалентними.

Література

1. *Винберг Э.Б.* Курс алгебры. — М.: Факториал Пресс, 2001.
2. *Лидл Р., Нидеррайтер Г.* Конечные поля. — М.: Мир, 1988. 2.2
3. *Cameron P.* Introduction to Algebra. 2nd edition — Oxford University Press, 2008.
4. *Hoffstein J., Pipher J., Silverman J.* An Introdustion to Mathematical Cryptography. 2nd edition. — Springer, 2014.
5. *Menezes A., van Oorschot P, Vanstone S.A.* Handbook of Applied Cryptography. — CRC Press, 1996.