Математична криптологія

Модульна арифметика.
Обернений елемент в кільці лишків.

Конгруенції та їх властивості.

$x \equiv y \pmod{n}$, якщо цілі x та y при діленні на натуральне n дають однакову остачу: $x \bmod n = y \bmod n$. Такі числа називають ***конгруентними*** або рівними за модулем n. Відношення між x та y називають конгруенцією або порівнянням.

Твердження

Наступні три умови еквівалентні:

1) $x \equiv y \pmod{n}$;

2) $x = y + kn$ *для деякого цілого* k;

3) $n \mid (x-y)$

Властивості конгруенцій

1) Відношення еквівалетності:
   a) $x \equiv y \pmod{n}$ (*рефлексивність*);
   b) якщо $x \equiv y \pmod{n}$, то $y \equiv x \pmod{n}$ (*симетричність*);
   c) якщо $x \equiv y \pmod{n}$ і $y \equiv z \pmod{n}$, то $x \equiv z \pmod{n}$ (*транзитивність*);
2) Конгруенції можна почленно додавати: якщо $x_1 \equiv y_1 \pmod{n}$ і $x_2 \equiv y_2 \pmod{n}$ тоді $x_1 + x_2 \equiv y_1 + y_2 \pmod{n}$.
   Зокерма, до обох частин можна додавати одне й те ж число.
3) Конгруенції можна почленно перемножувати: якщо $x_1 \equiv y_1 \pmod{n}$ і $x_2 \equiv y_2 \pmod{n}$ тоді $x_1 x_2 \equiv y_1 y_2 \pmod{n}$.
   Зокерма, обидві частини можна домножувати на одне й те ж число.
4) Обидві частини конгруенції можна скорочувати на їх спільний дільник, якщо він взаємно простий з модулем: якщо $d \mid x$, $d \mid y$ та НСД $(d, n) = 1$, то $x \equiv y \pmod{n}$ випливає $x/d \equiv y/d \pmod{n}$.
5) Обидві частини конгруенції і модуль можна скорочувати на їхній спільний дільник: якщо $d \mid x$, $d \mid y$ та $d \mid n$, то з $x \equiv y \pmod{n}$ випливає $x/d \equiv y/d \pmod{n/d}$.

Конгруенції та їх властивості

6) Якщо m | n, то з $x \equiv y \pmod{n}$ випливає $x \equiv y \pmod{m}$;
7) Для p і q простих, $x \equiv y \pmod{pq}$ тоді і лише тоді, коли одночасно $x \equiv y \pmod{p}$ і $x \equiv y \pmod{q}$.

Приклад. За допомогою конгруенцій показати що число 73524 ділиться на 11.

$10 \equiv -1 \pmod{11}$ | 2
$100 \equiv 1 \pmod{11}$ | 5
$1000 \equiv -1 \pmod{11}$ | 3
$10000 \equiv 1 \pmod{11}$ | 7

$73520 \equiv 7 \pmod{11}$ |+4
$73524 \equiv 11 \pmod{11}$
$73524 \equiv 0 \pmod{11}$

Вправа. За допомогою конгруенцій довести що число ділиться на 9 тоді і тільки тоді, коли на 9 ділиться сума цифр його десяткового запису.

Кільця.

Кільцем називається множина R з двома заданими на ній операціями додавання та множення, яка має такі властивості:

1) Відносно додавання *R* утворює абелеву групу;
2) Операція множення асоціативна;
3) Множення дистрибутивне за додаванням, що означає виконання рівностей:

$(x+y)z=xz+yz$, $z(x+y)=zx+zy$ для всіх $x, y, z \in R$

Якщо окрім того операція множення комутативна, то кільце називається комутативним. R називається кільцем з одиницею, якщо в ньому є нейтральний елемент відносно множення. Прикладом комутативного кільця з одиницею є множина *Z* цілих чисел.

Елемент $x \in R$ кільця з одиницею називається *оборотнім справа [зліва]*, якщо $x \quad x' = 1$ $[x' \quad x = 1]$ для деякого $x' \in R$. Кажуть, що елемент x' є *правим [лівим] оберненим* до x. Елемент x називається *оборотнім* або *дільником одиниці*, якщо він оборотній і зліва, і справа. Кожен оборотній елемент має єдиний лівий і єдиний правий обернені елементи, які рівні між собою. Цей єдиний елемент називається оберненим до x і позначається через x^{-1}. Для оборотних елементів x і y неважко перевірити рівність $(x \cdot y)^{-1} = y^{-1} \quad x^{-1}$. Звідси випливає, що множина всіх оборотних елементів кільця з одиницею R утворює групу, яка називається *мультиплікативною групою кільця* R і позначається через R^* Наприклад, $\mathbb{Z}^* = \{1, -1\}$. Зрозуміло, що мультиплікативна група комутативного кільця сама є комутативною.

Кільце лишків

Для натурального n через Z_n позначаємо множину {0, 1,…, n-1}, наділену операціями додавання та множення за модулем *n*:

1) $(x+y) \bmod n$;
2) $(xy) \bmod n$

Відносно цих операцій Z_n є комутативним кільцем з одиницею, яке називається кільцем зведених лишків за модулем *n*. Через Z_n^* позначаємо мультиплікативну групу елементів, для яких в Z_n є обернені відносно множення.

Твердження 2.8. *$\mathbb{Z}_n^*$ складається з елементів x, взаємно простих з n, і лише з них.*

Доведення. Якщо НСД $(x, n) = 1$, то за твердженням 2.2 маємо $ux + vn = 1$ для деяких цілих u і v. Звідси $ux = 1 \pmod n$ і $x' = u \bmod n$ є оберненим за множенням до x в $\mathbb{Z}_n$.

Навпаки, якщо $xx' = 1$ в $\mathbb{Z}_n$, то добуток x та x' як цілих чисел дає остачу 1 при діленні на n: $xx' = qn + 1$. Отже, кожен спільний дільник чисел x та n ділить також 1, звідки НСД $(x, n) = 1$. ∎

Обернений елемент в кільці лишків

Елемент, обернений до $x \in \mathbb{Z}_n^*$ відносно множення, будемо позначати через $x^{-1} \bmod n$ або просто x^{-1} Ділення на x в $\mathbb{Z}_n$ означатиме множення на x^{-1}. Елемент, обернений до $x \in \mathbb{Z}_n$ відносно додавання, будемо позначати через $-x$. Зокрема, $-1 = n - 1$ в $\mathbb{Z}_n$. Як звичайно, в $\mathbb{Z}_n$ можна ввести операцію віднімання: $x - y = x + (-y)$.

Приклад 2.9. Нехай ми хочемо знайти елемент, обернений до 79 в $\mathbb{Z}_{211}^*$. У прикладі 2.3 була отримана рівність $1 = 3 \quad 211 + (-8) \quad 79$. З неї негайно випливає $(-8) \quad 79 \equiv 1 \pmod{211}$. Отже, $79^{-1} \bmod 211 = (-8) \bmod 211 = 203$.

Вправа. Знайти $8^{-1} \bmod 35$

Поле

Б.7. Поля. *Полем* **називається множина F з двома заданими на ній операціями, $+$ (додавання) та $\ $ (множення), яка має такі властивості:**

1) **відносно додавання F утворює абелеву групу з нейтральним елементом 0;**
2) **відносно множення $F^* = F \setminus \{0\}$ утворює абелеву групу з нейтральним елементом 1;**
3) **множення дистрибутивне за додаванням.**

Функція Ейлера

Наслідок 2.10. *Для простого модуля p, кільце $\mathbb{Z}_p$ є полем.* ■

Через $\phi(n)$ позначаємо порядок групи $\mathbb{Z}_n^*$. Іншими словами, значення $\phi(n)$ дорівнює кількості натуральних чисел, що не перевищують n і взаємно прості з n. ϕ називається *функцією Ойлера*.

Теорема Ойлера (1763). *Для взаємно простих цілого x і натурального n справедлива конгруенція $x^{\phi(n)} \equiv 1 \pmod{n}$.*

Доведення. Припустимо $1 \leq x < n$ і розглянемо x як елемент мультиплікативної групи $\mathbb{Z}_n^*$. За теоремою Лагранжа порядок елемента x є дільником порядку групи, $\phi(n)$ в нашому випадку. Тому $x^{\phi(n)} = 1$ в $\mathbb{Z}_n^*$, звідси й випливає теорема.

Випадок довільного x зводимо до попереднього, використавши конгруенцію $x^{\phi(n)} \equiv (x \bmod n)^{\phi(n)} \pmod{n}$. ■

Як легко бачити, $\phi(p) = p - 1$ для простого p. Звідси отримуємо такий наслідок теореми Ойлера.

Мала теорема Ферма (1640). *Якщо ціле x не ділиться на просте p, то $x^{p-1} \equiv 1 \pmod{p}$.* ■

Китайська теорема про остачі

Китайська теорема про остачі (I ст. до н.е.). *Для будь-якої пари взаємно простих натуральних чисел n_1 і n_2 та для будь-якої пари цілих чисел x_1 і x_2, можна знайти таке ціле x, де $x \equiv x_1 \pmod{n_1}$ і $x \equiv x_2 \pmod{n_2}$.*

Доведення. За твердженням 2.2 для деяких цілих u_1 і u_2 маємо рівність $u_1 n_1 + u_2 n_2 = 1$, з якої випливають співвідношення $u_1 n_1 \equiv 1 \pmod{n_2}$ і $u_2 n_2 \equiv 1 \pmod{n_1}$. Використовуючи останні, легко пересвідчитись, що $x = x_2 u_1 n_1 + x_1 u_2 n_2$ задовільняє потрібні умови. ∎

Приклад 2.11. Нехай ми хочемо знайти ціле x, яке при діленні на 211 давало б остачу 100, а при діленні на 79 остачу 10. У прикладі 2.3 була отримана рівність $1 = 3 \quad 211 + (-8) \quad 79$. Отже, в якості x можна взяти $10 \cdot 3 \cdot 211 + 100 \cdot (-8) \cdot 79 = -56870$. Зрозуміло, що це число можна замінити його остачею від ділення на $211 \quad 79 = 16669$. В результаті отримуємо 9806.

Ізоморфізм кілець

Відображення $f \quad R \to R'$ називається *гомоморфізмом*, якщо воно зберігає операції додавання та множення. Для кілець з одиницею повинна виконуватись ще одна умова: f має відображати одиницю кільця R в одиницю кільця R'. *Ядром* гомоморфізму $f \quad R \to R'$ є множина всіх тих елементів кільця R, які f відображає в нуль кільця R'. Прикладом гомоморфізму кілець є відображення із $\mathbb{Z}$ в $\mathbb{Z}_n$, яке кожному цілому числу ставить у відповідність його остачу від ділення на натуральне n. Ядро утворюють цілі числа, кратні n. Як і у випадку груп, гомоморфізм $f \quad R \to R'$ є ін'єктивним тоді і лише тоді, коли його ядро *тривіальне*, тобто складається тільки із нуля кільця R. Гомоморфізм, який є бієктивним відображенням, називається *ізоморфізмом*. Кільця R і R' *ізоморфні*, якщо існує ізоморфізм з R на R'.

Для кілець R_1 і R_2 через $R_1 \oplus R_2$ позначаємо їх *прямий добуток* — множину пар (x_1, x_2), де $x_1 \in R_1$ а $x_2 \in R_2$, із покомпонентним додаванням та множенням. Неважко впевнитись, що прямий добуток кілець є кільцем. Простим наслідком означень є

ТВЕРДЖЕННЯ Б.2. *Мультиплікативні групи* $(R_1 \oplus R_2)^*$ *і* $R_1^* \times R_2^*$ *ізоморфні.*

Ізоморфізм кілець

Твердження 2.12. *Нехай $n = n_1 n_2$, де n_1 і n_2 взаємно прості. Тоді відображення $f : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$, задане співвідношенням*

$$f(x) = (x \bmod n_1, x \bmod n_2), \tag{1}$$

є ізоморфізмом кілець.

Доведення. Перевірка того, що f є гомоморфізмом, зводиться до перевірки того, що відображення $f_i(x) = x \bmod n_i$ є гомоморфізмом із $\mathbb{Z}_n$ в $\mathbb{Z}_{n_i}$ для $i = 1, 2$. Останнє справді має місце, оскільки n_i ділить n.

Сюр'єктивність є безпосереднім наслідком Китайської теореми про остачі.

Ін'єктивність випливає із тривіальності ядра — найменшим натуральним числом, яке ділиться націло на кожне із взаємно простих чисел n_1 і n_2, є добуток $n_1 n_2 = n$. ∎

Слід зауважити, що як f, так і обернене відображення f^{-1} обчислюються ефективним чином (див. приклад 2.11).

Попереднє твердження разом із твердженням Б.2 дає

Наслідок 2.13. *Нехай $n = n_1 n_2$, де n_1 і n_2 взаємно прості. Тоді звуження відображення (1) на $\mathbb{Z}_n^*$ є ізоморфізмом із цієї групи на прямий добуток груп $\mathbb{Z}_{n_1}^* \times \mathbb{Z}_{n_2}^*$.* ∎

Наслідок 2.14. (Мультиплікативність функції Ойлера) *Для попарно взаємно простих $n_1, n_2, \ldots, n_l$ справедлива рівність $\phi(n_1 n_2 \ldots n_l) = \phi(n_1)\phi(n_2)\ldots\phi(n_l)$.*

Доведення. Випадок $l = 2$ безпосередньо випливає з наслідку 2.13. Загальне твердження доводиться індукцією за l. ∎

Формула для функції Ейлера

Формула для функції Ойлера. *Нехай* $n = p_1^{\alpha_1} \cdot p_l^{\alpha_l}$ *— розклад натурального числа* n *на прості співмножники. Тоді* $\phi(n) = n(1 - 1/p_1) \cdot \ldots \cdot (1 - 1/p_l)$.

Доведення. Спочатку розглянемо випадок $l = 1$, тобто $n = p^\alpha$ для деякого простого p. Числами, які не перевищують число p^α і не взаємно прості з ним, є $p, 2p, 3p, \ldots, p^\alpha = p^{\alpha-1}p$ — всього $p^{\alpha-1}$ штук. Звідси $\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha(1 - 1/p)$. Для $l > 1$ формула випливає з мультиплікативності функції Ойлера. ∎

Твердження 2.15. $\phi(n) > n/(6 \ln \ln n)$ *для* $n > 4$.

Кільце матриць

Матриця розміру $k \times k$ називається *квадратною* матрицею *порядку* k. Коефіцієнти a_{ii}, $i \leq k$, квадратної матриці (a_{ij}) називаються *діагональними*. Квадратні матриці заданого порядку k відносно операцій додавання та множення утворюють кільце, яке ми позначаємо $\mathrm{M}_k(R)$. Це кільце з одиницею, в ролі якої виступає *одинична* матриця I_k, діагональні коефіцієнти якої рівні одиниці кільця R, а всі інші — нулю.

Твердження Б.3. *Кільця* $\mathrm{M}_k(\mathrm{M}_l(R))$ *і* $\mathrm{M}_{kl}(R)$ *ізоморфні.*

Це означає, що матриці порядку kl можна розбити на блоки розміру l на l, після чого додавати і множити такі матриці поблоково.

$\mathrm{M}_k(R)^*$, мультиплікативна група оборотних матриць, має назву *повної лінійної групи* і позначається також як $\mathrm{GL}_k(R)$.

Далі кільце R вважається комутативним.

Визначник $\det A$ квадратної матриці $A = (a_{ij})$ порядку k дорівнює наступному виразу:

$$\det A = \sum_{\sigma} \varepsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{k\sigma(k)},$$

де сумування проводиться за всіма перестановками σ з S_n, а $\varepsilon(\sigma)$ означає знак перестановки.

Твердження Б.4. *Визначник добутку матриць дорівнює добутку їх визначників:* $\det AB = \det A \det B$. ∎

Формула оберненої матриці

якщо матриця A оборотна зліва або справа,

$$\text{то } \det A \in R^*. \tag{1}$$

Алгебраїчним доповненням елемента a_{ij} матриці A називається значення $A_{ij} = (-1)^{i+j} M_{ij}$, де M_{ij} — визначник матриці, яка отримується із матриці A після викреслення її i-го рядка та j-го стовпчика. Має місце

ФОРМУЛА ОБЕРНЕНОЇ МАТРИЦІ. *Для матриці $A' = (a'_{ij})$ з коефіцієнтами $a'_{ij} = A_{ji}$ виконуються співвідношення $AA' = A'A = (\det A) I_k$. Отже, в матриці A^{-1}, оберненій до A, коефіцієнт з індексами ij дорівнює $A_{ji}(\det A)^{-1}$* (порядок індексів помінявся!).

З формули випливає імплікація, що доповнює (1): якщо $\det A \in R^*$, то матриця A має обернену. Зафіксуємо отриманий зв'язок у наступному твердженні.

ТВЕРДЖЕННЯ Б.5.

1) *$A \in \mathrm{M}_k(R)^*$ тоді і лише тоді, коли $\det A \in R^*$*

2) *Якщо матриця $A \in \mathrm{M}_k(R)$ має праву або ліву обернену, то вона оборотня, тобто має матрицю, що є одночасно і правою, і лівою оберненою.*

За твердженням Б.4 відображення $\det \ \mathrm{M}_k(R)^* \to R^*$, яке співставляє матриці її визначник, є гомоморфізмом мультиплікативних груп. Ядром цього гомоморфізму є підгрупа матриць з визначником 1, яка має назву *спеціальної лінійної групи* і позначається $\mathrm{SL}_k(R)$.

Кільце матриць

Твердження 2.16. *Нехай $n = n_1 n_2$, де n_1 і n_2 взаємно прості. Тоді відображення $f_k \quad \mathrm{M}_k(\mathbb{Z}_n) \to \mathrm{M}_k(\mathbb{Z}_{n_1}) \oplus \mathrm{M}_k(\mathbb{Z}_{n_2})$, яке співставляє матриці A пару матриць A_1 та A_2, коефіцієнти яких є лишками відповідних коефіцієнтів матриці A за модулями n_1 та n_2, є ізоморфізмом кілець.*

Доведення. Очевидно, що f_k переводить одиницю кільця $\mathrm{M}_k(\mathbb{Z}_n)$ в одиницю кільця $\mathrm{M}_k(\mathbb{Z}_{n_1}) \oplus \mathrm{M}_k(\mathbb{Z}_{n_2})$. Нескладно перевірити також, що f_k зберігає операції додавання та множення; ключовим фактом при цьому є те, що n ділиться на n_1 і n_2. Отже, f_k є гомоморфізмом.

Щоб встановити сюр'єктивність, зауважимо, що f_k діє покомпонентно і на кожній із k^2 компонент це відображення є сюр'єктивним за Китайською теоремою про остачі.

Ін'єктивність випливає із тривіальності ядра. ∎

За твердженням Б.2 отримуємо

Наслідок 2.17. *Звуження відображення f_k на $\mathrm{M}_k(\mathbb{Z}_n)^*$ є ізоморфізмом із цієї групи на прямий добуток груп $\mathrm{M}_k(\mathbb{Z}_{n_1})^* \times \mathrm{M}_k(\mathbb{Z}_{n_2})^*$* ∎

Наслідок 2.18. *Функція ϕ_k мультиплікативна: для попарно взаємно простих $n_1, n_2, \ldots, n_l$ справедлива рівність $\phi_k(n_1 n_2 \ldots n_l) = \phi_k(n_1)\phi_k(n_2)\ldots\phi_k(n_l)$.*

Доведення. Випадок $l = 2$ безпосередньо випливає з наслідку 2.17. Загальне твердження доводиться індукцією за l. ∎

Кільце матриць

Теорема 2.19. *Нехай* $n = p_1^{\alpha_1} \qquad p_l^{\alpha_l}$ — *розклад натурального числа* n *на прості співмножники. Тоді* $\phi_k(n) = n^{k^2} \prod_{i=1}^{k}(1 - 1/p_1^i)$ $\prod_{i=1}^{k}(1 - 1/p_l^i)$.

Доведення.

Випадок 1: $n = p$ — просте.

Для $\phi_k(p)$, кількості оборотних матриць порядку k над $\mathbb{Z}_p$, нам належить показати, що

$$\phi_k(p) = p^{k^2} \prod_{i=1}^{k}(1 - 1/p^i) = \prod_{i=1}^{k}(p^k - p^{i-1}). \qquad (1)$$

Будемо опиратись на той факт, що $\mathbb{Z}_p$ є полем, а відтак оборотність матриці A із $\mathrm{M}_k(\mathbb{Z}_p)$ рівносильна її невиродженості. Через $X_1, X_2, \ldots, X_k$ позначимо стовпчики матриці A. Питання, скількома способами можна вибрати матрицю в $\mathrm{M}_k(\mathbb{Z}_p)^*$, еквівалентне такому — скількома способами можна вибрати послідовність k лінійно незалежних векторів $X_1, X_2, \ldots, X_k$ в $\mathbb{Z}_p^k$?

Вектор X_1 можна вибрати довільним за винятком нульового, тобто $p^k - 1$ способом. Далі, для $1 < i \leq k$ лінійна оболонка векторів $X_1, \ldots, X_{i-1}$ є $(i-1)$-вимірним векторним підпростором простору $\mathbb{Z}_p^k$, і X_i може бути довільним вектором поза цим підпростором. $(i-1)$-вимірний підпростір містить p^{i-1} елементів, тому для вибору X_i є $p^k - p^{i-1}$ можливість. Звідси випливає (1).