

Дискретна математика 2

(Discrete mathematics)

Лекция начинается

-Сегодня у нас клуб упоротых любителей математики.

Contents

1	Лекція 1	4
1.1	Подільність чисел	4
1.2	Найбільший спільний дільник	5
1.3	Алгоритм Евкліда	6
2	Лекція 2	8
2.1	Найменше спільне кратне	8
2.2	Евклідові послідовності	9
3	Лекція 3	11
3.1	Розширений алгоритм Евкліда	11
3.2	Лінійні діафантові рівняння	12
4	Лекція 4	14
4.1	Прості числа	14
4.2	Розподіл простих чисел	14
4.3	Основна теорема арифметики	16
5	Лекція 5	17
5.1	Мультиплікативні функції	17
5.2	Кількість та сума дільників	18
5.3	Досконалі числа	19
5.4	Функція Мебіуса	19
6	Лекція 6	21
6.1	Порівняння за модулем	21
6.2	Степені за модулем	22
6.3	Обернені елементи за модулем	23
7	Лекція 7	24
7.1	Китайська теорема про остачі	24
7.2	Функція Ойлера	25
7.3	Теорема Ойлера та мала теорема Ферма	26
8	Лекція 8	27
8.1	Функція Кармайкла	27

9	Лекція 9	29
9.1	Системи числення	29
9.2	Ознака подільності числа	29
9.3	Подільність біноміальних коефіцієнтів	31
10	Лекція 10	33
10.1	Лінійні порівняння за модулем	33
10.2	Елементи загальної теорії розв'язування порівнянь	33
10.3	Розклад Тейлора для поліномів	35
10.4	Поліноміальні порівняння за модулем степеня простого числа (1) . . .	36
11	Лекція 11	37
11.1	Поліноміальні порівняння за модулем степеня простого числа (2) . . .	37
11.2	Квадратичні лишки, критерій квадратичності Ойлера	38
11.3	Критерій квадратичності Гаусса	39
12	Лекція 12	40
12.1	Символ Лежандра та його властивості	40
12.2	Символ Якобі та його властивості	41
13	Лекція 1	44
13.1	Алгебраїчні системи з однією операцією	44
13.2	Приклади алгебраїчних систем з однією операцією	45
13.3	Властивості елементів моноїдів. Циклічні моноїди	46
14	Лекція 2	47
14.1	Властивості елементів груп. Циклічні групи	47
14.2	Порядок групи, порядок елементу групи. Підгрупи	48
14.3	Класи суміжності, індекс підгрупи, теорема Лагранжа та наслідки з неї	50
15	Лекція 3	52
15.1	Властивості циклічних груп та їх елементів	52
15.2	Структура циклічних груп	53
15.3	Нормальні підгрупи	54
15.4	Фактор-групи	54
Appendices		
Appendix A	A	57
A.1	Подільність многочленів	57
A.2	Наслідок з подільності(теорема Безу)	57
A.3	Наслідок з теореми Безу	57
A.4	Теорема Вієта	58
A.5	Схема Горнера	58
A.6	Ланцюгові дроби	58
A.7	Чим більше знаємо дробів - тим точніше α	59
A.8	Кожен скінченний дріб описує одне раціональне число	59

A.9 Наближення числа π	60
--------------------------------------	----

Основа теорії чисел

(Fundamentals of Number theory)

CHAPTER 1

Лекція 1

1.1 Подільність чисел

- властивості натуральних чисел

$$\mathbb{N} = \{1, 2, 3, \dots\}$$

$$\mathbb{N}_0 = \{0, 1, 2, 3, \dots\}$$

$$\mathbb{Z} = \{-1, 0, 1, -2, 2, \dots\}$$

Definition 1.1.1. a поділяється на b — $a \div b$ або b ділить a (b є дільником) $b \mid a$.

$$a \div b \Leftrightarrow \exists k \in \mathbb{Z} : a = kb$$

Property.

1. $a \neq 0, a \div 0$

2. $a \neq 0, 0 \div a$

3. $a \div b, b \div c \Rightarrow a \div c$

4. $a \div 1$

5. $a \div c, b \div c \Rightarrow (\alpha a \pm \beta b) \div c$

6. $a \div b \Leftrightarrow ac \div bc, c > 0$

Theorem 1.1.1 (Euclidean division).

$$\forall a, b \in \mathbb{Z} \exists! q, r : q \in \mathbb{Z}, r \in \mathbb{N} \ 0 \leq r < |b| \ a = bq + r$$

Proof.

1. Існування

$bq, q \in \mathbb{Z}$ - росте необмежено. $\exists q; bq \leq a \leq b(q+1), r = a - bq$.

2. Єдиність

Нехай $a = bq + r, a = bq' + r'$

$0 = b(q - q') + (r - r') \Rightarrow (r - r') \div b, -|b| < r - r' < |b| \Rightarrow$
 $\Rightarrow r - r' = 0, q = q'.$

□

$q = \lfloor \frac{a}{b} \rfloor$ - частка.

$r = a + b \cdot \lfloor \frac{a}{b} \rfloor$ - остача $= a \bmod b$.

1.2 Найбільший спільний дільник

Найбільший спільний дільник: НСД(a, b)(українська нотація), $\gcd(a, b)$ (англійська нотація), (a, b)(спеціалізована література з теорії чисел).

Definition 1.2.1. $\gcd(a, b) = d :$

1. $a \div d, b \div d$

2. d — max додатне число, яке задовільняє 1.

Property.

1. $\gcd(a, b) = b \Leftrightarrow a \div b$

2. $a \neq 0 : \gcd(a, 0) = a$

3. $\gcd(a, b)$ поділяється на довільний спільний дільник a та b

4. $c > 0 : \gcd(ac, bc) = c \gcd(a, b)$

5. $d = \gcd(a, b) \Rightarrow \gcd(\frac{a}{d}, \frac{b}{d})$

Lemma 1.2.1.

$$\gcd(a, b) = \gcd(b, a - b)$$

Proof.

$$d = \gcd(a, b), d' = \gcd(b, a - b)$$

Нехай $d > d'$

$$a : d, b : d \Rightarrow (a - b) : d \Rightarrow d - \text{спільний дільник } b \text{ та } a - b \Rightarrow d' : d - \text{Упс!}$$

Нехай $d < d'$

$$b : d', a - b \Rightarrow b + (a - b) = a : d' - \text{Упс!}$$

□

Consequence.

$$a \geq b : \gcd(a, b) = (b, a \bmod b)$$

Proof. $a = bq + r$

$$\gcd(a, b) = \underbrace{\dots}_{q \text{ разів}} \gcd(r, b)$$

□

1.3 Алгоритм Евкліда

Вхід: $a, b \in \mathbb{N}$ Вихід: $d = \gcd(a, b)$

$$r_0 := a, r_1 := b$$

$$r_0 = r_1 q_1 + r_2$$

$$r_1 = r_2 q_2 + r_3$$

$$r_2 = r_3 q_3 + r_4$$

$$\vdots$$

$$r_{n-1} = r_n q_n, r_n = d$$

Proof. $r_{i+1} = r_i \bmod r_{i-1}$

$$r_0 \geq r_1 > r_2 > \dots > r_n > r_{n+1} = 0$$

$$\begin{aligned} \gcd(a, b) &= \gcd(r_0, r_1) = \gcd(r_1, r_2) = \gcd(r_2, r_3) = \dots = \\ &= \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = 0 \end{aligned}$$

□

Lemma 1.3.1.

$$\forall i, r_{i+2} < \frac{r_i}{2}$$

Proof. $r_i = r_{i+1} q_{i+1} + r_{i+2} \geq r_{i+1} + r_{i+2} > r_{i+2} + r_{i+2} = 2r_{i+2}$

□

 \Rightarrow АЕ зробить $\leq 2 \lceil \log_2 a \rceil$ кроків.**Example:**

$$\gcd(123, 456).$$

$$123 = 456 \cdot 0 + 123$$

$$456 = 3 \cdot 123 + 87$$

$$123 = 87 \cdot 1 + 36$$

$$87 = 36 \cdot 2 + 15$$

$$36 = 15 \cdot 2 + 6$$

$$15 = 6 \cdot 2 + 3$$

$$6 = 3 \cdot 2 \Rightarrow \gcd = 3$$

Example:

Для яких n : $\frac{3n+1}{5n+1}$ - скоротний?

$$5n+2 = (3n+1) \cdot 1 + (2n+1)$$
$$3n+1 = (2n+1) \cdot 1 + n$$
$$2n+1 = n \cdot 2 + 1$$
$$n = 1 \cdot n \Rightarrow \gcd(3n+1, 5n+2) = 1$$

CHAPTER 2

Лекція 2

2.1 Найменше спільне кратне

Definition 2.1.1. $a, b \in \mathbb{N}$

$M = HCK(a, b), lcm(a, b), [a, b]$

1. $M : a, M : b$

2. M — min таке число

Property.

1. $lcm(a, 0)$ - 'на доске был нарисован грустный смайлик'

2. $lcm(a, b) = a \Leftrightarrow a : b$

3. a, b - взаємнопрості $\Rightarrow lcm(a, b) = a \cdot b$

4. Довільне спільне кратне a та $b : lcm(a, b)$

5. $\forall c > 0, lcm(ac, bc) = c lcm(a, b)$

6. $\frac{lcm(a, b)}{a}$ та $\frac{lcm(a, b)}{b}$ - взаємнопрості

Theorem 2.1.1.

$$\forall a, b \in \mathbb{N} : gcd(a, b) \cdot lcm(a, b) = a \cdot b$$

Proof. Нехай $d = gcd(a, b)$, $a = a_1 \cdot d$, $b = b_1 \cdot d$.

$$gcd(a_1, b_1) = 1, lcm(a_1, b_1) = a_1 \cdot b_1, lcm(a, b) = d \cdot a_1 \cdot b_1$$

$$d \cdot lcm(a, b) = (a_1 \cdot d) \cdot (b_1 \cdot d) = a \cdot b$$

□

Theorem 2.1.2.

$$\forall a, b \in \mathbb{N} : gcd(a, b, c) = gcd(gcd(a, b), c) = gcd(a, gcd(b, c))$$

Proof. $d = gcd(a, b, c)$

$$d' = gcd(a, b) \Rightarrow d' : d, c : d \Rightarrow d = gcd(c, d')$$

□

$$\text{lcm}(a, b, c) = \text{lcm}(\text{lcm}(a, b), c) = \text{lcm}(a, \text{lcm}(b, c))$$

Theorem 2.1.3.

$$\forall a, b, c \in \mathbb{N} : \text{lcm}(a, b, c) = \frac{a \cdot b \cdot c \cdot \text{gcd}(a, b, c)}{\text{gcd}(a, b) \cdot \text{gcd}(b, c) \cdot \text{gcd}(c, a)}$$

Решітка (*lattice*) - $\langle A, \leq, \sup, \inf \rangle$

Example:

1. множини, \subseteq, \cap, \cup

$$|A| + |B| = |A \cup B| + |A \cap B|$$

2. $\mathbb{R}, \leq, \max, \min$

$$a + b = \max\{a, b\} + \min\{a, b\}$$

3. $\mathbb{N}, \cdot, \text{lcm}, \text{gcd}$

$$a \cdot b = \text{lcm}(a, b) \cdot \text{gcd}(a, b)$$

$$\max\{a_1, \dots, a_n\} = a_1 + \dots + a_n - \min\{a_1, a_2\} - \dots - \min\{a_{n-1}, a_n\} + \min\{a_1, a_2, a_3\} - \min\{a_1, a_2, a_3, a_4\}$$

2.2 ЕВКЛІДОВІ ПОСЛІДОВНОСТІ

Definition 2.2.1. Послідовність $a_0, a_1, \dots, a_i \in \mathbb{R}$ - евклідова,

$$\text{якщо } \forall n, m \in \mathbb{N}_0 \quad n > m :$$

$$\text{gcd}(a_n, a_m) = \text{gcd}(a_m, a_{n-m}) \Rightarrow \text{gcd}(a_n, a_m) = \text{gcd}(a_m, a_{n \bmod m})$$

Theorem 2.2.1.

$$(a_i) - \text{евклідова і } a_0 = 0, \text{ то } \forall n, m : \text{gcd}(a_n, a_m) = a_{\text{gcd}(n, m)}$$

Proof. $n = m$ - очевидна.

$n > m :$

$d = \text{gcd}(n, m)$ АЕ породжує послідовність r_0, r_1, \dots, r_t , де $r_0 = n$,

$$r_1 = m, r_t = d, r_{t+1} = 0, r_{i+1} = r_{i-1} \bmod r_i$$

$$\text{gcd}(a_n, a_m) = \text{gcd}(a_{r_0}, a_{r_1}) = \text{gcd}(a_n, a_m) = \text{gcd}(a_{r_1}, a_{r_2} = \dots = \text{gcd}(a_{t_0}, a_{t_{i+1}}) = a_{r_i} = a_0 \quad \square$$

Consequence.

$$\text{Якщо додатково } a_1 = 1, \text{ то } \text{gcd}(n, m) = 1 \Rightarrow \text{gcd}(a_n, a_m)$$

Example:

$$a_k = k$$

Example:

$$\begin{aligned} a_k &= 2^k - 1 \\ \gcd(a_n, a_m) &\stackrel{?}{=} \gcd(a_m, a_{n-m}) \\ a_n &= 2^n - 1 = 2^n - 2^m - 1 = 2^m(2^{n-m} - 1) + (2^m - 1) = 2^m \cdot a_{n-m} + a_m = a_n \\ \gcd(2^n - 1, 2^m - 1) &= 2^{\gcd(n, m)} - 1 \end{aligned}$$

Example:

$$\begin{aligned} a_k &= \alpha^k - 1, \alpha \in \mathbb{N}, \alpha \geq 2 \\ a_0 &= 0, a_1 = \alpha - 1 \neq 1 \end{aligned}$$

Example:

$$a_k = \alpha^k - \beta^k, \alpha, \beta \in \mathbb{N}, \alpha > \beta \geq 2$$

(a_i) - евклідова і $a_0 = 0$, то $\forall n > m : \gcd(a_n, a_m) = 1$

CHAPTER 3

Лекція 3

3.1 Розширений алгоритм Евкліда

Theorem 3.1.1 (Little Bezout's theorem).

$$\forall a, b \in \mathbb{N}, d = \gcd(a, b) \quad \exists u, v \in \mathbb{Z}, d = au + bv$$

Proof.

$$r_0 = r_1 q_1 + r_2$$

$$r_1 = r_2 q_2 + r_3$$

$$r_2 = r_3 q_3 + r_4$$

\vdots

$$r_{n-3} = r_{n-2} q_{n-2} + r_{n-1}$$

$$r_{n-2} = r_{n-1} q_{n-1} + r_n$$

$$r_{n-1} = r_n q_n$$

$$\text{Тоді } d = r_n = r_{n-2} - r_{n-1} q_{n-1} = r_{n-2} - q_{n-1}(r_{n-3} - r_{n-2} q_{n-2}) = \dots =$$

$$= u \cdot r_0 + v \cdot r_1$$

□

Consequence.

1. $d = au + bv \Rightarrow$ одне з чисел u, v - недодатне, а інше - невід'ємне.
2. $d = \gcd(x_1, x_2, \dots, x_k) \Rightarrow a_1, a_2, \dots, a_k \in \mathbb{Z} : d = a_1 x_1 + a_2 x_2 + \dots + a_k x_k$
3. $\forall i : u_i, v_i \in \mathbb{Z} \quad r_i = au_i + bv_i \Rightarrow u_0 = 1, v_0 = 0, u_1 = 0, v_1 = 1$
 $u_{i+1} = u_{i-1} - u_i q_i, v_{i+1} = v_{i-1} - v_i q_i, r_{i+1} = r_{i-1} - q_i r_i = (au_{i-1} + bv_{i-1}) -$
 $- q_i(au_i + bv_i) = a \underbrace{(u_{i-1} - q_i u_i)}_{u_{i+1}} + b \underbrace{(v_{i-1} - q_i v_i)}_{v_{i+1}}$

Example:

$$\gcd(123, 456).$$

$$123 = 456 \cdot 0 + 123$$

$$456 = 3 \cdot 123 + 87 \quad q_1 = 3$$

$$123 = 87 \cdot 1 + 36 \quad q_2 = 1$$

$$87 = 36 \cdot 2 + 15 \quad q_3 = 2$$

$$36 = 15 \cdot 2 + 6 \quad q_4 = 2$$

$$15 = 6 \cdot 2 + 3 \quad q_5 = 2$$

$$6 = 3 \cdot 2 \quad q_6 = 2 \Rightarrow \gcd = 3$$

		q_1	q_2	q_3	q_4	q_5	
		3	1	2	2	2	
u_i	1	0	1	-1	3	-7	17
v_i	0	1	-3	4	-11	26	-63

Theorem 3.1.2.

$\gcd(a, b)$ – min додатне число, яке має форму $au + bv$, $u, v \in \mathbb{Z}$

Proof.

$$1. C = \{au + bv \mid u, v \in \mathbb{Z}\}$$

$$d' = \min\{d' > 0\}, d \in C \text{ тоді } \forall d \in C : c \vdots d'$$

$$\text{Нехай } c' = au' + bv', c' \vdots d', \text{ тоді } c = q'd' + r', 0 < r' < d'$$

$$r' = c' - q'd' = (au' + bv') - q'(au'_\alpha + bv'_\alpha) =$$

$$= a(u' - q'u'_\alpha) + b(v' - q'v'_\alpha) - \text{Упс!}$$

$$2. d = au + bv = \gcd(a, b) \Rightarrow d \vdots d'$$

$$a = a \cdot 1 + b \cdot 0 \Rightarrow a \vdots d', b = a \cdot 0 + b \cdot 1 \Rightarrow b \vdots d'$$

$$\Rightarrow d' - \text{спільний дільник } a \text{ та } b \Rightarrow d' = au'_\alpha + bv'_\alpha \vdots d \Rightarrow d = d'$$

□

3.2 Лінійні діафантові рівняння

Definition 3.2.1. $f(x_1, x_2, \dots, x_n) = 0, x_i \in \mathbb{Z}$

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = c, a_i \in \mathbb{Z}, c \in \mathbb{Z}$$

$$ax + by = c, a, b, c \in \mathbb{Z} - \text{коефіцієнти, } x, y \in \mathbb{Z} - \text{невідомі.}$$

Theorem 3.2.1.

$$\text{Нехай } ax + by = c, d = \gcd(a, b)$$

$$1. \text{ рівняння має розв'язки } \Leftrightarrow c \vdots d$$

$$2. a = a_0 \cdot d, b = b_0 \cdot d, c = c_0 \cdot d, (x_0, y_0) - \text{якийсь розв'язок рівняння.}$$

Тоді довільний розв'язок (x, y) :

$$\begin{cases} x = x_0 + b_0 \cdot t \\ y = y_0 - a_0 \cdot t \end{cases} \quad t \in \mathbb{Z}$$

Proof.

$$1. \text{ Якщо } c \vdots d, \text{ але } ax + by \vdots d \text{ то Упс!}$$

$$\text{Якщо } c \vdots d, \text{ то } a_0x + b_0y = c_0 - \text{еквівалентне рівняння}$$

$$1 = a_0u + b_0v \Rightarrow x_0 = u \cdot c_0, y_0 = v \cdot c_0 - \text{розв'язки.}$$

$$2. \quad ax + by = a(x_0 + b_0t) + b(y_0 - a_0t) = \underbrace{(ax_0 + by_0)}_{=c} + \underbrace{(ab_0t - ba_0t)}_{a_0b_0dt - a_0b_0dt} = c$$

Нехай (x, y) - розв'язок рівняння

$$ax + by = 0, \quad ax_0 + by_0 = c \Rightarrow a(x - x_0) + b(y - y_0) = 0 \Rightarrow$$

$$\Rightarrow a_0(x - x_0) + b_0(y - y_0) = 0 \quad \gcd(a_0, b_0) = 1 \Rightarrow 1 = a_0u + b_0v \Rightarrow$$

$$\Rightarrow 0 = \underbrace{a_0u}_{=(1-b_0v)}(x - x_0) + b_0v(y - y_0) = (x - x_0) + b_0(u(y - y_0) - v(x - x_0)) \Rightarrow$$

$$\Rightarrow x - x_0 \div b_0, \quad x - x_0 = b_0 \cdot t, \quad t \in \mathbb{Z} \Rightarrow a_0 \cdot b_0t + b_0(y - y_0) = 0 \Rightarrow$$

$$\Rightarrow y - y_0 = a_0t$$

□

Example:

$$15x + 9y = 27$$

$$15 = 9 \cdot 1$$

$$9 = 6 \cdot 1 + 3$$

$$6 = 3 \cdot 2 \Rightarrow 3 = 15 \cdot (-1) + 9 \cdot 2$$

$27 \div 3 \Rightarrow$ розв'язки існують

$$5x + 3y = 9$$

$$1 = 5 \cdot (-1) + 3 \cdot 2$$

$$x_0 = 9, \quad y_0 = 18$$

$$\begin{cases} x = -9 + 3 \cdot t \\ y = 18 - 5 \cdot t \end{cases} \quad t = 10 : \quad x = -9 + 30 = 21, \quad y = 18 - 50 = -32$$

$$5 \cdot 21 - 3 \cdot 32 = 105 - 96 = 9$$

$$?t : \quad x > 0, \quad y > 0$$

$$\begin{cases} -9 + 3t > 0 \\ 18 - 5t > 0 \end{cases} \Rightarrow \begin{cases} t > 3 \\ t < 3,6 \end{cases}$$

CHAPTER 4

Лекція 4

4.1 Прості числа

Definition 4.1.1. $n \in \mathbb{N}$

- *просте* \Leftrightarrow має рівно два дільники 1 та n

- *складене* $\Leftrightarrow \exists a : 1 < a < n \quad n : a$

1 - не просте, не складене

Lemma 4.1.1.

$$n \in \mathbb{N} : \gcd(n, n+1) = 1$$

Theorem 4.1.2 (Euclid).

Якщо $A = \{p_1, p_2, \dots, p_n\}$ - скінченна сукупність простих чисел, то існує просте $P \notin A$

Proof.

$$Q = p_1 p_2 p_3 \dots p_n + 1 \Rightarrow Q : p_i, \quad n = \overline{1, n}$$

Q - або просте, або має простий дільник □

Consequence.

Простих чисел нескінченно багато

Lemma 4.1.3.

$$n \in \mathbb{N} - \text{складене} \quad d > 1 - \min \text{ дільник } n \Rightarrow d - \text{просте}$$

Proof. Нехай d - складене, $d = a \cdot b$, $a, b \neq 1$, $d : a$, $n : d \Rightarrow n : a$ - УПСВ! □

4.2 Розподіл простих чисел

Сито Ератросфена(пошук простих чисел?)

2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

// Беремо перше число яке тут є. Це число 2 - воно просте. Після чого беремо і викреслюємо кожне друге число.

② 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ 9 ~~10~~ 11 ~~12~~ 13 ~~14~~ 15 ~~16~~ 17 ~~18~~ 19 ~~20~~

// Беремо перше незакреслене число. Це число 3 - воно просте. Викреслюємо кожне третє число в цьому ряду.

② ③ ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~

// Беремо наступне. Це 5 - просте. Викреслюємо кожне п'яте число. Ну вони вже викреслині. Тому далі уже нічого не викреслюється.

② ③ ~~4~~ ⑤ ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~

Lemma 4.2.1.

$$n = a \cdot b, \quad 1 < a, b < n \Rightarrow \min\{a, b\} \leq \sqrt{n} \leq \max\{a, b\}$$

Proof. Від супротивного □

Consequence.

У ситі Ератросфена для $2 \dots N$ після викреслень чисел $\leq \sqrt{n}$ залишаються прості.

Example:

$\forall m \in \mathbb{N}$: існують m послідовних натуральних складених чисел.

$(m+1)! : 2, (m+1)! : 3, (m+1)! : 5, \dots, (m+1)! : (m+1).$

Example:

Прості числа-близнюки p, q : прості, $p - q = 2$

Наразі найбільша відома пара чисел близнюків: $2996863034895 \cdot 2^{1290000} \pm 1$

Example:

Прості числа Мерсена: $M_p = 2^p - 1$ - просте, $M_n = 2^n - 1$ - складене

Lemma 4.2.2.

$$M_p - \text{просте} \Rightarrow p - \text{просте} . p = a \cdot b \Rightarrow M_p = 2^{ab} - 1 : 2^a - 1$$

Постулат Бертрана

$\forall n \in \mathbb{N}, \geq 4$. інтервал $n \dots 2n - 2$ містить просте число.

Функція розподіла простих чисел $\Pi(x)$

$\Pi(x)$ = кількість простих чисел $< x$.

$$\frac{1}{2} \cdot \frac{x}{\log_2 x} \leq \Pi(x) \leq 5 \cdot \frac{x}{\log_2 x} \rightarrow \alpha \cdot \frac{x}{\ln x} \leq \Pi(x) \leq \beta \cdot \frac{x}{\ln x}, \quad \alpha = 0.92129, \beta = 1,10555$$

Theorem 4.2.3 (Adamer, Vallee).

$$\Pi(x) \sim \frac{x}{\ln x} (\Pi(x) \sim \int_2^x \frac{dt}{\ln t}) \Rightarrow p_n \sim n \cdot \ln n$$

Theorem 4.2.4 (Dirichlet).

Якщо $\gcd(a, b) = 1$, то існує ∞ простих чисел виду $a \cdot m + b$

4.3 Основна теорема арифметики

Lemma 4.3.1 (Euclid).

$$p - \text{просте}, ab \vdots p \Rightarrow \begin{cases} a \vdots p \\ b \vdots p \end{cases}$$

Proof. Нехай $ab \vdots p$, але $a \nvdots p \Rightarrow \gcd(a, p) = 1 \Rightarrow \Rightarrow \exists u, v, \quad au + pv = 1 \Rightarrow \underbrace{ab}_{\vdots p} \cdot u + \underbrace{p}_{\vdots p} \cdot bv = \underbrace{b}_{\vdots p}$ □

Theorem 4.3.2 (Fundamental theorem of arithmetics).

$\forall n \in \mathbb{N} : n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}, \text{ де } p_1 < p_2 < \dots < p_t - \text{ прості, } \alpha_i \geq 1 - \text{ натуральні.}$

Proof.

1. Існування

Нехай все вірне, n_0 — min число, яке не розкладається $\Rightarrow n_0$ - складене $\Rightarrow \exists a : 1 < a < n_0 : n = a \cdot b$

2. Єдність

Нехай $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t} = q_1^{\beta_1} q_2^{\beta_2} \dots q_t^{\beta_t}, \quad n \vdots p_1 \Rightarrow q_1^{\beta_1} \dots q_t^{\beta_t} \vdots p_1 \exists i : q_i^{\beta_i} \vdots p_1 \Rightarrow \Rightarrow q_i = p_i$

□

Example:

Приклад Гільберта

Розглянемо числа виду $4k + 1$

5, 9, 13, 17, 21, 25

$((4k_1 + 1)(4k_2 + 1) = 4(\dots) + 1$

Example:

1. $d \mid n \Rightarrow d = q_1^{\beta_1} q_2^{\beta_2} \dots q_t^{\beta_t}, \quad 0 \leq \beta_i \leq \alpha_i$

2. $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}, \quad \alpha_i \geq 0, \quad b = p_1^{\beta_1} p_2^{\beta_2} \dots p_t^{\beta_t}, \quad \beta_i \geq 0$
 $\gcd(a, b) = \prod_{i=1}^t p_i^{\min\{\alpha_i, \beta_i\}}, \quad \text{lcm}(a, b) = \prod_{i=1}^t p_i^{\max\{\alpha_i, \beta_i\}}$

3. $a \vdots b, \quad a \vdots c, \quad \gcd(b, c) = 1 \Rightarrow a \vdots (b \cdot c)$

CHAPTER 5

Лекція 5

5.1 Мультиплікативні функції

Definition 5.1.1. $f(n)$ - мультиплікативна:

1. $f(n) \neq$
2. $\forall a, b \in \mathbb{N} : \quad \gcd(a, b) = 1 \Rightarrow f(ab) = f(a)f(b)$

Example:

$$\begin{aligned} f(n) &= 1 \\ f(n) &= n \\ f(n) &= n^S \end{aligned}$$

Property.

1. $f(1) = 1; f(n) = f(n \cdot 1) = f(n)f(1)$
2. Якщо x_1, x_2, \dots, x_t - попарно взаємнопрості, то $f(x_1 x_2 \dots x_t) = f(x_1) \dots f(x_t)$
3. Якщо $f(n), g(n)$ - мультиплікативні, то $h(n) = f(n) \cdot g(n)$ - мультиплікативна
4. $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}, f(n) = f(p_1^{\alpha_1}) \cdot f(p_2^{\alpha_2}) \dots f(p_t^{\alpha_t})$

Definition 5.1.2. $f(n)$ - мультиплікативна.

$$\text{Числовий інтеграл } g(n) = \sum_{d|n} f(d)$$

Theorem 5.1.1 (S).

$$f(n) - \text{мультиплікативна} \Rightarrow g(n) - \text{також}.$$

Proof.

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}, d | n \Rightarrow d = p_1^{\beta_1} p_2^{\beta_2} \dots p_t^{\beta_t}, 0 \leq \beta_i \leq \alpha_i$$

$$g(n) = \sum_{d|n} f(d) = \sum_{\beta_1=0}^{\alpha_1} \sum_{\beta_2=0}^{\alpha_2} \dots \sum_{\beta_t=0}^{\alpha_t} f(p_1^{\beta_1} \dots p_t^{\beta_t}) =$$

$$= \sum_{\beta_1} \dots \sum_{\beta_t} \prod_i i = 1^t f(p_i^{\beta_t}) = \prod_{i=1}^t \sum_{\beta_i=0}^{\alpha_i} f(p_i^{\beta_i})$$

□

$$g(n) = \prod_{i=1}^t \sum_{\beta_i=0}^{\alpha_i} f(p_i^{\beta_i})$$

5.2 Кількість та сума дільників

Definition 5.2.1. *Кількість дільників*

$$\tau(n) = \sum_{d|n} 1$$

Definition 5.2.2. *Сума дільників*

$$\sigma(n) = \sum_{d|n} d$$

Proposition.

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}, \quad p_t^{\alpha_t} : \tau(n) = (1 + \alpha_1)(1 + \alpha_2) \dots (1 + \alpha_t)$$

$$\sigma = \prod_{i=1}^t \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$$

Proof.

$$\begin{aligned} p - \text{просте.} \quad \tau(p) &= 2 \quad \tau(p^\alpha) = 1 + \alpha \\ \tau(n) &= \tau(p_1^{\alpha_1}) \dots \tau(p_t^{\alpha_t}) = (1 + \alpha_1)(1 + \alpha_2) \dots (1 + \alpha_t) \\ \sigma(p) &= 1 + p \quad \sigma = 1 + p + p^2 + \dots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1} \\ \sigma(n) &= \sigma(p_1^{\alpha_1}) \sigma(p_2^{\alpha_2}) \dots \sigma(p_t^{\alpha_t}) \end{aligned}$$

□

Example:

$$\begin{aligned} n &= 1000 = 2^3 5^3 \\ \tau(1000) &= (1 + 3)(1 + 3) = 16 \\ \sigma(1000) &= \frac{2^4 - 1}{2 - 1} \cdot \frac{5^4 - 1}{5 - 1} = 2340 \end{aligned}$$

Example:

$$\begin{aligned} n &= 1001 = 7 \cdot 11 \cdot 13 \\ \tau(1001) &= (1 + 1)(1 + 1)(1 + 1) = 8 \\ \sigma(1001) &= (1 + 7)(1 + 11)(1 + 13) = 1344 \end{aligned}$$

Property.

1. $\tau(n) \leq 2\sqrt{n}$
 $n : d \Rightarrow n = d \cdot d'$
 $\sigma(n) \geq n + 1$
2. $\tau(n)$ - непарне $\Leftrightarrow n = m^2$
3. σ - непарне $\Leftrightarrow \begin{cases} m^2 \\ 2m^2 \end{cases}$

5.3 Досконалі числа

Definition 5.3.1. Досконале число n :

$$n = \text{сумі усіх дільників окрім власне } n \text{ або } \sigma(n) = 2n$$

Example:

$$n = 6 : \quad 1 + 2 + 3 = 6$$

Example:

$$n = 28 : \quad 1 + 2 + 4 + 7 + 14 = 28$$

Theorem 5.3.1 (Euclid-Euler).

Парне n - досконале $\Leftrightarrow n = 2^{p-1} \cdot M_p$, де $M_p = 2^p - 1$ - просте число Марсена

Proof.

1. $n = 2^{p-1} \cdot M_p$, $p > 2$
 $\sigma(n) = \sigma(2^{p-1} \cdot M_p) = \sigma(2^{p-1})\sigma(M_p) = (2^p - 1)(M_p + 1) = 2^p(2^p - 1) = n$
2. Нехай n - парне досконале, $n = 2^k \cdot b$, b - непарне
 $\sigma(n) = \sigma(2^k \cdot b) = (2^k - 1) \cdot \sigma(b) = 2^k \cdot b = 2n \Rightarrow$
 $\Rightarrow b \mid (2^k - 1)$, $b = (2^k - 1) \cdot c$ $(2^k - 1)\sigma(b) = 2^k(2^k - 1) \cdot c$
 $\sigma(b) = 2^k \cdot c = (2^k - 1 + 1) \cdot c = b + c$
 $b \mid c$, $c \neq 1$, $c \neq b \Rightarrow \sigma(b) > 1 + b + c \Rightarrow c = 1$.
 $b = 2^k - 1$, $\sigma(b) = b + 1 \Rightarrow b$ - просте. $n = 2^{k-1} \underbrace{(2^k - 1)}_{\text{просте}}$

□

5.4 Функція Мебіуса

Definition 5.4.1. $\mu(n)$:

$$\mu(p^\alpha) = \begin{cases} -1, & \alpha = 1 \\ 0, & \alpha > 1 \end{cases} \Rightarrow M(n) = \begin{cases} (-1)^k, & n = p_1 p_2 \dots p_t \\ 0, & n \vdots a^2 \end{cases}$$

Lemma 5.4.1 (характеризаційна властивість μ).

$$\sum_{d \mid n} M(d) = \begin{cases} 1, & n = 1 \\ 0, & n \neq 1 \end{cases}$$

Proof.

$$p^\alpha : \quad \mu(1) + \mu(p) + \mu(p^2) + \dots + \mu(p^\alpha) = 1 + (-1) + 0 + 0 + \dots + 0 = 0$$

За теоремою 5.1.1 $\sum_{d \mid n} \mu(d) = \prod_i \sum_{\beta} \mu(p_i^\beta)$

□

Proposition. $f(n)$ - мультиплікативна, $n = p_1^{\alpha_1} \dots p_t^{\alpha_t}$

$$\sum_{d|n} M(d)f(d) = (1 - f(p_1))(1 - f(p_2)) \dots (1 - f(p_t))$$

Proof. За теоремою 5.1.1 $\sum_{\beta} \mu(p_1^{\beta})f(p_1^{\beta}) = \mu(1)f(1) + \mu(p_1)f(p_1) + \dots + \mu(p_1^2)f(p_1^2) + \dots = 1 + (-1)f(p_1) = 1 - f(p_1)$ □

Theorem 5.4.2 (закон обертання Мебіуса).

$$f(n) - \text{мультиплікативна, } g(n) = \sum_{d|n} f(d) \Rightarrow f(n) = \sum_{d|n} M(d) \cdot g\left(\frac{n}{d}\right)$$

Proof.

$$\begin{aligned} \sum_{d|n} M(d) \cdot \sum_{\substack{\delta|n \\ d|\frac{n}{\delta}}} f(\delta) &= \sum_{(d,\delta), d\delta|n} \mu(d \cdot f(\delta)) = \sum_{\delta|n} \sum_{d|\frac{n}{\delta}} \mu(d)f(\delta) = \\ &= \sum_{\delta|n} f(\delta) \cdot \sum_{\substack{d|\frac{n}{\delta} \\ d=1 \Rightarrow \delta=n}} \mu(d) = f(n) \end{aligned} \quad \square$$

Example:

$$\begin{aligned} a_0, a_1, \dots, a_n \\ A(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} - \text{ряд Діріхле.} \quad B(s) = \sum_{n=1}^{\infty} \frac{b_n}{n^s} \\ C(s) = A(s) \cdot B(s) = \sum_{n=1}^{\infty} \frac{c_n}{n^s} \Rightarrow C_n = \sum_{d|n} a_d \cdot b_{\frac{n}{d}} \quad \xi(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \\ \frac{1}{\xi(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} \quad C(s) = A(s) \cdot \xi(s) \quad C_n = \sum_{d|n} a_d \\ A(s) = C(s) \cdot (\xi(s))' \Rightarrow a_n = \sum_{d|n} \mu(d) c_{\frac{n}{d}} \end{aligned}$$

CHAPTER 6

Лекція 6

6.1 Порівняння за модулем

Definition 6.1.1. $a, b \in \mathbb{N}$, a та b порівнюювані за $\bmod n$:

$$a \equiv b(\bmod n), a \equiv_n b, \text{ коли: } \begin{aligned} (1) & \exists t \in \mathbb{Z} : a = b + nt \\ (2) & a \bmod n = b \bmod n \\ (3) & (a - b) : n \end{aligned}$$

Property.

1. $a \equiv a(\bmod n), a \equiv b(\bmod n) \Rightarrow b \equiv a(\bmod n),$
 $a \equiv b(\bmod n), b \equiv c(\bmod n) \Rightarrow a \equiv c(\bmod n)$
2. $a \equiv b(\bmod n), c \equiv d(\bmod n) \Rightarrow$
 $\Rightarrow a \pm c \equiv b \pm d(\bmod n), ac \equiv bd \bmod n$

Proof. $a = b + nt_1, c = d + nt_2, \quad ac = bd + \underbrace{nt_1d + nt_2b + n^2t_1t_2}_{n \cdot T, T \in \mathbb{Z}} \quad \square$

$p(x_1, x_2, \dots, x_t)$ - поліном з цілими коефіцієнтами,
 $(a_i), (b_i) : a_i \equiv b_i(\bmod n) \Rightarrow p(a_1, a_2, \dots, a_t) \equiv p(b_1, b_2, \dots, b_t)(\bmod n)$

3. Якщо $ca \equiv cb(\bmod n), \gcd(c, n) = 1$, то $a \equiv b(\bmod n)$
Але $6 \equiv 2(\bmod 4), 3 \not\equiv (\bmod 4)$

Proof. $ca - cb : n, c(a - b) : n \Rightarrow (a - b) : n \quad \square$

4. (a) $a \equiv b(\bmod n), k \neq 0 \Rightarrow ak \equiv bk(\bmod nk)$
(b) $d = \gcd(a, b, n)$
 $a = a_1d_1, b = b_1d_1, n = n_1d_1, a \equiv b(\bmod n) \Rightarrow a_1 \equiv b_1(\bmod n)$

Proof. $a = b + nt, \quad a_1d_1 = b_1d_1 + n_1d_1t \quad \square$

5. $a \equiv b(\bmod n), n : d \Rightarrow a \equiv b(\bmod d)$

$$\begin{aligned}
6. \quad & a \equiv b \pmod{n_1}, \\
& a \equiv b \pmod{n_2}, \\
& \vdots \\
& a \equiv b \pmod{n_t}, \\
& a \equiv b \pmod{\text{lcm}(n_1, \dots, n_t)}
\end{aligned}$$

$$7. \quad a \equiv b \pmod{n} \Rightarrow \gcd(a, n) = \gcd(b, n)$$

Definition 6.1.2. *Лишок за модулем n :* $k, [k], \underline{k}$

$$\{k + nt \mid k \in \mathbb{Z}\}$$

Definition 6.1.3. *Повна система лишків(кільце):*

$$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$$

6.2 Степені за модулем

Lemma 6.2.1 (A).

$$a \cdot \mathbb{Z}_n + b = \mathbb{Z}_n$$

Якщо x пробігає усі елементи \mathbb{Z}_n і $\gcd(a, n) = 1$, то $\forall b \in \mathbb{Z} \ y = (ax + b) \pmod{n}$ - також пробігає усі лишки з \mathbb{Z}_n

Proof. Нехай $ax_1 + b \equiv ax_2 + b \pmod{n}$, $ax_1 \equiv ax_2 \pmod{n}$, $x_1 = x_2 \pmod{n}$ □

Example:

$$x^6 = 105y + 5$$

$$\begin{array}{c|c|c|c}
\text{mod } 3 & & & \\
\hline
x & 0 & 1 & -1 \\
\hline
x^2 & 0 & 1 & 1 \\
\hline
x^3 & 0 & 1 & -1 \\
\hline
\end{array} \Rightarrow x^2 \pmod{3} \neq 2, \quad x^6 = (x^3)^2 \equiv 2 \pmod{3}$$

Example:

$$x^6 = 105y + 4$$

mod 5

x	0	1	-1	2	-2
x^2	0	1	1	-1	-1
x^3	0	1	-1	-2	2

$$\Rightarrow \begin{array}{l} x^2 \bmod 5 \in \{0, \pm 1\}, x^6 = (x^3)^2 \equiv -1 \pmod{5} \\ x^2 = 5k + 4 = 5k - 1 \Rightarrow x = 5t \pm 2 \end{array} \quad \bmod 7$$

x	0	1	-1	2	-2	3	-3
x^2	0	1	1	-3	-3	2	2
x^3	0	1	-1	1	-1	-1	1

$$\Rightarrow \begin{array}{l} x^2 \bmod 7 \in \{0, 1, 2, 4\} \\ x^3 \bmod 7 \in \{0, \pm 1\} \end{array}$$

mod 6

x	0	1	-1	2	-2	3
x^2	0	1	1	-2	-2	3
x^3	0	1	-1	2	-2	3

$$\Rightarrow \begin{array}{l} x^2 \bmod 7 \in \{0, 1, 2, 4\} \\ x^3 \bmod 7 \in \{0, \pm 1\} \end{array}$$

6.3 Обернені елементи за модулем

Definition 6.3.1. $\forall a \in \mathbb{Z}, n \in \mathbb{N}$ Обернене до a за $\bmod n$ $a^{-1} \bmod n$:

$$a \cdot a^{-1} \equiv a^{-1} \cdot a \equiv 1 \pmod{n}$$

Theorem 6.3.1.

$$\exists a^{-1} \bmod n \Leftrightarrow \gcd(a, n) = 1$$

Proof.

1. Нехай $\gcd(a, n) = 1$

$$\text{Тоді } \exists u, v \quad a \cdot u + n \cdot v = 1 \Rightarrow a \cdot u \equiv 1 \pmod{n} \Rightarrow u = a^{-1} \bmod n$$

2. Нехай $\forall a^{-1} \bmod n, \gcd(a, n) = d > 1$

$$a \cdot a^{-1} = 1 + nt, \quad 1 = a \cdot a^{-1} - nt \quad \text{:- Упс!}$$

□

Definition 6.3.2. Зведена ϕ -ма лишків (мультимікативна група кільця \mathbb{Z}_n)

$$\mathbb{Z}_n^* = \{a \mid \gcd(a, n) = 1\}$$

Definition 6.3.3. Функція Ойлера

$$\varphi(n) = |\mathbb{Z}_n^*|$$

CHAPTER 7

Лекція 7

7.1 Китайська теорема про остачі

Theorem 7.1.1 (Chinese remainder theorem).

$$\begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \\ \vdots \\ x \equiv b_t \pmod{n_t} \end{cases} \quad \begin{array}{l} \text{усі } n_i \text{ попарно взаємнопрости} \\ \text{Тоді існує рівно один клас лишків} \\ \text{mod } n_1 n_2 \dots n_t, \\ \text{який є розв'язком системи.} \end{array}$$

Proof.

1. Нехай x_1 та x_2 - різні розв'язки.

$$\begin{aligned} x_1 \equiv x_2 \equiv b_i \pmod{n_i} &\Rightarrow (x_1 - x_2) \vdots n_i, \ i = \overline{1, t} \Rightarrow \\ &\Rightarrow (x_1 - x_2) \vdots n_1 n_2 \dots n_t \end{aligned}$$

$$2. \quad \begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \end{cases} \Rightarrow \begin{matrix} x = b_1 + n_1 k, & k \in \mathbb{Z} \\ n_1 k + b_1 \pmod{n_2}, & k = \overline{1, n_2 - 1} \\ & =_{b_2} \end{matrix}$$

З леми А: $\exists! k \ n_1 k + b_1 \equiv b_2 \pmod{n_2}$

Повторюємо для n_1n_2 та n_3 , $n_1n_2n_3$ та $n_4 \dots$

3. $N = n_1 n_2 \dots n_t$, $N_i = \frac{N}{n_i}$, $M_i = N_i^{-1} \pmod{n_i}$

$$x_0 = (b_i N_1 M_1 + b_2 N_2 M_2 + \dots + B_i N_i M_i) \bmod N - \text{розв'язок}$$

$$x_0 \bmod n_1 \equiv b_1 N_1 M_1 \bmod n_1 \equiv b_1 N_1 N_1^{-1} \bmod n_1 = b_1 \bmod n_1$$

Example:

$$\begin{cases} x \equiv 1 \pmod{2} & n_1 = 2 & N_1 = 21 & M_1 = 1 \\ x \equiv 2 \pmod{3} & n_2 = 3 & N_2 = 14 & M_2 = 14^{-1} \pmod{3} = 2 \\ x \equiv 3 \pmod{7} & n_3 = 7 & N_3 = 6 & M_3 = 6^{-1} \pmod{7} = 6 \end{cases}$$

$$N = 42, \quad x_0 = 1 \cdot 4 \cdot 1 + 2 \cdot 14 \cdot 2 + 3 \cdot 6 \cdot 6 \equiv 17 \pmod{42}$$

7.2 Функція Ойлера

Definition 7.2.1.

$\varphi(n) = |\mathbb{Z}_n^*|$ = к-ть чисел в інтервалі $1 \dots n$, які взаємнопрости з n

Proposition.

$\varphi(n)$ - мультиплікативна.

Proof.

$$n = ab, \gcd(a, b) = 1$$

$$\forall x: \quad \gcd(x, n) = 1 \Leftrightarrow \begin{cases} \gcd(x, a) = 1 \\ \gcd(x, b) = 1 \end{cases} \quad (\text{Впливає з ОТА}) \quad \varphi(n) = \varphi(a \cdot b)$$

$$x \equiv x_0 \pmod{n} \Leftrightarrow \begin{cases} x \equiv x_0 \pmod{a} & x_0 = x_0 \pmod{a} & \varphi(a) \\ x \equiv x_0 \pmod{b} & x_0 = x_0 \pmod{b} & \varphi(b) \end{cases}$$

$$(x_a, x_n): \quad \varphi(a) \cdot \varphi(b)$$

□

$$n = p: \quad \varphi(p) = p - 1 \quad (\text{всі окрім } p)$$

$$n = p^\alpha: \quad \varphi(p) = p^\alpha - p^{\alpha-1} \quad (\text{всі окрім } p, 2p, 3p, 4p, \dots, (p^{\alpha-1} - 1, p^\alpha))$$

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}: \quad \varphi(n) = \prod_{i=1}^t (p_i^{\alpha_i} - p_i^{\alpha_i-1}) = n \cdot \prod_{i=1}^t \left(1 - \frac{1}{p_i}\right)$$

Example:

$$\varphi(31) = 30$$

$$\varphi(32) = \varphi(2^5) = 16$$

$$\varphi(33) = \varphi(3 \cdot 11) = 30$$

Proposition.

$$\sum_{d|n} \varphi(d) = n$$

Proof.

$$\varphi(n) = \#x: \quad \gcd(x, n) = 1,$$

$$N_d = \#x: \quad \gcd(x, n) = d, \quad x = x_1 \cdot d, \quad n = n_1 \cdot d, \quad \gcd(x_1, n_1) = 1 \Rightarrow$$

$$\Rightarrow N_\alpha = \varphi(n_1) = \varphi\left(\frac{n}{d}\right) \Rightarrow n = \sum_{d|n} N_d = \sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{d|n} \varphi(d)$$

□

$$\begin{aligned} \sum_{d|n} \varphi(d) = n &\Rightarrow \varphi(n) = \sum_{d|n} \mu(d) \cdot \frac{n}{d} = n - \frac{n}{p_1} - \frac{n}{p_2} - \dots - \frac{n}{p_t} + \frac{n}{p_2 p_3} + \dots + \frac{n}{p_{t-1} p_t} - \\ &- \frac{n}{p_1 p_2 p_3} - \dots + (-1)^t \frac{n}{p_1 p_2 \dots p_t} \end{aligned}$$

7.3 Теорема Ойлера та мала теорема Ферма

Theorem 7.3.1 (Euler).

$$\forall n \in \mathbb{N}, \forall a \in \mathbb{Z}_n^* : a^{\varphi(n)} \equiv 1 \pmod{n}$$

Proof.

$\forall a \in \mathbb{Z}_n^* : a\mathbb{Z}_n^* = \mathbb{Z}_n^*$ якщо x пробігає усі значення \mathbb{Z}_n^* , то ax також пробігає \mathbb{Z}_n^*

$$ax \equiv ay \pmod{n} \Rightarrow x \equiv y \pmod{n}$$

$$\mathbb{Z}_n^* = \{b_1, b_2, \dots, b_{\varphi(n)}\} = \{ab_1, ab_2, \dots, ab_{\varphi(n)}\} \Rightarrow$$

$$\Rightarrow \cancel{b_1} \cancel{b_2} \dots \cancel{b_{\varphi(n)}} \equiv a \cancel{b_1} \cdot a \cancel{b_2} \dots a \cancel{b_{\varphi(n)}} 1 \equiv a^{\varphi(n)} \pmod{n} \quad \square$$

Consequence. $n = p$

$$a \not\equiv 0 \pmod{p} \Rightarrow a^{p-1} \equiv 1 \pmod{p}$$

Theorem 7.3.2 (Fermat's little theorem).

$$p - \text{просте}: \forall a \not\equiv 0 \pmod{p} : a^p \equiv a \pmod{p}$$

Proof.

$$a \not\equiv 0 \pmod{p} : a^p \equiv a \pmod{p}$$

$$a \not\equiv 0 \pmod{p} : a^{p-1} \equiv 1 \pmod{p} \quad \square$$

Example:

$$5555^{2222} + 2222^{5555} \pmod{7}$$

$$2222 \equiv 3 \pmod{7} \quad 5555 \equiv 4 \pmod{7}$$

$$3^{5555} + 4^{2222} \pmod{7} \quad 3^6 \equiv 1 \pmod{7}$$

$$2222 \equiv 2 \pmod{6} \quad 5555 \equiv 5 \pmod{6}$$

$$3^5 + 4^2 \equiv 9 \cdot 9 \cdot 9 \cdot 3 + 16 \equiv 2 \cdot 2 \cdot 3 + 2 \equiv 14 \equiv 0 \pmod{7}$$

CHAPTER 8

Лекція 8

8.1 Функція Кармайкла

$$\mathbb{Z}_8^* = \{1, 3, 5, 7\}, \varphi(8) = 4$$

$$1^2 \equiv 1 \pmod{8}, 3^2 \equiv 1 \pmod{8}, 5^2 \equiv 1 \pmod{8}, 7^2 \equiv 1 \pmod{8}$$

Proposition. $n > 3$, a - непарне

$$a^{2^{n-2}} \equiv 1 \pmod{2^n}$$

Proof. Доведемо за MMI.

База: $n = 3$

$$a = 2k + 1 \quad a^2 = (2k + 1)^2 = 4k(k + 1) + 1 \equiv 1 \pmod{8}$$

Крок: n

$$a^{2^{n-2}} \equiv 1 \pmod{2^n} \quad a^{2^{n-2}} = 1 + 2^n \cdot t$$

$$a^{2^{n-1}} = (1 + 2^n \cdot t)^2 = 1 + 2 \cdot 2^n \cdot t + 2^{2n} \cdot t^2 = 1 + 2^{n+2} \cdot t_1 \equiv 1 \pmod{2^{n+1}} \quad \square$$

Definition 8.1.1 (Функція Кармайкла: $\lambda(n)(\psi(n))$).

$$\lambda(n) = \min\{u : \forall a \in \mathbb{Z}_n^* : a^u \equiv 1 \pmod{n}\}$$

Lemma 8.1.1.

$$\forall a \in \mathbb{Z}_n^* : a^\omega \equiv 1 \pmod{n} \Rightarrow \omega : \lambda(n)$$

Proof.

Нехай $\omega : \lambda(n) \Rightarrow \omega = q \cdot \lambda(n) + r, 0 \leq r < \lambda(n)$

$$1 \equiv a^\omega \equiv a^{q \cdot \lambda(n) + r} \equiv (a^{q \cdot \lambda(n)}) (a^r) \equiv a^r \pmod{n} - \text{Упс!} \quad \square$$

Lemma 8.1.2.

$$n = p^\alpha, p \geq 3 \Rightarrow \exists a \in \mathbb{Z}_n^k : 1, a, a^2, \dots, a^{\varphi(n)-1} - \text{попарно різні лишки}$$

Proof. Доведення буде пізніше \square

Consequence.

$$\lambda(p^\alpha) = \varphi(p^\alpha)$$

Theorem 8.1.3 (Carmichael).

1. $n = p$

$$\lambda(n) = \begin{cases} \varphi(n), & n = 2, 4, p^\alpha, p \geq 3 \\ \frac{1}{2}\varphi(n), & n = 2, \alpha > 3 \end{cases} \quad (\lambda(p^\alpha) = \varphi(p^\alpha), \lambda(2^\alpha) = 2^{\alpha-1}, \alpha = 3)$$

2. $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$

$$\lambda(n) = \text{lcm}(\lambda(p_1^{\alpha_1}), (\lambda(p_2^{\alpha_2})), \dots, (\lambda(p_t^{\alpha_t})))$$

Proof.

2) Нехай $a^\omega \equiv 1 \pmod{n}$, $\forall a \in \mathbb{Z}_n^* \Rightarrow a^\omega \equiv 1 \pmod{p_i^{\alpha_i}} \Rightarrow \omega \vdots \lambda(p_i^{\alpha_i}) \Rightarrow \Rightarrow \min \omega = \text{lcm}(\lambda(p_1^{\alpha_1}), (\lambda(p_2^{\alpha_2})), \dots, (\lambda(p_t^{\alpha_t}))) = \lambda(n)$

□

Example:

$$n = 35 = 5 \cdot 7$$

$$\varphi(35) = 4 \cdot 5 = 24 \quad \lambda(35) = \text{lcm}(4, 6) = 12$$

Example:

$$n = 1000 = 2^3 \cdot 5^3$$

$$\varphi(1000) = \varphi(2^3)\varphi(5^3) = 4 \cdot 100 = 400 \quad \lambda(1000) \text{lcm}(\lambda(2^3), \lambda(5^3)) = \text{lcm}(2, 100) = 100$$

CHAPTER 9

Лекція 9

9.1 Системи числення

- представлення чисел у вигляді послідовності символів обмеженого алфавіту.

(Позиційна) система числення за основою B :

$$n = (a_{k-1}a_{k-2} \dots a_1a_0)_B = a_{k-1}B^{k-1} + a_{k-2}B^{k-2} + \dots + a_1B + a_0,$$

$$\forall i : 0 \leq a_i < B, a_{k-1} \neq 0$$

$$n = n_1 \cdot B + a_0 = n_2 \cdot B^2 + a_1 \cdot B + a_0, n_1 = n_2 \cdot B + a_0$$

Популярні системи числення: $B = 2$, $B = 10$, $B = 16$

Непозиційні системи:

1. римська
2. фібоначчієва
3. факторіальна

Example:

$$\overline{11010}_2 = 2 + 8 + 16 = 26$$
$$2^n = \underbrace{100 \dots 0}_n_2$$

Example:

$$70 \text{ y } B = 3$$
$$70 = 23 \cdot 3 + 1$$
$$23 = 7 \cdot 3 + 2$$
$$7 = 2 \cdot 3 + 1$$
$$2 = 0 \cdot 3 + 2$$
$$70 = \overline{2121}_3$$

9.2 Ознака подільності числа

Theorem 9.2.1 (Pascal's divisibility rule).

$$\text{Нехай } n = a_{k-1}a_{k-2} \dots a_1a_0, m \in \mathbb{N}, \quad r_0 := 1, r_{i+1}r_1B \pmod m$$

$$\text{Тоді } n \equiv \sum_{i=0}^{k-1} a_i r_i \pmod{m}, \quad n : m \Leftrightarrow \sum_{i=0}^{k-1} a_i r_i : m$$

Proof.

$$r_i \equiv B^i \pmod{m}, \quad n = a_{k+1}B^{k+1} + \dots + a_1B + a_0 = \sum_{i=0}^{k-1} a_i B^i = \sum_{i=0}^{k-1} a_i r_i \pmod{m} \quad \square$$

Remark.

$$1. \quad n \leq B^k, \quad \sum a_i r_i \leq k \cdot m \cdot B$$

2. Якщо $\gcd(B, m) = 1$, то послідовність (r_i) є періодичною.
Період $\leq \lambda(m)$. Якщо $\gcd(B, m) \neq 1$

Example:

$$(B = 10), \quad m = 3$$

$$r_0 = 1 \quad r_1 = 10 \cdot 1 \pmod{3} = 1 \Rightarrow n \equiv \sum a_i \pmod{3}$$

Example:

$$(B = 10), \quad m = 4$$

$$r_0 = 1 \quad r_1 = 10 \cdot 1 \pmod{4} = 2 \quad r_2 = 10 \cdot 2 \pmod{4} = 0 \Rightarrow$$

$$\Rightarrow n \equiv 2a_i + a_0 \pmod{4}$$

Example:

$$(B = 10), \quad m = 7$$

$$r_0 = 1 \quad r_1 = 10 \cdot 1 \pmod{7} = 3 \quad r_2 = 10 \cdot 3 \pmod{7} = -1$$

$$r_4 = -3 \quad r_5 = -2 \quad r_6 = 1$$

$$12345678 \equiv 8 \cdot 1 + 7 \cdot 3 + 6 \cdot 2 - 5 \cdot 1 - 4 \cdot 3 - 3 \cdot 2 + 2 \cdot 1 + 1 \cdot 3 \equiv 2 \pmod{7}$$

Example:

$$(B = 10), \quad m = 7, 11, 13$$

$$1001 = 7 \cdot 11 \cdot 13 \equiv -1 \pmod{7, 11, 13} \Rightarrow$$

$$\Rightarrow n \equiv \overline{a_2 a_1 a_0} - \overline{a_5 a_4 a_3} + \overline{a_8 a_7 a_6} - \overline{a_{11} a_{10} a_9} + \dots + \left(\pmod{7, 11, 13} \right)$$

$$m = 11 : \quad 10 \equiv -1 \pmod{11}$$

$$n \equiv a_0 - a_1 + a_2 - a_3 + \dots = \sum_{i=0}^{k-1} (-1)^i a_i \pmod{11}$$

Lemma 9.2.2.

$$1. \quad \text{Якщо } m \mid (B - 1), \text{ то } n \equiv \sum_{i=0}^{k-1} a_i \pmod{m}$$

$$2. \quad \text{Якщо } m \mid (B + 1), \text{ то } n \equiv \sum_{i=0}^{k-1} (-1)^i a_i \pmod{m}$$

9.3 Подільність біноміальних коефіцієнтів

$$C_n^k = \frac{n!}{k!(n-k)!}$$

Proposition.

p - *просте*:

$$C_p^k \mod p = \begin{cases} 1, k = 0, p \\ 0, 0 < k < p \end{cases}$$

Proof.

$$C_p^0 = C_p^p = 1 \quad C_p^k = \frac{p!}{k!(p-k)!} \div p$$

□

Proposition ("біном для дурників").

$$\forall a, b \in \mathbb{Z}, p - \text{просте} \quad (a+b)^p \equiv a^p + b^p \pmod{p}$$

Theorem 9.3.1 (Lucas').

$$p - \text{просте}, n = \overline{n_{k-1}n_{k-2} \dots n_1n_0}, m = \overline{m_{k-1}m_{k-2} \dots m_1m_0}$$

$$C_m^n \equiv C_{n_0}^{m_0} C_{n_1}^{m_1} \dots C_{n_{k-1}}^{m_{k-1}} \pmod{p}$$

Proof.

$$n = \tilde{n}p + n_0, m = \tilde{m}p + m_0, C_n^m \equiv C_{\tilde{n}}^{\tilde{m}} C_{n_0}^{m_0} \pmod{p}$$

Розглянемо біном $\text{coef}[x^m] = C_n^m$

$$(1+x)^n = (1+x)^{\tilde{n}p}(1+x)^{n_0} \equiv (1+x^p)^{\tilde{n}}(1+x)^{n_0} \quad m = \tilde{m}p + m_0$$

$$x^m \text{ одержуємо } x^{\tilde{m}p} \text{ з } (1+x^p)^{\tilde{n}} \Rightarrow x^{\tilde{m}} \text{ з } (1+x)^{\tilde{n}} \Rightarrow \text{coef}[x^m] = C_{\tilde{n}}^{\tilde{m}} C_{n_0}^{m_0}$$

□

Consequence.

1. Якщо $\exists i : m_i > n_i$, то $C_n^m \equiv 0 \pmod{p}$

2. $n = p^k = (\underbrace{100 \dots 0}_k)_p$

$\forall m : 0 < m < p^k \quad \forall i : m_i \neq 0, 0 \leq i \leq k \Rightarrow C_{p^k}^m \not\equiv 0 \pmod{p}$

CHAPTER 10

Лекція 10

10.1 Лінійні порівняння за модулем

$$ax \equiv b \pmod{n}$$

1. Якщо $\gcd(a, n) = 1$, то $x \equiv a^{-1} \cdot b \pmod{n}$

2. Якщо $ax \equiv b \pmod{n}$, $b = ax - nt$

Якщо $b \nmid d$ - розв'язків немає

Якщо $b \mid d$, то $a = a_1d$, $b = b_1d$, $n = n_1d$ $\gcd(a_1, n_1) = 1$

$$b_1 = a_1x - n_1t \Rightarrow a_1x \equiv b_1 \pmod{n_1}$$

$x_0, x_0 + n_1, x_0 + 2n_1, x_0 + (d-1)n_1$ - d розв'язків

Example:

$$12x \equiv 5 \pmod{25}$$

$$x \equiv 12^{-1} \cdot 5 \pmod{25} \equiv 15 \pmod{25}$$

Example:

$$12x \equiv 5 \pmod{27}$$

$$\gcd(12, 27) = 3, 5 \nmid 3 \Rightarrow \emptyset$$

Example:

$$12x \equiv 9 \pmod{27}$$

$$\gcd(12, 27) = 3, 9 \div 3$$

$$4x \equiv 3 \pmod{9}$$

$$x_0 \equiv 3 \cdot 4^{-1} \pmod{9} \equiv 3(-2) \equiv -6 \equiv 3 \pmod{9}$$

$$\left\{ \begin{array}{l} x_0 \equiv 3 \\ x_0 \equiv 3 + 9 \equiv 12 \\ x_0 \equiv 12 + 9 \equiv 21 \end{array} \right\} \pmod{27}$$

10.2 Елементи загальної теорії розв'язування порівнянь

$f(x) = a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$ - поліном з цілими коефіцієнтами. $f(x) \equiv 0 \pmod{m}$

1. Якщо $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$, то

$$f(x) \equiv 0 \pmod{m} \Leftrightarrow \begin{cases} f(x) \equiv 0 \pmod{p_1^{\alpha_1}} \\ f(x) \equiv 0 \pmod{p_2^{\alpha_2}} \\ \vdots \\ f(x) \equiv 0 \pmod{p_t^{\alpha_t}} \end{cases}$$

2. $f(x) \equiv 0 \pmod{p}$

$f(x) \equiv 0 \pmod{p}$ та $g(x) \equiv 0 \pmod{p}$

- еквівалентні, якщо множини розв'язків співпадають

Lemma 10.2.1. $\forall h(x), f(x) :$

$f(x) \equiv 0 \pmod{p}, f(x) - (x^p - x) \cdot h(x) \equiv 0 \pmod{p}$ - еквівалентні

$\Rightarrow f(x) \equiv 0 \pmod{p}, f(x) \pmod{(x^p - x)} \equiv 0 \pmod{p}$

можна розглядати $f : \deg f < p$

Theorem 10.2.2 (Fundamental theorem of arithmetics for \mathbb{Z}_p).

$f(x) \in \mathbb{Z}_p[x], \deg f = n < p$

Якщо $a_n \not\equiv 0 \pmod{p}$, то $f(x) \equiv 0 \pmod{p}$ має $\leq n$ розв'язків

Proof. MMI за n

1. $n = 1$

$a_1 x + a_0 \equiv 0 \pmod{p}, \gcd(a_1, p) = 1 \Rightarrow$ рівно один розв'язок

2. Для усіх поліномів $\deg \leq n - 1$ - вірно

$f(x) \equiv 0 \pmod{p}$

(a) Якщо розв'язків немає - ок

(b) Якщо x_0 - розв'язок, то

$f(x) = (x - x_0) \cdot g(x) + f(x_0) \equiv (x - x_0) \cdot g(x) \pmod{p}$

$g(x)$ - поліном з цілими коефіцієнтами, $\deg g = n - 1$

$\text{coef}[x^{n-1}]g = a_n \not\equiv 0 \pmod{p} \Rightarrow g(x) \equiv 0 \pmod{p}$ має $\leq n - 1$ розв'язків

□

Consequence.

Якщо $f(x) \equiv 0 \pmod{p}$ має $> n$ розв'язків, то $\forall i : a_i \equiv 0 \pmod{p}$

Proof.

$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \equiv 0 \pmod{p}$

$a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \equiv 0 \pmod{p}$

\vdots

$a_0 \equiv 0 \pmod{p}$

□

Theorem 10.2.3 (Wilson).

$$n - \text{просте} \Leftrightarrow ((n+1)! + 1) \div n$$

Proof.

1. p - просте, $p > 3$ $(p-1)! \equiv -1 \pmod{p}$?
 $f(x) = (x-1)(x-2)(x-3)\dots(x-(p-1)) - (x^{p-1} - 1)$
 $\deg f = p-2$, $1, 2, 3, \dots, p-1$ - корені \pmod{p}
 $p=2$ - очевидна

2. Нехай $n = a \cdot b$, $1 < a < n \Rightarrow (n-1)! \div a$
 $\Rightarrow (n-1)! + 1 \div n$

□

10.3 Розклад Тейлора для поліномів

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = \sum_{t=0}^n a_t x^t$$

$$f'(x) = f^{(1)}(x) = \sum_{t=1}^n a_t t x^{t-1}$$

$f'(x)$ - поліном з цілими коефіцієнтами $\deg f = n-1$ k -тий похідний поліном:

$$f^{(k)}(x) = \sum_{t=k}^n a_t t(t-1)\dots(t-k+1)x^{t-k}$$

Lemma 10.3.1.

$$\frac{f^{(k)}(x)}{k!} = \sum_{t=k}^n C_t^k a_t x^{t-k}$$

Proof.

$$\frac{t(t-1)\dots(t-k+1)}{k!} \dots \frac{(t-k)!}{(t-k)!} = \frac{t!}{k!(t-k)!}$$

□

Remark. $f^{(0)}(x) \equiv f(x)$

Theorem 10.3.2 (Taylor series). $\forall f(x) : \forall x_0, \alpha$

$$f(x + \alpha) = \sum_{k=0}^n \frac{f^{(k)}(x_0)}{k!} \alpha^k$$

Proof.

$$f(x_0 + \alpha) = \sum_{t=0}^n a_t (x_0 + \alpha)^t = \sum_{t=0}^n \sum_{k=0}^t a_t C_t^k x_0^{t-k} \alpha^k$$

$$\begin{array}{cccccc}
t & 0 & 1 & 2 & 3 & \dots & n \\
k: & 0 & 0 & 0 & 0 & \dots & 0 \\
& & 1 & 1 & 1 & \dots & 1 \\
& & & 2 & 2 & \dots & 2 \\
& & & & 3 & \dots & 3 \\
& & & & & \ddots & \vdots \\
& & & & & & n
\end{array}$$

$$= \sum_{k=0}^n \left(\sum_{t=k}^n C_t^k a_t x_0^{t-k} \right) \alpha^k = \sum_{k=0}^n \frac{f^{(k)}(x_0)}{k!} \alpha^k \quad \square$$

10.4 Поліноміальні порівняння за модулем степеня простого числа (1)

Theorem 10.4.1. $f(x)$ - поліном з цілими коефіцієнтами x_0 .

$$f(x_0) \equiv 0 \pmod{p^k}, f'(x_0) \not\equiv 0 \pmod{p}$$

Тоді існує єдиний лишок $x_k : f(x_k) \equiv 0 \pmod{p^k}, x_k \equiv x_0 \pmod{p}, \forall k$

Proof. MMI за k

1. $k = 1$

2. $k = 2$

Нехай x_k - задовільняє умовам

$$f(x_k) \equiv 0 \pmod{p^k}, f'(x_k) \not\equiv 0 \pmod{p}, x_k \equiv x_0 \pmod{p}$$

$$\Rightarrow f'(x_k) \equiv f'(x_0) \pmod{p} \Rightarrow f'(x_k) \not\equiv 0 \pmod{p}$$

Шукаємо $x_{k+1} = x_k + p^k \cdot t, 0 \leq t \leq p-1$

$$f(x_{k+1}) \equiv 0 \pmod{p^{k+1}}$$

$$f(x_k + p^k t) = f(x_k) + f'(x_k) \cdot p^k t + \frac{f''(x_k)}{2!} (p^k t)^2 + \dots \equiv$$

$$\equiv f(x_k) + f'(x_k) \cdot p^k t \pmod{p^k} \Rightarrow 0 \equiv f(x_k) + f'(x_k) \cdot p^k t \pmod{p^k}$$

$$f'(x_k) \cdot t \equiv -\frac{f(x_k)}{p^k} \pmod{p} \Rightarrow \text{існує єдине } t \Rightarrow \text{існує єдине значення}$$

□

CHAPTER 11

Лекція 11

11.1 Поліноміальні порівняння за модулем степеня простого числа (2)

Theorem 11.1.1. $f(x)$ - поліном з цілими коефіцієнтами

$$\begin{array}{lcl} x_0 : & f(x_0) \equiv 0 \pmod{p}, & f'(x_0) \not\equiv 0 \pmod{p} \\ x_k : & f(x_k) \equiv 0 \pmod{p^k}, & x_k \equiv x_0 \pmod{p} \end{array}$$

Тоді:

1. Якщо $f(x) \not\equiv 0 \pmod{p^{k+1}}$, то

$$f(x) \equiv 0 \pmod{p^{k+1}} \text{ - не має розв'язків}$$

2. Якщо $f(x_k) \equiv 0 \pmod{p^{k+1}}$, то

$$\text{розв'язками} \pmod{p^{k+1}} \text{ є усі числа } x_k + p^k t, t = \overline{0, p-1}$$

Proof.

$$x_{k+1} = x_t + p^k t, t = \overline{0, p-1}$$

$$f(x_{k+1}) = f(x_k + p^k t) = f(x_k) + f'(x_k) \cdot p^k t + \dots \equiv f(x_k) \pmod{p^{k+1}}$$

$$f(x_{k+1}) \equiv 0 \pmod{p^{k+1}} \Rightarrow f(x_k) \equiv 0 \pmod{p^{k+1}}$$

□

Example:

$$\begin{array}{l} x^4 + 7x + 4 \equiv 0 \pmod{27} \\ f(x) = x^4 + 7x + 4 \quad f'(x) = 4x^3 + 7 \end{array}$$

$$1. f(x) \equiv 0 \pmod{3}$$

$$x_0 \equiv 1 \pmod{3}$$

$$f'(1) = 4 + 7 = 11 \equiv -1 \pmod{3}$$

$$2. f(x) \equiv 0 \pmod{9}$$

$$x_1 = x_0 + 3 \cdot t_0$$

$$f'(1) \cdot t_0 \equiv -\frac{f(1)}{3} \pmod{3}$$

$$2t_0 \equiv -4 \equiv 2 \pmod{3}$$

$$t_0 = 1 \quad x_1 = 1 + 3 = 4 \pmod{9}$$

$$3. f(x) \equiv 0 \pmod{27}$$

$$x_2 = x_1 + 9t_1$$

$$\begin{aligned}
 f'(4) \cdot t_1 &\equiv -\frac{f(4)}{9} \pmod{3} \\
 263t_1 &\equiv -32 \pmod{3} \\
 2t_1 &\equiv 1 \pmod{3} \\
 t_1 &\equiv \pmod{3} \quad x_2 = 4 + 9 \cdot 2 \equiv 22 \pmod{27}
 \end{aligned}$$

11.2 Квадратичні лишки, критерій квадратичності Ойлера

$ax^2 + bx + c \equiv 0 \pmod{p}$ - квадратичне порівняння. $\Rightarrow x^2 \equiv \alpha \pmod{p}$

Definition 11.2.1. $\alpha \in \mathbb{Z}_p^*$ - квадратичний лишок за \pmod{p} , якщо

$$\exists x : \quad x^2 \equiv \alpha \pmod{p}$$

$$\mathbb{Z}_p^* = \{1, 2, 3, \dots, p-1\}, \quad \mathbb{Z}_p^\otimes = \left\{-\frac{p-1}{2}, \dots, -2, -1, 1, 2, \dots, \frac{p-1}{2}\right\}_{(p>3)},$$

$$Y_p = \{1, 2, \dots, \frac{p-1}{2}\}$$

$$f(x) = x^2 - \alpha$$

x_0 - корінь, то $(-x_0)$ також корінь

Lemma 11.2.1.

\mathbb{Z}_p^* має рівно $\frac{p-1}{2}$ квадратичних лишків та $\frac{p-1}{2}$ квадратичних не лишків

Proof.

Квадратичні лишки: $(1)^2, 2^2, 3^2, \dots, \left(\frac{p-1}{2}\right)^2 \Rightarrow \frac{p-1}{2}$ штук

Але $0 < u < v \leq \frac{p-1}{2} : u^2 \equiv v^2 \pmod{p}$ то $x^2 \equiv u^2 \pmod{p}$

має 4 розв'язки $\pm u, \pm v \Rightarrow$ квадратичних лишків $\frac{p-1}{2}$ штук □

Theorem 11.2.2 (Euler's criterion).

$$a^{\frac{p-1}{2}} \pmod{p} \equiv \begin{cases} 1, & a - \text{квадратичний лишок} \\ -1, & a - \text{квадратичний нелишок} \end{cases}$$

Proof.

$a \equiv 0 \pmod{p}$ - очевидно

$$a \not\equiv 0 \pmod{p} \Rightarrow a^{p-1} \equiv 1 \pmod{p} \quad a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod{p}$$

Нехай $a = b^2 \Rightarrow a^{\frac{p-1}{2}} = b^{p-1} \equiv 1 \pmod{p}$

$f(x)x^{\frac{p-1}{2}} - 1$ - має $\leq \frac{p-1}{2}$ коренів, усі квадратичні лишки - корені □

11.3 Критерій квадратичності Гаусса

Theorem 11.3.1 (Gauss' criterion). $a \in \mathbb{Z}_p^*$, $a \cdot Y_p = \{a, 2a, 3a, \dots, \frac{p-1}{2}a\}$, l - кількість від'ємних лишок у $a \cdot Y_p$

$$(-1)^l = \begin{cases} 1, & a - \text{квадратичний лишок} \\ -1, & a - \text{квадратичний нелишок} \end{cases}$$

Proof.

$$\forall u \in Y_p : lu \in \{0, 1\}, r_u \in Y_p, a \cdot u \equiv (-1)^{lu} \cdot r_u \pmod{p}$$

$$u \not\equiv v \Rightarrow r_u \not\equiv r_v \pmod{p}$$

$$\begin{cases} u \not\equiv v \\ r_u \equiv r_v \end{cases} \Rightarrow \begin{cases} au \not\equiv av \\ r_u \equiv r_v \end{cases} \Rightarrow au \equiv av \pmod{p}$$

$$a(u+v) \not\equiv p, \text{ але } 0 < \frac{u}{v} \leq \frac{p-1}{2} \Rightarrow 0 < u+v \leq p-1 < p \Rightarrow u+v \not\equiv p - \text{Упс!}$$

$$\Rightarrow \{r_1, r_2, \dots, r_{\frac{p-1}{2}}\} = Y_p$$

$$(a \cdot 1)(a \cdot 2)(a \cdot 3) \dots (a \cdot \frac{p-1}{2}) \equiv (-1)^{l_1+l_2+\dots+l} \frac{p-1}{2} r_1 r_2 \dots r_{\frac{p-1}{2}} \pmod{p}$$

$$a^{\frac{p-1}{2}} \equiv (-1)^{l_1+l_2+\dots+l} \frac{p-1}{2} \pmod{p} \equiv (-1)^l \pmod{p}$$

□

CHAPTER 12

Лекція 12

12.1 Символ Лежандра та його властивості

$x^2 \equiv a \pmod{p}$, $p \geq 3$ - просте

Definition 12.1.1. Символ Лежандра -

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & a - \text{квадратичний лишок} \\ -1, & a - \text{квадратичний нелішок} \\ 0, & a \div p \end{cases}$$

Ойлер: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$

Гаусс: $\left(\frac{a}{p}\right) \equiv (-1)^l$

Property.

1. $\left(\frac{a}{p}\right) = 1$, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$,
 $p = 4k + 3 : \left(\frac{-1}{p}\right) = -1$, $p = 4k + 1 : \left(\frac{-1}{p}\right) = 1$

2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$
 $\left(\frac{a^2}{p}\right) = 1$, $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$

3. $\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{8}}$
 $p = 8k \pm 1 : \left(\frac{2}{p}\right) = 1$, $p = 8k \pm 3 : \left(\frac{2}{p}\right) = -1$

4. Закон квадратичної взаємодії Гаусса

p, q - непарні прості,
$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{q}{p}\right)$$

Proof.

$$\left(\frac{2}{p}\right) = \begin{cases} +1, & p = 8k \pm 1 \\ -1, & p = 8k \pm 3 \end{cases}, \quad \left(\frac{2}{p}\right) = (-1)^l, \quad l - \text{кількість від'ємних лишків у } \mathbb{Z}_p^*$$

серед чисел $2 \cdot 1, 2 \cdot 2, 2 \cdot 3, \dots, 2 \cdot \dots \frac{p-1}{2} = 2, 4, 6, \dots, (p+1)$

Якщо число $> \frac{p}{2}$, то воно від'ємне у \mathbb{Z}_p^*

Число, яке $< \frac{p}{2} : \lfloor \frac{p}{4} \rfloor \Rightarrow l = \frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor$

$$p = 8k + 1 : \quad l = 4k - 2k = 2k$$

$$p = 8k + 3 : \quad l = 4k + 1 - 2k = 2k + 1$$

$$p = 8k + 5 : \quad l = 4k + 2 - (2k + 1) = 2k + 1$$

$$p = 8k + 7 : \quad l = 4k + 3 - (2k + 1) = 2k + 2$$

□

12.2 Символ Якобі та його властивості

n - непарне, a - довільне

Definition 12.2.1. Символ Якобі

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^\alpha \left(\frac{a}{p_2}\right)^\alpha \dots \left(\frac{a}{p_t}\right)^\alpha$$

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}, \quad \left(\frac{a}{n}\right) \in \{-1, 1, 0\}, \quad \left(\frac{a}{n}\right) = 0 \Leftrightarrow \gcd(a, n) \neq 1,$$

$$\left(\frac{a}{n}\right) = -1 \Leftrightarrow a - kb \text{ квадратний нелишок } \pmod{n}, \quad \left(\frac{a}{n}\right) = 1 \Leftrightarrow ?$$

Property.

$$1. \quad \left(\frac{1}{n}\right) = 1, \quad \left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$$

$$2. \quad \left(\frac{a \cdot b}{n}\right) = \left(\frac{a}{n}\right) \left(\frac{b}{n}\right)$$

$$3. \quad \left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$$

$$4. \quad \left(\frac{a}{n}\right) = (-1)^{\frac{a-1}{2} \frac{n-1}{2}} \left(\frac{a}{n}\right), \quad a, n - \text{непарні}$$

Example:

$$\begin{aligned} x^2 &\equiv 59 \pmod{97} \\ \left(\frac{59}{97}\right) &= (-1)^{\frac{59-1}{2} \frac{97-1}{2}} \left(\frac{59}{97}\right) = (-1)^{\frac{a-1}{2} \frac{n-1}{2}} \left(\frac{38}{29}\right) = \left(\frac{2}{29}\right) \left(\frac{19}{29}\right) = (-1) \left(\frac{19}{59}\right) = \\ &= (-1)(-1)^{\frac{19-1}{2} \frac{59-1}{2}} = \end{aligned}$$

$$\left| \right. = (+1) \left(\frac{2}{19} \right) = -1$$

Вступ до абстрактної алгебри

(Introduction to Abstract algebra)

CHAPTER 13

Лекція 1

13.1 Алгебраїчні системи з однією операцією

$\mathcal{A}, \cdot (\mathcal{A} \times \mathcal{A} \rightarrow \mathcal{A})$

Операція \cdot - замкнена на множині \mathcal{A} , бо вона приймає аргументи з множини \mathcal{A} і повертає значення з цієї множини

$B \subseteq \mathcal{A}$, якщо $\forall b_1, b_2 \in B : b_1 \cdot b_2 \in B$ - B замкнена відносно \cdot .

Definition 13.1.1.

$\langle \mathcal{A}, \cdot \rangle$ - алгебраїчна система з однією операцією

Property (можливі).

1. асоціативність: $\forall a, b, c \in \mathcal{A} : a \cdot (b \cdot c) = (a \cdot b) \cdot c$

2. комутативність: $\forall a, b \in \mathcal{A} : a \cdot b = b \cdot a$

3. нейтральний елемент: $e_L \in \mathcal{A}$ - лівий нейтральний $\Leftrightarrow \forall a \in \mathcal{A} : e_L \cdot a = a$
 $e_R \in \mathcal{A}$ - правий нейтральний $\Leftrightarrow \forall a \in \mathcal{A} : a \cdot e_R = a$
 $e \in \mathcal{A}$ - нейтральний \Leftrightarrow одночасно лівий і правий

4. "нуль": $z_L \in \mathcal{A}$ - лівий нуль $\Leftrightarrow \forall a \in \mathcal{A} : z_L \cdot a = z_L$
 $z_R \in \mathcal{A}$ - правий нуль $\Leftrightarrow \forall a \in \mathcal{A} : a \cdot z_R = z_R$
 $z \in \mathcal{A}$ - нейтральний \Leftrightarrow одночасно лівий і правий

5. наявність обернених елементів: (за умови наявності нейтрального!)

$a \in \mathcal{A}$ має лівий обернений $a_L^{-1} : a_L^{-1} \cdot a = e$

$a \in \mathcal{A}$ має правий обернений $a_R^{-1} : a \cdot a_R^{-1} = e$

$a^{-1} \in \mathcal{A}$ - обернений до $a \in \mathcal{A}$, якщо $a \cdot a^{-1} = a^{-1} \cdot a = e$

Definition 13.1.2.

$\langle \mathcal{A}, \cdot \rangle$ - напівгрупа, якщо операція \cdot - асоціативна

Definition 13.1.3.

$\langle \mathcal{A}, \cdot \rangle$ - моноїд, якщо \cdot - асоціативна, $\exists e \in \mathcal{A} \forall a \in \mathcal{A} : e \cdot a = a \cdot e = a$

Definition 13.1.4.

$\langle \mathcal{A}, \cdot \rangle$ - група, якщо вона моноїд і $\forall a \in \mathcal{A} \exists a^{-1} \in \mathcal{A} : a \cdot a^{-1} = a^{-1} \cdot a = e$

Remark.

\cdot - комутативна \Rightarrow комутативна напівгрупа
 комутативний моноїд
 абелева група

Remark.

Форми запису:

Мультиплікативна	Адитивна
$a \cdot b$	$a + b$
$a^n, n \in \mathbb{Z}$	$n \cdot a, n \in \mathbb{Z}$
a^{-1}	$-a$
"множення"	"додавання"

13.2 Приклади алгебраїчних систем з однією операцією**Example:**

$\langle \mathbb{N}, + \rangle$ - комутативна напівгрупа,

$\langle \mathbb{N}_0, + \rangle$ - комутативний моноїд,

$\langle \mathbb{Z}, + \rangle$ - абелева група,

$\langle \mathbb{N}, - \rangle$ - не алгебраїчна система,

$\langle \mathbb{Z}, + \rangle$ - не напівгрупа,

$\langle \mathbb{N}, \cdot \rangle$ - комутативний моноїд,

$\langle \mathbb{Z}, + \cdot \rangle$ - комутативний моноїд, $\rightarrow 1^n = 1, (-1)^{-1} = -1$

$\langle \mathbb{Q}, \cdot \rangle$ - комутативний моноїд, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\} \Rightarrow \langle \mathbb{Q}^*, \cdot \rangle$ - абелева група,

$\langle \mathbb{Z}_{>}, + \bmod m \rangle$ - абелева група,

$\langle \mathbb{Z}_{>}, \cdot \bmod m \rangle$ - комутативний моноїд,

$\langle \mathbb{Z}_{>}^*, + \bmod m \rangle$ - абелева група

$Mat_{n \times m}(\mathbb{R})$: за додаванням - абелева група

за множенням - моноїд

$GL_n(\mathbb{R}) = \{M \in M_{n \times n}(\mathbb{R}) \mid \det M \neq 0\}$ - загальна лінійна група

$X^X = \{f \mid f : X \rightarrow X, \langle X^X, \circ \rangle$ - моноїд

$Sym(X)$ - множина бієктивних відображень $\Rightarrow \langle Sym(X), \circ \rangle$ - група (симетрична група підстановок на X)

$\langle 2^A, \cup \rangle$ - комутативний моноїд, \emptyset - нейтральний

$\langle 2^A, \setminus \rangle$ - не напівгрупа, $(B \setminus C) \setminus D \stackrel{?}{=} B \setminus (C \setminus D)$

$\langle 2^*, \Delta \rangle$ - абелева група, $A \Delta \emptyset = A, A = A^{-1}$

$\langle A^*, \parallel \rangle$ - моноїд

13.3 Властивості елементів моноїдів. Циклічні моноїди

$\langle \mathcal{M}, \cdot \rangle$ - моноїд

Lemma 13.3.1.

У \mathcal{M} існує лише один нейтральний елемент

Proof. Нехай e_1, e_2 - нейтральні елементи

$$\forall g \in \mathcal{M} : \begin{array}{l} g = e_1 \cdot g = e_2 \cdot g \\ \Rightarrow e_1 = e_2 \end{array} \quad \text{НЕ МОЖНА!!!}$$

/ *

Скорочуваність - теж властивість. Вона може бути, а може і не бути. І опки ви не доведете, використовувати її не можна.

*/

$$e_1 = e_1 \cdot e_2 = e_2 \quad (\text{аксіома про нейтральний елемент})$$

□

Lemma 13.3.2.

Якщо $a \in \mathcal{M}$ має лівий та правий обернені елементи, то вони співпадають

$$\begin{array}{l} \text{Proof. } a_l^{-1}, a_R^{-1} : a_L^{-1} \cdot a \cdot a_R^{-1} = a_L^{-1} \cdot e = a_L^{-1} \\ a_L^{-1} \cdot a \cdot a_R^{-1} = a_R^{-1} \cdot e = a_R^{-1} \end{array}$$

□

Lemma 13.3.3.

Якщо $a \in \mathcal{M}$ - оборотний, то він має рівно один обернений елемент

Proof.

□

Definition 13.3.1. Степінь елемента $a \in \mathcal{M}$:

$$a^0 = e, a^1 = a, a^{n+1} = a^n \cdot a, n \geq 1$$

$$\langle a \rangle = \{e, a, a^2, \dots\} = \{a^n \mid n \in \mathbb{N}\}$$

\mathcal{M} - циклічний моноїд $\Leftrightarrow \exists g : \mathcal{M} = \langle g \rangle \Rightarrow g$ - твірний елемент/генератор

Theorem 13.3.4.

$$\forall a \in \mathcal{M}, \forall m, n \in \mathbb{N}_0 : a^m \cdot a^n = a^{m+n}$$

Proof. MMI:

$$\forall m - \text{фіксоване: } n = 0 (\text{база}): a^m \cdot a^0 = a^m \cdot e = a^m = a^{m+0}$$

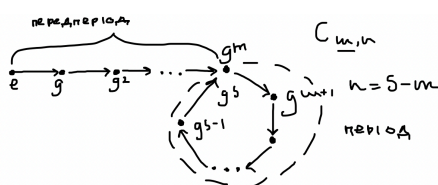
$$n \rightarrow n + 1 \quad a^m \cdot a^{n+1} = a^m \cdot a^n \cdot a = a^{n+m} \cdot a = a^{m+n+1}$$

□

⊕ Циклічні моноїди - комутативні

Fact.

Існує фактично один нескінченний циклічний моноїд: $\langle \mathbb{N}_0, + \rangle$



$$\mathcal{M} = \langle g \rangle : g^k \mapsto k$$

Нехай існує $\mathcal{M} = \langle g \rangle, |\mathcal{M}| < \infty$

$$\Rightarrow \exists \min g : g^s = g^m, m < s$$

$$\langle 2 \rangle \in \mathbb{Z}_{20} \text{ за } \cdot \langle 2 \rangle = \{ \overbrace{1, 2}^{\text{передн.}}, \overbrace{4, 8, 16, 32}^{\text{цикл}} \} \sim C_{2,4}$$

CHAPTER 14

Лекція 2

14.1 Властивості елементів груп. Циклічні групи

- $\langle G, \cdot \rangle$ - замкненість
- асоціативність
- \exists нейтральний елемент
- $\forall a \exists a^{-1} : a \cdot a^{-1} = a^{-1} \cdot a = e$

Property.

1. *Правило скорочення:*

$$\forall a, x, y \in G : \quad ax = ay \Rightarrow x = y, \quad xa = ya \Rightarrow x = y$$

2. $\forall a, b \in G : \quad \begin{array}{l} ax = b \\ ya = b \end{array} \quad - \text{ мають єдиний розв'язок}$

Proof.

$$(a) \quad x = a^{-1}b : \quad ax = a(a^{-1} \cdot b) = (a \cdot a^{-1})b = e \cdot b = b \Rightarrow - \text{ розв'язок}$$

$$(b) \quad \text{Нехай } x_1, x_2 - \text{ розв'язки } ax = b \quad \Rightarrow b = ax_1 = ax_2 \Rightarrow x_1 = x_2$$

□

3.

Proposition. $\forall a, b \in G$

$$(a) \quad e^{-1} = e$$

$$(b) \quad (a^{-1})^{-1} = a$$

$$(c) \quad (ab)^{-1} = b^{-1}a^{-1}$$

$$(d) \quad \forall m \in \mathbb{Z} : (a^{-1})^m = (a^m)^{-1}$$

Proof.

$$(c) \quad (ab)^{-1} \cdot \underbrace{(ab)}_x = e, \quad (ab)^{-1} \cdot a \cdot b \cdot b^{-1} = (ab)^{-1} \cdot a = e \cdot b^{-1} = b^{-1}, \quad (ab)^{-1} = b^{-1} \cdot a^{-1}$$

□

4.

Theorem 14.1.1. $\forall a \in G, \forall m, n \in \mathbb{Z} :$

$$a^m \cdot a^n = a^{m+n}, \quad (a^m)^n = a^{mn}$$

Proof.

(a)

$$a^m \cdot a^n = a^{m+n} : \begin{aligned} (1) & \ m, n > 0 - \text{доведено для } \forall \text{ моноїд} \\ (2) & \ n, m < 0 - a^m \cdot a^n = (a^{-1})^{-m} (a^{-1})^{-n} - \text{див. п. (1)} \\ & \ m > 0 \quad a^m a^n = a^m (a^{-1})^t = \underbrace{aaa \dots a}_m \underbrace{a^{-1} a^{-1} \dots a^{-1}}_t \\ (3) & \ n < 0 \quad m \geq t := a^{m-t} = a^{m+n} \\ & \ t = -n < 0 \quad m < t := (a^{-1})^{t-m} = a^{m-t} = a^{m+n} \\ (4) & \ m < 0, n > 0 - \text{аналогічно} \end{aligned}$$

(b)

$$\begin{aligned} n \geq 0 : & \ (a^m)^n = a^m \cdot a^m \dots a^m = a^{mn} \\ n < 0 : & \ (a^m)^n = ((a^m)^{-1})^{-n} = ((a^{-1})^m)^{-n} = (a^{-1})^{-mn} = a^{mn} \end{aligned}$$

□

Fact. Циклічні групи

$$G - \text{циклічна} \Leftrightarrow \exists g : G = \langle g \rangle$$

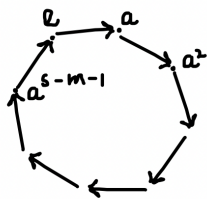
$$\Rightarrow \text{усі циклічні групи зводяться до } \langle \mathbb{Z}, + \rangle$$

$$\text{усі циклічні групи зводяться до } \langle \mathbb{Z}_m, + \rangle$$

14.2 Порядок групи, порядок елементу групи. Підгрупи

Lemma 14.2.1.

$$\langle G, \cdot \rangle, a \in G, \langle a \rangle - \text{скінченна} \Rightarrow \langle a \rangle \text{ н містить передпорядку}$$

Proof.

$$\langle a \rangle - \text{скінченна} \Rightarrow \exists m, s : s > m > 0. \\ a^s = a^m \Rightarrow a^s \cdot (a^m)^{-1} = e, a^{s-m} = e.$$

□

Definition 14.2.1. $\langle a \rangle$ - орбіта елемента a **Definition 14.2.2.** $\text{ord } G$

$$\text{Порядок групи} = |G|$$

Definition 14.2.3. $\text{ord } a$

$$\text{Порядок елементу} = |\langle a \rangle|$$

Якщо $\exists n \in \mathbb{N} : a^n = e$, то $\text{ord } a = \min\{n \mid a^n = e\}$, інакше $\text{ord } a = \infty$

Example:

$$\text{ord } e = 1, \quad \text{ord } a = 1 \Leftrightarrow a = e$$

Example:

$$\begin{aligned} \langle \mathbb{Z}, + \rangle : \text{ord } 0 = 1, \text{ord } 1 = \infty \\ \langle \mathbb{Z}_4, + \rangle : \text{ord } 0 = 1, \text{ord } 1 = 4, \text{ord } 2 = 2 \end{aligned}$$

Lemma 14.2.2.

Якщо $g \in G$ має скінченний порядок: $\text{ord } g^u = n < \infty$, то $g = e \Leftrightarrow u \vdots n$

Proof.

$$\Leftrightarrow u = k \cdot n \Rightarrow g^u = (g^n)^k = e^k = e$$

$$\Leftrightarrow \text{Нехай } u \vdots n \Rightarrow u = nq + r, 0 < r < n$$

$$e \cdot g^u = (g^n)^q \cdot g^r = e^q \cdot g^r = g^r \Rightarrow n - \text{не порядок } g - \text{Упс!}$$

□

Definition 14.2.4. Підгрупа

$$H \subseteq G - \text{підгрупа } G \Leftrightarrow H - \text{група}$$

- $\langle H, \cdot \rangle$ — замкненість
- асоціативність
- наявність e
- наявність обернених

Example:

$$\begin{aligned} \langle \mathbb{Z}, + \rangle : 2\mathbb{Z} - \text{підгрупа} \\ n\mathbb{Z} = \{nm \mid m \in \mathbb{Z}\} - \text{підгрупа} \\ 2\mathbb{Z} + 1 - \text{не підгрупа (не замкнена)} \\ \mathbb{Z}_n - \text{підгрупа } \mathbb{Z} \end{aligned}$$

Example:

$$SL_n(\mathbb{R}) \subseteq GL_n(\mathbb{R}), SL_n(\mathbb{R}) = \{M \in GL_n(\mathbb{R}) \mid \det M = 1\} - \text{спеціальна підгрупа}$$

Тривіальні підгрупи: $\{e\}$, G , інші підгрупи - власні

Proposition.

$$H \subseteq G - \Leftrightarrow \forall a, b \in H : a \cdot b^{-1} \in H$$

14.3 Класи суміжності, індекс підгрупи, теорема Лагранжа та наслідки з неї

Definition 14.3.1. Нехай $\langle G, \cdot \rangle$ - група, $H \subseteq G$ - підгрупа

Елементи g_1, g_2 - (ліво) конгурентні відносно H : $g_1 \equiv g_2 \pmod{H} \Leftrightarrow g_1^{-1} \cdot g_2 \in H \Leftrightarrow \Leftrightarrow \exists h \in H : g_2 = g_1 \cdot h, g_1 = g_2 \cdot h^{-1}$
(право) конгурентні $\longrightarrow g_1 \cdot g_2^{-1} \in H \exists h \in H : g_2 = h \cdot g_1$

Lemma 14.3.1.

$$\equiv \pmod{H} \leftarrow g_1 \underset{H}{\sim} g_2 \text{ (відношення еквівалентності на } G \text{)}$$

лівий клас суміжності $g \in G : gH = \{gh \mid h \in H\}$ правий : $Hg = \{hg \mid h \in H\}$
 $\Rightarrow G = \bigcup_{g \in G} gH$

Proposition. усі класи суміжності рівнопотужні

$$\forall g \in G \quad |gH| = |H|$$

Proof. Розглянемо відображення $fg : H \rightarrow gH$

$fg(x) = g \cdot x$ - сюр'єктивне за побудовою gH

- ін'єктивне: $x_1, x_2 \in H \quad fg(x_1) = fg(x_2), g \cdot x_1 = g \cdot x_2, x_1 = x_2$

$\Rightarrow fg$ - бієкція $\Rightarrow |gH| = |H|$

□

Definition 14.3.2.

Індекс підгрупи H у групі G : $[G : H] = \text{кількість різних класів суміжності}$

G - скінченна \Rightarrow індекс скінченний

G - не скінченна \Rightarrow що завгодно

Example:

$$[G : \{e\}] = |G|, [G : G] = 1, \langle \mathbb{Z}, + \rangle, H = n\mathbb{Z}, [\mathbb{Z} : n\mathbb{Z}] = n$$

Theorem 14.3.2 (Lagrange).

$$|G| = [G : H] \cdot |H|, \text{ якщо } G \text{ - скінченна}$$

Proof. $G = \bigcup_g |gH| = \# \text{ класів суміжності} \cdot |H| = [G : H] \cdot |H|$

□

Consequence. Нехай $|G| = n < \infty$

$$1. \forall H \text{ - підгрупа: } n \vdots |H|$$

$$2. \forall g \in G : n \vdots \text{ord } g$$

Proof. $\text{ord } g = |\langle g \rangle|$, $\langle g \rangle$ - підгрупа G

□

3. $\forall g \in G : g^n = e$

4. \forall група простого порядку є циклічною

Proof. $|G| = p$, $p \geq 2$ - просте, $\exists g \neq e \Rightarrow \text{ord } g \mid p$, $\text{ord } g \neq 1 \Rightarrow \text{ord } g = p \Rightarrow$
 $\Rightarrow |\langle g \rangle| = p \Rightarrow |\langle g \rangle| = G$

□

Theorem 14.3.3 (Sylow).

$|G| = n$, n - складене, $p^\alpha \mid n$, p - просте $\Rightarrow \exists H \subseteq G$ - підгрупа, $|H| = p^\alpha$

Theorem 14.3.4.

G - нециклічна скінченна абелева група, $|G| = n \Rightarrow \exists u \mid n$, $u < n : \forall g \in G : g^u = e$

Для $\langle \mathbb{Z}_m^*, \cdot \rangle$ число u визначається функцією Кармайкла $\lambda(m)$

15.1 Властивості циклічних груп та їх елементів

$$G = \langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$$

Генератор групи - довільне $g' \in G = \langle g' \rangle$

Lemma 15.1.1.

$\forall H \subseteq G$ - підгрупа: H - циклічна

Proof. H - тривіальна - то очевидно ($H = \{e\}$ - ок, $H = G$ - за умови)

H - не тривіальна $\Rightarrow \exists g^k \in H, g^k \neq e \Rightarrow H$ містить: $g^k : g^{-k} \Rightarrow \exists k > 0 : g^k \in H$

Нехай $s = \min\{k > 0 : g^k \in H\} \Rightarrow \langle g^k \rangle \subseteq H : ? \subseteq \langle g^k \rangle$

$$\forall t : g^t \in H \Rightarrow t \div s$$

Нехай $t \div s$, тоді $t = sq + r, 0 < r < s \Rightarrow g^r = g^{t-sq} = g^t \cdot (g^s)^{-q} \in H$ - Упс!

$$\Rightarrow t \div s \Rightarrow g^t = (g^s)^q \subseteq \langle g^s \rangle \Rightarrow H \subseteq \langle g^s \rangle$$

□

Lemma 15.1.2.

$$\text{ord } g^k = \frac{n}{\gcd(n, k)}, \text{ якщо } n = |G| < \infty$$

Proof. $\text{ord } g^k = \min\{U > 0 : (g^k)^U = e\} \Rightarrow ku \div n : \text{ord } g \Rightarrow ku \div n$. Нехай $d = \gcd(k, n)$

$$k = k_1 \cdot d \quad k_1 \cdot d \cdot u \div n$$

$$\gcd(k_1, n) = 1 \quad d \cdot u \div n$$

$$\Rightarrow \min u = \frac{n}{d} \Rightarrow \text{ord } g^k = \frac{n}{d} = \frac{n}{\gcd(n, k)}$$

□

Consequence.

Група G містить $\varphi(n)$ генераторів

Lemma 15.1.3.

Якщо $d = \gcd(n, k)$, то $\langle g^k \rangle = \langle g^d \rangle$

Proof. З одного боку, $k \div d \Rightarrow g^k = (g^d)^{\dots} \in \langle g^d \rangle \Rightarrow \langle g^k \rangle \subseteq \langle g^d \rangle$

З іншого боку, $\text{ord } g^k = |\langle g^k \rangle| = \frac{n}{d}, \text{ord } g^d = |\langle g^d \rangle| = \frac{n}{\gcd(n, d)} = \frac{n}{d} \Rightarrow$

$$\Rightarrow |\langle g^k \rangle| = |\langle g^d \rangle| \Rightarrow \langle g^k \rangle = \langle g^d \rangle$$

□

Consequence.

Усі підгрупи G однакового порядку співпадають

Proof. $|\langle g^k \rangle| = |\langle g^M \rangle| \Rightarrow \text{ord } g^k = \text{ord } g^M \Rightarrow \gcd(n, k) = \gcd(n, M) = d$

$$\Rightarrow \langle g^k \rangle = \langle g^d \rangle = \langle g^M \rangle$$

□

15.2 Структура циклічних груп

Proposition. $G = \langle g \rangle$, $|G| = n < \infty$

- $\forall d \mid n$:
- існує єдинна підгрупа індексу d
 - існує єдинна підгрупа порядку d
 - існує рівно $\varphi(d)$ елементів порядку d

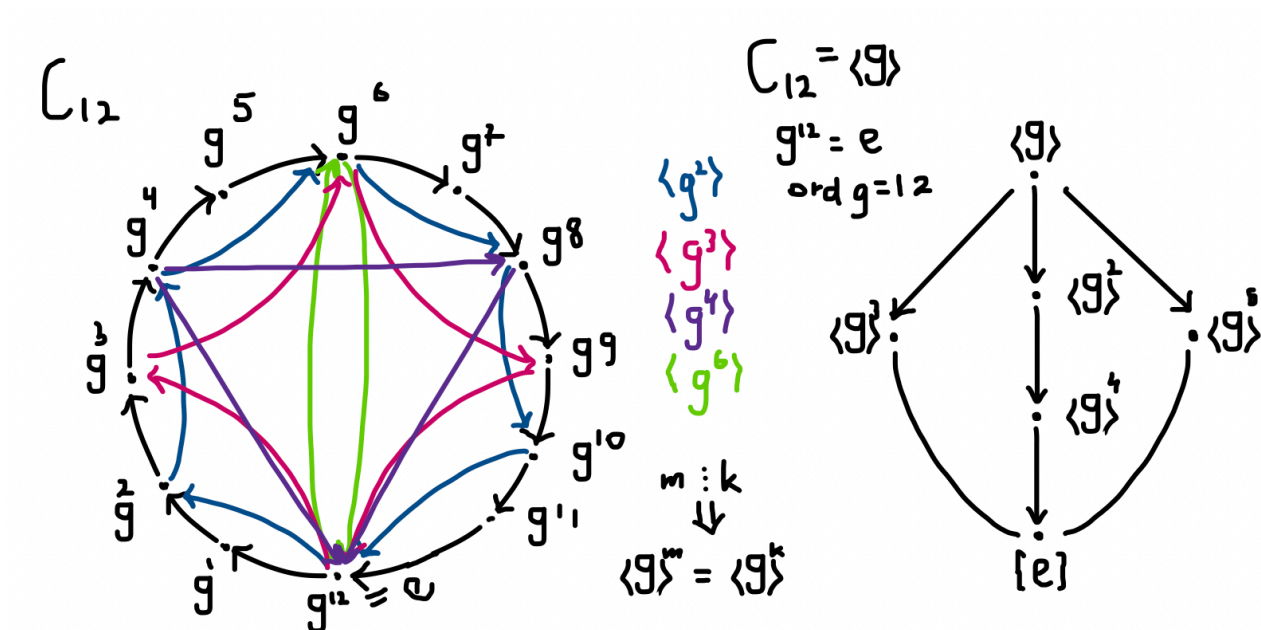
Proof.

1. $d \mid n \Rightarrow \langle g^d \rangle$ - підгрупа порядку $\frac{n}{d} \Rightarrow [G : \langle g^d \rangle] = \frac{n}{n/d} = d$
2. $d' = \frac{n}{d} : \mid \langle g^{d'} \rangle$ - підгрупа порядку d
3. елементи порядку d - генератори $\langle g^{d'} \rangle \Rightarrow \exists \varphi(d)$ генераторів

Consequence.

$$\sum_{d \mid n} \varphi(d) = n$$

□



15.3 Нормальні підгрупи

Definition 15.3.1. $H \triangleleft G$

$$H \subseteq G - \text{нормальна} \Leftrightarrow \forall g \in G, \forall h \in H : ghg^{-1} \in H$$

У абелевої групи усі підгрупи нормальні

Theorem 15.3.1 (equivalent conditions).

- (1) $H \triangleleft G$
- (2) $\forall g \in G : gHg^{-1} = H$
- (3) $\forall g \in G : gH = Hg$

Proof.

(1) \sim (2) за означенням : $gHg^{-1} \subseteq H : H? \subseteq gHg^{-1} : \forall h \in H : \exists h' \in H : h = gHg^{-1}$

Нехай $h' = g^{-1} \cdot h \cdot g \in H$ - з означення нормальності для g^{-1}

$$\text{Тоді } gh'g^{-1} = gg^{-1}hgg^{-1} = h$$

(2) \sim (3) $gHg^{-1} = H \Leftrightarrow gH = Hg$

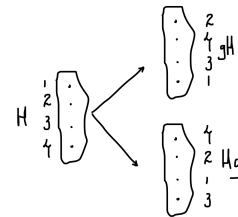
□

Введемо $G/H = \{gh \mid g \in G\}$ - множина усіх класів суміжності. $\langle G, \cdot \rangle \Rightarrow \langle G/H, \cdot \rangle$.

$$(g_1H) \cdot (g_2H) = (g_1g_2)H$$

$$fg(x) = gx$$

$$hg(x) = xg$$



15.4 Фактор-групи

Theorem 15.4.1.

Якщо $H \triangleleft G$, то $\langle G/H, \cdot \rangle$ - група (фактор-група)

Proof.

- замкненість - з побудови
- успадкування з $\langle G, \cdot \rangle$
- нейтральний елемент : $eH = H$
- обернений елемент : $(gH)^{-1} = (g^{-1})H$ де пастка?

$$\begin{array}{ccc} (g_1H) \cdot (g_2H) & = & (g_1g_2)H \\ \parallel & & \parallel \\ (a_1H) \cdot (a_2H) & = & (a_1a_2)H \end{array}$$

□

Appendices

APPENDIX A

Appendix

A.1 Подільність многочленів

$$1 + x + x^2 + x^3 + \dots + x^{n-1} = S(x)$$

$$1 + x(1 + x + x^2 + \dots + x^{n-2}) = 1 + x(s(x) - x^{n-1}) = S(x)$$

$$x^{n-1} = (X - 1)(x^{n-1} + x^{n-2} + \dots + x + 1)$$

A.2 Наслідок з подільності(теорема Безу)

$$x \rightarrow \frac{x}{y} : \quad \frac{x^n}{y^n} - 1 = \left(\frac{x}{y} - 1\right)\left(\frac{x^{n-1}}{y^{n-1}} + \frac{x^{n-2}}{y^{n-2}} + \dots + \frac{x}{y} + 1\right) \quad | \quad x \quad \cdot y^n$$

$$x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \dots + xy^{n-2} + y^{n-1})$$

$$\Rightarrow (x^n - y^n) : (x - y)$$

Поліном: $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, $a_n \in \mathbb{R}$, $a_n \neq 0$, $\deg p = n$

$$p(x) - p(y) = a_n(x^n - y^n) + a_{n-1}(x^{n-1} - y^{n-1}) + \dots + a_1(x - y) + a_0 \cdot 0$$

$$p(x) - p(y) : (x - y), \quad p(x) - p(y) = (x - y) \cdot Q(x, y), \quad Q(x, y) - \text{поліном від } x, y$$

Theorem (Безу).

$$p(x) - \text{поліном}, \forall \alpha - \text{число} \Rightarrow p(x) - p(\alpha) : (x - \alpha)$$

або

$$\forall \alpha - \text{число} \exists q(x) : p(x) = (x - \alpha) \cdot q(x) + p(\alpha), \quad \deg q = \deg p - 1$$

A.3 Наслідок з теореми Безу

1. якщо α - корінь $p(x)$, то $p(x) : (x - \alpha)$

$$p(\alpha) = 0 \Rightarrow p(x) = (x - \alpha) \cdot q(x) + p(\alpha) = (x - \alpha) \cdot q(x)$$

2. якщо $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{C}$ - усі корені з урахуванням кратності, то

$$p(x) = a_n(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$$

A.4 Теорема Вієта

$$\begin{aligned}
 x^n &: a_n = a_n \\
 x^{n-1} &: a_{n-1} = a_n(-\alpha_1 - \alpha_2 - \dots - \alpha_n) \Rightarrow \alpha_1 + \alpha_2 + \dots + \alpha_n = -\frac{a_{n-1}}{a_n} \\
 p(x) &= a_3x^3 + a_2x^2 + a_1x + a_0 = a_3(x - \alpha_1)(x - \alpha_2)(x - \alpha_3) = a_3(x^3 - \alpha_1x^2 - \\
 &\quad - \alpha_2x^2 - \alpha_3x^2 + \alpha_1\alpha_2x + \alpha_1\alpha_3x + \alpha_2\alpha_3x - \alpha_1\alpha_2\alpha_3) \\
 x^3 &: a_3 = a_3 \\
 x^2 &: a_2 = a_3(-\alpha_1 - \alpha_2 - \alpha_3) & x^k &: a_k = a_n \cdot (-1)^{n-k} \sum \alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_k} \\
 \Rightarrow x &: a_1 = a_3(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) & 1 \leq i_1 < i_2 < \dots < i_n \leq n \\
 x^0 = 1 &: a_0 = a_3(-\alpha_1\alpha_2\alpha_3) \\
 \Rightarrow \alpha_1 + \alpha_2 + \dots + \alpha_n &= -\frac{a_{n-1}}{a_n}, & \alpha_1\alpha_2 \dots \alpha_n &= (-1)^n \cdot \frac{a_0}{a_n}
 \end{aligned}$$

A.5 Схема Горнера

$$\begin{aligned}
 p(x) &= a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \\
 q(x) &= b_nx^n + b_{n-1}x^{n-1} + \dots + b_1x + b_0 \\
 p(x) &= (x - \alpha) \cdot q(x) + p(\alpha) = (x - \alpha)(b_{n-1}x^{n-1} + \dots + b_1x + b_0) + p(\alpha) = \\
 &= b_{n-1} \cdot x^n + b_{n-2} \cdot x^{n-1} + b_{n-3} \cdot x^{n-2} + \dots + b_1 \cdot x^2 + b_0 \cdot x \\
 &\quad - \alpha b_{n-1}x^{n-1} - \alpha b_{n-2}x^{n-2} - \dots - \alpha b_2x^2 - \alpha b_1x - \alpha b_0 + p(\alpha) = \\
 &= a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \dots + a_1x + a_0 \\
 a_n &= b_{n-1} & b_{n-1} &= a_n \\
 a_{n-1} &= b_{n-2} - \alpha \cdot b_{n-1} & b_{n-2}a_{n-1} + \alpha \cdot b_{n-1} \\
 a_{n-2} &= b_{n-3} - \alpha \cdot b_{n-2} & b_{n-3} = a_{n-2} + \alpha \cdot b_{n-2} \\
 \Rightarrow \vdots & & \vdots \\
 a_1 &= b_0 - \alpha b_1 & b_0 &= a_1 + \alpha b_1 \\
 a_0 &= p(\alpha) - \alpha b_0 & p(\alpha) &= a_0 + \alpha b_0
 \end{aligned}$$

	a_n	a_{n-1}	a_{n-2}	\dots	a_n	a_1	a_0
α	b_{n-1}	b_{n-2}	b_{n-3}	\dots	b_1	b_0	$p(\alpha)$
α_2	c_{n-2}	c_{n-3}	c_{n-4}	\dots	c_0	$q(\alpha_2)$	

/ *

Задача схеми Горнера - поділити многочлен на $(x - \alpha)$, не обчислюючи усі степені α . Ефективніший за ділення у стовпчик - простий (лише 1 "+" та 1 "x" на одну клітинку) та швидкий (один цикл for + перекладання з одного масиву у інший)

*/

A.6 Ланцюгові дроби

$$\begin{aligned}
 \alpha \in \mathbb{R}: \quad \alpha &= a_1 + a_0, \quad a_i \in \mathbb{Z}, \quad 0 \leq \alpha_1 < 1 \\
 \alpha &= a_1 + \frac{1}{\frac{1}{\alpha_1}} = a_1 + \frac{1}{\frac{1}{a_2}} = a_1 + \frac{1}{a_2 + \frac{1}{\frac{1}{\alpha_2}}} = a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \alpha_3}} = \dots
 \end{aligned}$$

Ланцюговий дріб α - представлення α у вигляді $a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{a_4 + \dots}}}$: $\alpha = [a_1; a_2, a_3, a_4, \dots]$,

$a_1 \in \mathbb{Z}$, $a_i \in \mathbb{N}_0$

А.7 Чим більше знаємо дробів - тим точніше α

$$\alpha = a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{a_4 + \frac{1}{a_5 + \dots}}}}$$

А.8 Кожен скінченний дріб описує одне раціональне число

Proposition.

$$\alpha \in \mathbb{Q}, \alpha = \frac{m}{n} \Leftrightarrow \alpha \text{ має скінченний ланцюговий дріб}$$

Proof.

$$\Leftrightarrow [a_1; a_2, a_3, \dots, a_t] = a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{\ddots + \frac{1}{a_{t-1} + \frac{1}{a_t}}}}} = \dots = \frac{m}{n}$$

\Rightarrow (Алгоритм Евкліда!)

$$\alpha = \frac{m}{n} = \frac{r_0}{r_1} = \frac{r_1 q_1 + r_2}{r_1} = q_1 + \frac{r_2}{r_1} = q_1 + \frac{1}{\frac{r_1}{r_2}} = q_1 + \frac{1}{q_2 + \frac{r_3}{r_2}} = \dots =$$

$$= q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{1}{\ddots + \frac{1}{q_n}}}} \Rightarrow \alpha = [q_1; q_2, q_3, \dots, q_n]$$

□

/ *

\Leftarrow Усі a_i - цілі, невід'ємні (нулі лише для ірраціональних випадків), крім a_1 - воно може бути від'ємним, цілим. (тому ми його відділяємо;)

\Rightarrow Алгоритм Евкліда скінченний, тому фокус такий.

*/

A.9 Наближення числа π

$$\begin{array}{lcl}
 \frac{22}{7} \approx \pi : & \begin{array}{rcl} 22 & = & \boxed{3} \cdot 7 + 1 \\ 7 & = & \boxed{7} \cdot 1 + 0 \end{array} & \Rightarrow & \frac{22}{7} = 3 + \frac{1}{7} \\
 \\
 \frac{25}{7} : & \begin{array}{rcl} 25 & = & \boxed{3} \cdot 7 + 4 \\ 7 & = & \boxed{1} \cdot 4 + 3 \\ 4 & = & \boxed{1} \cdot 3 + 1 \\ 3 & = & \boxed{3} \cdot 1 + 0 \end{array} & \Rightarrow & \begin{array}{l} \frac{25}{7} = 3 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{3}}}} = 3 + \frac{1}{1 + \frac{4}{3}} = \\ = 3 + \frac{1}{\frac{7}{4}} = \frac{25}{7} \end{array}
 \end{array}$$