

Дискретна математика 2

Лекция начинается

-Сегодня у нас клуб упоротых любителей математики.

Contents

1	Лекція 1	3
1.1	Подільність чисел	3
1.2	Найбільший спільний дільник	4
1.3	Алгоритм Евкліда	5
2	Лекція 2	7
2.1	Найменше спільне кратне	7
2.2	Евклідові послідовності	8
3	Лекція 3	10
3.1	Розширений алгоритм Евкліда	10
3.2	Лінійні діафантові рівняння	11
4	Лекція 4	14
4.1	Прості числа	14
4.2	Розподіл простих чисел	15
4.3	Основна теорема арифметики	16
5	Лекція 5	18
5.1	Мультиплікативні функції	18
5.2	Кількість та сума дільників	19
5.3	Досконалі числа	20
5.4	Функція Мебіуса	21
6	Лекція 6	23
6.1	Порівняння за модулем	23
6.2	Степені за модулем	24
6.3	Обернені елементи за модулем	25
7	Лекція 7	26
7.1	Китайська теорема про остачі	26
7.2	Функція Ойлера	27
7.3	Теорема Ойлера та мала теорема Ферма	28

8	Лекція 8	29
8.1	Функція Кармайкла	29
9	Лекція 9	31
9.1	Системи числення	31

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 — $a \dot{:} b$ або b ділить a (b є дільником) $b | a$.

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

Property.

1. $a \neq 0, a \dot{:} 0$

2. $a \neq 0, 0 \dot{:} a$

3. $a \dot{:} b, b \dot{:} c \Rightarrow a \dot{:} c$

4. $a \dot{:} 1$

5. $a \dot{:} c, b \dot{:} c \Rightarrow (\alpha a \pm \beta b) \dot{:} c$

6. $a \dot{:} b \Leftrightarrow ac \dot{:} bc, c > 0$

Theorem 1.1.1 (про ділення з остачею).

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

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

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

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

□

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

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

□

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

Theorem 2.1.3.

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

Решітка(*lattice*) - $< A, \leq, \sup, \inf >$

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. $\mathbb{N}, \mid, \text{lcm}, \gcd$
 $a \cdot b = \text{lcm}(a, b) \cdot \gcd(a, b)$

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

2.2 ЕВКЛІДОВІ ПОСЛІДОВНОСТІ

Definition 2.2.1. Послідовність $a_0, a_1, \dots, a_i \in \mathbb{R}$ - евклідова, якщо $\forall n, m \in \mathbb{N}_0 \quad n > m : \gcd(a_n, a_m) = \gcd(a_m, a_{n-m}) \Rightarrow \gcd(a_n, a_m) = \gcd(a_m, a_{n \bmod m})$

Theorem 2.2.1.

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

Proof.

$n = m$ - очевидна.

$n > m$:

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

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

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

$a_{r_t} = a_0$ □

Consequence.

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

Example:

$$a_k = k$$

Example:

$$a_k = 2^k - 1$$

$$\gcd(a_n, a_m) \stackrel{?}{=} \gcd(a_m, a_{n-m})$$

$$a_n = 2^n - 1 = 2^n - 2^m - 1 = 2^m(2^{n-m} - 1) + (2^m - 1) = 2^m \cdot a_{n-m} + a_m = a_n$$

$$\gcd(2^n - 1, 2^m - 1) = 2^{\gcd(n, m)} - 1$$

Example:

$$a_k = \alpha^k - 1, \alpha \in \mathbb{N}, \alpha \geq 2$$

$$a_0 = 0, a_1 = \alpha - 1 \neq 1$$

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 (Лема Безу).

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

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

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

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

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

$$\begin{aligned} \text{Тоді } d = r_n &= r_{n-2} - r_{n-1} q_{n-1} = r_{n-2} - q_{n-1} (r_{n-3} - r_{n-2} q_{n-2}) = \dots = \\ &= u \cdot r_0 + v \cdot r_1 \end{aligned}$$

□

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. $\forall i : u_i, v_i \in \mathbb{Z} \quad r_i = au_i + bv_i \Rightarrow u_0 = 1, v_0 = 0, u_1 = 0, v_1 = 1$
$$u_{i+1} = u_{i-1} - u_i q_i, \quad v_{i+1} = v_{i-1} - v_i q_i, \quad r_{i+1} = r_{i-1} - q_i r_i = (au_{i-1} + bv_{i-1}) - q_i(au_i + bv_i) = a \underbrace{(u_{i-1} - q_i u_i)}_{u_{i+1}} + b \underbrace{(v_{i-1} - q_i v_i)}_{v_{i+1}}$$

Example:

$$\begin{aligned}
& \gcd(123, 456). \\
123 &= 456 \cdot 0 + 123 \\
456 &= 3 \cdot 123 + 87 & q_1 &= 3 \\
123 &= 87 \cdot 1 + 36 & q_2 &= 1 \\
87 &= 36 \cdot 2 + 15 & q_3 &= 2 \\
36 &= 15 \cdot 2 + 6 & q_4 &= 2 \\
15 &= 6 \cdot 2 + 3 & q_5 &= 2 \\
6 &= 3 \cdot 2 & q_6 &= 2 \Rightarrow \gcd = 3
\end{aligned}$$

		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.

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

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

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

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

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

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

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

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

□

3.2 Лінійні діафантові рівняння

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

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

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

Theorem 3.2.1.

Нехай $ax + by = c$ $d = \gcd(a, b)$

1. рівняння має розв'язки $\Leftrightarrow c : d$

2. $a = a_0 \cdot d$, $b = b_0 \cdot d$, $c = c_0 \cdot d$, (x_0, y_0) - 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. Якщо $c : d$, але $ax + by : d$ то Упс!

Якщо $c : d$, то $a_0x + b_0y = c_0$ - еквівалентне рівняння

$1 = a_0u + b_0v \Rightarrow x_0 = u \cdot c_0$, $y_0v \cdot c_0$ - 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

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

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

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

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

$$\Rightarrow y - y_0 = a_0t$$

□

Example:

$$15x + 9y = 27$$

$$15 = 9 \cdot 1$$

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

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

$$27 : 3 \Rightarrow \text{розв'язки існують}$$

$$5x + 3y = 9$$

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

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

$$\begin{cases} x = -9 + 3 \cdot t \\ y = 18 - 5 \cdot t \end{cases}$$

$$t = 10 : \quad x = -9 + 30 = 21, \quad y = 18 - 50 = -32$$

$$\left| \begin{array}{l} 5 \cdot 21 - 3 \cdot 32 = 105 - 96 = 9 \\ ?t : \quad x > 0, y > 0 \\ \begin{cases} -9 + 3t > 0 \\ 18 - 5t > 0 \end{cases} \Rightarrow \begin{cases} t > 3 \\ t < 3,6 \end{cases} \end{array} \right|$$

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

$n \in \mathbb{N}$ - *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 (Евклід).

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

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.

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

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.

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

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 $< x$.

$$\frac{1}{2} \cdot \frac{x}{\log_2 x} \leq \Pi(x) \leq 5 \cdot \frac{x}{\log_2 x} \rightarrow \alpha \cdot \frac{x}{\ln x} \leq \Pi(x) \leq \beta \cdot \frac{x}{\ln x}, \quad \alpha = 0.92129, \quad \beta = 1.10555$$

Theorem 4.2.3 (Адамер, Вале).

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

Theorem 4.2.4 (Діріхле).

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 $a \not\vdots p \Rightarrow \gcd(a, p) = 1 \Rightarrow$

$$\Rightarrow \exists u, v, \quad au + pv = 1 \Rightarrow \underbrace{ab}_{\vdots p} \cdot u + \underbrace{p}_{\vdots p} \cdot bv = \underbrace{b}_{\vdots p}$$

□

Theorem 4.3.2 (основна теорема арифметики).

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

Proof.

1. Існування

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

□

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. $d \mid n \Rightarrow d = q_1^{\beta_1} q_2^{\beta_2} \dots q_t^{\beta_t}$, $0 \leq \beta_i \leq \alpha_i$
2. $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$, $\alpha_i \geq 0$, $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_t^{\beta_t}$, $\beta_i \geq 0$
 $\gcd(a, b) = \prod_{i=1}^t p_i^{\min\{\alpha_i, \beta_i\}}$, $\text{lcm}(a, b) = \prod_{i=1}^t p_i^{\max\{\alpha_i, \beta_i\}}$
3. $a : b$, $a : c$, $\gcd(b, c) = 1 \Rightarrow a : (b \cdot c)$

CHAPTER 5

Лекція 5

5.1 Мультиплікативні функції

$f(n)$ - 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 взаємнопрости, 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 5.1.1. $f(n)$ - мультиплікативна. Числовий інтеграл $g(n) = \sum_{d|n} f(d)$

Theorem 5.1.1 (S).

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

Proof.

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

$$\begin{aligned} g(n) &= \sum_{d \mid n} f(d) = \sum_{\beta_1=0}^{\alpha_1} \sum_{\beta_2=0}^{\alpha_2} \dots \sum_{\beta_t=0}^{\alpha_t} f(p_1^{\beta_1} \dots p_t^{\beta_t}) = \\ &= \sum_{\beta_1} \dots \sum_{\beta_t} \prod_i f(p_i^{\beta_i}) = \prod_{i=1}^t \sum_{\beta_i=0}^{\alpha_i} f(p_i^{\beta_i}) \end{aligned}$$

□

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

5.2 Кількість та сума дільників

$$\text{Кількість дільників } \tau(n) = \sum_{d \mid n} 1$$

$$\text{Сума дільників } \sigma(n) = \sum_{d \mid n} d$$

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.

$$1. \tau(n) \leq 2\sqrt{n}$$

$$n : d \Rightarrow n = d \cdot d'$$

$$\sigma(n) \geq n + 1$$

$$2. \tau(n) - \text{непарне} \Leftrightarrow n = m^2$$

$$3. \sigma - \text{непарне} \Leftrightarrow \begin{cases} m^2 \\ 2m^2 \end{cases}$$

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 (Евклід-Ойлер).

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

Proof.

$$1. n = 2^{p-1} \cdot M_p, \quad p > 2$$

$$\sigma(n) = \sigma(2^{p-1} \cdot M_p) = \sigma(2^{p-1})\sigma(M_p) = (2^p - 1)(M_p + 1) = 2^p(2^p - 1) = n$$

$$2. \text{ Нехай } n - \text{парне досконале, } n = 2^k \cdot b, \quad b - \text{непарне}$$

$$\sigma(n) = \sigma(2^k \cdot b) = (2^k - 1) \cdot \sigma(b) = 2^k \cdot b = 2n \Rightarrow$$

$$\Rightarrow b : (2^k - 1), \quad b = (2^k - 1) \cdot c \quad (2^k - 1)\sigma(b) = 2^k(2^k - 1) \cdot c$$

$$\sigma(b) = 2^k \cdot c = (2^k - 1 + 1) \cdot c = b + c$$

$$b : c, \quad c \neq 1, \quad c \neq b \Rightarrow \sigma(b) > 1 + b + c \Rightarrow c = 1.$$

$$b = 2^k - 1, \quad \sigma(b) = b + 1 \Rightarrow b - \text{просте. } n = 2^{k-1} \underbrace{(2^k - 1)}_{\text{просте}}$$

□

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).

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

Proof.

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

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

□

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.

$$\begin{aligned} \text{За теоремою 5.1.1 } \sum_{\beta} \mu(p_1^\beta) f(p_1^\beta) &= \mu(1) f(1) + \mu(p_1) f(p_1) + \\ &+ \mu(p_1^2) f(p_1^2) + \dots = 1 + (-1) f(p_1) = 1 - f(p_1) \end{aligned}$$

□

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.

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

□

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 порівнювані за $\bmod n$:

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

Property.

1. $a \equiv a \pmod{n}$, $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$,
 $a \equiv b \pmod{n}$, $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$
2. $a \equiv b \pmod{n}$, $c \equiv d \pmod{n} \Rightarrow$
 $\Rightarrow a \pm c \equiv b \pm d \pmod{n}$, $ac \equiv bd \pmod{n}$

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

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

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

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

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

$$\text{Proof. } a = b + nt, \quad a_1d = b_1d + n_1dt \quad \square$$

$$5. a \equiv b \pmod{n}, n \mid d \Rightarrow a \equiv b \pmod{d}$$

$$6. a \equiv b \pmod{n_1},$$

$$a \equiv b \pmod{n_2},$$

$$\vdots$$

$$a \equiv b \pmod{n_t},$$

$$a \equiv b \pmod{\text{lcm}(n_1, \dots, n_t)}$$

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

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.

$$\text{Нехай } ax_1 + b \equiv ax_2 + b \pmod{n}, ax_1 \equiv ax_2 \pmod{n}, x_1 = x_2 \pmod{n} \quad \square$$

Example:

$$x^6 = \overset{3 \cdot 5 \cdot 7}{105}y + 5$$

mod 3

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

$$\Rightarrow x^2 \pmod{3} \neq 2, x^6 = (x^3)^2 \equiv 2 \pmod{3}$$

Example:

$$x^6 = \overset{3 \cdot 5 \cdot 7}{105}y + 4$$

$$\begin{array}{c|c|c|c|c|c} \text{mod } 5 & x & 0 & 1 & -1 & 2 & -2 \\ \hline & x^2 & 0 & 1 & 1 & -1 & -1 \\ \hline & x^3 & 0 & 1 & -1 & -2 & 2 \end{array} \Rightarrow \begin{array}{l} x^2 \bmod 5 \in \{0, \pm 1\}, x^6 = (x^3)^2 \equiv -1 \pmod{5} \\ x^2 = 5k + 4 = 5k - 1 \Rightarrow x = 5t \pm 2 \end{array}$$

$$\begin{array}{c|c|c|c|c|c|c|c} \text{mod } 7 & x & 0 & 1 & -1 & 2 & -2 & 3 & -3 \\ \hline & x^2 & 0 & 1 & 1 & -3 & -3 & 2 & 2 \\ \hline & x^3 & 0 & 1 & -1 & 1 & -1 & -1 & 1 \end{array} \Rightarrow \begin{array}{l} x^2 \bmod 7 \in \{0, 1, 2, 4\} \\ \underline{x^3 \bmod 7 \in \{0, \pm 1\}} \end{array}$$

$$\begin{array}{c|c|c|c|c|c|c} \text{mod } 6 & x & 0 & 1 & -1 & 2 & -2 & 3 \\ \hline & x^2 & 0 & 1 & 1 & -2 & -2 & 3 \\ \hline & x^3 & 0 & 1 & -1 & 2 & -2 & 3 \end{array} \Rightarrow \begin{array}{l} x^2 \bmod 7 \in \{0, 1, 2, 4\} \\ \underline{x^3 \bmod 7 \in \{0, \pm 1\}} \end{array}$$

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 с-ма лишків (мультиплікативна 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 (КТО).

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

Proof.

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

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

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

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

Повторюємо для $n_1 n_2$ та n_3 , $n_1 n_2 n_3$ та $n_4 \dots$

3. $N = n_1 n_2 \dots n_t$, $N_i = \frac{N}{n_i}$, $M_i = N_i^{-1} \pmod{n_i}$
 $x_0 = (b_1 N_1 M_1 + b_2 N_2 M_2 + \dots + b_t N_t M_t) \pmod{N}$ - розв'язок
 $x_0 \pmod{n_1} \equiv b_1 N_1 M_1 \pmod{n_1} \equiv b_1 N_1 N_1^{-1} \pmod{n_1} = b_1 \pmod{n_1}$

□

Example:

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

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

7.2 Функція Ойлера

Definition 7.2.1.

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

Proposition.

$\varphi(n)$ - мультиплікативна.

Proof.

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

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

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

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

□

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

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

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

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.

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

$$N_d = \#x : \gcd(x, n) = d, x = x_1 \cdot d, n = n_1 \cdot d, \gcd(x_1, n_1) = 1 \Rightarrow \\ \Rightarrow N_\alpha = \varphi(n_1) = \varphi\left(\frac{n}{d}\right) \Rightarrow n = \sum_{d|n} N_d = \sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{d|n} \varphi(d) \quad \square$$

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

7.3 Теорема Ойлера та мала теорема Ферма

Theorem 7.3.1 (Ойлер).

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

Proof.

$$\forall a \in \mathbb{Z}_n^* : a\mathbb{Z}_n^* = \mathbb{Z}_n^* \text{ якщо } x \text{ пробігає усі значення } \mathbb{Z}_n^*, \text{ то } ax \text{ також пробігає } \mathbb{Z}_n^* \\ ax \equiv ay \pmod{n} \Rightarrow x \equiv y \pmod{n} \\ \mathbb{Z}_n^* = \{b_1, b_2, \dots, b_{\varphi(n)}\} = \{ab_1, ab_2, \dots, ab_{\varphi(n)}\} \Rightarrow \\ \Rightarrow \cancel{b_1} \cancel{b_2} \dots \cancel{b_{\varphi(n)}} \equiv a \cancel{b_1} \cdot a \cancel{b_2} \dots a \cancel{b_{\varphi(n)}} 1 \equiv a^{\varphi(n)} \pmod{n} \quad \square$$

Consequence. $n = p$

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

Theorem 7.3.2 (Мала теорема Ферма).

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

Proof.

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

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.

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

Proof.

Доведення буде пізніше \square

Consequence.

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

Theorem 8.1.3 (Кармайкл).

1. $n = p$

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

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.

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

□

Example:

$$\begin{aligned} n &= 35 = 5 \cdot 7 \\ \varphi(35) &= 4 \cdot 5 = 24 \quad \lambda(35) = \text{lcm}(4, 6) = 12 \end{aligned}$$

Example:

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

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:

$$70 \text{ y } B = 3$$

$$70 = 23 \cdot 3 + 1$$

$$23 = 7 \cdot 3 + 2$$

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

$$2 = 0 \cdot 3 + 2$$

$$70 = \overline{2121}_3$$