Дискретна математика 2

Лекция начинается

-Сегодня у нас клуб уопоротых любителей математики.

Contents

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 – $a \vdots b$ або b ділить a(b є дільникома) $b|a$.*
$a \vdots b \Leftrightarrow \exists k \in \mathbb{Z} : \ \ a = kb$

Property.

1. $a \neq 0, \ \ a \vdots 0$
2. $a \neq 0, \ \ 0 \vdots a$
3. $a \vdots b, \ b \vdots c \Rightarrow a \vdots c$
4. $a \vdots 1$
5. $a \vdots c, \ b \vdots c \Rightarrow (\alpha a \pm \beta b) \vdots c$
6. $a \vdots b \Leftrightarrow ac \vdots bc, \ c > 0$

Theorem 1.1.1 (про ділення з остачею)**.**

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

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

$\square$

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

1.2 Найбільший спільний дільник

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

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

1. $a \vdots d,\ b \vdots d$
2. $d\ -\ \max$ *додатне число, яке задовільняє 1.*

Property.

1. $\gcd(a,\ b) = b \Leftrightarrow a \vdots b$
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 $d > d'$
$a \vdots d,\ b \vdots d \Rightarrow (a-b) \vdots d \Rightarrow d$ - спільний дільник b та a-b $\Rightarrow d' \vdots d$ - Упс!
Нехай $d < d'$
$b \vdots d',\ a-b \Rightarrow b + (a-b) = a \vdots d'$ - Упс! ☐

Consequence. $a \geq b:\ \ \gcd(a,\ b) = (b,\ a \mod b)$

Proof. $a = bq + r$
$\gcd(a,\ b)\underbrace{= \cdots =}_{q \text{ разів}}\gcd(r,\ b)$ ☐

1.3 Алгоритм Евкліда

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

$$\begin{aligned}
&r_0 := a,\ r_1 := b \\
&r_0 = r_1 q_1 + r_2 \\
&r_1 = r_2 q_2 + r_3 \\
&r_2 = r_3 q_3 + r_4 \\
&\quad\vdots \\
&r_{n-1} = r_n q_n,\ \ r_n = d
\end{aligned}$$

Proof. $r_{i+1} = r_i \mod r_{i-1}$
$r_0 \geq r_1 > r_2 > \cdots > r_n > r_{n+1} = 0$
$\gcd(a,\ b) - \gcd(r_0,\ r_1) = \gcd(r_1,\ r_2) = \gcd(r_2,\ r_3) = \cdots =$
$= gcd(r_{n-1},\ r_n) = \gcd(r_n,\ 0) = 0$ ☐

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:**
> $\gcd(123,\ 456)$.
> $123 = 456 \cdot 0 + 123$

$456 = 3 \cdot 123 + 87$
$123 = 87 \cdot 1 + 36$
$87 = 36 \cdot 2 + 15$
$36 = 15 \cdot 2 + 6$
$15 = 6 \cdot 2 + 3$
$6 = 3 \cdot 2 \Rightarrow \text{gcd} = 3$

Example:

Для яких n : $\frac{3n+1}{5n+1}$ - скоротний?
$5n + 2 = (3n + 1) \cdot 1 + (2n + 1)$
$3n + 1 = (2n + 1) \cdot 1 + n$
$2n + 1 = n \cdot 2 + 1$
$n = 1 \cdot n \Rightarrow \text{gcd}(3n + 1,\ 5n + 2) = 1$

Chapter 2

Лекція 2

2.1 Найменше спільне кратне

Definition 2.1.1. $a,\ b \in \mathbb{N}$
M = НСК(a, b), lcm(a, b), [a, b]

1. $M \vdots a,\ \ M \vdots b$
2. $M\ -\ \min$ *таке число*

Property.

1. $\operatorname{lcm}(a,\ 0)$ - *'на доске был нарисован грустный смайлик'*
2. $\operatorname{lcm}(a,\ b) = a \Leftrightarrow a \vdots b$
3. $a,\ b$ *-взаємнопрості* $\Rightarrow \operatorname{lcm}(a,\ b) = a \cdot b$
4. *Довільне спільне кратне a та b* $\vdots \operatorname{lcm}(a,\ b)$
5. $\forall c > 0,\ \operatorname{lcm}(ac,\ bc) = c \operatorname{lcm}(a,\ b)$
6. $\frac{\operatorname{lcm}(a,\ b)}{a}$ *та* $\frac{\operatorname{lcm}(a,\ b)}{b}$ *- взаємнопрості*

Theorem 2.1.1.

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

Proof. Нехай $d = \gcd(a,\ b),\ a = a_1 \cdot d,\ b = b_1 \cdot d.$
$\gcd(a_1,\ b_1) = 1,\ \operatorname{lcm}(a_1,\ b_1) = a_{,1} \cdot b_1,\ \operatorname{lcm}(a,\ b) = d \cdot a_1 \cdot b_1$
$d \cdot \operatorname{lcm}(a,\ b) = (a_1 \cdot d) \cdot (b_1 \cdot d) = a \cdot b$ □

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. $d = \gcd(a,\ b,\ c)$
$d' = \gcd(a,\ b) \Rightarrow d' \vdots\, d,\ c \vdots\, d \Rightarrow d = \gcd(c,\ d')$ □

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

Theorem 2.1.3.

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

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. $\mathbb{N},\ \vdots\,,\ \operatorname{lcm},\ \gcd$
   $a \cdot b = \operatorname{lcm}(a,\underline{\ }) \cdot \gcd(a,\ b)$

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

2.2 Евклідові послідовності

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

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.

$n > m:$

$d = \gcd(n,\ m,)$ AE породжує послідовність $r_0,\ r_1,\ \ldots, r_t$, де $r_0 = n$, $r_1 = m,\ r_t = d,\ r_{t+1} = 0,\ r_{i+1} = r_{i-1} \mod r_i$

$\gcd(a_n, a_m) = \gcd(a_{r_0}, a_{r_1} = \gcd(a_n, a_m) = \gcd(a_{r_1}, a_{r_2} = \cdots = \gcd(a_{t_0}, a_{t_{i+1}}) = a_{r_t} = a_0$ □

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

Example:

$a_k = k$

Example:

$a_k = 2_k - 1$

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

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

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

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.
$r_0 = r_1 q_1 + r_2$
$r_1 = r_2 q_2 + r_3$
$r_2 = r_4 q_4 + r_5$
$\vdots$
$r_{n-3} = r_{n-2} q_{n-2} + r_{n-1}$
$r_{n-2} = r_{n-1} q_{n-1} + r_n$
$r_{n-1} = r_n q_n$
Тоді $d = r_n = r_{n-2} - r_{n-1} q_{n-1} = r_{n-2} - q_{n-1}(r_{n-3} - r_{n-2} q_{n-2}) = \cdots =$
$= u \cdot r_0 + v \cdot r_1$ □

Consequence.

1. $d = au + bv \Rightarrow$ *одне з чисел* $u,\ v$ *- недодатне, а інше - невід'ємне.*
2. $d = \gcd(x1, x_2, \ldots, x_k) \Rightarrow a_1, a_2, \ldots, a_k \in \mathbb{Z} :\ d = a_1 x_1 + a_2 + x_2 + \cdots + a_k x_k$
3. $\forall i :\ \ u_i,\ v_i \in \mathbb{Z}\ \ r_i = au_i + bv_i \Rightarrow u_0 = 1,\ v_0 = 0,\ u_1 = 0,\ v_1 = 1$
   $u_{i+1} = u_{i-1} - u_i q_i,\ v_{i+1} = v_{i-1} - v_i q_i,\ r_{i+1} = r_{i-1} - q_i r_i = (au_{i-1} + bv_{i-1}) -$
   $- q_i(au_i + bv_i) = a\underbrace{(u_{i-1} - q_i u_i)}_{u_{i+1}} + b\underbrace{(v_{i-1} - q_i v_i)}_{vi+1}$

Example:
$\gcd(123,\ 456)$.
$123 = 456 \cdot 0 + 123$
$456 = 3 \cdot 123 + 87 \qquad q_1 = 3$
$123 = 87 \cdot 1 + 36 \qquad q_2 = 1$

$87 = 36 \cdot 2 + 15 \qquad q_3 = 2$
$36 = 15 \cdot 2 + 6 \qquad q_4 = 2$
$15 = 6 \cdot 2 + 3 \qquad q_5 = 2$
$6 = 3 \cdot 2 \qquad q_6 = 2 \Rightarrow \gcd = 3$

		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.

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

Proof.

1. $C = \{au + bv \mid u, v \in \mathbb{Z}\}$
   $d' = \min\{d' > 0\}, \ d \in C$ тоді $\forall d \in C: \ c \vdots d'$
   Нехай $c' = au' + bv', \ c' \vdots d'$, тоді $c = q'd' + r', \ 0 < r' < d'$
   $r' = c' - q'd' = (au' + bv') - q'(au'_\alpha + bv'_\alpha) =$
   $= a(u' = -q'u'_\alpha) + b(v' - q'v'_\alpha)$ - Упс!

2. $d = au + bv = \gcd(a, b) \Rightarrow d \vdots d'$
   $a = a \cdot 1 + b \cdot 0 \Rightarrow a \vdots d', \ \ b = a \cdot 0 + b \cdot 1 \Rightarrow b \ \cdots \ d'$
   $\Rightarrow d'$ - спільний дільник a та $b \Rightarrow d' = au'_\alpha + bv'_\alpha \vdots d \Rightarrow d = d'$

□

3.2 Лінійні діафантові рівняння

Definition 3.2.1. $f(x_1, x_2, \ldots, x_n) = 0, \ x_i \in \mathbb{Z}$
$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c, \ a_i \in \mathbb{Z}, \ c \in \mathbb{Z}$
$ax + by = c, \ \ a, b, c \in \mathbb{Z}$ - *коефіцієнти,* $x, y \in \mathbb{Z}$ - *невідомі.*

Theorem 3.2.1.

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

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

2. *$a = a_0 \cdot d,\ b = b_0 \cdot d,\ c = c_0 \cdot d,\ (x_0,\ y_0)$ - 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 $c \not\vdots\, d$, але $ax + by \vdots\, d$ то Упс!
   Якщо $c \vdots\, d$, то $a_0x + b_0y = c_0$ - еквівалентне рівняння
   $1 = a_ou + b_0v \Rightarrow x_0 = u \cdot c_0,\ y_0v \cdot c_0$ - розв'язки.
2. $ax + by = a(x_0 + b_0t) + b(y_0 - a_0t) = \underbrace{(ax_0 + by_0)}_{=c} + \underbrace{(ab_0t - ba_0t)}_{a_0b_0dt - a_ob_0dt} = c$

Нехай $(x,\ y)$ - розв'язок рівняння
$ax + by = 0,\ ax_0 + by_0 = c \Rightarrow a(x - x_0) + b(y - y_0) = 0 \Rightarrow$
$\Rightarrow a_0(x - x_0) + b_0(y - y_0) = 0\ \gcd(a_0,\ b_0) = 1 \Rightarrow 1 = a_0u + b_0v \Rightarrow$
$\Rightarrow 0 = \underbrace{a_0u}_{=(1-b_0v)}(x - x_0) + b_0v(y - y_0) = (x - x_0) + b_0(u(y - y_0) - v(x - x_0)) \Rightarrow$
$\Rightarrow x - x_0 \vdots\, b_0,\ x - x_0 = b_0 \cdot t,\ t \in \mathbb{Z} \Rightarrow a_0 \cdot b_0t + b_0(y - y_0) = 0 \Rightarrow$
$\Rightarrow y - y_0 = a_0t$ □

> **Example:**
> $15x + 9y = 27$
> $15 = 9 \cdot 1$
> $9 = 6 \cdot 1 + 3$
> $6 = 3 \cdot 2 \Rightarrow 3 = 15 \cdot (-1) + 9 \cdot 2$
> $27 \vdots\, 3 \Rightarrow$ розв'язки існують
> $5x + 3y = 9$
> $1 = 5 \cdot (-1) + 3 \cdot 2$
> $x_0 = 9,\ y_0 = 18$
> $\begin{cases} x = -9 + 3 \cdot t \\ y = 18 - 5 \cdot t \end{cases} \quad t = 10 : \qquad x = -9 + 30 = 21,\ y = 18 - 50 = -32$
> $5 \cdot 21 - 3 \cdot 32 = 105 - 96 = 9$
> $?t : \qquad x > 0,\ y > 0$
> $\begin{cases} -9 + 3t > 0 \\ 18 - 5t > 0 \end{cases} \Rightarrow \begin{cases} t > 3 \\ t < 3,6 \end{cases}$

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*
$n \in \mathbb{N}$ - складене $\Leftrightarrow \exists a: \ 1 < a < n \quad n \vdots a$

1 - не просте, не складене

Lemma 4.1.1.

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

Theorem 4.1.2 (Евклід)**.**

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

Proof.
$Q = p_1 p_2 p_3 \ldots p_n + 1 \Rightarrow Q \,\bar{\vdots}\, p_i, \ n = \overline{1, n}$
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, $d = a \cdot b, \ \ a, \, b \neq 1, \ d \vdots a, \ n \vdots d \Rightarrow n \vdots a$ - 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.
$2\ 3\ \cancel{4}\ 5\ \cancel{6}\ 7\ \cancel{8}\ 9\ \cancel{10}\ 11\ \cancel{12}\ 13\ \cancel{14}\ 15\ \cancel{16}\ 17\ \cancel{18}\ 19\ \cancel{20}$
// Беремо перше незакреслене число. Це число 3 - воно просте. Викреслюємо кожне трете число в цьому ряду.
$2\ 3\ \cancel{4}\ 5\ \cancel{6}\ 7\ \cancel{8}\ \cancel{9}\ \cancel{10}\ 11\ \cancel{12}\ 13\ \cancel{14}\ \cancel{15}\ \cancel{16}\ 17\ \cancel{18}\ 19\ \cancel{20}$
// Беремо настпуне. Це 5 - просте. Викреслюємо кожне п'яте число. Ну вони вже викреслині. Тому далі уже нічого не викреслюєтся.
$2\ 3\ \cancel{4}\ 5\ \cancel{6}\ 7\ \cancel{8}\ \cancel{9}\ \cancel{10}\ 11\ \cancel{12}\ 13\ \cancel{14}\ \cancel{15}\ \cancel{16}\ 17\ \cancel{18}\ 19\ \cancel{20}$

Lemma 4.2.1.

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

Proof. Від супротивного □

Consequence. *У ситі Ератросфена для* $2 \ldots N$ *після викреслень чисел* $\le \sqrt{n}$ *залишаются прості.*

> **Example:**
> $\forall m \in \mathbb{N}$: існують m послідовних натуральних складених чисел.
> $(m+1)! \vdots 2,\ (m+1)! \vdots 3,\ (m+1)! \vdots 5,\ \ldots,\ (m+1)! \vdots (m+1).$

> **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.

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

Постулат Бертрана
$\forall n \in \mathbb{N},\ \ge 4.$ інтервал $n \ldots 2n - 2$ містить просте число.

Функція розподіла простих чисел $\Pi(x)$
$\Pi(x) =$ кількість простих чисел $< x$.
$\frac{1}{2} \cdot \frac{x}{\log_2 x} \le \Pi(x) \le 5 \cdot \frac{x}{log_2 x} \to \alpha \cdot \frac{x}{\ln x} \le \Pi(x) \le \beta \cdot \frac{x}{\ln x},\ \ \alpha = 0.92129,\ \beta = 1,10555$

Theorem 4.2.3 (Адамер, Вале)**.**

$$\Pi(x) \sim \frac{x}{\ln x}(\Pi(x) \sim \int\limits_2^x \frac{dt}{\ln t}) \Rightarrow p_n \sim n \cdot \ln n$$

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)**.**

$$p \text{ - просте, } ab \,\vdots\, p \Rightarrow \left[\begin{array}{l} a \,\vdots\, p \\ b \,\vdots\, p \end{array}\right.$$

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

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

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

□

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

Chapter 5

Лекція 5

5.1 Мультиплікативні функції

$f(n)$ - мультіплікативна:

1. $f(n) \not\equiv$
2. $\forall a,\ b \in \mathbb{N}: \qquad \gcd(a,\ b) = 1 \Rightarrow f(ab) = f(a)f(b)$

> **Example:**
>
> $f(n) = 1$
> $f(n) = n$
> $f(n) = n^S$

Property.

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

Definition 5.1.1. *$f(n)$ - мультиплікативна. Числовий інтеграл $g(n) = \sum\limits_{d \mid n} f(d)$*

Theorem 5.1.1 (S).

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

Proof.
$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_t^{\alpha_t},\ \ d \mid n \Rightarrow d = p_1^{\beta_1} p_2^{\beta_2} \ldots p_t^{\beta_t},\ \ 0 \le \beta_i \le \alpha_i$
$g(n) = \sum\limits_{d \mid n} f(d) = \sum\limits_{\beta_1=0}^{\alpha_1} \sum\limits_{\beta_2=0}^{\alpha_2} \cdots \sum\limits_{\beta_t=0}^{\alpha_t} f(p_1^{\beta_1} \ldots p_t^{\beta_t}) =$
$= \sum\limits_{\beta_1} \cdots \sum\limits_{\beta_t} \prod i = 1^t f(p_i^{\beta_t}) = \prod\limits_{i=1}^{t} \sum\limits_{\beta_i=0}^{\alpha_i} f(p_i^{\beta_i})$ $\square$

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

5.2 Кількість та сума дільників

Кількість дільників $\tau(n) = \sum\limits_{d \mid n} 1$

Сума дільників $\sigma(n) = \sum\limits_{d \mid n} d$

Proposition.

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

$$\sigma = \prod_{i=0}^{t} \frac{p_i^{\alpha+1}}{p_i - 1}$$

Proof.
p - просте. $\qquad \tau(p) = 2 \qquad \tau(p^\alpha) = 1 + \alpha$
$\tau(n) = \tau(p_1^{\alpha_1}) \dots \tau(p_t^{\alpha_t}) = (1+\alpha_1)(1+\alpha_2)\dots(1+\alpha_t)$
$\sigma(p) = 1 + p \qquad \sigma = 1 + p + p^2 = \dots + p^\alpha = \frac{p^{\alpha+1}-1}{p-1}$
$\sigma(n) = \sigma(p_1^{\alpha_1})\sigma(p_2^{\alpha_2})\dots\sigma(p_t^{\alpha_t})$ □

> **Example:**
> $n = 1000 = 2^3 5^3$
> $\tau(1000) = (1+3)(1+3) = 16$
> $\sigma(1000) = \frac{2^4-1}{2-1} \cdot \frac{5^4-1}{5-1} = 2340$

> **Example:**
> $n = 1001 = 7 \cdot 11 \cdot 13$
> $\tau(1001) = (1+1)(1+1)(1+1) = 8$
> $\sigma(1001) = (1+7)(1+11)(1+13) = 1344$

Property.

1. $\tau(n) \leq 2\sqrt{n}$
   $n \vdots d \Rightarrow n = d \cdot d'$
   $\sigma(n) \geq n + 1$
2. $\tau(n)$ - *непарне* $\Leftrightarrow n = m^2$
3. σ - *непарне* $\Leftrightarrow \left[\begin{array}{l} m^2 \\ 2m^2 \end{array}\right.$

5.3 Досконалі числа

Definition 5.3.1. *Досконале число* n*:*
n *= сумі усіх дільників окрім власне* n *або* $\sigma(n) = 2n$

> **Example:**
> $n = 6: \qquad 1 + 2 + 3 = 6$

> **Example:**
> $n = 28: \qquad 1 + 2 + 4 + 7 + 14 = 28$

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

2. Нехай n - парне досконале, $n = 2^k \cdot b,\ b$ - непарне
   $\sigma(n) = \sigma(2^k \cdot b) = (2^k - 1) \cdot \sigma(b) = 2^k \cdot b = 2n \Rightarrow$
   $\Rightarrow b \vdots (2^k - 1),\ b = (2^k - 1) \cdot c \qquad (2^k - 1)\sigma(b) = 2^k(2^k - 1) \cdot c$
   $\sigma(b) = 2^k \cdot c = (2^k - 1 + 1) \cdot c = b + c$
   $b \vdots c,\ c \neq 1,\ c \neq b \Rightarrow \sigma(b) > 1 + b + c \Rightarrow c = 1.$
   $b = 2^k - 1,\ \sigma(b) = b + 1 \Rightarrow b$ - 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 (характерізаційна властивість μ)**.**

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

Proof.
$p^\alpha :\qquad \mu(1)+\mu(p)+\mu(p^2)+\dots+\mu(p^\alpha)=1+(-1)+0+0+\dots+0=0$
За теоремою 5.1.1 $\sum\limits_{d\,|\,n}\mu(d)=\prod\limits_{i}\sum\limits_{\beta}\mu(p_i^\beta)$ ☐

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

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

Proof. За теоремою 5.1.1 $\sum\limits_{\beta}\mu(p_1^\beta)f(p_i{}^\beta)=\mu(1)f(1)+\mu(p_i)f(p_i)+$
$+\mu(p_i^2)f(p_i^2)+\dots=1+(-1)f(p_i)=1-f(p_i)$ ☐

Theorem 5.4.2 (закон обертання Мебіуса)**.**

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

Proof.
$\sum\limits_{d\,|\,n}M(d)\cdot\sum\limits_{\delta\,|\,\frac{n}{d}}f(\delta)=\sum\limits_{(d,\,\delta),\,d\delta\,|\,n}\mu(d\cdot f(\delta)=\sum\limits_{\delta\,|\,n}\sum\limits_{d\,|\,\frac{n}{d}}\mu(d)f(\delta)=$
$=\sum\limits_{\delta\,|\,n}f(\delta)\cdot\sum\limits_{d\,|\,\frac{n}{d}=1\Rightarrow\delta=n}\mu(d)=f(n)$ ☐

Example:

$a_0,\ a_1,\ \ldots,\ a_n$

$A(s) = \sum\limits_{n=1}^{\infty} \frac{a_n}{n^s}$ - ряд Діріхле. $\qquad B(s) = \sum\limits_{n=1}^{\infty} \frac{b_n}{n^s}$

$C(s) = A(s) \cdot B(s) = \sum\limits_{n=1}^{\infty} \frac{c_n}{n^s} \Rightarrow C_n = \sum\limits_{d \mid n} a_d \cdot b_{\frac{n}{d}} \qquad \xi(s) = \sum\limits_{n=1}^{\infty} \frac{1}{n^S}$

$\frac{1}{\xi(s)} = \sum\limits_{n=1}^{\infty} \frac{\mu(n)}{n^S} \qquad C(s) = A(s) \cdot \xi(s) \qquad C_n = \sum\limits_{d \mid n} a_d$

$A(s) = C(s) \cdot (\xi(s))' \Rightarrow a_n = \sum\limits_{d \mid n} \mu(d) c_{\frac{n}{d}}$

Chapter 6

Лекція 6

6.1 Порівняння за модулем

Definition 6.1.1. $a,\, b \in \mathbb{N}$, *a та b порівнювані за* $\mod n$:

$$a \equiv b(\mod n),\ a \equiv_n b,\ \textit{коли:}\ \begin{array}{l} (1)\ \exists t \in \mathbb{Z}:\ a = b + nt \\ (2)\ a \mod n = b \mod n \\ (3)\ (a-b) \,\vdots\, n \end{array}$$

Property.

1. $a \equiv a(\mod n),\ a \equiv b(\mod n) \Rightarrow b \equiv a(\mod n),$
   $a \equiv b(\mod n),\ b \equiv c(\mod n) \Rightarrow a \equiv c(\mod n)$

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

   Proof. $a = b + nt_1,\ c = d + nt_2,\qquad ac = bd + \underbrace{nt_1 d + nt_2 b + n^2 t_1 t_2}_{n\cdot T,\, T \in \mathbb{Z}}$ □

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

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

   Proof. $ca - cb \,\vdots\, n,\ c(a-b) \,\vdots\, n \Rightarrow (a-b) \,\vdots\, n$ □

4. (a) $a \equiv b(\mod n),\ k \neq 0 \Rightarrow ak \equiv bk(\mod nk)$

   (b) $d = \gcd(a,\, b,\, n)$
   $a = a_1 d_1,\ b = b_1 d_1,\ n = n_1 d_1,\ a \equiv b(\mod n) \Rightarrow a_1 \equiv b_1(\mod n)$

   Proof. $a = b + nt,\qquad a_1 \cancel{d} = b_1 \cancel{d} + n_1 \cancel{d} t$ □

5. $a \equiv b(\mod n),\ n \vdots d \Rightarrow a \equiv b(\mod d)$

6. $a \equiv b(\mod n_1)$,
   $a \equiv b(\mod n_2)$,
   $\vdots$
   $a \equiv b(\mod n_t)$,
   $a \equiv b(\mod \operatorname{lcm}(n_1, \dots, n_t))$

7. $a \equiv b(\mod n) \Rightarrow \gcd(a,\ n) = \gcd(b,\ n)$

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

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

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* $\forall b \in \mathbb{Z}\ y = (ax+b) \mod n$ - *також пробігає усі лишки з* $\mathbb{Z}_n$

Proof. Нехай $ax_1 + b \equiv ax_2 + b(\mod n)$, $ax_1 \equiv ax_2(\mod n)$, $x_1 = x_2(\mod n)$ □

Example:

$x^6 = \overset{3\cdot5\cdot7}{105}y + 5$

mod 3

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

$\Rightarrow x^2 \mod 3 \neq 2,\ x^6 = (x^3)^2 \equiv 2(\mod 3)$

Example:

$$x^6 = \overset{3\cdot5\cdot7}{105}y + 4$$

mod 5

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

$\Rightarrow$ $x^2 \mod 5 \in \{0,\ \pm\},\ x^6 = (x^3)^2 \equiv -1(\mod 5)$
$x^2 = 5k + 4 = 5k - 1 \Rightarrow x = 5t \pm 2$

mod 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

$\Rightarrow$ $x^2 \mod 7 \in \{0,\ 1,\ 2,\ 4\}$
$\underline{x^3 \mod 7 \in \{0,\ \pm1\}}$

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

$\Rightarrow$ $x^2 \mod 7 \in \{0,\ 1,\ 2,\ 4\}$
$\underline{x^3 \mod 7 \in \{0,\ \pm1\}}$

6.3 Обернені елементи за модулем

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

$$a \cdot a^{-1} \equiv a^{-1} \cdot a \equiv 1(\mod n)$$

Theorem 6.3.1.

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

Proof.

1. Нехай $\gcd(a,\ n) = 1$
   Тоді $\exists u,\ v \qquad a \cdot u + n \cdot v = 1 \Rightarrow a \cdot u \equiv 1(\mod n) \Rightarrow u = a^{-1} \mod n$
2. Нехай $\forall a^{-1} \mod n, \gcd(a,\ n) = d > 1$
   $a \cdot a^{-1} = 1 + nt,\ 1 = a \cdot a^{-1} - nt \,\vdots$ - Упс!

$\square$

Definition 6.3.2. *Зведена с-ма лишків(мультиплікативна группа 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)**.**

$$\begin{cases} x \equiv b_1(\mod n_1) \\ x \equiv b_2(\mod n_2) \\ \quad\vdots \\ x \equiv b_t(\mod n_t) \end{cases}$$

усі n_i попарно взаємнопрості
Тоді існує рівно один класс лишків $\mod n_1 n_2 \dots n_i$,
який є розв'язком системи.

Proof.

1. Нехай x_1 та x_2 - різні розв'язки.
   $x_1 \equiv x_2 \equiv b_i(\mod n_i) \Rightarrow (x_1 - x_2) \vdots n_i,\ i = \overline{1,t} \Rightarrow$
   $\Rightarrow (x_1 - x_2) \vdots n_1 n_2 \dots n_t$

2. $\begin{cases} x \equiv b_1(\mod n_1) \\ x \equiv b_2(\mod n_2) \end{cases} \Rightarrow \begin{array}{c} x = b_1 + n_1 k,\ k \in \mathbb{Z} \\ \underbrace{n_1 k + b_1}_{=b_2}(\mod n_2),\ k = \overline{1, n_2 - 1} \end{array}$
   З леми А: $\exists! k\ \ n_1 k + b_1 \equiv b_2(\mod n_2)$
   Повторюємо для $n_1 n_2$ та n_3, $n_1 n_2 n_3$ та $n_4 \dots$

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

$\square$

Example:

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

$N = 42, \qquad x_0 = 1 \cdot 4 \cdot 1 + 2 \cdot 14 \cdot 2 + 3 \cdot 6 \cdot 6 \equiv 17 \mod 42$

7.2 Функція Ойлера

Definition 7.2.1.

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

Proposition.

$$\varphi(n)\textit{- мультиплікативна.}$$

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

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

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

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

$n = p : \qquad \varphi(p) = p - 1$ (всі окрім p)
$n = p^\alpha : \qquad \varphi(p) = p^\alpha - p^{\alpha-1}$ (всі окрім $p,\ 2p,\ 3p,\ 4p, \dots,\ (p^{\alpha-1} - 1,\ p^\alpha)$
$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t} : \qquad \varphi(n) = \prod\limits_{i=1}^{t} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = n \cdot \prod\limits_{i=1}^{t} (1 - \frac{1}{p_i})$

Example:
$\varphi(31) = 30$
$\varphi(32) = \varphi(2^5) = 16$
$\varphi(33) = \varphi(3 \cdot 11) = 30$

Proposition.

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

Proof.
$\varphi(n) = \#x : \qquad \gcd(x,\ n) = 1,$

$N_d = \#x: \qquad \gcd(x,\, n) = d,\; x = x_1 \cdot d,\; n = n_1 \cdot d,\; \gcd(x_1,\, n_1) = 1 \Rightarrow$
$\Rightarrow N_\alpha = \varphi(n_1) = \varphi(\frac{n}{d}) \Rightarrow n = \sum\limits_{d\,|\,n} N_d = \sum\limits_{d\,|\,n} \varphi(\frac{n}{d}) = \sum\limits_{d\,|\,n} \varphi(d)$ □

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

7.3 Теорема Ойлера та мала теорема Ферма

Theorem 7.3.1 (Ойлер)**.**

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

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 $\mathbb{Z}_n^*$
$ax \equiv ay(\mod n) \Rightarrow x \equiv y(\mod n)$
$\mathbb{Z}_n^* = \{b_1,\, b_2, \dots,\, b_{\varphi(n)}\} = \{ab_1,\, ab_2, \dots,\, ab_{\varphi(n)}\} \Rightarrow$
$\Rightarrow \cancel{b_1} \cancel{b_2} \dots \cancel{b_{\varphi(n)}} \equiv a\cancel{b_1} \cdot a\cancel{b_2} \dots a\cancel{b_{\varphi(n)}} 1 \equiv a^{\varphi(n)}(\mod n)$ □

Consequence. $n = p$

$$a \,\overline{\vdots}\, p \Rightarrow a^{p-1} \equiv 1(\mod n)$$

Theorem 7.3.2 (Мала теорема Ферма)**.**

$$p \textit{ - просте: } \forall a \qquad a^p \equiv p(\mod a)$$

Proof.

$a \,\vdots\, p \qquad a^p \equiv a \equiv 0(\mod p)$

$a \,\overline{\vdots}\, p \qquad a^{p-1} \equiv 1(\mod p)$ □

> **Example:**
> $\quad 5555^{2222} + 2222^{5555} \,\vdots\, 7$
> $2222 \equiv 3(\mod 7) \qquad 5555 \equiv 4(\mod 7)$
> $3^{5555} + 4^{2222}(\mod 7) \qquad 3^6 \equiv 1(\mod 7)$
> $2222 \equiv 2(\mod 6) \qquad 5555 \equiv 5(\mod 6)$
> $3^5 + 4^2 \equiv 9 \cdot 9 \cdot 9 \cdot 3 + 16 \equiv 2 \cdot 2 \cdot 3 + 2 \equiv 14 \equiv 0(\mod 7)$

Chapter 8

Лекція 8

8.1 Функція Кармайкла

$\mathbb{Z}_8^* = \{1,\ 3,\ 5,\ 7\},\ \ \varphi(8) = 4$
$1^2 \equiv 1(\mod 8),\ 3^2 \equiv 1(\mod 8),\ 5^2 \equiv 1(\mod 8),\ 7^2 \equiv 1(\mod 8)$

Proposition. $n > 3$, a *- непране*

$$a^{2^{n-2}} \equiv 1(\mod 2^n)$$

Proof. Доведемо за ММІ.
База: $n = 3$
$a = 2k + 1 \qquad a^2 = (2k + 1)^2 = 4k(k + 1) + 1 \equiv 1(\mod 8)$
Крок: n
$a^{2^{n-2}} \equiv 1(\mod 2^n) \qquad a^{2^{n-2}} = 1 + 2^n \cdot t$
$a^{2^{n-1}} = (1 + 2^n \cdot t)^2 = 1 + 2 \cdot 2^n \cdot t + 2^{2n} \cdot t^2 = 1 + 2^{n+2} \cdot t_1 \equiv 1(\mod 2^{m+1})$ □

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

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

Lemma 8.1.1.

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

Proof.
Нехай $\omega \,\bar{\vdots}\, \lambda(n) \Rightarrow \omega = q \cdot \lambda(n) + r,\ 0 \leq r \leq \lambda(n)$
$1 \equiv a^\omega \equiv a^{q\cdot\lambda(n)+r} \equiv (a^{q\cdot\lambda(n)})(a^r) \equiv a^r(\mod n)$ - Упс! □

Lemma 8.1.2.

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

Proof. Доведення буде пізніше □

Consequence.

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

Theorem 8.1.3 (Кармайкл)**.**

1. $n = p$

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

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

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

Proof.

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

□

Example:
$n = 35 = 5 \cdot 7$
$\varphi(35) = 4 \cdot 5 = 24 \qquad \lambda(35) = \operatorname{lcm}(4,\ 6) = 12$

Example:
$n = 1000 = 2^3 \cdot 5^3$
$\varphi(1000) = \varphi(2^3)\varphi(5^3) = 4 \cdot 100 = 400 \qquad \lambda(1000) \operatorname{lcm}(\lambda(2^3),\ \lambda(5^3)) = \operatorname{lcm}(2,\ 100) = 100$

Chapter 9

Лекція 9

9.1 Системи числення

- представлення чисел у вигляді послідовності символів обмеженого алфавіту.
(Позиційна) система числення за основою B:
$n = \overline{(a_{k-1}a_{k-2}\dots a_1a_0)_B} = a_{k-1}B^{k-1} + a_{k-2}B^{k-2} + \dots + a_1B + a_0,$
$\forall i: \ 0 \le a_i < B, \ a_{k-1} \neq 0$
$n = n_1 \cdot B + a_0 = n_2 \cdot B^2 + a_1 \cdot B + a_0, \ n_1 = n_2 \cdot B + a_0$

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

Непозиційні системи:

1. римська
2. фібоначчієва
3. факторіальна

Example:
$\overline{11010}_2 = 2 + 8 + 16 = 26$
$2^n = \underbrace{100\dots0_2}_{n}$

Example:
70 у $B = 3$
$70 = 23 \cdot 3 + 1$
$23 = 7 \cdot 3 + 2$
$7 = 2 \cdot 3 + 1$
$2 = 0 \cdot 3 + 2$
$70 = \overline{2121}_3$

9.2 Ознака подільності числа

Theorem 9.2.1 (Ознака подільності Паскаля)**.**

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

$$\textit{Тоді } n \equiv \sum_{i=0}^{k-1} a_ir_i(\mod m), \qquad n \mathrel{\vdots} m \Leftrightarrow \sum_{i=0}^{k-1} a_ir_i \mathrel{\vdots} m$$

Proof.

$r_i \equiv B^i \mod m, n = a_{k+1}B^{k+1} + \dots + a_1B + a_0 = \sum_{i=0}^{k-1} a_iB^i = \sum_{i=0}^{k-1} a_ir_i(\mod m)$ □

***Remark*.**

1. $n \leq B^k,\ \sum a_ir_i \leq k \cdot m \cdot B$
2. *Якщо* $\gcd(B,\ m) = 1$, *то послідовність* (r_i) *є періодичною.*
   Період $\leq \lambda(m)$. *Якщо* $\gcd(B,\ m) \neq 1$

Example:
$(B = 10),\ m = 3$
$r_0 = 1 \qquad r_1 = 10 \cdot 1 \mod 3 = 1 \Rightarrow n \equiv \sum a_i(\mod 3)$

Example:
$(B = 10),\ m = 4$
$r_0 = 1 \qquad r_1 = 10 \cdot 1 \mod 4 = 2 \qquad r_2 = 10 \cdot 2 \mod 4 = 0 \Rightarrow$
$\Rightarrow n \equiv 2a_i + a_0(\mod 4)$

Example:
$(B = 10),\ m = 7$
$r_0 = 1 \qquad r_1 = 10 \cdot 1 \mod 7 = 3 \qquad r_2 = 10 \cdot 3 \mod 7 = -1$
$r_4 = -3 \qquad r_5 = -2 \qquad r_6 = 1$
$12345678 \equiv 8 \cdot 1 + 7 \cdot 3 + 6 \cdot 2 - 5 \cdot 1 - 4 \cdot 3 - 3 \cdot 2 + 2 \cdot 1 + 1 \cdot 3 \equiv 2(\mod 7)$

Example:
$(B = 10),\ m = 7, 11, 13$
$$1001 = 7 \cdot 11 \cdot 13 \equiv -1 \left(\mod \begin{matrix} 7 \\ 11 \\ 13 \end{matrix} \right) \Rightarrow$$

$$\Rightarrow n \equiv \overline{a_2a_1a_0} - \overline{a_5a_4a_3} + \overline{a_8a_7a_6} - \overline{a_{11}a_{10}a_9} + \dots + \left(\mod \begin{array}{c} 7 \\ 11 \\ 13 \end{array} \right)$$

$m = 11$: $\qquad 10 \equiv -1(\mod 11)$

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

Lemma 9.2.2.

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

9.3 Подільність біноміальних коєфіцієнтів

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

Proposition.
p - просте:

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

Proof.
$C_p^0 = C_p^p = 1 \qquad C_p^k = \frac{p!}{k!(p-k!)} \vdots\, p$ □

Proposition ("біном для дурників").

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

Theorem 9.3.1 (Люка).

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

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

Proof.
$n = \widetilde{n}p + n_0,\ m = \widetilde{m}p + m_0,\ C_n^m, \equiv C_{\widetilde{n}}^{\widetilde{m}} C_{n_0}^{m_0}(\mod p)$
Розглянемо біном $\qquad \text{coef}[x^m] = C_n^m$
$(1+x)^n = (1+x)^{\widetilde{n}p}(1+x)^{n_0} \equiv (1+x^p)^{\widetilde{n}}(1+x)^{n_0} \qquad m = \widetilde{m}p + m_0$
x^m одержуємо $x^{\widetilde{m}p}$ з $(1+x^p)^{\widetilde{n}} \Rightarrow x^{\widetilde{m}}$ з $(1+x)^{\widetilde{n}} \Rightarrow \text{coef}[x^m] = C_{\widetilde{n}}^{\widetilde{m}} C_m^n$ □

Consequence.

1. *Якщо* $\exists i:\ m_i > n_i$, *то* $C_n^m \equiv 0 (\mod p)$
2. $n = p^k = (\underbrace{100\ldots0}_{k})_p$

   $\forall m:\ 0 < m < p^k \qquad \forall i:\ m_i \neq 0,\ 0 \leq i \leq k \Rightarrow C_{p^k}^m \,\vdots\, p$

Chapter 10

Лекція 10

10.1 Лінійні порівняння за модулем

$ax \equiv (\mod n)$

1. Якщо $\gcd(a,\, n) = 1$, то $x \equiv a^{-1} \cdot b(\mod n)$
2. Якщо $a\underline{x} = b + nt,\; b = ax - nt$

   Якщо $b \,\vdots\, d$ - розв'язків немає

   Якщо $b \,\vdots\, d$, то $a = a_1 d,\; b = b_1 d,\; n = n_1 d \qquad \gcd(a_1,\, n_1) = 1$
   $b_1 = a_1 x - n_1 t \Rightarrow a_1 x \equiv b_1(\mod n_1)$
   $x_0,\; x_0 + n_1,\; x_0 + 2n_1,\; x_0 + (d-1)n_1$ - d розв'язків

Example:
$12x \equiv 5(\mod 25)$
$x \equiv 12^{-1} \cdot 5(\mod 25) \equiv 15(\mod 25)$

Example:
$12x \equiv 5(\mod \underline{2}7)$

$\gcd(12,\, 27) = 3,\; 5 \,\underline{\vdots}\, 3 \Rightarrow \varnothing$

Example:
$12x \equiv 9(\mod 27)$

$\gcd(9,\, 27) = 3,\; 9 \,\vdots\, 9$
$4x \equiv 3(\mod 9) \qquad x_0 \equiv 3 \cdot 4^{-1} \mod 9 \equiv 3(-2) \equiv = 6 \equiv 3 \mod 9$

$$\left\{ \begin{array}{l} x_0 \equiv 3 \\ x_0 \equiv 3 + 9 \equiv 12 \\ x_2 \equiv 12 + 9 \equiv 21 \end{array} \right\} \mod 27$$