Дискретна математика 2

(Discrete mathematics)

Лекция начинается

-Сегодня у нас клуб упоротых любителей математики.

Contents

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 – $a \vdots b$ або b ділить a(b є дільникома) $b \mid a$.*

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

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 (Euclidean divisiom)**.**

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

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. $\gcd(a,\ b)$ *поділяеться 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: $d = \gcd(a,\ b)$

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

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:**
> $\gcd(123,\ 456)$.
> $123 = 456 \cdot 0 + 123$
> $456 = 3 \cdot 123 + 87$
> $123 = 87 \cdot 1 + 36$
> $87 = 36 \cdot 2 + 15$
> $36 = 15 \cdot 2 + 6$
> $15 = 6 \cdot 2 + 3$

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

Example:

Для яких n : $\dfrac{3n+1}{5n+1}$ - 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 = 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. $\dfrac{\operatorname{lcm}(a,\ b)}{a}$ *та* $\dfrac{\operatorname{lcm}(a,\ b)}{b}$ - *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. $d = \gcd(a,\ b,\ c)$
$d' = \gcd(a,\ b) \Rightarrow d' \vdots d,\ c \vdots d \Rightarrow d = \gcd(c,\ d')$ □

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

Theorem 2.1.3.

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

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

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

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

2.2 Евклідові послідовності

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

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

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

Theorem 2.2.1.

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

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.

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

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 (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.
$r_0 = r_1 q_1 + r_2$
$r_1 = r_2 q_2 + r_3$
$r_2 = r_4 q_4 + r_5$
$\vdots$
$r_{n-3} = r_{n-2} q_{n-2} + r_{n-1}$
$r_{n-2} = r_{n-1} q_{n-1} + r_n$
$r_{n-1} = r_n q_n$
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. $\forall i: \ \ u_i,\ v_i \in \mathbb{Z}\ r_i = a u_i + b v_i \Rightarrow u_0 = 1,\ v_0 = 0,\ u_1 = 0,\ v_1 = 1$
   $u_{i+1} = u_{i-1} - u_i q_i,\ v_{i+1} = v_{i-1} - v_i q_i,\ r_{i+1} = r_{i-1} - q_i r_i = (a u_{i-1} + b v_{i-1}) -$
   $- q_i(a u_i + b v_i) = a \underbrace{(u_{i-1} - q_i u_i)}_{u_{i+1}} + b \underbrace{(v_{i-1} - q_i v_i)}_{vi+1}$

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

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

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

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 $c \,\bar{\vdots}\, d$, 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
$ax+by=0,\ ax_0+by_0=c\Rightarrow a(x-x_0)+b(y-y_0)=0\Rightarrow$
$\Rightarrow a_0(x-x_0)+b_0(y-y_0)=0\ \gcd(a_0,\ b_0)=1\Rightarrow 1=a_0u+b_0v\Rightarrow$
$\Rightarrow 0=\underbrace{a_0u}_{=(1-b_0v)}(x-x_0)+b_0v(y-y_0)=(x-x_0)+b_0(u(y-y_0)-v(x-x_0))\Rightarrow$
$\Rightarrow x-x_0\,\vdots\,b_0,\ x-x_0=b_0\cdot t,\ t\in\mathbb{Z}\Rightarrow a_0\cdot b_0t+b_0(y-y_0)=0\Rightarrow$
$\Rightarrow y-y_0=a_0t$ $\square$

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. $n \in \mathbb{N}$

$$\text{- \textit{просте}} \Leftrightarrow \text{\textit{має рівно два дільники 1 та n}}$$

$$\text{- \textit{складене}} \Leftrightarrow \exists a: \ 1 < a < n \quad n \,\vdots\, a$$

1 - не просте, не складене

Lemma 4.1.1.

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

Theorem 4.1.2 (Euclid)**.**

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.

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

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.

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

Proof. Від супротивного □

Consequence.

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

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

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

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

Theorem 4.2.3 (Adamer, Vallee)**.**

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

Theorem 4.2.4 (Dirichlet)**.**

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

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

Theorem 4.3.2 (Fundamental theorem of arithmetics)**.**

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

Proof.

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

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

□

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

Definition 5.1.1. $f(n)$ - *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 5.1.2. $f(n)$ - *мультиплікативна.*

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

Theorem 5.1.1 (S).

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

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

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

5.2 Кількість та сума дільників

Definition 5.2.1. *Кількість дільників*

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

Definition 5.2.2. *Сума дільників*

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

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. $\quad \tau(p) = 2 \quad \tau(p^\alpha) = 1 + \alpha$
$\tau(n) = \tau(p_1^{\alpha_1}) \dots \tau(p_t^{\alpha_t}) = (1+\alpha_1)(1+\alpha_2)\dots(1+\alpha_t)$
$\sigma(p) = 1 + p \quad \sigma = 1 + p + p^2 = \dots + p^\alpha = \dfrac{p^{\alpha+1} - 1}{p - 1}$
$\sigma(n) = \sigma(p_1^{\alpha_1})\sigma(p_2^{\alpha_2})\dots\sigma(p_t^{\alpha_t})$ ☐

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

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:*

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

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

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

Theorem 5.3.1 (Euclid-Euler)**.**

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

Proof.

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

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 $\sum\limits_{d \mid n} \mu(d) = \prod\limits_i \sum\limits_\beta \mu(p_i^\beta)$ □

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

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

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

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

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

Proof.
$\sum_{d \mid n} M(d) \cdot \sum_{\delta \mid \frac{n}{d}} f(\delta) = \sum_{(d,\, \delta),\, d\delta \mid n} \mu(d \cdot f(\delta) = \sum_{\delta \mid n} \sum_{d \mid \frac{n}{d}} \mu(d) f(\delta) =$
$= \sum_{\delta \mid n} f(\delta) \cdot \sum_{d \mid \frac{n}{d}_{=1 \Rightarrow \delta = n}} \mu(d) = f(n)$ □

Example:

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

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

   $p(x_1, x_2, \ldots,\ x_t)$ - *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) $d = \gcd(a,\ b,\ n)$
   $a = a_1d_1,\ b = b_1d_1,\ n = n_1d_1,\ a \equiv b(\mod n) \Rightarrow a_1 \equiv b_1(\mod n)$

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

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 :* $k,\ [k],\ \underline{k}$

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

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:

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

mod 3

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

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

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 (Chinese remainder theorem)**.**

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

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. $\begin{cases} x \equiv b_1(\mod n_1) \\ x \equiv b_2(\mod n_2) \end{cases} \Rightarrow \begin{matrix} x = b_1 + n_1 k,\ k \in \mathbb{Z} \\ \underbrace{n_1 k + b_1}_{=b_2}(\mod n_2),\ k = \overline{1, n_2 - 1} \end{matrix}$
   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. $N = n_1 n_2 \dots n_t,\ N_i = \dfrac{N}{n_i},\ M_i = N_i^{-1} \mod n_i$
   $x_0 = (b_i N_1 M_1 + b_2 N_2 M_2 + \dots + B_i N_i M_i) \mod N$ - 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.

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

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

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

Proposition.

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

Proof.
$\varphi(n) = \#x : \qquad \gcd(x,\ n) = 1,$
$N_d = \#x : \qquad \gcd(x,\ n) = d,\ x = x_1 \cdot d,\ n = n_1 \cdot d,\ \gcd(x_1,\ n_1) = 1 \Rightarrow$
$\Rightarrow N_\alpha = \varphi(n_1) = \varphi(\frac{n}{d}) \Rightarrow n = \sum_{d \mid n} N_d = \sum_{d \mid n} \varphi(\frac{n}{d}) = \sum_{d \mid n} \varphi(d)$ □

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

7.3 Теорема Ойлера та мала теорема Ферма

Theorem 7.3.1 (Euler)**.**

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

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. $n = p$

$$a \not\vdots\, p \Rightarrow a^{p-1} \equiv 1(\mod n)$$

Theorem 7.3.2 (Fermat's little theorem)**.**

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

Proof.
$a \vdots p \qquad a^p \equiv a \equiv 0(\mod p)$
$a \not\vdots\, p \qquad a^{p-1} \equiv 1(\mod p)$ ☐

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

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

Lemma 8.1.2.

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

Proof. Доведення буде пізніше □

Consequence.

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

Theorem 8.1.3 (Carmichael)**.**

1. $n = p$

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

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:
$n = \overline{(a_{k-1}a_{k-2}\dots a_1a_0)_B} = a_{k-1}B^{k-1} + a_{k-2}B^{k-2} + \dots + a_1B + a_0,$
$\forall i:\ 0 \le a_i < B,\ a_{k-1} \ne 0$
$n = n_1 \cdot B + a_0 = n_2 \cdot B^2 + a_1 \cdot B + a_0,\ n_1 = n_2 \cdot B + a_0$

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

Непозиційні системи:

1. римська
2. фібоначчієва
3. факторіальна

> **Example:**
> $\overline{11010}_2 = 2 + 8 + 16 = 26$
> $2^n = \underbrace{\overline{100\dots0}_2}_{n}$

> **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 (Pascal's divisibility rule)**.**

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

$$\text{Тоді } n \equiv \sum_{i=0}^{k-1} a_i r_i (\mod m), \qquad n \vdots m \Leftrightarrow \sum_{i=0}^{k-1} a_i r_i \vdots m$$

Proof.

$r_i \equiv B^i \mod m,\ n = a_{k+1}B^{k+1} + \cdots + a_1 B + a_0 = \sum_{i=0}^{k-1} a_i B^i = \sum_{i=0}^{k-1} a_i r_i (\mod m)$ □

Remark.

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

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

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

$$1001 = 7 \cdot 11 \cdot 13 \equiv -1 \begin{pmatrix} & 7 \\ \mod & 11 \\ & 13 \end{pmatrix} \Rightarrow$$

$$\Rightarrow n \equiv \overline{a_2 a_1 a_0} - \overline{a_5 a_4 a_3} + \overline{a_8 a_7 a_6} - \overline{a_{11} a_{10} a_9} + \cdots + \begin{pmatrix} & 7 \\ \mod & 11 \\ & 13 \end{pmatrix}$$

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

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

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

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

Proposition.
p - просте:

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

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

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 (Lucas')**.**

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

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

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 $\quad \text{coef}[x^m] = C_n^m$
$(1+x)^n = (1+x)^{\widetilde{n}p}(1+x)^{n_0} \equiv (1+x^p)^{\widetilde{n}}(1+x)^{n_0} \qquad m = \widetilde{m}p + m_0$
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 $b \not\vdots\, d$ - 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:
$12x \equiv 5(\mod \underline{2}7)$
$\gcd(12,\, 27) = 3,\ 5 \vdots 3 \Rightarrow \varnothing$

Example:
$12x \equiv 9(\mod 27)$
$\gcd(9,\, 27) = 3,\ 9 \vdots 9$
$4x \equiv 3(\mod 9) \qquad x_0 \equiv 3 \cdot 4^{-1} \mod 9 \equiv 3(-2) \equiv = 6 \equiv 3 \mod 9$

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

10.2 Елементи загальної теорії розв'язування порівнянь

$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ - поліном з цілими коефіцієнтами. $f(x) \equiv 0(\mod m)$

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

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

2. $f(x) \equiv 0(\mod p)$
   $f(x) \equiv 0(\mod p)$ та $g(x) \equiv 0(\mod p)$
   - еквівалентні, якщо множини розв'язків спіспадають

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

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

$$\Rightarrow f(x) \equiv 0(\mod p),\ f(x) \mod (x^p - x) \equiv 0(\mod p)$$

$$\textit{можна розглядати } f: \qquad \deg f < p$$

Theorem 10.2.2 (Fundamental theorem of arithmetics for $\mathbb{Z}_p$)**.**
$f(x) \in \mathbb{Z}_p[x]$, $\deg f = n < p$

$$\textit{Якщо } a_n \,\bar{\vdots}\, p, \textit{ то } f(x) \equiv 0(\mod p) \textit{ має } \leq n \textit{ розв'язків}$$

Proof. MMI за n

1. $n = 1$
   $a_1 x + a_0 \equiv 0(\mod p)$, $\gcd(a_1,\ p) = 1 \Rightarrow$ рівно один розв'язок
2. Для усіх поліномів deg $\leq n - 1$ - вірне
   $f(x) \equiv 0(\mod p)$
   (a) Якщо розв'язків немає - ок
   (b) Якщо x_0 - розв'язок, то
   $f(x) = (x - x_0) \cdot g(x) + f(x_0) \equiv (x - x_0) \cdot g(x)(\mod p)$
   $g(x)$ - поліном з цілими коєфіцієнтами, $\deg g = n - 1$
   $coef[x^{n-1}]g = a_n \,\bar{\vdots}\, p \Rightarrow g(x) \equiv 0(\mod p)$ має $\leq n - 1$ розв'язків

□

Consequence.

$$\textit{Якщо } f(x) = 0(\mod p) \textit{ має } > n \textit{ розв'язків, то } \forall i:\ a_i \,\vdots\, p$$

Proof.
$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \equiv 0(\mod p)$
$a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \equiv 0(\mod p)$
$\vdots$
$a_0 \equiv 0(\mod p)$ □

Theorem 10.2.3 (Wilson)**.**

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

Proof.

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

2. Нехай $n = a \cdot \underset{\geq}{b},\ ! < a < n \Rightarrow (n-1)! \vdots a$
   $\Rightarrow (n-1)! + 1 \vdots n$

□

10.3 Розклад Тейлора для поліномів

$f(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 = \sum\limits_{t=0}^{n} a_t x^t$
$f'(x) = f^{(1)}(x) = \sum\limits_{t=1}^{n} a_t t x^{t-1}$
$f'(x)$ - поліном з цілими коефіцієнтами $\deg f = n - 1$ К-тий похідний поліном: $f^{(k)}(x) = \sum\limits_{t=k}^{n} a_t t(t-1)\dots(t-k+1)x^{t-k}$

Lemma 10.3.1.

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

Proof.
$\dfrac{t(t-1)\dots(t-k+1)}{k!} \cdots \dfrac{(t-k)!}{(t-k)!} = \dfrac{t!}{k!(t-k)!}$ □

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.
$f(x_0 + \alpha) = \sum\limits_{t=0}^{n} a_t (x_0 + \alpha)^t = \sum\limits_{t=0}^{n}\sum\limits_{k=0}^{t} a_y C_t^k x_0^{t-k}\alpha^k$

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

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

10.4 Поліноміальні порівняння за модулем степеня простого числа (1)

Theorem 10.4.1. *$f(x)$ - поліном з цілими коефіцієнтами x_0.*
$f(x_0) \equiv 0(\mod p^k),\ f'(x_0) \not\vdots\, p$

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

Proof. MMI за k

1. $k = 1$
2. $k = 2$
   нНехай x_k - задовільняє умовам
   $f(x_k) \equiv 0(\mod p^k),\ f'(x_k) \not\vdots\ p,\ x_k \equiv x_0(\mod p)$
   $\Rightarrow f'(x_k) \equiv f'(x_0)(\mod p) \Rightarrow f'(x_k) \not\vdots\, p$
   Шукаємо $x_{k+1} = x_k + p^k \cdot t,\ 0 \le t \le p-1$
   $f(x_{k+1}) \equiv 0(\mod p^{k+1})$
   $f(x_k + p^k t) = f(x_k) + f'(x_k) \cdot p^k t + \dfrac{f''(x_k)}{2!}(p^k t)^2 + \cdots \equiv$
   $\equiv f(x_k) + f'(x_k) \cdot p^k t(\mod p^k) \Rightarrow 0 \equiv f(x_k) + f'(x_k) \cdot p^k t \mod p^k)$
   $f'(x_k) \cdot t \equiv -\dfrac{f(x_0)}{p^k}(\mod p) \Rightarrow$ існує єдине $t \Rightarrow$ існує єдине значення

□

Chapter 11

Лекція 11

11.1 Поліноміальні порівняння за модулем степеня простого числа (2)

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

$$\begin{aligned} x_0: \quad & f(x_0) \equiv 0(\mod p), \quad f'(x_0) \vdots p \\ x_k: \quad & f(x_k) \equiv 0(\mod p^k), \quad x_k \equiv x_0(\mod p) \end{aligned}$$

Тоді:

1. *Якщо* $f(x) \bar{\vdots} p^{k+1}$, *то*

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

2. *Якщо* $f(x_k)p^{k+1}$, *то*

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

Proof.
$x_{k+1} = x_t + p^k t,\ t = \overline{0, p-1}$
$f(x_{k+1}) = f(x_k + p^k t) = f(x_k) + f'(x_k) \cdot p^k t + \cdots \equiv f(x_k)(\mod p^{k+1})$
$f(x_{k+1}) \equiv 0(\mod p^{k+1}) \Rightarrow f(x_k) \equiv 0(\mod p^{+1})$ □

Example:
$x^4 + 7x + 4 \equiv 0(\mod 27)$
$f(x) = x^4 + 7x + 4 \qquad f'(x) = 4x^3 + 7$

1. $f(x) \equiv 0(\mod 3)$
   $x_0 \equiv 1(\mod 3)$
   $f'(1) = 4 + 7 = 11 \equiv -1(\mod 3)$

2. $f(x) \equiv 0(\mod 9)$
   $x_1 = x_0 + 3 \cdot t_0$
   $f'(1) \cdot t_0 \equiv -\frac{f(1)}{3}(\mod 3)$
   $2t_0 \equiv -4 \equiv 2(\mod 3)$
   $t_0 = 1 \qquad x_1 = 1 + 3 = 4(\mod 9)$

3. $f(x) \equiv 0(\mod 27)$
   $x_2 = x_1 + 9t_1$

$f'(4) \cdot t_1 \equiv -\frac{f(4)}{9}(\mod 3)$
$263t_1 \equiv -32(\mod 3)$
$2t_1 \equiv 1(mod3)$
$t_1 = (\mod 3) \qquad x_2 = 4 + 9 \cdot 2 \equiv 22(\mod 27)$

11.2 Квадратичні лишки, критерій квадратичності Ойлера

$ax^2 + bx + c \equiv 0(\mod p)$ - квадратичне порівняння. $\Rightarrow x^2 \equiv \alpha(\mod p)$

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

$$\exists x : \qquad x^2 \equiv \alpha(\mod p)$$

$\mathbb{Z}_p^* = \{1,\ 2,\ 3, \dots,\ p-1\}$, $\mathbb{Z}_p^{\circledast} = \{-\frac{p-1}{2}, \dots,\ -2,\ -1,\ 1,\ 2, \dots,\ \frac{p-1}{2}\}_{(p>3)}$,
$Y_p = \{1,\ 2, \dots,\ \frac{p-1}{2}\}$

$f(x) = x^2 - \alpha$
x_0 - корінь, то $(-x_0)$ також корінь

Lemma 11.2.1.

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

Proof.
Квадратичні лишки: $(1)^2,\ 2^2,\ 3^2, \dots,\ \left(\frac{p-1}{2}\right)^2 \Rightarrow \frac{p-1}{2}$ штук
Але $0 < u < v \leq \frac{p-1}{2}$: $u^2 \equiv v^2(\mod p)$ то $x^2 \equiv u^2(\mod p)$
має 4 розв'язки $\pm u,\ \pm v \Rightarrow$ квадратичних лишків $\frac{p-1}{2}$ штук ☐

Theorem 11.2.2 (Euler's criterion).

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

Proof.
$a \equiv 0(\mod p)$ - очевидно
$a \not\equiv 0(modp) \Rightarrow a^{p-1} \equiv 1(\mod p) a^{p-1} - 1 = (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0(\mod p)$
Нехай $a = b^2 \Rightarrow a^{\frac{p-1}{2}} = b^{p-1} \equiv 1(\mod p)$
$f(x) x^{\frac{p-1}{2}} - 1$ - 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 лишків у* $a \cdot Y_p$

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

Proof.
$\forall u \in Y_p : \ lu \in \{0,\ 1\},\ r_u \in Y_p,\ a \cdot u \equiv (-1)^{lu} \cdot r_u(\mod p)$
$u \not\equiv v \Rightarrow r_u \not\equiv r_v(\mod p)$
$\begin{cases} u \not\equiv v \\ r_u \equiv r_v \end{cases} \Rightarrow \begin{cases} au \not\equiv av \\ r_u \equiv r_v \end{cases} \Rightarrow au \equiv av(\mod p)$
$a(u+v) \vdots p$, але $0 < \begin{matrix} u \\ v \end{matrix} \le \frac{p-1}{2} \Rightarrow 0 < u+v \le p-1 < p \Rightarrow u+v \overset{-}{\vdots} p$ - Упс!
$\Rightarrow \{r_1,\ r_2, \dots,\ r_{\frac{p-1}{2}}\} = Y_p$

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

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

Chapter 12

Лекція 12

12.1 Символ Лежандра та його властивості

$x^2 \equiv a(\mod p)$, $p \geq 3$ - просте

Definition 12.1.1. *Символ Лежандра -*

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

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

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

Property.

1. $\left(\frac{a}{p}\right) = 1$, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$,
   $p = 4k+3 : \left(\frac{-1}{p}\right) = -1, \qquad p = 4k+1 : \left(\frac{-1}{p}\right) = -1$
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
   $\left(\frac{a^2}{p}\right) = 1, \qquad \left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$
3. $\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{8}}$
   $p = 8k \pm 1 = \left(\frac{2}{p}\right) = 1, \qquad p = 8k \pm 3 \left(\frac{2}{p}\right) = -1$
4. *Закон квадратичноЇ взаємодії Гаусса*
   p, q *- непарні прості,* $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}} (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right)$

Proof.
$\left(\frac{2}{p}\right) = \begin{cases} +1, & p = 8k \pm 1 \\ -1, & p = 8k \pm 3 \end{cases}$, $\quad \left(\frac{2}{p}\right) = (-1)^l$, l - кількість від'ємних лишків у $\mathbb{Z}_p^{\circledast}$
серед чисел $2 \cdot 1,\ 2 \cdot 2,\ 2 \cdot 3, \ldots,\ 2 \cdots \frac{p-1}{2} = 2,\ 4,\ ,6, \ldots,\ (p+1)$
Якщо число $> \frac{p}{2}$, то воно від'ємне у $\mathbb{Z}_p^{\circledast}$
Число, яке $< \frac{p}{2}$: $\lfloor \frac{p}{4} \rfloor \Rightarrow l = \frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor$

$$\begin{array}{ll} p = 8k+1: & l = 4k - 2k = 2k \\ p = 8k+3: & l = 4k+1-2k = 2k+1 \\ p = 8k+5: & l = 4k+2-(2k+1) = 2k+1 \\ p = 8k+7: & l = 4k+3-(2k+1) = 2k+2 \end{array}$$

□

12.2 Символ Якобі та його властивості

n - непарне, a - довільне

Definition 12.2.1. *Символ Якобі*

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

$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_t^{\alpha_t}$, $\left(\frac{a}{n}\right) \in \{-1,\ 1,\ 0\}$, $\left(\frac{a}{n}\right) = 0 \Leftrightarrow \gcd(a,\ n) \neq 1$,
$\left(\frac{a}{n}\right) = -1 \Leftrightarrow a - kb$ *квадратний нелишок* $\mod n$, $\left(\frac{a}{n}\right) = 1 \Leftrightarrow ?$

Property.

1. $\left(\frac{1}{n}\right) = 1$, $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$
2. $\left(\frac{a \cdot b}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$
3. $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$
4. $\left(\frac{a}{n}\right) = (-1)^{\frac{a-1}{2}\frac{n-1}{2}}\left(\frac{a}{n}\right)$, $\qquad$ *a, n - непарні*

Example:
$x^2 \equiv 59(\mod 97)$
$\left(\frac{59}{97}\right) = (-1)^{\frac{59-1}{2}\frac{97-1}{2}}\left(\frac{59}{97}\right) = (-1)^{\frac{a-1}{2}\frac{n-1}{2}}\left(\frac{38}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{19}{29}\right) = (-1)\left(\frac{19}{59}\right) =$
$(-1)(-1)^{\frac{19-1}{2}\frac{59-1}{19}} =$

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

Вступ до абстрактної алгебри

(Introduction to Abstract algebra)

Chapter 13

Лекція 1

13.1 Алгебраїчні системи з однією операцією

$\mathcal{A}$, $\cdot$ $(\mathcal{A} \times \mathcal{A} \to \mathcal{A})$
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.

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

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 обернениз елементів:(за умови наявность нейтрального!)*
$a \in \mathcal{A}$ *має лівий обернений* $a_L^{-1}:\ a_L^{-1} \cdot a = e$
$a \in \mathcal{A}$ *має лівий обернений* $a_R^{-1}:\ a \cdot a_R^{-1} = e$
$a^{-1} \in \mathcal{A}$ *- обереннений до* $a \in \mathcal{A}$*, якщо* $a \cdot a^{-1} = a^{-1} \cdot a = e$

Definition 13.1.2.

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

Definition 13.1.3.

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

Definition 13.1.4.

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

Remark.
$\cdot$ - *комутативна* $\Rightarrow$ *комутативна напівгрупа*
комутативний моноїд
абелева група

Remark.
Форми запису:

Мулітиплікативна	*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}^* = $ ıı$\backslash\{0\} \Rightarrow \langle \mathbb{Q}^*,\ \cdot \rangle$ - абелева группа,
$\langle \mathbb{Z}_{\gtrdot},\ + \mod m \rangle$ - абелева група,
$\langle \mathbb{Z}_{\gtrdot},\ \cdot \mod m \rangle$ - комутативний моноїд,
$\langle {\mathbb{Z}_{\gtrdot}}^*,\ + \mod m \rangle$ - абелева група
$Mat_{n\times m}(\mathbb{R})$: за додаванням - абелева група
за множенням - моноїд
$\mathcal{G}L_n(\mathbb{R}) = \{M \in M_{a+n\times m}(\mathbb{R}) |\det M \neq 0\}$ - загальна лінійна група
$X^X = \{f \mid f : X \to X,\ \langle X^X,\ \circ \rangle$ - 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, $\varnothing$ - нейтральний
$\langle 2^A,\ \backslash \rangle$ - не напів група, $(B\backslash C)\backslash D \stackrel{?}{=} B\backslash(C\backslash D)$
$\langle 2^*,\ \triangle \rangle$ - абелева група, $A \triangle \varnothing = A,\ A = A^{-1}$
$\langle A^*,\ \| \rangle$ - 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 $\cancel{\forall g \in \mathcal{M}: \; g = e_1 \cdot g = e_2 \cdot g}$
$\Rightarrow e_1 = e_2$ НЕ МОЖНА!!!

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

*/

$e_1 = e_1 \cdot e_2 = e_2$(аксіома про нейтральний елемент) □

Lemma 13.3.2.

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

Proof. $a_l^{-1}, a_R^{-1}: \; a_L^{-1} \cdot a \cdot a_R^{-1} = a_L^{-1} \cdot e = a_L^{-1}$
$a_L^{-1} \cdot a \cdot a_R^{-1} = a_R^{-1} \cdot e = a_R^{-1}$ □

Lemma 13.3.3.

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

Proof. □

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

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

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

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

Theorem 13.3.4.

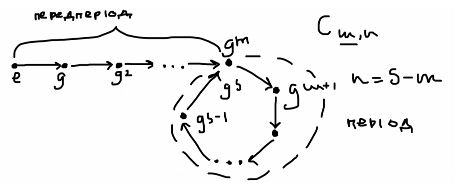
$$\forall a \in \mathcal{M}, \; \forall m, \; n \in \mathbb{N}_0: \; a^m \cdot a^n = a^{m+n}$$

Proof. ММІ:
$\forall m$ - фіксоване: $n = 0$(база): $a^m \cdot a^0 = a^m \cdot e = a^m = a^{m+0}$
$n \to n+1 \qquad a^m \cdot a^{n+1} = a^m \cdot a^n \cdot a = a^{n+m} \cdot a = a^{m+n+1}$ □

$\ominus$ Ціклічні 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 $\mathcal{M} = \langle g \rangle, \; |\mathcal{M}| < \infty$
$\Rightarrow \exists \min g: \; g^s = g^m, \; m < s$

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

Chapter 14

Лекція 2

14.1 Властивості елементів груп. Циклічні групи

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

Property.

1. *Правило скорочення:*
   $\forall a,\ x,\ y \in G :\qquad ax = ay \Rightarrow x = y,\ xa = ya \Rightarrow x = y$

2. $\forall a,\ b \in G :\qquad \begin{matrix} ax = b \\ ya = b \end{matrix}$ *- мають єдиний розв'язок*

   Proof.

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

   (b) Нехай $x_1,\ x_2$ - розв'язки $ax = b \qquad \Rightarrow b = ax_1 = ax_2 \Rightarrow x_1 = x_2$

   □

3.

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

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

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

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

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

   Proof.

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

   □

4.

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

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

Proof.

(a)

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

(b)

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

□

Fact. *Циклічні групи*

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

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

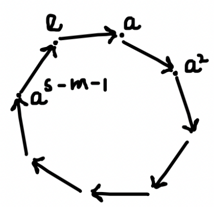
$$\text{усі циклічні групи зводятся до } \langle \mathbb{Z}_m,\ + \rangle$$

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.



$\langle a \rangle$ - 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. $\operatorname{ord} G$

$$\text{Порядок групи} = |G|$$

Definition 14.2.3. $\operatorname{ord} a$

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

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

Example:
$\operatorname{ord} e = 1, \qquad \operatorname{ord} a = 1 \Leftrightarrow a = e$

Example:
$\langle \mathbb{Z}, +\rangle : \ \operatorname{ord} 0 = 1, \ \operatorname{ord} 1 = \infty$
$\langle \mathbb{Z}_4, +\rangle : \ \operatorname{ord} 0 = 1, \ \operatorname{ord} 1 = 4, \ \operatorname{ord} 2 = 2$

Lemma 14.2.2.

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

Proof.
$\Leftarrow$ $u = k \cdot n \Rightarrow g^u = (g^n)^k = e^k = e$
$\Rightarrow$ Нехай $u \not\vdots\, n \Rightarrow u = nq + r, \ 0 < r < n$
$e \cdot g^u = (g^n)^q \cdot g^r = e^q \cdot g^r = g^r \Rightarrow n$ - не порядок g - Упс! ☐

Definition 14.2.4. *Підгрупа*

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

$$\langle H, \cdot \rangle \quad \begin{array}{l} - \textit{замкненість} \\ - \textit{асоціативність} \\ - \textit{наявність } e \\ - \textit{наявність обернених} \end{array}$$

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

Example:
$\mathcal{SL}_n(\mathbb{R}) \subseteq \mathcal{GL}_n(\mathbb{R})$, $\mathcal{SL}_n(\mathbb{R}) = \{M \in \mathcal{GL}_n(\mathbb{R}) \mid \det M = 1\}$ - спеціальна підгрупа

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

Proposition.

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

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

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

$$\text{Елементи} g_1,\ g_2 - \text{(ліво) конгуретні відносно} H: \begin{array}{l} g_1 \equiv g_2(\mod n) \Leftrightarrow g_1^{-1} \cdot g_2 \in H \Leftrightarrow \\ \Leftrightarrow \exists h \in H : g_2 = g_1 \cdot h,\ g_1 = g_2 \cdot h^{-1} \end{array}$$

$$\text{(право) конгурентні} \longrightarrow g_1 \cdot g_2^{-1} \in H\ \exists h \in H:\ g_2 = h \cdot g_1$$

Lemma 14.3.1.

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

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

Proposition. *усі класи суміжно рівнопотужні*

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

Proof. Розглянемо відображення $fg : H \to gH$
$fg(x) = g \cdot x$ $-$ сюр'єктивне за побудовою gH
$-$ ін'єктивне: $x_1,\ x_2 \in H\ \ fg(x_1) = fg(x_2),\ g \cdot x_1 = g \cdot x_2,\ x_1 = x_2$
$\Rightarrow fg$ - бієкція $\Rightarrow |gH| = |H|$ ☐

Definition 14.3.2.

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

$G -$ 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. $G = \bigcup\limits_{g} |gH| = \#$класів сумижності $\cdot |H| = [G : H] \cdot |H|$ ☐

Consequence. *Нехай* $|G| = n < \infty$

1. $\forall H$ *- підгрупа:* $n \,\vdots\, |H|$
2. $\forall g \in G:\ n \,\vdots\, \operatorname{ord} g$

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

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

4. $\forall$ *група простого порядку є циклічною*

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

Theorem 14.3.3 (Sylow)**.**

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

Theorem 14.3.4.

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

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

Chapter 15

Лекція 3

15.1 Властивості циклічних груп та їх елементів

$G = \langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$
Генератор групи - довільне g' $G = \langle g' \rangle$

Lemma 15.1.1.

$$\forall H \subseteq G \text{ - підгрупа: } H \text{- циклічна}$$

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

$\forall t :\ g^t \in \underline{H} \Rightarrow t \,\vdots\, s$

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

$\Rightarrow t \,\vdots\, s \Rightarrow g^t = (g^s)^q \subseteq \langle g^s \rangle \Rightarrow H \subseteq \langle g^s \rangle$ □

Lemma 15.1.2.

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

Proof. $\operatorname{ord} g^k = \min\{U > 0\ :\ \left(g^k\right)^u = e\} \Rightarrow ku \,\vdots\, \operatorname{ord} g \Rightarrow ku \,\vdots\, n$. Нехай $d = gcd(k,\ n)$

$k = k_1 \cdot d \qquad k_1 \cdot d \cdot u \,\vdots\, u$

$\gcd(k_1,\ n) = 1 \qquad d \cdot u \,\vdots\, n$

$\Rightarrow \min u = \dfrac{n}{d} \Rightarrow \operatorname{ord} g^k = \dfrac{n}{d} = \dfrac{n}{\gcd(n,\ k)}$ □

Consequence.

$$\text{Група } G \text{ містить } \varphi(n) \text{ генераторів}$$

Lemma 15.1.3.

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

Proof. З одного боку, $k \,\vdots\, d \Rightarrow g^k = \left(g^d\right)^{\cdots} \in \langle g^d \rangle \Rightarrow \langle g^k \rangle = \langle g^d \rangle$
З іншого боку, $\operatorname{ord} g^k = |\langle g^k \rangle| = \dfrac{n}{d},\ \operatorname{ord} g^d = |\langle g^d \rangle| = \dfrac{n}{\gcd(n,\ d)} = \dfrac{n}{d} \Rightarrow$
$\Rightarrow |\langle g^k \rangle| = |\langle g^d \rangle| \Rightarrow \langle g^k \rangle = \langle g^d \rangle$ □

Consequence.

Consequence.

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)

$x \to \frac{x}{y}: \qquad \frac{x^n}{y^n} - 1 = (\frac{x}{y} - 1)(\frac{x^{n-1}}{y^{n-1}} + \frac{x^{n-2}}{y^{n-2}} + \frac{x}{y} + 1) \qquad \big| x \qquad \cdot y^n$

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

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

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

Theorem (Безу)**.**

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

або

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

A.3 Наслідок з теореми Безу

1. якщо α - корінь $p(x)$, то $p(x) \vdots (x - \alpha)$
   $p(\alpha) = 0 \Rightarrow p(x) = (x - \alpha) \cdot q(x) + p(\alpha) = (x - \alpha) \cdot q(x)$

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

$$x^n: \ a_n = a_n$$
$$x^{n-1}: \ a_{n-1} = a_n(-\alpha_1 - \alpha_2 - \dots - \alpha_n) \Rightarrow \alpha_1 + \alpha_2 + \dots + \alpha_n = -\frac{a_{n-1}}{a_n}$$

$$p(x) = a_3x^3 + a_2x^2 + a_1x + a_0 = a_3(x-\alpha_1)(x-\alpha_2)(x-\alpha_3) = a_3(x^3 - \alpha_1x^2 -$$
$$- \alpha_2x^2 - \alpha_3x^2\alpha_1\alpha_2x + \alpha_1\alpha_3x + \alpha_2\alpha_3x - \alpha_1\alpha_2\alpha_3)$$

$$\Rightarrow \begin{array}{rl} x^3: & a_3 = a_3 \\ x^2: & a_2 = a_3(-\alpha_1 - \alpha_2 - \alpha_3) \\ x: & a_1 = a_3(\alpha_1\alpha + \alpha_1\alpha_3 + \alpha_2\alpha_3) \\ x^0 = 1: & a_0 = a_3(-\alpha_1\alpha_2\alpha_3) \end{array} \qquad \begin{array}{c} x^k: a_k = a_n \cdot (-1)^{n-k} \sum \alpha_{i_1}\alpha_{i_2}\dots\alpha_{i_k} \\ 1 \le i_1 < i_2 < \dots < i_n \le n \end{array}$$

$$\Rightarrow \alpha_1 + \alpha_2 + \dots + \alpha_n = -\frac{a_{n-1}}{a_n}, \qquad \alpha_1\alpha_2\dots\alpha_n = (-1)^n \cdot \frac{a_0}{a_n}$$

A.5 Схема Горнера

$$p(x) = a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$$
$$q(x) = b_nx^n + b_{n-1}x^{n-1} + \dots + b_1x + b_0$$

$$p(x) = (x-\alpha)\cdot q(x) + p(\alpha) = (x-\alpha)(b_{n-1}x^{n-1} + \dots + b_1x + b_0) + p(\alpha) =$$
$$\begin{array}{llllllll} = b_{n-1}\cdot x^n & +b_{n-2}\cdot x^{n-1} & +b_{n-3}\cdot x^{n-2} & +\dots & +b_1\cdot x^2 & +b_0\cdot x & \\ & -\alpha b_{n-1}x^{n-1} & -\alpha b_{n-2}x^{n-2} & -\dots & -\alpha b_2x^2 & -\alpha b_1x & -\alpha b_0 + p(\alpha) = \end{array}$$
$$= a_n\cdot x^n + a_{n-1}\cdot x^{n-1} + \dots + a_1x + a_0$$

$$\Rightarrow \begin{array}{l} a_n = b_{n-1} \\ a_{n-1} = b_{n-2} - \alpha\cdot b_{n-1} \\ a_{n-2} = b_{n-3} - \alpha\cdot b_{n-2} \\ \quad\vdots \\ a_1 = b_0 - \alpha b_1 \\ a_0 = p(\alpha) - \alpha b_0 \end{array} \Rightarrow \begin{array}{l} b_{n-1} = a_n \\ b_{n-2}a_{n-1} + \alpha\cdot b_{n-1} \\ b_{n-3} = a_{n-2} + \alpha\cdot b_{n-2} \\ \quad\vdots \\ b_0 = a_1 + \alpha b_1 \\ p(\alpha) = a_0 + \alpha b_0 \end{array}$$

	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

$\alpha \in \mathbb{R}: \ \alpha = a_1 + a_0, \ a_{\in}\mathbb{Z}, \ 0 \le \alpha_1 < 1$

$$\alpha = a_1 + \frac{1}{\frac{1}{\alpha_1}} = a_1 + \frac{1}{\frac{a_2}{\alpha_2}} = a_1 + \frac{1}{a_2 + \frac{1}{\frac{1}{\alpha_2}}} = a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \alpha_3}} = \dots$$

Ланцюговий дріб α - представлення α у вигляді $a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\alpha_3}}$: $\alpha=[a_1;a_2,a_3,a_4,\dots]$,

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

A.7 Чим більше знаємо дробів - тим точніше α

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

A.8 Кожен скінченний дріб описує одне раціональне число

Proposition.

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

Proof.

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

$\Rightarrow$ (Алгоритм Евкліда!)

$$\alpha=\frac{m}{n}=\frac{r_0}{r_1}=\frac{r_1q_1+r_2}{r_1}=q_1+\frac{r_2}{r_1}=q_1+\cfrac{1}{\cfrac{r_1}{r_2}}=q_1+\cfrac{1}{q_2+\cfrac{r_3}{r_2}}=\dots=$$

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

□

/ *

$\Leftarrow$ Усі a_i - цілі, невід'ємні (нулі лише для ірраціональних випадків), крім $_1$ - воно може бути від'ємним, цілим. (тому ми його відділяємо;)

$\Rightarrow$ Алгоритм Евкліда скінченний, тому фокус такий.

*/

A.9 Наближення числа π

$$\frac{22}{7} \approx \pi: \qquad \begin{array}{ccccccc} 22 & = & \boxed{3} & \cdot & 7 & + & 1 \\ 7 & = & \boxed{7} & \cdot & 1 & + & 0 \end{array} \qquad \Rightarrow \qquad \frac{22}{7} = 3 + \frac{1}{7}$$

$$\frac{25}{7}: \qquad \begin{array}{ccccccc} 25 & = & \boxed{3} & \cdot & 7 & + & 4 \\ 7 & = & \boxed{1} & \cdot & 4 & + & 3 \\ 4 & = & \boxed{1} & \cdot & 3 & + & 1 \\ 3 & = & \boxed{3} & \cdot & 1 & + & 0 \end{array} \qquad \Rightarrow \qquad \begin{array}{l} \frac{25}{7} = 3 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3}}} = 3 + \cfrac{1}{1 + \cfrac{4}{3}} = \\ = 3 + \cfrac{1}{\cfrac{7}{4}} = \frac{25}{7} \end{array}$$