Дискретна математика 2

Лекция начинается
-Сегодня у нас клуб упоротых 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 дільником) $b|a$.*
$a \vdots b \Leftrightarrow \exists k \in \mathbb{Z} :\ \ a = kb$

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. $\exists q\ ;\ bq \le a \le b(q+1),\ r = a - bq.$
2. Єдиність
   Нехай $a = bq + r,\ \ a = bq' + r'$
   $0 = b(q - q') + (r - r') \Rightarrow (r - r') \vdots b,\ -|b| < r - r' < |b| \Rightarrow$
   $\Rightarrow r - r' = 0,\ q = q'.$

□

$q = \lfloor \frac{a}{b} \rfloor$ - 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. $d\ -\ \max$ *додатнє 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).
$123 = 456 \cdot 0 + 123$

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

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

Chapter 2

Лекція 2

2.1 Найменше спільне кратне

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

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

Property.

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

Theorem 2.1.1.

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

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

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. $\mathbb{N},\ \vdots,\ \operatorname{lcm},\ \gcd$
> $a \cdot b = \operatorname{lcm}(a, \_) \cdot \gcd(a,\ b)$
>
> $\max\{a_1, \ldots, a_n\} = a_1 + \cdots + a_n - \min\{a_1,\ a_2\} - \cdots - \min\{a_{n-1},\ a_n\} + \min\{a_1,\ a_2,\ a_3\} - \min\{a_1,\ a_2,\ a_3,\ a_4\}$

2.2 Евклідові послідовності

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

Theorem 2.2.1.

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

Proof.
$n = m$ - очевидна.

$n > m$:

$d = \gcd(n,\ m,)$ АЕ 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* $u,\ v$ *- недодатнє, 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.

$\gcd(a,\ b)\ -\ \min$ *додатнє 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

$f(x_1,\ x_2\ , \ldots,\ x_n) = 0,\ x_i \in \mathbb{Z}$
$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c,\ a_i \in \mathbb{Z},\ c \in \mathbb{Z}$
$ax + by = c,\ \ a,\ b,\ c \in \mathbb{Z}$ - 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 $c \dot{\vdots} d$, 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
$5x + 3y = 9$
$1 = 5 \cdot (-1) + 3 \cdot 2$
$x_0 = 9,\ y_0 = 18$
$$\begin{cases} x = -9 + 3 \cdot t \\ y = 18 - 5 \cdot t \end{cases}$$
$t = 10 : \qquad x = -9 + 30 = 21,\ y = 18 - 50 = -32$

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

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

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

Chapter 4

Лекція 4

4.1 Прості числа

$n \in \mathbb{N}$ - 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.

$Q = p_1 p_2 p_3 \ldots p_n + 1 \Rightarrow Q \vdots p_i,\ n = \overline{1, n}$

Q - або просте, або має простий дільник □

Consequence.

Простих чисел нескінченно багато

Lemma 4.1.3.

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

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 ~~4~~ 5 ~~6~~ 7 ~~8~~ 9 ~~10~~ 11 ~~12~~ 13 ~~14~~ 15 ~~16~~ 17 ~~18~~ 19 ~~20~~
// Беремо перше незакреслене число. Це число 3 - воно просте. Викреслюємо кожне трете число в цьому ряду.
(2) (3) ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~
// Беремо наступне. Це 5 - просте. Викреслюємо кожне п'яте число. Ну вони вже викреслині. Тому далі уже нічого не викреслюється.
(2) (3) ~~4~~ (5) ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~

Lemma 4.2.1.

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

Proof. Від супротивного □

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

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

> **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 (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)**.**

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

Proof.

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

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 чысло, 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