1 Paskaita.

Dalumo su liekana teorema. Didžiausias bendras daliklis.Euklido algoritmas. Tarpusavyje pirminiai skaičiai. Pirminiai skaičiai. Pagrindinė aritmetikos teorema.

Apibrėžimas. Tegu a ir b yra sveikieji skaičiai. Sakysime, kad a dalijasi iš b (be liekanos), jeigu egzistiuoja toks sveikasis skaičius c, kad $a = b \cdot c$. Sakome, kad skaičius b yra a daliklis. Žymėsime $a \vdots b$.

Išvados. 1. Tegu $a, b, c \in Z$ ir $a \vdots c$, $b \vdots c$. Tada $(a \pm b) \vdots c$.

2.Tegu $a, b, c \in Z$ ir $a \vdots c$. Tada $ab \vdots c$.

3.Tegu $a \in Z, a \neq 0$. Tada $0 \vdots a$.

4.Tegu $a \in Z$. Tada $a \vdots 1$.

5.Tegu $a \in Z, 1 \vdots a$. Tada $a = \pm 1$.

Visiško sutvarkymo principas. Tegu k_0- sveikasis skaičius. Bet kuris netuščias sveikųjų skaičių ne mažesnių už k_0 ($\geq k_0$) poaibis turi mažiausią elementą. Bet kuris netuščias sveikųjų skaičių ne didesnių už k_0 ($\leq k_0$) poaibis turi didžiausią elementą.

Teorema(dalybos su liekana teorema). Tegu a ir $b-$ sveikieji skaičiai ir $b \neq 0$. Tada egzistuoja vienintėliai sveikieji skaičiai q ir r su kuriais teisinga lygybė $a = bq + r$, čia $0 \leq r < |b|$.

Įrodymas. Nagrinėkime sveikųjų skaičių seką$\{a - k \cdot b | k \in Z\}$:

$$\ldots, a - 2k, a - k, a, a + k, a + 2k, \ldots .$$

Šioje sekoje yra tiek teigiami ,tiek neigiami skaičiai. Pagal Visiško sutvarkymo principą neneigiamų (kai $k_0 = 0$) sekos narių posekyje galima rasti mažiausią skaičių $r = a - qb \geq 0$. Tada

$$a = bq + r \text{ ir } 0 \leq r < |b| .$$

Parodysime, kad taip parinktas r yra vienintėtis. Tegu turime

$$a = bq_1 + r_1 \text{ ir } 0 \leq r < |b|$$

ir tegu $r \neq r_1$, beto $r_1 < r$. Tada yra teisinga $0 < r - r_1 < |b|$ ir galioja lygybė

$$r - r_1 = (q_1 - q)\, b \ ,$$

t.y. $r - r_1$ dalijasi iš b, o tai prieštarauja tam, kad $0 < r - r_1 < |b|$.
Įrodyta.

Apibrėžimas. Tegu $a, b \in Z$. Sveikasis skaičius $d > 0$ vadinamas skaičių a ir b **didžiausiu bendru dalikliu**, jeigu

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

2. Jeigu $a \vdots c . a \vdots c$, tai $d \vdots c$.

Didžiausio bendro daliklio žymuo: $d = \mathrm{BDD}(a, b) = (a, b)$.

Pastaba. $(0, 0) = 0$.

Teorema. Su visais $a, b \in Z, a \neq 0, b \neq 0$ egzistuoja tokie sveikieji skaičiai x_0 ir y_0, kad $(a, b) = ax_0 + by_0$.

Įrodymas.Nagrinėkime sveikųjų skaičių aibę $M = \{ax + by | x, y \in Z\}$. Ši aibė yra netuščia, nes $a, b \in M$. Aibėje M yra tiek teigiami, tiek neigiami skaičiai. Pagal Visiško sutvarkymo principą teigiamų (kai $k_0 = 1$) aibės M poaibyje galima rasti mažiausią skaičių $0 \neq d = ax_0 + by_0$. Parodysime, kad skaičius d ir yra didžiausiais bendras a ir b daliklis: $d = (a, b)$. Parašykime skaičių porai a ir d dalybos su liekana lygybę:

$$a = dq + r, 0 \leq r < d.$$

Tada

$$0 \leq r = a - dq = a - (ax_0 + by_0)\, q = (1 - x_0 q)\, a + (-y_0 q)\, b \in M.$$

Bet d yra mažiausias teigiamas skaičius iš M, todėl $r = 0$, t.y. $a \vdots d$. Panašiai galima parodyti, kad ir $b \vdots d$.

Tegu dabar yra toks sveikas c, kad $a \vdots c$ ir $b \vdots c$. Tada

$$d = \underbrace{\underbrace{a \cdot x_0}_{\text{dalijasi iš } c} + \underbrace{b \cdot y_0}_{\text{dalijasi iš } c}}_{\text{dalijasi iš } c}.$$

Pagal apibrėžimą $d = (a, b)$.
Įrodyta.

Nevienintėlis reiškimas: $6 = (12, -30) = 12 \cdot 3 + (-30) \cdot 1 = 12 \cdot (-2) + (-30) \cdot (-1)$.

Euklido algoritmas BDD skaičiavimui. Turime skaičius a ir b. Rašysime dalybos su liekana teoremą:
Tegu $a_0 = a$ ir $a_1 = b$. Tada

$$\begin{array}{cc} a_0 = a_1 q_1 + a_2 & 0 < a_2 < |a_1| \\ a_1 = a_2 q_2 + a_3 & 0 < a_3 < a_2 \\ \cdots & \cdots \\ a_{k-2} = a_{k-1} q_{k-1} + a_k & 0 < a_k < a_{k-1} \\ a_{k-1} = a_k q_k & \end{array}$$

Sveikieji skaičiai sudaro mažėjančią seką $|a_1| > a_2 > a_3 > \cdots > a_k > a_{k+1} > 0$. Tada $(a, b) = a_{k+1}$.

Apibrėžimas. Du skaičiai $a, b \in Z$ vadinami tarpusavyje pirminiais, jeigu $(a, b) = 1$.

Teorema. Skaičiai $a, b \in Z$ yra **tarpusavyje pirminiai** tada ir tik tada, kada egzistuoja tokie $x, y \in Z$, kad $ax + by = 1$.

Įrodymas. Teiginys iš kairės į dešinę yra teisingas pagal apibrėžimą. Tegu dabar $ax + by = 1$ ir $(a, b) = d$. Tada

$$1 = \underbrace{\underbrace{a \cdot x}_{\text{dalijasi iš } d} + \underbrace{b \cdot y}_{\text{dalijasi iš } d}}_{\text{dalijasi iš } d},$$

t,y. 1 dalijasi iš d ir todėl $d = 1$.
Įrodyta.

Teiginys(tarpusavyje pirminių skaičių savybė). Tegu $a_1, ..., a_m$ ir $b_1, ..., b_n$ yra dvi tokios sveikųjų skaičių sekos, kad $(a_i, b_j) = 1$ su visais $1 \leq i \leq m, 1 \leq j \leq n$. Tada $(a_1 \cdots a_m, b_1 \cdots b_n) = 1$.
Be įrodymo.

Išvados. 1.Jeigu $\frac{a}{b}$ yra nesuprastinama trupmena , tai ir trupmena $\frac{a^n}{b^n}$ yra nesuprastinama su visais natūraliaisiais n.
2. Tegu $c \in Z$ ir $n > 1$. Tada $\sqrt[n]{c}$ yra arba sveikasis skaičius, arba iracionalusis skaičius.

Apibrėžimas. Skaičius $n \in N, n > 1$ vadinamas pirminiu skaičiumi, jeigu jis turi tik šiuos daliklius: $\pm 1, \pm n$.

Teiginys. Bet kuris sveikasis skaičius, nelygus ± 1, dalijasi iš kurio nors pirminio skaičiaus.

Teorema(Euklidas). Yra be galo daug pirminių skaičių.

Įrodymas. Įrodysime prieštaros būdu. Sakykime, egzistuoja baigtinis pirminių skaičių kiekis: $p_1, p_2, ..., p_m$. Skaičius $n = p_1 p_2 \cdots p_m + 1$ dalijasi iš pirminio, taigi egzistuoja toks $i, 1 \leq i \leq m$, kad $n \vdots p_i$. Tada

$$1 = \underbrace{\underbrace{n}_{\text{dalijasi iš } p_i} - \underbrace{p_1 p_2 \cdots p_m}_{\text{dalijasi iš } p_i}}_{\text{dalijasi iš } p_i},$$

t.y. $1 \vdots p_i$, o tai prieštarauja pirminio skaičiaus apibrėžimui($p_i > 1$).
Įrodyta.

Pastaba. Pastebėsime, kad pirmieji pavidalo $p_1 p_2 \cdots p_m + 1$ skaičiai yra pirminiai: $2+1 = 3, 2 \cdot 3 + 1 = 7, 2 \cdot 3 \cdot 5 + 1 = 31, 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211, 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$. Tačiau skaičius $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$ yra sudėtinis.

Teiginys(pirminių skaičių savybė). Tegu $a_1, ..., a_m$ yra tokia sveikųjų skaičių seka, kad skaičius $a_1 \cdot \cdots a_m$ dalijasi iš pirminio p. Tada egzistuoja toks $j, 1 \leq j \leq m$, kad a_j dalijasi iš p.

Be įrodymo.

Pagrindinė aritmetikos teorema. Su kiekvienu natūraliuoju $n > 1$ egzistuoja tokie pirminiai $p_1, p_2, ..., p_s$ (tarp jų gali būti sutampančių), kad $n = p_1 \cdot p_2 \cdot \cdots \cdot p_s$.

Be įrodymo.