Paskaita 6.

Pirminių skaičių savybės (faktorizacija)

Def. Skaičius $p > 1$, $p \in \mathbb{N}$ yra pirminis, jei jis turi lygiai du daliklius – 1 ir p (t.y. dalus tik iš p).

$24 : 6 = 4$
$8 \cdot 3$ – 6 nėra pirminis

T.1 Jei pirminis p yra skaičiaus ab daliklis, tai jis yra bent vieno iš skaičių a ir b daliklis (atrodo trivialu bet reikia įrodyti).

◁ Tarkime, kad a – nesidalina iš p. Tada $\gcd(a, p) = 1$. Egzistuoja $x, y \in \mathbb{Z}$

$$ax + py = 1. \quad \text{(dauginame iš } b\text{)}$$

$$abx + pby = b.$$

ab yra dalus iš p, pb yra dalus iš p,
$\Rightarrow$ b yra dalus iš p: $b = pl$. ▷

Kiekvienas $a \in \mathbb{N}$, $a > 1$ turi pirminį daliklį.

◁ Kiekvienas $a > 1$ turi daliklį $a > 1$. Tačiau a ne būtinai pirminis!

Tarp visų daliklių > 1 egzistuoja mažiausias. (priminti natūralių skaičių aksiomas!)

Pažymėkime jį p. Tada p būtinai yra pirminis, priešingu atveju būtų daliklis b:

$$1 < b < p \le a,$$

O tuo pačiu b būtų ir a daliklis. Šis prieštaravimas įrodo teiginį. ▷

T3. Jeigu pirminis skaičius $p > 1$ yra daliklis skaičiaus, sudaryto iš pirminių skaičių sandaugos

$$a = \prod_{j=1}^{k} q_j, \quad q_j > 1, \quad q_j \text{ – pirminiai},$$

tai p yra lygus vienam iš q_j.

◁ Mat. indukc. metodas. Jei $k = 1$, tai p yra $q_1 > 1$ daliklis. Bet q_1 turi tik vieną daliklį q_1 $\Rightarrow$ $p = q_1$.

parodysime, kad teiginys teisingas visiems

$1 \le k < K$ $\quad (k \le K-1)$

$$\underbrace{q_1}_{a}\, \underbrace{q_2 \cdots q_K}_{} = q_1 \overbrace{(q_2 \cdots q_K)}^{b}$$

Iš T1 seka, kad p yra arba q_1

arba $(q_2 \cdots q_K)$ daliklis $\Rightarrow$ pagal indukcinę prielaidą ~~sutampa~~ lygus kuriam nors skaičiui q_j.

T4. Kiekvieno sveiko skaičiaus $a > 1$

~~gali~~ vieninteliu būdu gali būti išskaidomas į pirminių skaičių sandaugą

(perstatymų prasme - vienintelis)

$$a = p_1 p_2 \cdots p_k, \quad p_j > 1.$$

Pirma parodysime kad skaidinys egzistuoja.

~~[illegible]~~ Tarkime $a = 2$,

tada teoremos teiginys yra teisingas.

Tegul $a > 2$. Tada a būtinai turi

pirminį daliklį p (T2)

Jei $a/p = 1$, tai $a = p$ (pirminis) skaidinį radome;

Jeigu $a/p > 1$, tai ~~pagal indukcijos prielaidą~~ $a/p = a_2$ ⇒ $a = p a_2$, $a_2 < a$

⇒ $a = p_1 p_2 \dots p_k$

Tai įrodo skaidinio egzistavimą.

Dabar įrodysime vienatį.

Tarkime kad a turi du skaidinius (a-yra mažiausias skaičius turintis du skaidinius)

$a = p_1 \dots p_k$ ir $a = q_1 \dots q_l$.

Tada p_1 yra ~~du~~ skaičiaus a daliklis ir iš T3 seka, jog p_1 yra lygus kažkuriam q_j. Perstatę $q_1, \dots, q_l$, galime laikyti, jog $p_1 = q_1$. Tada pagal matematinės indukcijos prielaidą

$a/p_1 = a/q_1$ yra išskaidomas vieninteliu būdu į pirminių skaičių sandaugą. ▷

šiuo metu ~~negzistuoja~~ nežinome kol kas greito algoritmo, kaip rasti n faktorizaciją pirminiais daugikliais.

Teoriniai ~~A~~ generuoti pirminius skaičius $(\leq \sqrt{n})$ ir tikrinti ar jie nėra dalikliai.

Išvada: tai užtikrina saugumą iš RSA algoritmo (bet, aišku, remiasi kad tai nėra visiškai saugus algoritmas)

Pirminių skaičių sekos sudarymas (faktorizacija)

T: Jei $n > 1$ ~~=~~ nėra pirminis, tai jis turi daliklį $p \leq \sqrt{n}$ (įrodyti)

◁ $n = p \cdot b$, $p > 1$ mažiausias pirminis daliklis, $p \leq b$

$p^2 \leq p \cdot b = n. \Rightarrow p \leq \sqrt{n}.$ ▷

Eratosteno rėtis

Eratosteno rėtis

Aptarti paprastą algoritmus (efektyvumas atnaujinimui!)

(a) daliname iš $2, \dots, n-1$

b) daliname iš $2, \dots, \sqrt{n}$

c) daliname iš p, $2 \le p \le \sqrt{n}$. – pirminių.

Algoritmas

1	2	3	...	...	...	n

for ($j = 2$, $j \le \sqrt{n}$, $j{+}{+}$)

if ($j \in P$) {

Pašaliname iš rėčio

jk, $k = 2, 3, \dots, \left[\frac{n}{j}\right]$

}

Skaičiai kurie liko aibėje P yra pirminiai

Labor 1) Išskaidyti 37800

2) $F_5 = 2^{2^5} + 1 = 641 \cdot 6700417$.