

Paskaita 6

Pirminieš skaicis saugbei (faktorizācija)

Skaicis

Def. $p > 1$
 $p \in \mathbb{N}$ yra pirminis, jei jis skai
lygiam du daliklius - 1 ir p .

(t.y. dalus tik $\bar{0}$ ir p).

$$\begin{array}{r} 24 : 6 = 4 \\ \text{"} \\ 8 \cdot 3 \leftarrow 6 \text{ nėra pirminis} \end{array}$$

T.1 Jei p yra ^{pirminis} skaičius a ir b daliklis,
tai jis yra bent vienas iš skaičių a ir b
daliklis (atodo formalu bet reikia
įrodyti)

▶ Tarkime, kad a - nesidalina $\bar{0}$ ir p

Tada $\gcd(a, p) = 1$. Egzistuoja

$x, y \in \mathbb{Z}$:

$$ax + py = 1.$$

(dauginame \bar{b})

$$abx + pby = b.$$

ab yra dalus $\bar{0}$ ir p , pby yra dalus $\bar{0}$ ir p ,
 $\Rightarrow b$ yra dalus $\bar{0}$ ir p : $b = pt$. ▶

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

▲ Kiekvienas $a > 1$ turi daliklį $a > 1$.
Tada a ^{ne būtina} ~~priminis~~?
Tarp visų daliklių > 1 egzistuoja mažiausias.
(priminti ~~teigiamas~~ natūralūs skaičiai akronomai)
Pažymėkime jį p . Tada p būtinai
yra priminis, nes p ^{p-turis} ~~būtinai~~ daliklis b :

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

o tuo pačiu a b būtų a daliklis.
Šis prieštaravimas grodo teigiamą. ▲

T3. Jeigu a ^{priminis skaičius} > 1 yra daliklis skaičiaus,
sudaryto iš pirminių skaičių sandaugos
 $a = \prod_{j=1}^k q_j$, $q_j > 1$, q_j - pirminiai,
tai p yra lygus vienam iš q_j .

▲ Mat indukcinės metodus. Jei $k=1$, tai
 p yra $q_1 > 1$ daliklis. Bet q_1 ^{taip} ~~taip~~ p q_1
niekas daliklis $q_1 \Rightarrow p = q_1$.

Jei $a/p = 1$, tai $a = p$ (primus)
skaidinys radome,

Jei $a/p > 1$, tai ~~pagal didulesio~~

~~prelaidy~~ $a/p = \frac{a_2}{p} \Rightarrow a = p a_2,$
 $a_2 < a$

$\Rightarrow a = p_1 p_2 \dots p_k.$

Tai godo skaidinio egzistavimas.

Dabar godysiu rekursi
a yra ^a mažiausias skaidinys kuriam

Tarluome, kad ~~Jedes skaidinys~~
~~yra mažiausias skaidinys kuriam~~

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

Tada p_1 yra da skaidinys a deliklis

ir is T^3 seka, jog p_1 yra lygus

kokiame q_j . Perstatyte $q_1, \dots, q_l,$

geline lankyti jog $p_1 = q_1$. Tadien

pagal matematines indukcijos prelaidy

$a/p_1 = a/q_1$ yra isskaidomas

reikinteliu kaidu ϵ puresnis skaidis

sandarys. \square

šio metu nepastovūs veiksmai
iš naujo greičiau algoritmus, kaip
reikš a faktorizacija į pirminius
daugiklius.

22. Tiesiog generuoti pirminius
skaičius ($\leq \sqrt{n}$) ir tikrinti ar
jie nėra dalikliai.

Tranda. Tai uždar. modeliuojama iš
reikš RSA algoritmus (bet, aišku,
kad tai nėra visiški sąlygų algoritmas)

Pirminis skaičių sekos sudarymas (faktorizacija)

T? Jei $n > 1$ nėra pirminis, tai
jis turi daliklį $p \leq \sqrt{n}$. (problema)

▶ $n = p \cdot b$ $b > 1$ mažesnis
pirminis daliklis. $p \leq b$
 $p^2 \leq p \cdot b = n \Rightarrow p \leq \sqrt{n}$.



eratostens reĳis

Eratostens reĳis

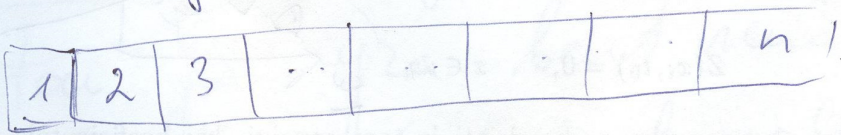
Aptarti paprasĳi algoritmus (efektives atminties naud)

a) delimitas is $2, \dots, n-1$

b) delimitas is $2, \dots, \sqrt{n}$

c) delimitas is $\# 2 \leq p \leq \sqrt{n}$ - primams

~~Algoritmas~~ Algoritmas



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

if ($j \in P$) {

Pašalinti is ~~to~~ arbes P

$$jk, \left(k = \frac{n}{j}, \dots, \left\lfloor \frac{n}{j} \right\rfloor \right)$$

}

Škarciai, kurie lieka arbes P yra primams

Labor 1) Išskendlyt 37800.

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