Paskaita 3

Euklido algoritmas gcd(a, b)

~~su~~ skaičiavimu

Algoritmo sudėtingumo analizė

Bendras didžiausias daliklis

Def. a ir b bendras daliklis yra toks sveikas skaičius, kurio ~~dalijasi~~ dalijasi abu skaičiai a ir b.

T. Tarp a ir b ~~d~~ (~~a~~ iš kurių bent vienas ≠0) ~~d~~ bendrų daliklių yra didžiausias daliklis. gcd(a, b).

~~Δ~~ Tarkime, kad a ≠ 0. Tada visi daliklai $d \le |a|$. Iš išvesties teoremos žinome, kad aprėžtoje aibėje egzistuoja didžiausias. ⊳

Def $g(0,0)=0$ ⟹ $g(a,b) \ge 0$

Pvz. $\gcd(18, 30) = 6$.

$\gcd(-14, 21) = 7$.

Nagrinėkime dėsnį sveikųjų skaičių $a, b \in \mathbb{Z}$ tiesinės kombinacijas

$$a\mathbb{Z} + b\mathbb{Z} = \{ az_1 + bz_2,\ z_1, z_2 \in \mathbb{Z} \}.$$

Pvz. $3\mathbb{Z} + 8\mathbb{Z}$ (kokia tai aibė?)

Kadangi $3 \cdot 3 + 8 \cdot (-1) = 1$, tai

$$3\mathbb{Z} + 8\mathbb{Z} = \mathbb{Z}. \quad (\text{sutampa su } \mathbb{Z}).$$

T. $a\mathbb{Z} + b\mathbb{Z} = \gcd(a, b)\,\mathbb{Z}$.

Akivaizdu pvz. $\gcd(3, 8) = 1$.

a ir b tiesinė kombinacija
yra išreiškiama taip:

$$a\mathbb{Z} + b\mathbb{Z} = \gcd(a,b)\mathbb{Z}.$$

▲ 1) Jei $a=b=0$, tai lygybė yra trivialė teisinga, nes

$$0 = 0.$$

2) Tarkime, kad $a \neq 0$.

Pažymėkime $\underline{I} = a\mathbb{Z} + b\mathbb{Z}$.

Tegul $g \in \mathbb{N}$ yra mažiausias teigiamas sveikas skaičius, priklausantis $\underline{I}$.
(Toks g - visada egzistuoja)
Parodysime, kad $\underline{I} = g\mathbb{Z}$. Imkime bet kokį $c \in \underline{I}$. Parodysime, kad tada

$$c = gq, \quad q \in \mathbb{Z}.$$

Iš dalybos su liekana formulės gausime

$$c = gq + r, \quad 0 \leq r < g.$$

Tada: $r = c - gq \in \underline{I}$. Bet g yra mažiausias $\underline{I}$ elem

Todėl $r=0$ ir $\boxed{c=gq.}$ ∇

Lieka parodyti, kad $g=\gcd(a,b)$

~~Kadangi $g\in I$~~

~~Kadangi $a\in I$, $b\in I$, tai g yra bendras a ir b daliklis~~

~~Kadangi $g\in I$~~, ~~todėl g yra jų bendras daliklis.~~

1) $a\in I$, $b\in I=g\mathbb{Z}$, tai g yra a ir b bendras daliklis $\Rightarrow g\le \gcd(a,b)$

2) $g\in I$, todėl $\exists x,y\in\mathbb{Z}$, $g=ax+by$.

Tegul d yra ~~bendras~~ skaičių a ir b bendras daliklis, tai jis yra ir g daliklis. Todėl turime $|d|\le g$. Daliklių aibė yra apribota $\Rightarrow$ ∃ didžiausias bendras daliklis. ~~Kadangi g yra maksimalus elementas $\subset I$~~

Todėl $g\ge\gcd(a,b)$

~~ir kadangi $\gcd(a,b)$ yra I elementas,~~ 1) I generuojama

~~g yra maksimalus~~ $g\le\gcd(a,b)\Rightarrow=$ ∎

Išvada. Lygtis (Realizuoji skaičius aukščiau turime teiginį spr.)

$ax+by=n$ yra išsprendžiama

$(x, y \in \mathbb{Z})$ tada ir tik tada, kai

$\gcd(a,b)$ yra n daliklis.

Įrodymas. 1) Tarkime, kad lygtis

$ax+by=n$ yra išsprendžiama.

Tada $n \in \gcd(a,b)\mathbb{Z}$ ~~$n \in$~~

$n \in a\mathbb{Z}+b\mathbb{Z}$. ir $\Rightarrow n = c\,\gcd(a,b)$

daliklis

2) Tarkime $n = c\,\gcd(a,b) \Rightarrow$ ~~$n \in \gcd$~~

$n \in \gcd(a,b)\mathbb{Z}$

Iš įrodytos teoremos tada seka, kad

$n \in a\mathbb{Z}+b\mathbb{Z} \Rightarrow n = ax+by$,

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

Euklido algoritmas

Šis algoritmas remiasi šiuo teiginiu:

T. 1. Jei $b = 0$, tai $\gcd(a, b) = |a|$

2 Jei $b \neq 0$, tai $\gcd(a, b) = \gcd(|b|, a \bmod |b|)$

◁ 1) teiginys teisingas pagal apibrėžimą

2) (dalyba su liekana) $a = q|b| + a \bmod |b|$

Todėl $\gcd(a, b)$ dalija $|b|$ (tiesiai)

ir $a \bmod |b|$ → yra vienas iš ~~dalik~~ daliklių

$\Rightarrow \gcd(a, b) \leq \gcd(|b|, a \bmod |b|)$

Teisingas ir priešingas teiginys

$\gcd(|b|, a \bmod |b|)$ dalija ir $|b|$ ir a.

Tai ir užbaigia įrodymą ▷

~~$S_2 = e^{-i\frac{\tau}{2}B} e^{+i\tau A} e^{-i\frac{\tau}{2}B}$~~

Visada galime imti $a \geq 0$, $b \geq 0$ (ir $a \geq b$).

$$\gcd(95, 35) = \gcd(35, 25)$$

$$= \gcd(25, 10) = \gcd(10, 5)$$

$$= \gcd(5, 0) = 5.$$

Algoritmas

```
int GCD( a, b) {
    a = |a|;
    b = |b|;
    while ( b != 0) {
        r = a % b;
        a = b;
        b = r;
    }
    return a;
}
```

Kadangi $r_k < b_k$, tai algoritmas užtikrintinai sustos per baigtinį skaičių žingsnių!

Reikia įvertinti kiek atsiras iteracijų (ar algoritmas efektyvus)

Pagrindinė algoritmo lygybė užrašoma šioje formoje

$$\boxed{r_{k-1} = q_k r_k + r_{k+1}}$$

$r_0 = a$, $r_1 = b$ – pradiniai reikšmės

$a = 100$, $b = 35$

k	0	1	2	3	4
r_k	100	35	30	5	0
q_k		2	1	6	

Lemma 1 $q_k \geq 1$, $1 \leq k < n$, $q_n \geq 2$.

◁ Kadangi $r_{k-1} > r_k > r_{k+1} \Rightarrow q_k \geq 1$.

Tarkime $q_n = 1$, $r_{n+1} = 0$.

$\boxed{r_{n-1} = r_n}$ → prieštara ▷

→ Phi - aukso pjūvio konst.

Tegul $\theta = (1+\sqrt{5})/2$. Tada Euklido algoritmo iteracijų skaičius yra nedidesnis nei $(\log b)/(\log\theta) + 1$.

◀ Kadangi iteracijų skaičius pilnumoje tik nuo (a/b) santykio, tai ~~post~~ egzistuoja nagrinėti atvejį:

~~gf~~ $\gcd(a, b) = r_n = 1$.

Išraiškime, kad

$$\boxed{r_k \geq \theta^{n-k}}, \quad 0 \leq k \leq n.$$

Tada ~~ob~~ $b = r_1 \geq \theta^{n-1}$

$$\log b \geq (n-1)\log\theta$$

$$\Rightarrow \boxed{n \leq \frac{\log b}{\log\theta} + 1.}$$

Nelygybės įrodymas gamsime mat. indukcijos metodu.

1. $r_n = 1 = \theta^0$ (teisinga nelygybė).

(indukcija atgal $k' = n - k$, $k = n \Rightarrow k' = 0$,)

2. $r_{n-1} = q_n r_n = q_n \geq 2 > \theta$ (teisinga nelygybė)

3. Tegul teisingos teisingos $\forall k' > k$.

$0 \leq k \leq n-2$

$$r_k = q_{k+1} r_{k+1} + r_{k+2} \geq r_{k+1} + r_{k+2}$$

(Aukso pjūvio lygtis:

$$x^2 - x - 1 = 0.$$

$$x = \frac{1 \pm \sqrt{1+4}}{2} = \frac{1 \pm \sqrt{5}}{2}$$

)

$$\geq \theta^{n-k-1} + \theta^{n-k-2} = \theta^{n-k-1}\left(1 + \frac{1}{\theta}\right) = \theta^{n-k}.$$

▷

Įrodysime, kad $\exists x, y$:

$$\gcd(a,b) = ax + by.$$

Pateiksime Euklido algoritmo modifikaciją, kuri suranda ir x, y:

$$r_{k-1} = q_k r_k + r_{k+1} \quad \text{(Euklido alg.)}$$

$$x_{k+1} = q_k x_k + x_{k-1}$$

$$y_{k+1} = q_k y_k + y_{k-1}$$

$x_0 = 1, \quad x_1 = 0$

$y_0 = 0, \quad y_1 = 1.$

Tada įrodysime lygybę

$$r_k = (-1)^k x_k a + (-1)^{k+1} y_k b.$$

$$\boxed{\gcd(a,b) = (-1)^n x_n a + (-1)^{n+1} y_n b.}$$

$\underbrace{\qquad}_{x} \qquad \underbrace{\qquad}_{y}$

Patikrinsime indukcines prielaidas

$$\boxed{a = r_0} = (-1)^0 x_0 a + (-1)^1 y_0 b = a$$

$$\boxed{b = r_1} = (-1)^1 x_1 a + (-1)^2 y_1 b = b.$$

Imkime $k \geq 2$ ir tarkime, kad lygybė teisinga $k' < k$. Tada:

$$r_k = r_{k-2} - q_{k-1} r_{k-1} = (-1)^{k-2} x_{k-2} a + (-1)^{k-1} y_{k-2} b$$

$$- q_{k-1} \left[(-1)^{k-1} x_{k-1} a + (-1)^{k} y_{k-1} b \right]$$

$$= (-1)^k a \left(x_{k-2} + q_{k-1} x_{k-1} \right) + (-1)^{k+1} b \left(y_{k-2} + q_{k-1} y_{k-1} \right)$$

$$\qquad\qquad \| \qquad\qquad\qquad\qquad \|$$

$$\qquad\quad x_k \qquad\qquad\qquad\quad y_k$$

$$= (-1)^k x_k a + (-1)^{k+1} y_k b. \quad \blacktriangleright$$

Galima įrodyti, kad

$$|x| \leq \frac{b}{2\gcd(a,b)}, \quad |y| \leq \frac{a}{2\gcd(a,b)}.$$