Matematične osnove

Jernej Tonejc

Euler

$\mathbb{Z}_n^*$

$a^p \equiv a \pmod{p}$

$\mathbb{Z}_p$

Fermat

$x \equiv a \pmod{n}$

MARS

19. avgust 2012

Načrt

- **Modularna aritmetika in deljivost**
- $\mathbb{Z}_p$, $\mathbb{Z}_n^*$, Fermatov in Eulerjev izrek
- Zahtevnost potenciranja
- Kitajski izrek o ostankih (KIO)

Oznake

- $\mathbb{Z}$ množica celih števil
- $\mathbb{N}$ množica naravnih števil $\{1, 2, 3, \ldots\}$
- $\mathbb{N}_0$ množica naravnih števil, skupaj z 0
- $\mathbb{P}$ množica praštevil $\{2, 3, 5, 7, \ldots\}$

Definicija

a deli b, $a \mid b$, če obstaja $k \in \mathbb{Z}$, da velja $b = ka$.

Definicija

Število p je praštevilo, če ima natanko dva delitelja, 1 in samega sebe.

Definicija

Največji skupni delitelj $\mathrm{D}(a, b)$ celih števil a in b je največje tako število $d \in \mathbb{Z}$, da velja $d \mid a$ in $d \mid b$.

Definicija

Celi števili a in b sta si tuji, če velja $\mathrm{D}(a,b)=1$.
Pišemo $a \perp b$.

Izrek (o deljivosti)

Za poljubni naravni števili a in b, $a \geqslant b$, obstajata $k, r \in \mathbb{N}$, $0 \leqslant r < b$, da velja $a = k \cdot b + r$.

Trditev

Za poljubne $a, b, c \in \mathbb{Z}$ velja $\mathrm{D}(a,b) = D(a - bc, b)$.

Izrek (Evklidov algoritem)

Naslednji algoritem izračuna največji skupni delitelj danih naravnih števil a in b, $a \geqslant b$.

1. $r_{-1} = a$, $r_0 = b$
2. *Dokler je* $r_i \neq 0$*, izračunaj* $r_{i+1} = r_{i-1} - q_i r_i$*, kjer je* $q_i \in \mathbb{N}$ *in* $0 \leqslant r_{i+1} < r_i$.
3. *Če je* $r_n \neq 0$ *in* $r_{n+1} = 0$*, potem je* $\mathrm{D}(a, b) = r_n$.

Izrek (o linearni diofantski enačbi)

Za poljubna $a, b \in \mathbb{Z}$, ne oba 0, ima enačba

$$ax + by = c$$

rešitev natanko tedaj, ko $\mathrm{D}(a, b) \mid c$.

Opomba. Rešitev dobimo z razširjenim Evklidovim algoritmom. Ker $\mathrm{D}(a, b)$ deli levo stran enačbe, je implikacija v desno očitna.

Posledica

Naj $c \mid a$ in $c \mid b$. Potem $c \mid \mathrm{D}(a, b)$.

Izrek

Naj bodo $a, b, c \in \mathbb{Z}$. Relacija deljivosti ima naslednje lastnosti.

(i) *Relacija je refleksivna ($a \mid a$) in tranzitivna ($a \mid b$ in $b \mid c \Rightarrow a \mid c$)*
(ii) *Če $c \mid a$ in $c \mid b$, potem $c \mid a \pm b$.*
(iii) *Če je $\mathrm{D}(a, b) = 1$ in $a \mid bc$, potem $a \mid c$.*
(iv) *Če je p praštevilo in $p \mid ab$, potem $p \mid a$ ali $p \mid b$.*

Definicija

Naj bo $m \in \mathbb{N}$. Celi števili a in b sta kongruentni po modulu m, z oznako $a \equiv b \pmod{m}$, če velja $m \mid a - b$.

Oznaka $x = a \bmod m$ pomeni, da a reduciramo po modulu m, rezultat x je število med 0 in $m - 1$.

Lema

Naj bodo $a, b, c \in \mathbb{Z}$ *in* $m \in \mathbb{N}$.

(i) *Relacija kongruentnosti je ekvivalenčna relacija.*

(ii) *Če je* $a \equiv b \pmod{m}$, *je* $ac \equiv bc \pmod{m}$ *in* $a \pm c \equiv b \pm c \pmod{m}$ *za poljuben* $c \in \mathbb{Z}$.

(iii) *Če je* $a \equiv b \pmod{m}$ *in* $c \equiv d \pmod{m}$, *potem je* $ac \equiv bd \pmod{m}$ *in* $a \pm c \equiv b \pm d \pmod{m}$.

(iv) *Če je* $\mathrm{D}(c, m) = 1$ *in* $ac \equiv bc \pmod{m}$, *potem je* $a \equiv b \pmod{m}$.

(v) *Če je* $\mathrm{D}(c, m) = d > 1$ *in* $ac \equiv bc \pmod{m}$, *potem je* $a \equiv b \pmod{\frac{m}{d}}$.

Načrt

- Modularna aritmetika in deljivost
- $\mathbb{Z}_p$, $\mathbb{Z}_n^*$, **Fermatov in Eulerjev izrek**
- Zahtevnost potenciranja
- Kitajski izrek o ostankih (KIO)

Definicija

Naj bo $p \in \mathbb{P}$. Množico ostankov po modulu p označimo z $\mathbb{Z}_p$. Množico neničelnih ostankov označimo z $\mathbb{Z}_p^*$.

Trditev

Vsak element $a \in \mathbb{Z}_p^*$ ima inverz, tj. obstaja tak $b \in \mathbb{Z}_p^*$, da velja $ab \equiv 1 \pmod{p}$.

Inverz elementa a označimo z $a^{-1} \bmod p$.

Poišči inverze vseh elementov $\mathbb{Z}_7^*$.

Poišči inverz elementa 112 modulo 131.

Izrek (Fermat)

Naj bo $p \in \mathbb{P}$. Potem za vsak element $a \in \mathbb{Z}_p$ velja

$$a^p \equiv a \pmod{p}.$$

OPOMBA. Alternativna oblika izreka pravi

$$a^{p-1} \equiv 1 \pmod{p}$$

za poljuben $a \in \mathbb{Z}$, $p \nmid a$.

Definicija

Naj bo $n \in \mathbb{N}$. Eulerjeva funkcija $\varphi(n)$ šteje, koliko števil, manjših ali enakih n, je tujih n.

Izračunaj $\varphi(6)$, $\varphi(11)$, $\varphi(31)$.

Naj bo $p \in \mathbb{P}$. Dokaži $\varphi(p) = p - 1$.

Definicija

Naj bo $n \in \mathbb{N}$. Množico ostankov po modulu n označimo z $\mathbb{Z}_n$. Množico tistih ostankov, ki so tuji proti n, označimo z $\mathbb{Z}_n^*$.

Izrek (Euler)

Naj bo $n \in \mathbb{N}$ *in* $D(a, n) = 1$. *Potem je*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Dokaz.

Naj bo $D(a, n) = 1$ in $\mathbb{Z}_n^* = \{x_1, x_2, \dots, x_{\varphi(n)}\}$. Potem je $\{ax_i \bmod n \mid 1 \leqslant i \leqslant \varphi(n)\} = \mathbb{Z}_n^*$ (kot množica), saj iz $ax_i \equiv ax_j \pmod{n}$ sledi $x_i \equiv x_j \pmod{n}$ po lemi na strani 10(iv). Potem pa je

$$\prod_{i=1}^{\varphi(n)} x_i \equiv \prod_{i=1}^{\varphi(n)} ax_i \equiv a^{\varphi(n)} \prod_{i=1}^{\varphi(n)} x_i \pmod{n}$$

in po krajšanju sledi $a^{\varphi(n)} \equiv 1 \pmod{n}$. $\square$

Načrt

- Modularna aritmetika in deljivost
- $\mathbb{Z}_p$, $\mathbb{Z}_n^*$, Fermatov in Eulerjev izrek
- **Zahtevnost potenciranja**
- Kitajski izrek o ostankih (KIO)

Potenciranje

- V Eulerjevem in Fermatovem izreku
- Uporablja se pri RSA
- Uporablja se pri Diffie-Hellmanu
- *Kako učinkovito potencirati?*

Izrek (Algoritem kvadriraj in množi)

Naj bosta a, m naravni števili in $m = b_{k-1} \ldots b_1 b_0$ dvojiška predstavitev števila m. Naslednji algoritem izračuna $a^m \bmod n$.

1. $c = 1$
2. *Za* $i = 0, 1, \ldots, k-1$, *ponavljaj:*
3. *Če je* $b_i = 1$, *potem* $c \leftarrow c \cdot a \bmod n$
4. $a \leftarrow a^2 \bmod n$
5. *Vrni* c

OPOMBA. Obstaja tudi alternativna varianta, ki temelji na Hornerjevem algoritmu:

1. $c = 1$
2. Za $i = k-1, \ldots, 0$ ponavljaj:
3. $\quad c \leftarrow c^2 \bmod n$
4. $\quad$ Če je $b_i = 1$, potem $c \leftarrow c \cdot a \bmod n$
5. Vrni c

S pomočjo vsake od različic algoritma izračunajmo 2^{25}. Koliko operacij potrebujemo?

Velja $25 = 11001_2$. Po prvi različici imamo po vrsti (prikazane so vrednosti po koncu vsake ponovitve zanke)

i	0	1	2	3	4
c	2	2	2	512	33554432
a	4	16	256	65536	4294967296

Po drugi različici pa dobimo (prikazana je vrednost c v 3. in 4. vrstici algoritma in vrednost m na začetku zanke):

i	4	3	2	1	0
c_3	1	4	64	4096	16777216
c_4	2	8	64	4096	33554432

V obeh primerih potrebujemo 5 kvadriranj in 3 množenja.

Načrt

- Modularna aritmetika in deljivost
- $\mathbb{Z}_p$, $\mathbb{Z}_n^*$, Fermatov in Eulerjev izrek
- Zahtevnost potenciranja
- **Kitajski izrek o ostankih (KIO)**

Poskusimo rešiti naslednjo nalogo.

Naloga

Babica ima nekaj kovancev. Če jih zlaga v kupčke po 2, ji ostane eden, če jih zlaga v kupčke po 3, se ji lepo izide, če pa v kupčke po 5, ji ostaneta 2. Koliko kovancev ima babica?

Izrek (KIO)

Naj bodo števila $m_1, \ldots, m_k$ *paroma tuja in naj bo* $a_i \in \mathbb{Z}_{m_i}$. *Sistem*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

ima enolično rešitev po modulu $M := \prod_{i=1}^{k} m_i$, *podano z*

$$x = \sum_{i=1}^{k} a_i M_i y_i,$$

kjer je $M_i = \frac{M}{m_i}$ *in* $y_i = M_i^{-1} \bmod m_i$.

Naloga

Babica ima vrečo orehov. Če jih zlaga v kupčke po 3, ji ostaneta 2, če jih zlaga v kupčke po 4, ji ostane 1, če pa jih zlaga v kupčke po 7, ji ostanejo 4. Koliko orehov ima babica, če vemo, da v vrečo ne gre več kot 100 orehov?

Rešujemo sistem enačb

$$\begin{aligned} x &\equiv 2 \pmod 3, \\ x &\equiv 1 \pmod 4, \\ x &\equiv 3 \pmod 7. \end{aligned}$$

Izračunajmo najprej $M = 3 \cdot 4 \cdot 7 = 84$ in $M_1 = 4 \cdot 7 = 28$, $M_2 = 3 \cdot 7 = 21$ in $M_3 = 3 \cdot 4 = 12$. Nato računamo

$$\begin{aligned} y_1 &= 28^{-1} \bmod 3 = 1^{-1} \bmod 3 = 1, \\ y_2 &= 21^{-1} \bmod 4 = 1^{-1} \bmod 4 = 1, \\ y_3 &= 12^{-1} \bmod 7 = 5^{-1} \bmod 7 = 3. \end{aligned}$$

Torej je

$$x \equiv 2{\cdot}1{\cdot}28 + 1{\cdot}1{\cdot}21 + 3{\cdot}3{\cdot}12 \equiv 56 + 21 + 108 \equiv 185 \equiv 17 \pmod{84}.$$