Modulárna aritmetika,
rozšírený Euklidov algoritmus

Modulárna aritmetika

• počítanie v $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, t.j.
všetky operácie $(+, -, \cdot)$ sú modulo n.
• $a \equiv b \,(\mathrm{mod}\, n)$, t.j. "$a$ je kongruentné s b modulo n", znamená, že po delení n dávajú a aj b rovnaký zvyšok.
• $a = t_1 \cdot n + q_1$, $b = t_2 \cdot n + q_2$. Keďže $q_1 = q_2$, tak $a - b = t_1 \cdot n - t_2 \cdot n = (t_1 - t_2) \cdot n$, t.j. $n | (a-b)$.
• Definícia: $a \equiv b \,(\mathrm{mod}\, n) \Longleftrightarrow n | (a-b)$.

Rozšírený Euklidov algoritmus

• Euklidov algoritmus $\rightarrow$ výpočet najväčšieho spoločného deliteľa dvoch čísel (aspoň jedno je rôzne od 0).
• Najväčší spoločný deliteľ dvoch čísel a, b, ozn. (a, b), je $d \in \mathbb{N}$ také, že

(1) $d|a$, $d|b$, t.j. d je spoločný deliteľ

(2) pre každé $k \in \mathbb{N}$: $k|a$, $k|b \Rightarrow k|d$, t.j. d je maximálny

• Platí veta (ako dôsledok Euklidovho algoritmu):
Ak $(a, b) = d$, tak $\exists\, u, v \in \mathbb{Z}$: $u \cdot a + v \cdot b = d$.
• rozšírený Euklidov algoritmus $\rightarrow$ hľadá k a, b hodnoty d, u, v:
- najprv sa spočíta d: (štandartný Euklidov algoritmus)

```
1. ak a < b, tak výmena a <-> b
2. (a >= b) Delenie so zvyškom:
   a : b = m zv. n
3. ak sa n nerovná 0, tak
      a = n, iterácia (n, b) t.j. GOTO 1.
   inak
      koniec ((a, b) = b)
```

- Z tohto postupu dostávame: ($d_{n+1} = 0$, t.j. $(a, b) = d_n$, $d_0 = a$, $d_1 = b$)

$$
\begin{array}{lll}
(1) & d_0 & = m_1 d_1 + d_2 \\
(2) & d_1 & = m_2 d_2 + d_3 \\
(3) & d_2 & = m_3 d_3 + d_4 \\
\ldots & & \\
(n-2) & d_{n-3} & = m_{n-2} d_{n-2} + d_{n-1} \\
(n-1) & d_{n-2} & = m_{n-1} d_{n-1} + d_n \\
(n) & d_{n-1} & = m_n d_n + d_{n+1}
\end{array}
$$

- $(a, b) = d_n = d_{n-2} - m_{n-1} d_{n-1} =$
(nahradíme d_{n-1} výrazom z $(n-2)$, t.j. výrazom $d_{n-3} - m_{n-2} d_{n-2}$)
$= d_{n-2} - m_{n-1}(d_{n-3} - m_{n-2} d_{n-2}) = (1 + m_{n-1} m_{n-2}) d_{n-2} - m_{n-1} d_{n-3} =$
(nahradíme d_{n-2} výrazom z $(n-3)$, t.j. $d_{n-4} - m_{n-3} d_{n-3}$)
$= A_{n-3} d_{n-4} + B_{n-3} d_{n-3} =$

$\dots$
$= A_1 a + B_1 b$
- Výstup: d, $u = A_1$, $v = B_1$

- Keď použití k-tej rovnice máme $d = A_k d_{k-1} + B_k d_k$, tak aplikovaním $(k-1)$. rovnice dostávame:

$d = A_k d_{k-1} + B_k d_k = A_k d_{k-1} + B_k(d_{k-2} - m_{k-1} d_{k-1}) = B_k d_{k-2} + (A_k - B_k \cdot m_{k-1}) d_{k-1} = A_{k-1} d_{k-2} + B_{k-1} d_{k-1}$

Preto:
- $A_n = 0$, $B_n = 1$
- $A_{k-1} = B_k$ a $B_{k-1} = A_k - B_k \cdot m_{k-1}$, pre $k = n, n-1, \dots, 2$.
- Výstup A_1, B_1.

Výpočet inverzných prvkov v $\mathbb{Z}_n$

- v je inverzný prvok k u v $\mathbb{Z}_n$, ak $u \cdot v \equiv 1 \pmod{n}$
- nemusí existovať, ak existuje označuje sa $u^{-1} \bmod n$
- Veta: $u^{-1} \bmod n$ existuje práve vtedy, keď $(u, n) = 1$

Dôkaz: ($\Rightarrow$) Existuje $u^{-1} \bmod n$, t.j. $u \cdot v \equiv 1 \pmod{n} \Leftrightarrow n | (u \cdot v - 1)$, t.j. $1 = u \cdot v - k \cdot n$, pre nejaké $k \in \mathbb{N}$. Nech $d = (u, n) \in \mathbb{N}$, potom keďže $d|u$ a $d|n$, tak $d|(u \cdot v - k \cdot n) = 1$. Čiže $d = 1$.

($\Leftarrow$) Nech $(u, n) = 1$. Z rozšíreného Euklidovho algoritmu dostávame, že existujú $U, V \in \mathbb{Z}$ také, že $U \cdot u + V \cdot n = 1 = (u, n)$. Zobraním poslednej rovnice modulo n dostávame: $U \cdot u \equiv 1 \pmod{n}$. Teda $U \bmod n = u^{-1} \bmod n$.

Z druhej časti dôkazu máme nasledujúci postup $(u, n) = 1$:
- Z rozšíreného Euklidovho algoritmu pre u, n dostávame celé čísla U, V také, že: $U \cdot u + V \cdot n = 1$
- Vyjadrením predošlej rovnosti cez $\bmod n$ máme:
  $U \cdot u \equiv 1 (\mathrm{mod\, n})$
- Preto v $\mathbb{Z}_n$ je $u^{-1} = U \bmod n$.

Príklady

- 1. Použite rozšírený Euklidov algoritmus na nasledujúce dvojice:
  (a) $(52, 14)$, (b) $(73, 18)$, (c) $(59, 27)$, (d) $(81, 11)$, (e) $(34, 19)$, (f) $(68080, 56957)$

- 2. Vypočítajte $u^{-1} \bmod n$ (ak existuje):
  (a) 2^{-1} v $\mathbb{Z}_6$, (b) 17^{-1} v $\mathbb{Z}_{20}$, (c) 23^{-1} v $\mathbb{Z}_{44}$, (d) u^{-1}, $\forall u \in \mathbb{Z}_{12}$,
  (e) u^{-1}, $\forall u \in \mathbb{Z}_{13}$, (f) 9^{-1} v $\mathbb{Z}_{29}$

Riešené príklady

- Použite rozšírený Euklidov algoritmus pre dvojicu $(85, 27)$.

Riešenie:
$85 : 27 = 3$ zv. 4
$27 : 4 = 6$ zv. 3
$4 : 3 = 1$ zv. 1
$3 : 1 = 3$ zv. 0
$1 = \mathbf{4} - 1 \cdot \underline{\mathbf{3}} = \mathbf{4} - 1 \cdot (\mathbf{27} - 6 \cdot \mathbf{4}) = 7 \cdot \underline{\mathbf{4}} - 1 \cdot \mathbf{27} = 7 \cdot (\mathbf{85} - 3 \cdot \mathbf{27}) - 1 \cdot \mathbf{27} = 7 \cdot \mathbf{85} - 22 \cdot \mathbf{27}$
Preto $(85, 22) = 1$ a $1 = 7 \cdot 85 - 22 \cdot 27$.
Alernatívne:
$(0, 1)$, $(1, 0 - 1 \cdot 1) = (1, -1)$, $(-1, 1 - (-1) \cdot 6) = (-1, 7)$, $(7, -1 - 7 \cdot 3) = (7, -22)$. T.j. $7 \cdot 85 + (-22) \cdot 27 = 1$

- Zistite $16^{-1} \bmod 53$ a $53^{-1} \bmod 16$ (ak existuje).

Riešenie:
(1) Použijeme zovšeobecnený Euklidov algoritmus pre dvojicu $(53, 16)$
$53 : 16 = 3$ zv. 5
$16 : 5 = 3$ zv. 1
$5 : 1 = 5$ zv. 0
$1 = 16 - 3 \cdot 5 = 16 - 3 \cdot (53 - 3 \cdot 16) = 10 \cdot 16 - 3 \cdot 53$.
Alebo: $(0, 1)$, $(1, 0 - 1 \cdot 3) = (1, -3)$, $(-3, 1 - (-3) \cdot 3) = (3, 10)$
$(53, 16) = 1$, preto existujú príslušné inverzné hodnoty.
(2) Pre výpočet $16^{-1} \bmod 53$ zoberieme poslednú rovnosť modulo 53:
$1 = 10 \cdot 16 - 3 \cdot 53 \mod 53 = 10 \cdot 16 \mod 53$, pre $16^{-1} \mod 53 = 10$.
(3) Pre výpočet $53^{-1} \mod 16$ zoberieme poslednú rovnosť modulo 16:
$1 = -3 \cdot 53 \mod 16$, $53^{-1} \mod 16 = -3 \mod 16 = 13$.