Užitočné algoritmy z teórie čísel

- najväčší spoločný deliteľ (GCD - greatest common divisor)
- Eulidov algoritmus
- rozšírený Euklidov algoritmus
- Fermatova veta

Primárny zdroj informácii k dnešnej prednáške:

[1] prof. Ing. Dušan Levický, CSc.
APLIKOVANÁ KRYPTOGRAFIA
od utajenia správ ku kybernetickej bezpečnosti
Elfa, Košice, 2018 (str.34-36, 123-124)

[2] Drutarovský, M.: Kryptografia pre vstavané kryptografické systémy. TUKE, 2017 (str.35-36)

[14] MENEZES, Alferd J.; OORSCHOT, Paul C.; VANSTONE, Scott A. *Handbook of Applied Cryptography*. 1st ed. New York: CRC Press, 1996. ISBN 0-8493-8523-7. Dostupné tiež z: http://cacr.uwaterloo.ca/hac/.

Cieľom tejto časti prednášky je **opísať vybrané vety a algoritmy**, ktoré sú pri implementácii kryptografických algoritmov najčastejšie využívané. Ich implementácie sú často **súčasťou kryptografických knižníc** a cieľom krátkeho úvodu je zosumarizovať základné informácie tak, aby mohli byť tieto vybrané algoritmy precvičené na cvičení. Zameriame sa na algoritmy, ktoré potrebujeme predovšetkým na výpočet algoritmu RSA, ktorý bol preberaný na minulej prednáške. Časť týchto algoritmov na cvičení overíme ručným výpočtom. V kryptografickej praxi však, samozrejme, realizujeme výpočty s veľkými číslami. Na tieto výpočty využijeme **Magma kalkulačku** a **špecializované knižnice**.

Deliteľnosť čísel na množine Z [1, str.34-35]

Definícia 3.13. Nech čísla $a,b \in Z$. Číslo ***b* je deliteľné číslom *a*** práve vtedy, ak existuje také číslo $q \in Z$, že

$$b = a \cdot q \,, \tag{3.1}$$

čo vyjadrujeme zápisom $a \mid b$. Ak takéto číslo $q \in Z$ neexistuje, hovoríme, že ***a nedelí b***, čo vyjadrujeme zápisom $a \nmid b$. Číslo *a* je deliteľom čísla *b*, číslo *b* je násobkom čísla *a*.

Najväčší spoločný deliteľ

Definícia 3.14. Nech $a,b \in Z$. **Najväčším spoločným deliteľom** čísel *a,b* nazývame najväčšie celé kladné číslo *d*, pre ktoré platí $d \mid a$ a zároveň $d \mid b$.

Najväčší spoločný deliteľ (greatest common divisor) čísel *a,b* budeme označovať symbolom $\gcd(a,b)$.

Uvedenú definíciu možno zapísať aj v tvare

$$\gcd(a,b) = \max \{\, d \in \square \text{ , také, že } d \mid a \text{ a } d \mid b \,\}$$

Pretože najväčší spoločný deliteľ má byť celé číslo, potom platí

$$\gcd(a,b) = \gcd(a,-b) = \gcd(-a,b) = \gcd(-a,-b) = \gcd(|a|,|b|)$$

Príklad

$$\gcd(60,24) = \gcd(60,-24) = 12$$

Definícia 3.15. Nech $a,b \in Z$. Ak $\gcd(a,b) = 1$, hovoríme, že ***a je nesúdeliteľné s b***. Vzhľadom k tomu, že $\gcd(a,b) = \gcd(b,a)$, namiesto výrazu *a* je nesúdeliteľné s *b*, hovoríme, že ***a,b sú nesúdeliteľné*** (relative prime).

Euklidov algoritmus

Systematickú metódu hľadania najväčšieho spoločného deliteľa vyvinul **Euklides**(1) a je známa ako **Euklidov algoritmus**. Uvedený algoritmus možno opísať schémou, ktorá vychádza z vety o delení so zvyškom.

Nech $b \nmid a$ a nech $b \neq 0$. Podľa vety o delení so zvyškom existujú také celé čísla q_1, r_2, pre ktoré je $a = b \cdot q_1 + r_2$ a $0 \leq r_2 < |b|$. Použijeme opäť vetu o delení so zvyškom na dvojicu b, r_2, podľa ktorej existujú také čísla q_2, r_3, pre ktoré platí $b = r_2 \cdot q_2 + r_3$ a $0 \leq r_3 < r_2$. Pretože zvyšky r_2, r_3 ... sú klesajúce nezáporné čísla, určite sa po konečnom počte krokov vyskytne nulový zvyšok.

Uvedený postup možno opísať schémou, ktorá sa nazýva **Euklidov algoritmus** a možno ho zapísať ako postupnosť krokov

$$
\begin{aligned}
a &= b \cdot q_1 + r_2 \quad \text{pričom podľa 3.14.3. platí} & \gcd(a,b) &= \gcd(b,r_2)\\
b &= r_2 \cdot q_2 + r_3 & \gcd(b,r_2) &= \gcd(r_2,r_3)\\
r_2 &= r_3 \cdot q_3 + r_4 & \gcd(r_2,r_3) &= \gcd(r_3,r_4)\\
&\vdots & &\vdots\\
r_{n-2} &= r_{n-1} \cdot q_{n-1} + r_n & \gcd(r_{n-2},r_{n-1}) &= \gcd(r_{n-1},r_n)\\
r_{n-1} &= r_n \cdot q_n + 0 & \gcd(r_{n-1},r_n) &= \gcd(r_n,0) = r_n
\end{aligned}
$$

teda $\gcd(a,b) = r_n$

Veta 3.4. Nech $a,b \in Z$, $b \neq 0$, $b \nmid a$, potom posledný nenulový zvyšok v Euklidovom algoritme pre dvojicu čísel a,b je najväčším spoločným deliteľom čísel a,b.

(1) **Euklides** – grécky matematik (4. stor. až začiatok 3. storočia p.n.l.)

Príklad

Nájdite $\gcd(a,b) = \gcd(252,158)$ *pomocou Euklidovho algoritmu.*

$$
\begin{aligned}
252 &= 1 \cdot 158 + 94 \\
158 &= 1 \cdot 94 + 64 \\
94 &= 1 \cdot 64 + 30 \\
64 &= 2 \cdot 30 + 4 \\
30 &= 7 \cdot 4 + 2 \qquad r_n = 2 \\
4 &= 2 \cdot 2 + 0
\end{aligned}
$$

Formálne môžeme Euklidov algoritmus zapísať takto [2, str.34]:

Algoritmus 3.7 Euklidov algoritmus pre výpočet najväčšieho spoločného deliteľa dvoch celých čísel [14, alg. 2.104]

Input: dve nezáporné celé čísla a a b, pričom $a \geqq b$
Output: najväčší spoločný deliteľ a a b

1: **while** $b \neq 0$ **do**
2: $\quad r \leftarrow a \bmod b,\ a \leftarrow b,\ b \leftarrow r$
3: **return** a

Modulárna inverzia a rozšírený Euklidov algoritmus [2, str.35-36]

V modulárnej aritmetike realizujeme operáciu delenia číslom a (ak pre dané a existuje) modulárnym násobením inverzným multiplikatívnym číslom a^{-1}, pre ktoré platí

$$a \cdot a^{-1} \equiv 1 \pmod{m}.$$

Inverzné multiplikatívne číslo a^{-1} existuje len pre také a, pre ktoré platí $\gcd(a, m) = 1$, takže a a m musia byť nesúdeliteľné[9], a symbolom gcd() označujeme operáciu GCD. Štandardný Euklidov algoritmus je využívaný na výpočet GCD dvoch kladných celých čísel a, b, $a \geqq b$, vypočítame ho pomocou algoritmu 3.7.

[9]Napríklad v $\mathbb{GF}(p)$ existuje inverzia pre každý nenulový prvok $\mathbb{GF}(p)$ a preto môžeme v $\mathbb{GF}(p)$ využívať operáciu „delenia" klasickým spôsobom, na ktorý sme zvyknutí v klasickej aritmetike.

Rozšírený Euklidov algoritmus (EEA – Extended Euclidean Algorithm) je efektívnou metódou výpočtu, pomocou ktorej môžeme vypočítať aj mutiplikatívnu inverziu, čo je v implementáciách kryptografických algoritmov pomerne často využívané. EEA pre dve kladné celé čísla a, b, $a \geqq b$ vypočíta okrem $d = \gcd(a, b)$ aj dve celé čísla x, y tak, aby platilo $ax + by = d$, Výpočet je možné realizovať pomocou algoritmu 3.8. V prípade že $b = m$, vráti algoritmus 3.8 hodnotu $x \equiv a^{-1} \pmod{m}$.

Algoritmus 3.8 Rozšírený Euklidov algoritmus [14, alg. 2.107]

Input: dve nezáporné celé čísla a a b, pričom $a \geqq b$
Output: $d = \gcd(a, b)$ a celé čísla x, y, pre ktoré platí $ax + by = d$

1: **if** $b = 0$ **then**
2: $\quad d \leftarrow a$, $x \leftarrow 1$, $y \leftarrow 0$
3: $\quad$ **return** d, x, y
4: $x_2 \leftarrow 1$, $x_1 \leftarrow 0$, $y_2 \leftarrow 0$, $y_1 \leftarrow 1$
5: **while** $b > 0$ **do**
6: $\quad q \leftarrow \lfloor a/b \rfloor$, $r \leftarrow a - qb$, $x \leftarrow x_2 - qx_1$, $y \leftarrow y_2 - qy_1$
7: $\quad a \leftarrow b$, $b \leftarrow r$, $x_2 \leftarrow x_1$, $x_1 \leftarrow x$, $y_2 \leftarrow y_1$, $y_1 \leftarrow y$
8: $d \leftarrow a$, $x \leftarrow x_2$, $y \leftarrow y_2$
9: **return** d, x, y

Aj keď Algoritmus 3.8 je **algoritmicky** stále **pomerne jednoduchý**, na cvičení využijeme na jeho výpočet vhodnú **funkciu v kalkulačke Magma**. Dôležité je predovšetkým pochopenie jeho **využitia na výpočet modulárnej inverzie** opísaný v tejto časti.

Modulárna inverzia a Fermatova veta [2, str.123-124]

Výpočet modulárnej inverzie je možné realizovať aj s využitím Fermatovej vety. Tento spôsob výpočtu modulárnej inverzie je **výpočtovo menej efektívny** ako využitie EEA. Využíva sa však často v prípadoch, ak výpočet **EEA nie je v cieľovom zariadení implementovaný** a výpočet modulárnej inverzie nie je **časovo kritickou** operáciou.

Fermatova[3] veta, niekedy tiež označovaná ako *Malá Fermatova veta*, má v kryptografii zásadný význam a bola formulovaná takto:

Veta 6.3. (Malá Fermatova veta) Nech $a \in Z$ a nech p je prvočíslo také, že $p \nmid a$. Potom

$$a^{p-1} \equiv 1 \bmod p \tag{6.4}$$

Dôsledok: Nech $a \in Z$ a nech p je prvočíslo. Potom

$$a^{p} \equiv a \bmod p \tag{6.5}$$

Ďalším použitím Malej Fermatovej vety je výpočet multiplikatívnej inverzie čísla $a \in N$ modulo p.

Veta 6.4. Nech $a \in N$ a p je prvočíslo také, že $p \nmid a$. Potom a^{p-2} je multiplikatívna inverzia čísla a modulo p.

Dôkaz: Ak $p \nmid a$, potom z Malej Fermatovej vety vyplýva, že $a^{p-1} = a \cdot a^{p-2} \equiv 1 \bmod p$. Z definície multiplikatívnej inverzie 3.20 vyplýva, že a^{p-2} je multiplikatívna inverzia čísla a modulo p.

Príklad
Nájdite multiplikatívnu inverziu čísla $2 \bmod 7$.

Pretože a=2, p=7 a teda $p \nmid a$, *platí podľa Malej Fermatovej vety, že* $2^6 \equiv 1 \bmod 7$, *resp. podľa vety 6.4 platí, že* $2 \cdot 2^5 \equiv 1 \bmod 7$. *Multiplikatívna inverzia čísla a=2 modulo 7 je potom* $2^5 \bmod 7 = 32 \bmod 7 = 4$.

Číslo 4 je teda multiplikatívna inverzia čísla 2 modulo 7.

Pre zaujímavosť:
https://sk.wikipedia.org/wiki/Ve%C4%BEk%C3%A1_Fermatova_veta

Veľká Fermatova veta

[nezobrazovať]

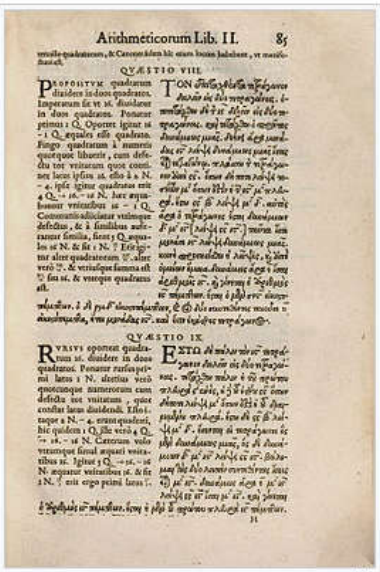
Veľká Fermatova veta je jedna z najslávnejších viet v dejinách matematiky. Znie nasledovne:

> Nejestvujú celé čísla x, y a z väčšie ako nula, pre ktoré by platilo $x^n + y^n = z^n$, kde n je prirodzené číslo väčšie ako 2.

Vetu si roku 1637 poznamenal francúzsky matematik Pierre de Fermat na okraji knihy *Arithmetica* pri Pytagorovej vete od Diofanta v tejto podobe:

> *Cubum autem in duos cubos, aut quadrato-quadratum in duos quadrato-quadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exigitas non caperet.*
>
> Po slovensky: *Nie je možné rozdeliť kocku do dvoch kociek, či štvrtú mocninu do dvoch štvrtých mocnín alebo všeobecne akúkoľvek mocninu vyššiu ako druhú do dvoch rovnakých mocnín. Objavil som naozaj taký zvláštny dôkaz, že tento okraj knihy je primalý na to, aby sa tam vošiel.*

Uvedený dôkaz ale nebol v jeho pozostalosti objavený. Vie sa však, že Fermat našiel dôkaz pre $n = 4$, ale pravdepodobne nie pre iné exponenty.



Strana 85 z Diofantovej knihy *Arithmetica* (vyd. 1621). Práve na strane 85 napísal Fermat svoje tvrdenie.

Obsah [skryť]

Dôkazy [upraviť | upraviť zdroj]

Počas nasledujúcich storočí sa podarilo dokázať niektoré ďalšie zvláštne prípady vety. Prípad $n = 4$ našiel vo Fermatovej pozostalosti matematik Leonhard Euler a pomocou komplexných čísel dokázal platnosť vety pre $n = 3$. Na základe jeho prác sa podarilo rozšíriť platnosť vety pre n rovné všetkým násobkom čísel 3 a 4 (3, 6, 9, ...; 4, 8, 12, ...).

Roku 1825 rozšírili platnosť vety Peter Gustav Lejeune Dirichlet a Adrien-Marie Legendre pre $n = 5$ a roku 1839 dokázal platnosť vety Gabriel Lamé aj pre $n = 7$.

Definitívny dôkaz pokrývajúci Fermatovo tvrdenie v celej jeho všeobecnosti získal až britský matematik Andrew Wiles roku 1994. Ide o jeden z najzložitejších matematických dôkazov v dejinách matematiky.

Vyššie opísané algoritmy sú len **malou časťou** v kryptografickej praxi využívaných algoritmov. S ich využitím (spolu s už prebranou modulárnou mocninou) je však možné implementovať pomerne **veľkú časť algoritmov** z oblasti kryptografie s verejným kľúčom (RSA, ECC, D-H, ...). Pre polia GF(2^k) existujú modifikácie uvedených algoritmov a je ich možné nájsť napr. v použitej literatúre.

Okrem kryptograficky orientovaných zdrojov môže byť pre študentov, z pohľadu matematiky, možno zaujímavá aj táto publikácia:

Jahoda, P.: Základy teorie čísel a jejích aplikací pro nematematiky. 2010, Dostupné tiež z: http://mi21.vsb.cz/sites/mi21.vsb.cz/files/unit/teorie_cisel_jahoda.pdf