

Matematická kryptografie

Algebraické struktury - na množině A je dána binární operace \circ , $\circ : A \times A \rightarrow A$

(A, \circ) je **pologrupa**, pokud platí asociativita, tj. $x \circ (y \circ z) = (x \circ y) \circ z$ pro $x, y, z \in A$

(A, \circ) je **monoid**, pokud mává existuje neutralní prvek $e \in A$, tedy pro $\forall x \in A$
platí $e \circ x = x = x \circ e$ např. $(\mathbb{Z}, +)$

(A, \circ) je **grupa**, pokud mává všechny prvky mají inverse, tedy $\forall x \exists y : x \circ y = e = y \circ x$

(A, \circ) je **Abelova grupa**, pokud mává je operace \circ komutativní, tedy $x \circ y = y \circ x$
- Abelovou grupou je např. $(\mathbb{Z}, +)$.

Májme množinu A s operacemi (binárními) $+$ a \circ . $(A, +, \circ)$ se nazývá **okruh**, iff:

1) $(A, +)$ je Abelova grupa s neutralním prvkem $e=0$

2) (A, \circ) je **pologrupa**

3) platí oba distributivní zákony: 1) $x \circ (y+z) = x \circ y + x \circ z$
2) $(x+y) \circ z = x \circ z + y \circ z$

- je-li mává nasobení v okruhu komutativní a má-li neutralní prvek (1),
mluvíme o komutativním okruhu s jednotkou např. $(\mathbb{Z}, +, \cdot)$

$(A, +, \circ)$ se nazývá **obor**, jestliže

1) Je to okruh s jednotkou

2) Je nekrivitelný, tedy $0 \neq 1$

3) Každým nenulovým prvkem lze králit, tj. $\forall a \in A$: 1) $ax = ay \Rightarrow x = y$
2) $x \circ a = y \circ a \Rightarrow x = y$

- je-li v oboru másobení komutativní, mluvíme o oboru integrity $(\mathbb{Z}, +, \circ)$

$(A, +, \circ)$ se nazývá **těleso**, jestliže:

1) Je to okruh s jednotkou

2) Je nekrivitelný, viz výše

3) Každý nenulový prvek má invizi $((A - \{0\}), \circ)$ je grupa)

$(\mathbb{Z}, +, \circ)$ nemá těleso, protože invizní
prvky mají jen $1 \text{ a } -1$

- je-li másobení komutativní, mluvíme o komutativním tělesu

Definice: Nechť $(A, +, \circ)$ je okruh, $a \neq 0$. Řekneme, že a je dělitel nuly, když
 $\exists b \neq 0$ tak, že $a \circ b = 0$

Tvrzení: Prvku a lze králit, pokud a není dělitel nuly.

Důkaz: ① Lze králit \Rightarrow není dělitel

Vím, že když $ax = ay$, tak nutně $x = y$. Z definice dělitel nuly, že existuje nějaké b , že $a \circ b = 0$, mává nyní pláns $a \circ 0 = 0$. Uzavřme $a \circ b = a \circ 0$, ale protože $b \neq 0$, tak a není žádoucím dělitelom nuly.

② a je dělitel nuly \Rightarrow nelze králit

$$\begin{array}{l} ax = ay \\ ax - ay = 0 \\ a(x-y) = 0 \end{array} \quad \left[\begin{array}{l} b = (x-y), b \neq 0 \\ x-y \neq 0 \\ \Rightarrow x \neq y \end{array} \right]$$

Věta o dělení se slyškem: $\forall a, b \in \mathbb{Z}, a, b > 0 \exists q, r \in \mathbb{Z}$ tak, že $a = qb + r$, a přítom $0 \leq r < b$ a q, r jsou jednoznačné.

Důkaz: ① Existence q a r

Vyvoříme množinu slyšků po dělení a označme ji M , $M \subseteq \mathbb{N}$, $M \neq \emptyset$
 $M = \{a - k \cdot b, k \in \mathbb{N}, a - k \cdot b > 0\}$

Kádá neprázdná podmnožina \mathbb{N} má nejménší prvek. Označme ho r a jemu příslušné k označme jako q .

$$a - q \cdot b = r$$

$$a = qb + r$$

Nutně platí $0 \leq r < b$, protože kdyby $r \geq b$, tak $r > a - (q+1) \cdot b$, což je ve sporu s tím, že r je minimální.

② Jednoznačnost q a r

Předpokládejme, že jsme a vyjádřili oběma způsoby jako $a = q_1 b + r_1 = q_2 b + r_2$,

kde $0 \leq r_1, r_2 < b$ máme dvě různé menší než b , všechny je od sebe, následkem lze lada

$$q_1 b - q_2 b = r_2 - r_1$$

/ vykrátíme b , protože je kladné

$$q_1 - q_2 < 1$$

$0 \leq q_1 - q_2 < 1 \leftarrow$ Rovněž může být kladný až v jednom případě,

$$q_1 - q_2 = 0$$

lze $q_1 - q_2 = 0$ nebo $q_2 - q_1$

$q_1 = q_2 \quad q_1, q_2$ jsou celá čísla, i jejich rozdíl musí být celý

$$(q_1 - q_2) \cdot b = r_2 - r_1$$

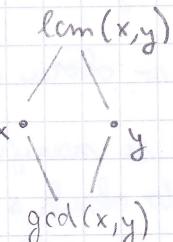
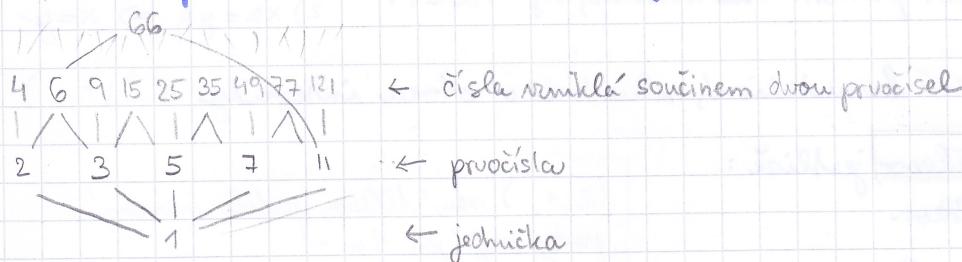
$$0 \cdot b = r_2 - r_1$$

$$0 = r_2 - r_1$$

$$r_1 = r_2$$

Požadujeme, že dvě různé dvojice q_1, r_1 nemůžou existovat.

Relace dělitelnosti na \mathbb{Z} je reflexivní, transitivní, a i antisymetrická. Je to tedy částečně uspořádaná množina, a můžeme ji znázornit Hasseovým diagramem.



Základní věta aritmetiky: Kádá $n \in \mathbb{N}, n \geq 2$ lze rozložit jako součin prvočísel

Def: Přirozené číslo $p \geq 2$ je prvočíslo iff je dělitelné pouze jedničkou a sebou samým.

Test prvočiselnosti: n je prvočíslo, pokud není lze slyšet dělitelné žádým prvočíslem p , $p \leq \sqrt{n}$. Tato úloha má exponentiální složitost vzhledem k rozdílu mezi počtem cifr čísla n . Minimálně vykonat $\sqrt{n} = 2^{\lfloor \frac{1}{2} \log_2(n) \rfloor}$ dělení.

Def: Největší společný dělitel dvou čísel $a, b \in \mathbb{Z}$ je takové číslo $d \in \mathbb{Z}$, které splňuje:

- 1) $d | a \wedge d | b$
 - 2) d je dělitelné všemi společnými děliteli obou čísel
 - 3) $d \geq 0$
- } Značíme $d = \gcd(a, b)$

Def: Nejmenší společný násobek je nejmenší $d \in \mathbb{Z}$, který je dělitelný a a takový, že dělí ho i b .

Euklidov algoritmus: umožňuje hledání $\gcd(a, b)$ v linearním čase v závislosti na počtu cifr menšího čísla.

- 1) $a = qb + r$, $0 \leq r < b$
- 2) pokud $r=0$, pak $\gcd(a, b) = b$
- 3) pokud $r \neq 0$, pak $\gcd(a, b) = \gcd(b, r)$

$$\gcd(105, 39) \Rightarrow 105 = 2 \cdot 39 + 27$$

$$\gcd(39, 27) \Rightarrow 39 = 1 \cdot 27 + 12$$

$$\gcd(27, 12) \Rightarrow 27 = 2 \cdot 12 + 3$$

$$\gcd(12, 3) \Rightarrow 12 = 4 \cdot 3 + \boxed{0}$$

$$\gcd(105, 39) = 3$$

Bezoutova věta: $\gcd(a, b) = sa + tb$, $s, t \in \mathbb{Z}$

- pro nalezení s, t lze použít rozšířený Euklidov algoritmus, který v každém kroku výsledek přeponí na a, b

a	b	a	b	
$\gcd(105, 39) \Rightarrow$	$105 = 2 \cdot 39 + 27$	$27 = a - 2b$		
$\gcd(39, 27) \Rightarrow$	$39 = 1 \cdot 27 + 12$	$b = 1 \cdot (a - 2b) + 12$	$12 = b - a + 2b = 3b - a$	
$\gcd(27, 12) \Rightarrow$	$27 = 2 \cdot 12 + 3$	$(a - 2b) = 2 \cdot (3b - a) + 3$		$3 = 3a - 8b$
$\gcd(12, 3) \Rightarrow$	$12 = 4 \cdot 3 + 0$			

$$\gcd(105, 39) = 3 = 3 \cdot 105 - 8 \cdot 39$$

Rovnice $ax + by = c$, kde $a, b, c \in \mathbb{Z}$ se nazývá difantická rovnice.

Věta: Difantická rovnice má řešení v \mathbb{Z} , právě když $\gcd(a, b) | c$.

- pokud nějaké celočíselné řešení existují, pak jich je nekonečně mnoho a jsou ve tvare:

$$(x, y) = (\underline{x_p}, \underline{y_p}) + k \cdot (\underline{x_0}, \underline{y_0}) \text{ pro } k \in \mathbb{Z}$$

partikulární řešení nezádělné řešení homogenní rovnice $(x_0, y_0) = \left(\frac{b}{d}, -\frac{a}{d}\right)$, $d = \gcd(a, b)$

Příklad: $105x + 39y = 3$

- 1) partikulární řešení majdeme pomocí rozšířeného Euklida

$$\gcd(105, 39) = \dots = 3 \cdot 105 - 8 \cdot 39 = 3$$

$$x_p = 3, y_p = -8$$

- 2) $105x + 39y = 0$ / rozdělíme \gcd , tedy trojnou

$$35x + 13y = 0$$

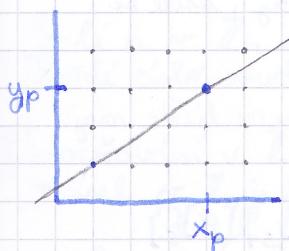
$$x_0 = 13, y_0 = -35$$

zvolíme libovolně, jde o směrový vektor

$$(x, y) = (3, -8) + k \cdot (13, -35), k \in \mathbb{Z}$$

Grafický pohled na difantické rovnice

Předměstka
21.2.2019



$\rightarrow \mathbb{R}$ je řešením průmětnice

$\rightarrow \mathbb{Z}$ je řešení, pokud některý a bod leží na průmětnice. Pokud jsou navíc koeficienty směrového vektoru celočíselné, proti průmětnice dálce body, tedy bude řešením nekonečno. Koeficienty navíc musí být nezádělné, jinak bude řešením některé body vyničkovat.

Tvrzení: Když $a/b \cdot c \sim \gcd(a, b) = 1$, pak a/b .

Důkaz: Z Bezoutovy věty: $1 = \gcd(a, b) = ta + sb$ / $\cdot c$

$$b = ta + sb$$

Z předpokladu máme, že $a/b \cdot c \sim a/b \cdot b$ a srovnání $a/b \cdot c$. Když a dělí oba sčítance, méně dělí i součet, tedy b .

Důsledek: Když $p/a \cdot b$ a p je prvočíslo, pak p/a nebo p/b .
 Kdyby p nedělilo a , tak $\gcd(p, a) = 1$. Dle předchozího tvrzení musí mít p/b .

Důkaz základní věty aritmetiky:

1) existence faktorisace indukce přes n

1) $n=2$, 2 je prvočíslo, $2=2^1$ ✓

2) předpokládáme: $\forall k \ 2 \leq k < n$, že k lze faktorizovat

chceme ukázat, že i n lze faktorizovat. Musíme rozdat dvě situace:

- n je prvočíslo, v tom případě máme faktorisaci

- n není prvočíslo, ke ho výjádřit jako $n=a \cdot b$, kde $2 \leq a, b < n$. Z předpokladu víme, že a i b lze rozložit, faktorisace n je součinem faktorisací a, b .

2) jednoznačnost faktorisace indukce přes r

$n = p_1 \cdot p_2 \cdots p_r = q_1 \cdot q_2 \cdots q_s$, p_i a q_j jsou prvočísla. Ukážeme, že na obou stranách je stejný počet stejných prvočísel.

1) $r=1$, $n = p_1 = q_1 \cdot q_2 \cdots q_s$

Kdyby s mělo být > 1 , pak dokážeme p_1 výjádřit jako součin prvočísel, což nelze, protože p_1 je prvočíslo. Musíme tedy $s=r=1$, a $p_1 = q_1$

2) indukční předpoklad: pro $r-1$ jsou faktorisace stejné
 chceme ukázat, že budou stejné i pro r

$n = p_1 \cdot p_2 \cdots p_r = q_1 \cdot q_2 \cdots q_s$, tedy $p_r \neq q_i$ pro všechny i .

Dle důsledku nahore na strance nutně $p_r \neq q_i$ pro všechny i , a protože všechny p_j, q_j jsou prvočísla, tak nutně $p_r = q_i$.

$$\frac{n}{p_r} = p_1 \cdot p_2 \cdots p_{r-1} = q_1 \cdot q_2 \cdots q_{i-1} \cdot q_{i+1} \cdots q_s$$

Dle indukčního předpokladu jsou tyto faktorisace stejné. ■

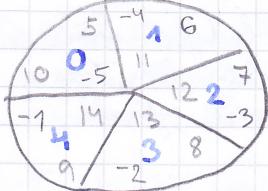
Def: Nechť $n \in \mathbb{N}$, pak čísla $a, b \in \mathbb{Z}$ jsou kongruentní modulo n , pokud $n|(b-a)$.
 Značíme to $a \equiv b \pmod{n}$.

Tvrzení: Jdyť tvrzení jsou ekvivalentní:

- $a \equiv b \pmod{n}$
- a i b mají stejný sbytek po dělení číslem n
- $b = a + kn$ pro nějaké $k \in \mathbb{Z}$

Kongruence modulo n je jako relace: reflexivní, symetrická, transitivní. Jde tedy o ekvivalence.

\Rightarrow kongruence rozdělí celá čísla na n kříd ekvivalence, tzv. zbytkové třídy, které se reprezentují základními zbytky, když $0, 1, 2, \dots, n-1$



\mathbb{Z} rozdělíme podle $n=5$ na 5 kříd, všechny čísla ve křídě mají stejný sbytek po dělení pěti.

$$\text{Značíme } \mathbb{Z}/\text{mod}5 = \mathbb{Z}_5 = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$$

Příkladem $[0]_5 = [150]_5$, a pro sjednocení všech v čáslaví příkladu píšeme v jakém \mathbb{Z}_n pracujeme a pak píšeme pouze zbytky bez $[\]_n$

Věta: Relace kongruence n je zachována při operacích \cdot a $+$.

Dk: $a = c + kn, b = d + ln$

$$a+b = c+d+k \overbrace{n+l}^{rn} = c+d+(k+l) \cdot n$$

$$a \cdot b = (c+kn)(d+ln) = cd + knd + cln + kln^2 = cd + \overbrace{(kd+cl+kln)}^{rn} \cdot n$$

Díky předešlé větě můžeme nyní napsat: \mathbb{Z}_5 zapisovat:

$$[1]_5 + [4]_5 = [5]_5 = [0]_5, \text{ tedy } 1+4=0$$

Inverze v \mathbb{Z}_5 : $a \cdot x = 1, x = a^{-1}$

$$1 \cdot 1 = 1 \checkmark$$

$$2 \cdot 3 = 6 = 1 \checkmark$$

$$4 \cdot 4 = 16 = 1 \checkmark$$

$$\left. \begin{array}{l} \\ \\ \end{array} \right\} \text{n } \mathbb{Z}_5 \text{ má jenom } 4 \text{ různých prvků inverzí, jde tedy o těleso}$$

Věta: Trojice $(\mathbb{Z}_n, +, \cdot)$ tvorí komutativní okruh s jednotkou, který se nazývá faktorový okruh slyšších tříd modulo n .

Lineární rovnice v \mathbb{Z}_n : Lineární rovnice $ax = b$ v \mathbb{Z}_n lze převést na difantickou

rovnici: $ax = b \text{ v } \mathbb{Z}_n$

$$ax = b \pmod{n} \text{ v } \mathbb{Z}$$

$$ax + ny = b \text{ v } \mathbb{Z}$$

Věta: Lineární rovnice $ax = b$ má v \mathbb{Z}_n řešení iFF $\gcd(a, n) | b$. Je-li x_p jedno řešení, pak každé řešení má tvar

$$x = x_p + k \cdot x_0, \text{ kde } x_0 = \frac{m}{\gcd(a, n)}$$

V okruhu \mathbb{Z}_n lze vzniknout celkem $\gcd(a, n)$ řešených řešení.

Důsledek: Rovnice $ax = 1$ bude mít řešení v \mathbb{Z}_n iFF $\gcd(a, n) = 1$. Řešením bude prvek inverzi k a .

Uvázení: Prvek $a \in \mathbb{Z}_n$ je invertibilní, pokud a a n jsou nezádělné.

Věta: Okruh $(\mathbb{Z}_n, +, \cdot)$ je těleso, právě když n je prvočíslo.

Př: Inverze v \mathbb{Z}_6

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$$1 \cdot 1 = 1, \text{ tedy } 1^{-1} = 1$$

$$5 \cdot 5 = 25 = 6 \cdot 4 + 1 = 1, \text{ tedy } 5^{-1} = 5$$

Ostatní čísla inverzi nemají

V \mathbb{Z}_6 nelze krátit!

$$2x = 4 \Rightarrow x = 2$$

Pokud vykrátíme dvojkou, přijde o řešení, například $x = 5$

Je-li $n \in \mathbb{Z}_n$ složené číslo, pak okruh $(\mathbb{Z}_n, +, \cdot)$ není ani obor integrity, protože každé číslo součitné s n je dělitelém nuly (není to ani obor, v oboru ke krátit).

Umocňování v \mathbb{Z}_n

- čísel v \mathbb{Z}_n je konečně mnoho, výsledky možností se budou opakovat, proto:

$$\exists k, l; k > l \in \mathbb{N} \text{ tak, že } a^k = a^l$$

- pokud je a invertibilní v \mathbb{Z}_n , násobíme $a^{k-l} = 1$, tedy možnosti čísla a se cyklu s periodou $k-l$.

Malá Fermatova věta: Nechť p je prvočíslo. Pro $a \neq 0 \pmod{p}$ je $a^{p-1} \equiv 1 \pmod{p}$

Euler - Fermatova věta: $\forall a \in \mathbb{Z}$ nezádělné s n platí $a^{\varphi(n)} \equiv 1 \pmod{n}$, tedy je-li základ nezádělný s n , můžeme exponent snížit modulo $\varphi(n)$.

Eulerova funkce $\varphi(n)$: množství menších čísel nesoudělných s n

$$\varphi(p) = p-1 \text{ pro prvočíslo } p$$

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$$

$$\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m) \text{ pro nesoudělná } m, n \quad (\gcd(m, n) = 1)$$

Příklad: spočítejte 5^{64} v \mathbb{Z}_{18}

Zkusíme použít Euler-Fermatovu větu. Předpokladem je, že 5 a 18 jsou nesoudělné, což je splněno.

$$\varphi(18) = \varphi(3 \cdot 3 \cdot 2) = \varphi(3^2) \cdot \varphi(2) = (3^1 \cdot 2) \cdot 1 = 6$$

$$5^{64} = \underbrace{(5^6)^{10}}_{=1 \text{ dle věty}} \cdot 5^4 = 5^4 = 25^2 = 7^2 = 49 = 31 = 13 \text{ v } \mathbb{Z}_{18}$$

↑ modulární rázba

Eulerova věta: Nechť (G, \cdot) je konečná grupa, σ m pravých s neutrálem 1. Pro každé $a \in G$ platí $a^n = \underbrace{a \cdot a \cdot a \cdots a}_{m\text{-krát}} = 1$ v G .

Důkaz pro komutativní grupy (věta \mathbb{Z}_n)

Okusíme levou stranu příkazu a jde o $\lambda_a : G \rightarrow G : g \mapsto a \cdot g$

ta je bijekce, protože je

- prostě: když $\lambda_a(x) = \lambda_a(y)$ pro $x \neq y$, znamená to, že $ax = ay$
- na: prostě sebacekní v konečné možnosti nutně musí být na

$$G = \{g_1, g_2, \dots, g_n\} = \{\lambda_a(g_1), \lambda_a(g_2), \dots, \lambda_a(g_n)\}$$

$$\prod_{i=1}^n g_i = \prod_{i=1}^n \lambda_a(g_i) = \prod_{i=1}^n a \cdot g_i = a^n \prod_{i=1}^n g_i, \text{ tedy } \prod_{i=1}^n g_i = a^n \prod_{i=1}^n g_i, \text{ tedy } a^n = 1$$

Cvičení
21.2.2019

Spočítejte pomocí Euklidova algoritmu:

$$\gcd(260, 84) = 4$$

$$\begin{array}{rcl} 260 & = & 3 \cdot 84 + 8 \\ 84 & = & 10 \cdot 8 + 4 \\ 8 & = & 2 \cdot 4 + 0 \end{array}$$

$$\gcd(114, 156) = 6$$

$$\begin{array}{rcl} 156 & = & 1 \cdot 114 + 42 \\ 114 & = & 2 \cdot 42 + 30 \\ 42 & = & 1 \cdot 30 + 12 \\ 30 & = & 2 \cdot 12 + 6 \\ 12 & = & 2 \cdot 6 + 0 \end{array}$$

Nakombinujte $6 = s \cdot 156 + t \cdot 114$

$$\begin{array}{rcl} 156 & = & 1 \cdot 114 + 42 \\ \downarrow a & \downarrow b & \downarrow a-b \\ 42 & = & a-b \end{array} \quad \left. \begin{array}{l} 42 = a-b \\ 114 = 2 \cdot 42 + 30 \\ 42 = 1 \cdot 30 + 12 \\ 30 = 2 \cdot 12 + 6 \\ 12 = 2 \cdot 6 + 0 \end{array} \right\} 42 = a-b$$

$$114 = 2 \cdot 42 + 30$$

$$\downarrow b \quad \downarrow a-b$$

$$42 = 1 \cdot 30 + 12$$

$$30 = 2 \cdot 12 + 6$$

$$30 = b - 2(a-b) = 3b - 2a$$

$$12 = (a-b) - (3b-2a) = 3a - 4b$$

$$6 = (3b-2a) - 2(3a-4b) = -8a + 11b$$

$$6 = -8 \cdot 156 + 11 \cdot 114, \text{ tedy } s = -8, t = 11$$

Najděte všechny možné kombinace v \mathbb{Z} , kde $156x + 114y = 6$ (řešte diag. rovnici)

Obecné řešení se zapiše jako $(x, y) = (x_p, y_p) + k \cdot (x_0, y_0)$, kde \vec{x}_p je partikulární řešení a \vec{x}_0 je řešení homogenní rovnice. k je libovolné celé číslo.

Homogenní řešení mám dle směru vektorem, a jde ho siskat více různobyl.

1) Řešení načleněním nezáporných koeficientů

$$156x + 114y = 0, \text{ proto } \gcd(156, 114) = 6, \text{ řešenou lze rovnici rozdělitme}$$

$$\frac{156}{6} \cdot x + \frac{114}{6} \cdot y = 0$$

$$26x + 19y = 0, \text{ tedy máme lidové řešení, tedy } (19, -26)$$

2) Počítacovním v Eulerově algoritmu

$$12 = 3a - 4b, 6 = -8a + 11b$$

$$30 = 2 \cdot 12 + 6, 6 = -8a + 11b$$

$$12 = 2 \cdot 6 + 0, 0 = (3a - 4b) - 2(-8a + 11b) = 3a - 4b + 16a - 22b = 19a - 26b.$$

Řešení diofantických rovnic pomocí uprav matice

- Začneme s maticí $\begin{pmatrix} 1 & 0 & | & a \\ 0 & 1 & | & b \end{pmatrix}$ a upravujeme ji tak, aby se dostala do normy $\begin{pmatrix} s & t & | & d \\ u & v & | & 0 \end{pmatrix}$,

kde $\gcd(a, b) = d$ a zároveň $(x_0, y_0) = (u, v)$, $(x_p, y_p) = (s, t)$.

- Při úpravách musíme: prohazovat řádky determinantu směrem směrem k první nebo oběma jednotkovým řádkům k jinému determinantu se nezmění nesmí: vynásobit řádek konstantou stejnou konstantou se změní i determinant $\uparrow \pm 1$ můžete směrem

- Jiné můžeme zaručeno, že determinant sustance ± 1 (povolené násobky jsou vlastně násobkem elementární matici' aleva)

$$\left(\begin{array}{cc|c} 1 & 0 & a \\ 0 & 1 & b \end{array} \right) = \left(\begin{array}{cc|c} s & t & d \\ u & v & 0 \end{array} \right)$$

$$\det(\cdot) \cdot \det(\cdot) \quad \det\left(\begin{array}{cc|c} 1 & 0 & a \\ 0 & 1 & b \end{array}\right) = \det\left(\begin{array}{cc|c} s & t & d \\ u & v & 0 \end{array}\right)$$

$$\underbrace{(-1) \cdot (-1) \cdot \dots}_{2 \text{ krát}} \quad \cdot 1 = sv - tw$$

$$(-1)^2 = sv - tw$$

$$\pm 1 = sv - tw, z toho plyne, že \begin{cases} \gcd(u, v) = 1 \text{ a navíc} \\ \gcd(s, t) = 1 \end{cases}$$

$$\text{Př.: } 156x + 114y = 6$$

$$\left(\begin{array}{cc|c} 1 & 0 & 156 \\ 0 & 1 & 114 \end{array} \right) = \frac{n_2}{n_1 - n_2} \left(\begin{array}{cc|c} 0 & 1 & 114 \\ 1 & -1 & 42 \end{array} \right) = \frac{n_2}{n_1 - 2n_2} \left(\begin{array}{cc|c} 1 & -1 & 42 \\ -2 & 3 & 30 \end{array} \right) = \frac{n_2}{n_1 - n_2} \left(\begin{array}{cc|c} -2 & 3 & 30 \\ 3 & -4 & 12 \end{array} \right) =$$

$$= \frac{n_2}{n_1 - 2n_2} \left(\begin{array}{cc|c} 3 & -4 & 12 \\ -8 & 11 & 6 \end{array} \right) = \frac{n_2}{n_1 - 2n_2} \left(\begin{array}{cc|c} -8 & 11 & 6 \\ 19 & -26 & 0 \end{array} \right) \begin{cases} (x_p, y_p) = (-8, 11) \\ (x_0, y_0) = (19, -26) \end{cases}$$

$$9x + 6y = 42 \quad \gcd(9, 6) = 3, \quad 3/42, \text{ proto řešení existuje}$$

$$\left(\begin{array}{cc|c} 1 & 0 & 9 \\ 0 & 1 & 6 \end{array} \right) = \left(\begin{array}{cc|c} 0 & 1 & 6 \\ 1 & -1 & 3 \end{array} \right) = \left(\begin{array}{cc|c} 1 & -1 & 3 \\ -1 & 2 & 3 \end{array} \right) = \left(\begin{array}{cc|c} -1 & 2 & 3 \\ 2 & -3 & 0 \end{array} \right) \xrightarrow{\text{obě řešení jsou správná, neboť}} \left(\begin{array}{cc|c} 1 & -1 & 3 \\ -2 & 3 & 0 \end{array} \right) \xrightarrow{\text{neboť v řešení, } x_p \text{ se liší méně.}}$$

$$1 \cdot 9 - 1 \cdot 6 = 3 \quad / \cdot 14, \text{ abych náspravo měla 42, tedy je n radařem} \\ 14 \cdot 9 - 14 \cdot 6 = 42$$

$$(x, y) = (14, -14) + (2, -3)k, k \in \mathbb{Z}.$$

$$12x = 6 \sim \mathbb{Z}_{45} \quad \gcd(12, 45) = 3, \quad 3/6, \text{ řešením existuje}$$

$$12x + 45y = 6 \quad \left(\begin{array}{cc|c} 1 & 0 & 12 \\ 0 & 1 & 45 \end{array} \right) = \frac{n_2 - 4n_1}{n_1} \left(\begin{array}{cc|c} -4 & 1 & -3 \\ 1 & 0 & 12 \end{array} \right) = \frac{n_1}{n_2 + 6n_1} \left(\begin{array}{cc|c} -4 & 1 & -3 \\ 15 & 4 & 0 \end{array} \right)$$

$$-4 \cdot 12 + 1 \cdot 45 = -3$$

$$8 \cdot 12 - 2 \cdot 45 = 6$$

$$x = x_p + k \cdot x_0 = \underline{\underline{8 + k \cdot 15}}$$

Majděte inverzi pro 51 mod 73.

$$51 \cdot x = 1 \pmod{73}$$

$$51 \cdot x + 73y = 1$$

$$\left(\begin{array}{cc|c} 1 & 0 & 51 \\ 0 & 1 & 73 \end{array} \right) \xrightarrow{\text{R}_2 - R_1} \left(\begin{array}{cc|c} 1 & 0 & 51 \\ -1 & 1 & 22 \end{array} \right) \xrightarrow{\text{R}_1 + 3\text{R}_2} \left(\begin{array}{cc|c} 3 & -2 & 7 \\ -1 & 1 & 22 \end{array} \right) \xrightarrow{\text{R}_1 + 3\text{R}_2} \left(\begin{array}{cc|c} 3 & -2 & 7 \\ 10 & 7 & 1 \end{array} \right) \xrightarrow{\text{R}_1 - 3\text{R}_2} \left(\begin{array}{cc|c} -10 & 7 & 1 \\ 73 & -51 & 0 \end{array} \right)$$

gcd = 1, $\frac{1}{1}$, lze ho mít
řešení

$$-10 \cdot 51 + 7 \cdot 73 = 1$$

$$-10 \equiv 63 \pmod{73}$$

$$51^{-1} = \underline{\underline{63}}$$

Matice výpočtu ke použití při hledání gcd několika čísel: $\text{gcd}(18, 21, 45)$

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & 18 \\ 0 & 1 & 0 & 21 \\ 0 & 0 & 1 & 45 \end{array} \right) \xrightarrow{\text{R}_2 - R_1} \left(\begin{array}{ccc|c} 1 & 0 & 0 & 3 \\ 1 & 0 & 0 & 18 \\ 0 & 0 & 1 & 45 \end{array} \right) \xrightarrow{\text{R}_1 - R_2} \left(\begin{array}{ccc|c} -1 & 1 & 0 & 3 \\ 1 & 0 & 0 & 18 \\ 0 & 0 & 1 & 45 \end{array} \right) \xrightarrow{\text{R}_2 - 6\text{R}_1} \left(\begin{array}{ccc|c} -1 & 1 & 0 & 3 \\ 7 & -6 & 0 & 0 \\ 0 & 0 & 1 & 45 \end{array} \right) \xrightarrow{\text{R}_3 - 15\text{R}_1} \left(\begin{array}{ccc|c} -1 & 1 & 0 & 3 \\ 7 & -6 & 0 & 0 \\ 15 & -15 & 1 & 0 \end{array} \right)$$

Nakombinováme' gcd: $3 = -18 + 21 \checkmark$

$$(-1 + 7k + 15l)^{18} a + (1 - 6k - 15l)^{21} b + lk^{45} c = 3 \\ -18 + 126k + 270l + 21 - 126k - 315l + 45l = 3 \\ 3 + 0k + 0l = 3 \\ 3 = 3$$

MKR přednáška
27.2.2019

Veta: Je-li (M, \cdot) monoid s neutrálem 1, a $M^* = \{a \in M \mid a^{-1} \in M\}$, pak (M^*, \cdot) je grupa (invertibilních prvků v monoidu M)

Dk: 1) $\text{množstv} (M^*, \cdot)$ funguje součinem

Když $a, b \in M^*$, existují inverze $a^{-1}, b^{-1} \in M^*$. Chci ukázat, že existuje $(a \cdot b)^{-1}$ takové, že $(a \cdot b) \cdot (a \cdot b)^{-1} = 1$, když že existuje inverze k $(a \cdot b)$.

$$(a \cdot b)^{-1} = (b^{-1} \cdot a^{-1}), \text{ protože } (ab)(ab)^{-1} = (ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a \cdot 1 \cdot a^{-1} = a \cdot a^{-1} = 1 \checkmark$$

2) platí asociačita násobení

$(a \cdot b) \cdot c = a \cdot (b \cdot c)$ platí pro libovolné $a, b, c \in M^*$, protože $M^* \subseteq M$ a M je monoid

3) $1 \in M^*$

Ano, protože $1 \cdot 1 = 1$, tedy inverze k 1 leží v M

4) $\forall a \in M^* \exists a^{-1} \in M$

Ano, protože $(a^{-1})^{-1} = a^1 = a$, tedy inverze k inverzi leží v M^* a tedy musí ležet i v M

Př: $\mathbb{Z}_6^* = \{a \in \mathbb{Z}_6, \text{gcd}(a, 6) = 1\} = \{1, 5\}$

$\varphi(6) = \varphi(2 \cdot 3) = \varphi(2) \cdot \varphi(3) = 1 \cdot 2 = 2$, tedy v \mathbb{Z}_6^* budou dva prvky

Ale očekávat tam nemusíme, \mathbb{Z}_6 má i rezidua 0 a 2, $1+1=2, 2 \notin \mathbb{Z}_6^*$

Umluva: Pokud mluvíme o grupě \mathbb{Z}_n^* , vždycky myslíme (\mathbb{Z}_n^*, \cdot) , protože + lze být nemusí. < rovnost

Pokud mluvíme o grupě \mathbb{Z}_n , vždycky myslíme $(\mathbb{Z}_n, +)$, protože \cdot není inverzi pro všechny prvky.

Důsledek E-F věty: počet invertibilních prvků $a^{-1} = a^{4(n)-1} \in \mathbb{Z}_n$

E-F věta říká, že pro a, n , $\text{gcd}(a, n) = 1$: $a^{4(n)} = 1 \in \mathbb{Z}_n$

$$a^{4(n)-1} \cdot a^1 = 1 \in \mathbb{Z}_n$$

tedy inverze k a je $a^{4(n)-1}$

Algoritmus opakovacích čtverčeků - umožňuje množit na velká čísla, nero v případě, že nejdle použí E-F větu. Např. pro výpočet $5^{17} \text{ v } \mathbb{Z}_{27}$:

1) exponent rozloží jako binární číslo

$$17 = 16 + 1 = 10001$$

2) dle kterého mení cifry binárního čísla násobem S , násobku, jednoukrát násobenou za X

$$10001 = 1S0S0S0S1 = 1SSSS1 = XSSSX$$

3) sčítání s jedničkou. Bin. číslo čtu zleva, pokud přečtu x , násobím sčítkadem. Pokud přečtu S , množím na druhou. Brutevně dělám modulo.

$$\begin{aligned} 1(XSSSX) &= 5(SSSX) = 25(SSX) = -2(SSX) = 4(SSX) = 16(SX) = \\ &= -11(SX) = 121(x) = 13(x) = 65 = 11 \end{aligned}$$

Tím mám následek, když $5^{17} \text{ v } \mathbb{Z}_{27} = 11$.

Prostorová náročnost algoritmu v \mathbb{Z}_n je n^2 , protože vždy potřebuju mít v paměti násobky $n \cdot n$, a hned na to použij rámce modulo. Časová náročnost je dáná počtem násobení, a těch bude $2 \cdot \lg(b)$, kde b je exponent (bereme jeho délku v binárnici).

Př: spočtejte $2^{13} \text{ v } \mathbb{Z}_{20}$. Protože $\gcd(2, 20) = 2 \neq 1$, nemůžu exponent omítnout pomocí E-F věty.

$$13 = 8+5 = 8+4+1 = 1101 \Rightarrow XSSSX$$

$$\begin{aligned} 1(XSXSSX) &= 2(SXSSX) = 4(XSSX) = 8(SSX) = 64(SX) = 4(SX) = \\ &= 16(x) = -4(x) = -8 = \underline{\underline{12}} \end{aligned}$$

Cínská věta o zbytcích: Nechť n_1, \dots, n_k jsou po dvou nesoudělná původem čísla, a_1, \dots, a_k jsou libovolná původem čísla. Pak soustava rovnic

$$x \equiv a_i \pmod{n_i} \quad \forall i \geq 1, i \leq k$$

má řešení. Navíc kandidátu řešení a, b jsou kongruentní modulo $n = \prod_{i=1}^k n_i$

Dоказ: 1) existence řešení. Najdu q_i , kdežto řešení soustavy $q_i \equiv 1 \pmod{n_i}$, $q_i \equiv 0 \pmod{n_j} \quad \forall j \neq i$. Rovnice 2 neřeším tak, že svolím $q_i = \prod_{j \neq i} n_j$, když q_i bude soudělně se všemi n_j .

Rovnice 1 říká, že $q_i \equiv 1 \pmod{n_i}$. Označme $q_i = \prod_{j \neq i} n_j$. Protože čísla n_j jsou nesoudělná, víme, že q_i je nesoudělné s n_i , když má invizi v \mathbb{Z}_{n_i} . Označme tu invizi t_i . Pak platí $q_i \cdot t_i \equiv 1 \pmod{n_i}$, a druhá rovnice vlastně nepotřebuji.

Svolím si $q_i = \prod_{j \neq i} n_j \cdot (\prod_{j \neq i} n_j)^{-1}$. Pak má následující řešení $x = a_1 q_1 + a_2 q_2 + \dots + a_k q_k$

2) jednoznačnost řešení. Označme $n = \prod_{i=1}^k n_i$. Když x a y obě řešily soustavu, pak $x - y = a_i - a_i = 0$ pro $i: 1 \dots k$, tedy $x - y = 0$. Tedy pro všechny $i: n_i / (x - y)$, když $\text{lcm}(n_1, n_2, \dots, n_k) / (x - y)$. Jenže $\text{lcm}(n_1, \dots, n_k) = \prod_{i=1}^k n_i$, protože jsou nesoudělná. Což znamená, že $n / (x - y)$, a to jde psát jako $(x - y) = n \cdot c$, $c \in \mathbb{Z}$. $(x - y) = n \cdot c \Rightarrow x = y + n \cdot c$. Z toho vidíme, že řešení j jsou od sebe vzdálená n , když je v \mathbb{Z}_n je pouze jedno řešení.

Př: Pomocí CRT řešte: $\begin{cases} x \equiv 2 \pmod{4} \\ x \equiv 0 \pmod{5} \\ x \equiv 1 \pmod{9} \\ x \equiv 2 \pmod{11} \end{cases}$ $\left. \begin{array}{l} q_4 \\ q_5 \\ q_9 \\ q_{11} \end{array} \right\} q \text{ snášíme podle } n_i$ $n = 4 \cdot 5 \cdot 9 \cdot 11 = 1980$

$$\begin{aligned} q_4 &= 5 \cdot 9 \cdot 11 \cdot 1 = 1 \pmod{4} \\ 1 \cdot 1 \cdot 3 \cdot 1 &= 1 \pmod{4} \end{aligned}$$

$$3 \cdot 1 = 1 \pmod{4}$$

$$A = 3$$

$$q_4 = 5 \cdot 9 \cdot 11 \cdot 3 = 1485$$

$$\begin{aligned} q_5 &= 4 \cdot 9 \cdot 11 \cdot 1 = 1 \pmod{5} \\ 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 &= 1 \pmod{5} \end{aligned}$$

$$A = 1$$

$$q_5 = 4 \cdot 9 \cdot 11 \cdot 1 = 396$$

$$\begin{aligned} q_9 &= 4 \cdot 5 \cdot 11 \cdot 1 = 1 \bmod 9 \\ 2 \cdot 2 \cdot 1 &= 1 \bmod 9 \\ 4 \cdot 1 &= 1 \bmod 9 \\ 1 &= 7 \\ q_9 &= 4 \cdot 5 \cdot 11 \cdot 7 = 1540 \end{aligned}$$

$$\begin{aligned} q_{11} &= 4 \cdot 5 \cdot 9 \cdot 1 = 1 \bmod 11 \\ 4 \cdot 1 &= 1 \bmod 11 \\ 1 &= 3 \\ q_{11} &= 4 \cdot 5 \cdot 9 \cdot 3 = 54 \\ &\quad \bmod n = 1980 \end{aligned}$$

$$x = 2q_5 + 0q_9 + 1q_{11} + 2q_{11} = 2 \cdot 1485 + 0 + 1540 + 1080 = 5590 = 3610 = 1630$$

Co by se stalo, když n mohla být neoddělná? Řešíme pomocí dvoj. koučic

- řešení nemusí existovat
- pokud řešení existuje, jsou všechna řešení kongruenční modulo lcm(n_1, \dots, n_k)
- po směnu slyšků (a_i) musíme přepočítat vše, v běžné čínské větě lychom přepočítali pouze poslední krok ($x = a_1q_1 + \dots + a_kq_k$).

Přednáška
28.2.2019

Uvod do residuální aritmetiky - slyšky po dělení 2, 3 a 6: $\mathbb{Z}_6 = \mathbb{Z}_2 \times \mathbb{Z}_3$

$\times \bmod 6$	$\times \bmod 2$	$\times \bmod 3$	sčítání: $2+4=8=2$ $(0,2) \cdot (0,1) = (0,0,2 \cdot 1) = (0,2)$
0	(0,0)		↳ stejně
1	(1,1)		
2	(0,2)		
3	(1,0)		
4	(0,1)		
5	(1,2)		
		násobení: $2 \cdot 4 = 8 = 0$ $(0,2) + (0,1) = (0,2+1) = (0,3) = (0,0)$	↳ stejně

\Rightarrow Slyšek po dělení 6 je jednoznačně určen slyšky po dělení 2 a 3.

Tvrzení: Nechť n_1, \dots, n_k jsou neoddělná přirozená čísla a nechť $n = \prod_{i=1}^k n_i$. Definujme
sobrarení: $\Theta: \mathbb{Z}_n \rightarrow \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k}: [\alpha]_n \mapsto ([\alpha]_{n_1}, \dots, [\alpha]_{n_k})$

- 1) Definice je korektní, nezávisí na volbě reprezentanta třídy $[\alpha]_n$
- 2) Sobrarení Θ je bijekce
- 3) Pro všechna $\alpha, \beta \in \mathbb{Z}_n$, kde $\Theta(\alpha) = (\alpha_1, \dots, \alpha_k), \Theta(\beta) = (\beta_1, \dots, \beta_k)$ platí:

$$\begin{aligned}\Theta(\alpha + \beta) &= (\alpha_1 + \beta_1, \dots, \alpha_k + \beta_k) \\ \Theta(0) &= (0, \dots, 0) \\ \Theta(-\alpha) &= (-\alpha_1, \dots, -\alpha_k) \\ \Theta(\alpha \cdot \beta) &= (\alpha_1 \cdot \beta_1, \dots, \alpha_k \cdot \beta_k) \\ \Theta(1) &= (1, \dots, 1)\end{aligned}$$

$\alpha \in \mathbb{Z}_n^*$ iff $\alpha_i \in \mathbb{Z}_{n_i}^*$ pro i . Tedy $\Theta(\alpha^{-1}) = (\alpha_1^{-1}, \dots, \alpha_k^{-1})$

Takovému sobrarení říkáme čínské slyškové sobrarení. Θ je okruhový izomorfismus, který respektuje inverzní pravky.

Důkaz:

1) Θ je korektně definovane'

Bědopohládajme, že máme $\alpha, \alpha' \in \mathbb{Z}_n$, $[\alpha]_n = [\alpha']_n$, tedy $\alpha \equiv \alpha' \pmod n$, kde $n = \prod_{i=1}^k n_i$.
Pak chci ukázat, že $\alpha \equiv \alpha' \pmod{n_i}$.

$$\alpha = \alpha' + l \cdot m = \alpha' + l \cdot \prod_{j=1}^k n_j = \alpha' + \underbrace{l \cdot \prod_{\substack{j=1 \\ j \neq i}} n_j \cdot n_i}_{=l} = \alpha' + l \cdot n_i, \text{ tedy } \alpha \equiv \alpha' \pmod{n_i}$$

Z toho plyne, že $\Theta([\alpha]_n) = ([\alpha]_{n_1}, \dots, [\alpha]_{n_k}) = ([\alpha]_{n_1}, \dots, [\alpha']_{n_k}) = \Theta([\alpha']_n)$

2) Θ je bijekce

Jádře n_1, \dots, n_k je neoddělná, takže díky CRT máme, že

- každá k -tice slyšků má rovnou $\Rightarrow \Theta$ je na

- rovnou je jediný v $\mathbb{Z}_n \Rightarrow \Theta$ je surjektivní

3) Θ respektuje $+$, \cdot

Kongruence modulo respektuje $+$, \cdot , proto to bude respektovat i Θ

Namí $1 \equiv 1 \pmod{n_i}$, $0 \equiv 0 \pmod{n_i}$

4) Θ respektuje inverzní pravky

Máme $[\alpha]_n \cdot [\beta]_n = [1]_n$, tedy $[\beta]_n = [\alpha]_n^{-1} \in \mathbb{Z}_n$. Chceme, aby $\Theta([\alpha \cdot \beta]_n) = \Theta(1)$

$$(\alpha \cdot \beta)_1, \dots, (\alpha \cdot \beta)_{n_k} = (1, \dots, 1)$$

V každém \mathbb{Z}_{n_i} je $\alpha_i \cdot \beta_i = 1$, tedy $\beta_i = \alpha_i^{-1} \in \mathbb{Z}_{n_i}$

Mimo jiné jsme ukažali, že když $[a]_n \in \mathbb{Z}_n^*$, pak pro $\theta([a]_n) = (a_1, \dots, a_k)$, kde $[a]_{n_i} = a_i$, je každý $a_i \in \mathbb{Z}_{n_i}^*$ invertibilní.

Naprosto: Když $[a]_n = a \in \mathbb{Z}_n - \mathbb{Z}_n^*$, pak a je soudělné s $n = \prod n_i$, tedy můžeme vložit n_i soudělné s $a_i + k \cdot n_i \Rightarrow a$ nemá inverzi. Neboť $(a_1, \dots, a_k) \cdot (b_1, \dots, b_k) \neq (1, 1, \dots, 1)$, jelikož to má i-té souřadnice.

Důsledek:

- $\theta' = \theta \upharpoonright \mathbb{Z}_n^*$, kde \upharpoonright znamená zkrácení na definicií oboru \mathbb{Z}_n^*
- θ' je bijekce mezi \mathbb{Z}_n^* a $\mathbb{Z}_{n_1}^* \times \dots \times \mathbb{Z}_{n_k}^*$
- θ' je okruhový isomorfismus
- θ' je grupový isomorfismus

Důsledek: když m a n jsou nesoudělné, pak $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$

Důkaz: m a n jsou nesoudělná sada. Můžu použít CRT, θ' je bijekce

$$\mathbb{Z}_{m \cdot n}^* \cong \mathbb{Z}_m^* \cdot \mathbb{Z}_n^* \leftarrow \text{isomorfismus, mají stejně prvky}$$

$$\varphi(m \cdot n) = |\mathbb{Z}_{m \cdot n}^*| = |\mathbb{Z}_m^* \cdot \mathbb{Z}_n^*| = |\mathbb{Z}_m^*| \cdot |\mathbb{Z}_n^*| = \varphi(m) \cdot \varphi(n)$$

Důsledek: residuální aritmetika

$$n = \prod_{i=1}^k p_i^{e_i}, \text{ nejméně nesoudělnou sadu } p_1^{e_1}, \dots, p_k^{e_k} = n_1, \dots, n_k, \text{ a místo v } \mathbb{Z}_n$$

budu počítat se slysky $\sim \mathbb{Z}_n$:

Př: $\sim \mathbb{Z}_{1980}$ spočítejte $a \cdot b$ pro $a = 31313131313, b = 123456789$
 $1980 = 4 \cdot 5 \cdot 9 \cdot 11, q_4 = 1485, q_5 = 396, q_9 = 1540, q_{11} = 540$

$$\begin{aligned} \sim \mathbb{Z}_4: & a = 13 = 1 \\ & b = 89 = 1 \end{aligned} \quad \left. \begin{array}{l} \text{Zbytek po dělení 4 se sjedí se dvou posledními ciframi, protože } 4/100. \\ a \cdot b = 1, \quad a^b = 1^b = 1, \quad a^{-1} = 1 \\ \quad \uparrow 1^k = 1 \quad \forall k \in \mathbb{Z} \end{array} \right\}$$

$$\sim \mathbb{Z}_5: \quad a = 3 \quad \text{Zbytek po dělení 5 je se sjedí s posledním cifrem} \\ b = 4 \\ a \cdot b = 12 = 2, \quad a^b = 3^{b \bmod 4} = 3^1 = 3, \quad a^{-1} = 2 \\ \varphi(5) = 4$$

$$\begin{aligned} \sim \mathbb{Z}_9: & \sum a_i = 5 \cdot (3+1) + 3 = 23 = 5 \\ & \sum b_i = 4 \cdot 10 + 5 = 45 = 0 \end{aligned} \quad \left. \begin{array}{l} \text{číslo je dělitelné 9, když čísla v součtu jsou dělitelné 9} \\ a \cdot b = 5 \cdot 0 = 0, \quad 5^b = ? \quad \sim \mathbb{Z}_9 = 5^{b \bmod 6} = 5^3 = 125 = 8, \quad a^{-1} = 2 \\ \varphi(9) = \varphi(3^2) = 3^1 \cdot 2 = 6 \end{array} \right\}$$

$$\begin{aligned} \sim \mathbb{Z}_{11}: & a = (3-1) \cdot 5 + 3 = 13 = 2 \\ & b = (9-8) + (7-6) + 3 = 5 \end{aligned} \quad \left. \begin{array}{l} x \equiv \sum_{i=0}^k a_i \cdot (-1)^i \pmod{11} \\ a \cdot b = 12 \cdot 5 = 10, \quad a^b = 2^b = 2^{b \bmod 10} = 2^9 = 6, \quad a^{-1} = 6 \\ \varphi(11) = 10 \end{array} \right\}$$

Zápis pomocí θ : $\theta(a) = (1, 3, 5, 2), \theta(b) = (1, 4, 0, 5)$

$$\theta(a \cdot b) = (1, 2, 0, -1) \quad \left| \begin{array}{l} a \cdot b = q_4 + 2q_5 - q_{11} = 1737 \sim \mathbb{Z}_{1980} \\ a^b = q_4 + 3q_5 + 8q_9 + 6q_{11} = 413 \sim \mathbb{Z}_{1980} \\ a^{-1} = q_4 + 2q_5 + 2q_9 + 6q_{11} = 677 \sim \mathbb{Z}_{1980} \end{array} \right.$$

$$\theta(a^b) = (1, 3, 8, 6) \quad \left| \begin{array}{l} a^b = q_4 + 3q_5 + 8q_9 + 6q_{11} = 413 \sim \mathbb{Z}_{1980} \\ a^{-1} = q_4 + 2q_5 + 2q_9 + 6q_{11} = 677 \sim \mathbb{Z}_{1980} \end{array} \right.$$

$$\theta(a^{-1}) = (1, 2, 2, 6) \quad \left| \begin{array}{l} a^{-1} = q_4 + 2q_5 + 2q_9 + 6q_{11} = 677 \sim \mathbb{Z}_{1980} \end{array} \right.$$

Asymptotická složitost v MKR: $O, \Omega, \Theta, \sigma, \sim$, kde $f \sim g$ iff $\lim_{x \rightarrow \infty} \frac{f(x)}{g(x)} = 1$

Reprezentace čísel v pc:

Délka celeho čísla a je počet bitů v binární reprezentaci 1a1, tedy

$$\text{len}(a) = \lfloor \log_2(a) \rfloor + 1 \text{ pro } a \neq 0$$

$$\text{len}(a) = 1 \text{ pro } a = 0$$

Tekoucí číslo se v paměti uchovává jako vektor slov délky $\text{len}(B)$ spojuje s následujícím listem
 $a = \sum_{i=0}^{\text{len}(B)-1} a_i B^i = \pm (a_{k-1}, a_{k-2}, \dots, a_0)_B$ \forall Číslo má 32 bit systému je $B = 2^{15}$

Tvrzení: Nechť $a, b \in \mathbb{Z}$. Předpokládáme, že nečlení číslo a na dva 1 jednotkové čísla

- $a \pm b$ mívá $O(\text{len}(a) + \text{len}(b))$

- $a \cdot b$ mívá $O(\text{len}(a) \cdot \text{len}(b))$

- Pokud $b \neq 0$, $a = qb + r$, částečný podíl q a sbytek r se spočítají v čase $O(\text{len}(b) \cdot \text{len}(q))$
 Příjem $\text{len}(a) - \text{len}(b) - 1 \leq \text{len}(q) \leq \text{len}(a) - \text{len}(b) + 1$

- Násobení a dělení čísla a mocninou 2^n se spočte v čase $O(\text{len}(a))$, jde o lítavý postup

Násobení jele vychlit - Karatsuba algoritmus

Tvrzení: Nechť $a, b \in \mathbb{Z}_n$, $\lambda \in \mathbb{N}$. Operace $\sim \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ moží mít složitost

- $a \cdot b$ mívá $O(\text{len}(n))$

- $a \cdot b$ mívá $O(\text{len}(n)^2)$ opakování čtverce

- a^λ mívá $O(\text{len}(a) \cdot \text{len}(n)^2)$ nebo $O(\text{len}(a) \cdot \text{len}(n) + \text{len}(n)^3)$ EF věta + opakování čtverce

- a^{-1} mívá $O(\text{len}(n)^3)$ opakování čtverce

Časová složitost Euklidova algoritmu

první rovnice: $a = qb + r \quad r_0 = r_1 \cdot q_1 + r_2 \quad \left. \begin{array}{l} r_i \text{ se zmenšuje}, \\ q_i \geq 1 \end{array} \right\} a \geq b > r_0$

i-tá rovnice: $r_{i-1} = r_i \cdot q_i + r_{i+1}$

λ -tá rovnice (poslední): $r_{\lambda-1} = r_\lambda + q_\lambda + 0$

$\left. \begin{array}{l} r_0 \geq r_1 > r_2 > r_3 > r_4 > \dots > r_\lambda > 0 \\ a \geq b > r_0 > r_1 > r_2 > \dots > r_\lambda > 0 \end{array} \right\} r_0 \geq r_1 > r_2 > r_3 > r_4 > \dots > r_\lambda > 0$

$r_{i-1} \geq 1 \cdot r_i + r_{i+1} > r_{i+1} + r_{i+1} = 2r_{i+1}$ ← Tedy r_{i+1} má aspoň o jeden bit meně než r_{i-1} a můžeme omerit počet rovin: $\lambda \leq 2 \cdot \text{len}(r_2) < 2 \cdot \text{len}(b)$

Hrubý odhad: $T \leq \sum_{i=1}^{\lambda} \text{len}(q_i) \cdot \text{len}(b) \leq 2 \cdot \text{len}(b) \cdot \text{len}(a) \cdot \text{len}(b) = 2 \cdot \text{len}(a) \cdot \text{len}(b)^2$

Jemnější odhad: $T = \sum_{i=1}^{\lambda} \text{len}(q_i) \cdot \text{len}(r_i) \leq \text{len}(b) \cdot \sum_{i=1}^{\lambda} \text{len}(q_i) =$

$$= \text{len}(b) \cdot \left(\sum_{i=1}^{\lambda} (\text{len}(r_{i-1}) - \text{len}(r_i) + 1) \right) = \text{len}(b) \cdot [(\text{len}(r_0) - \text{len}(r_1) + 1) + (\text{len}(r_1) - \text{len}(r_2) + 1) + \dots + (\text{len}(r_{\lambda-1}) - \text{len}(r_\lambda) + 1)]$$

$$= \text{len}(b) \cdot [\text{len}(r_0) - \text{len}(r_\lambda) + \lambda] \leq \text{len}(b) \cdot (\text{len}(r_0) + \lambda) \leq \text{len}(b) \cdot (\text{len}(a) + 2 \cdot \text{len}(b)) \leq$$

$$\leq \text{len}(b) \cdot 3 \cdot \text{len}(a)$$

MKR úloha Umocňování v \mathbb{Z}_n

28.2.2019 $\gcd(13, 5) = 1$, můžu použít EF větu

$$5^{200} \mod 13 \quad \varphi(13) = 12$$

$$5^{200 \mod 12} = 5^{170} = 5^{50} = 5^2 = 25 = \underline{\underline{12}}$$

$$31^{57} \mod 14 \quad \gcd(31, 14) = 1, \varphi(14) = \varphi(2) \cdot \varphi(7) = 1 \cdot 6 = 6$$

$$31^{57 \mod 6} = 31^3 \mod 14 = 3^3 = 27 = \underline{\underline{13}}$$

$$137 \stackrel{131}{\sim} \mathbb{Z}_{26} \quad \gcd(137, 26) = 1, \quad \varphi(26) = \varphi(2) \cdot \varphi(13) = 1 \cdot 12 = 12$$

$$137 \stackrel{131 \bmod 12}{\sim} \bmod 26 = 137 \stackrel{11}{\sim} \bmod 26 = 7^{11} \leftarrow \text{je to kladný nezáporný, použijeme opakování} \square$$

$$11 = 8 + 2 + 1 = 1011 = XSSXSX$$

$$\begin{aligned} 1(XSSXSX) &= 7(SSXSX) = 49(SXSX) = -3(SXSX) = 9(SSX) = 63(SX) = 11(SX) = \\ &= 121(x) = -9x = -63 = \underline{\underline{15}} \end{aligned}$$

$$4 \stackrel{21}{\sim} \mathbb{Z}_4 \quad \gcd(4, 14) = 2, \text{ nelze použít EF}$$

$$21 = 16 + 4 + 1 = 10101 = XSSXSX$$

$$\begin{aligned} 1(XSSXSX) &= 4(SSXSX) = 16(SXSX) = 2(SXSX) = 4(XSSX) = 16(SSX) = 2(SSX) = \\ &= 4(SX) = 16x = 2x = \underline{\underline{8}} \end{aligned}$$

$$3^{-1} \sim \mathbb{Z}_{54} \quad \gcd(3, 54) = 3, \text{ nemá' inverzi}$$

$$7^{-1} \sim \mathbb{Z}_{54} \quad \gcd(7, 54) = 1 \quad \varphi(54) = \varphi(3^3) \cdot \varphi(2) = 3^2 \cdot 2 \cdot 1 = 18$$

$$\begin{aligned} a^{\varphi(n)} &= 1 & a \cdot a^{\varphi(n)-1} &= 1 \\ 7^{-1} &= 7^{18-1} & 7^{17} & \end{aligned}$$

$$17 = 16 + 1 = 10001 = XSSXSX$$

$$\begin{aligned} 1(XSSXSX) &= 7(SSXSX) = 49(SSX) = -5(SSX) = 25(SSX) = 625(SX) = -23(SX) = \\ &= 529(x) = -11(x) = -77 = \underline{\underline{31}} \end{aligned}$$

Čínská věta o zbytcích

Pluk má méně než 1000 vejáčků. Pokud nastoupí do sednic, slyde jich 0, nebo 11 tisících jich alespoň 7, a ne 13 tisících 10. Kolik je vejáčků?

$$\left. \begin{array}{l} x \equiv 0 \pmod{7} \\ x \equiv 7 \pmod{11} \\ x \equiv 10 \pmod{13} \end{array} \right\} n = 7 \cdot 11 \cdot 13 = 1001$$

$$\begin{array}{c|c|c} q_7 = 11 \cdot 13 \cdot 1 \equiv 1 \pmod{7} & q_{11} = 7 \cdot 13 \cdot 1 \equiv 1 \pmod{11} & q_{13} = 7 \cdot 11 \cdot 1 \equiv 1 \pmod{13} \\ 4 \cdot (-1) \cdot 1 \equiv 1 \pmod{7} & 7 \cdot 2 \cdot 1 \equiv 1 \pmod{11} & 12 \cdot 1 \equiv 1 \pmod{13} \\ -3 \cdot 1 \equiv 1 \pmod{7} & 3 \cdot 1 \equiv 1 \pmod{11} & -1 \cdot 1 \equiv 1 \pmod{13} \\ 1 \equiv 5 & 1 \equiv 4 & 1 \equiv 12 \\ q_7 = 11 \cdot 13 \cdot 5 = 715 & q_{11} = 7 \cdot 13 \cdot 4 = 364 & q_{13} = 7 \cdot 11 \cdot 12 = 924 \end{array}$$

$$x = 0q_7 + 7q_{11} + 10q_{13} = 2548 + 9240 = 11788 = \underline{\underline{777}} \sim \mathbb{Z} 1001$$

ypočítejte residualně : $A \cdot B, A^B, A^{-1} \sim \mathbb{Z}_{132}, A = 12345678903, B = 312131213121$

$$132 = n = 3 \cdot 4 \cdot 11$$

$$q_3 = 441 = 88$$

$$\sim \mathbb{Z}_3 : A = 48 = 0,$$

$$B = 3 \cdot 7 = 0$$

$$\varphi(3) = 2$$

$$q_4 = 31 = 33$$

$$\sim \mathbb{Z}_4 : A = 03 = 3,$$

$$B = 21 = 1$$

$$\varphi(2^2) = 2 \cdot 1 = 2$$

$$q_{11} = 121 = 12$$

$$\sim \mathbb{Z}_{11} : A = 8,$$

$$B = 2$$

$$\varphi(11) = 10$$

$$\begin{array}{c|c} & A \cdot B \\ \sim \mathbb{Z}_3 & 0 \cdot 0 = 0 \\ \sim \mathbb{Z}_4 & 3 \cdot 1 = 3 \\ \sim \mathbb{Z}_{11} & 8 \cdot 2 = 16 = 5 \end{array}$$

$$\begin{array}{c|c} & A^B \\ A^0 & = 1 \\ 3^B & = 3^{B \bmod 2} = 3^1 = 3 \\ 8^B & = 8^{B \bmod 10} = 8^1 = 8 \end{array}$$

$$\begin{array}{c|c} & A^{-1} \\ A^{-1} & ? \text{ nelze vypočítat, protože } \gcd(A, 3) = 3 \\ 3^{-1} & = 3 \\ 8^{-1} & = 7 \end{array}$$

$$\begin{array}{c|c} & A \cdot B \\ \sim \mathbb{Z}_{132} & 0 \cdot 88 + 33 \cdot 3 + 12 \cdot 5 = \\ & = 159 = 27 \end{array}$$

$$\begin{array}{c|c} & A^B \\ A^0 & = 1 \\ 3^B & = 3^{B \bmod 2} = 3^1 = 3 \\ 8^B & = 8^{B \bmod 10} = 8^1 = 8 \end{array}$$

$$\begin{array}{c|c} & A^{-1} \\ A^{-1} & ? \text{ nelze vypočítat, protože } \gcd(A, 3) = 3, \text{ nutně bude} \\ & \gcd(A, 132) \neq 1, \text{ ledy bylo možné udělat inverzi} \\ & \sim \mathbb{Z}_{132} \end{array}$$