Y36BEZ – Bezpečnost přenosu a zpracování dat

Róbert Lórencz

1. přednáška

Úvod

http://service.felk.cvut.cz/courses/Y36BEZ
lorencz@fel.cvut.cz

Obsah přednášky

- Historie
- Základy modulární aritmetiky
- Základy teorie čísel
- Základní věta aritmetiky

Historie

- Moderní kryptografie – matematický aparát teorie čísel.
- Teorie čísel – studium vlastností přirozených $\mathbb{N} = \{1, 2, \dots\}$ a celých čísel $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$.
- Jedna z nejstarších matematických disciplín – antika.
- Některé algoritmy z období antiky – součást moderních kryptografických systémů, např. Euklidův algoritmus.
- Práce L. Eulera (1707-1783) a C. F. Gausse (1777-1855) položily základ moderní teorie čísel a algebry.
- Velmi důležitý pojem kongruence zaveden Gaussem: $a \equiv b \pmod{m}$ – a je kongruentní b modulo m.
- Algebra – vyšetřuje vlastnosti množin a jejich prvků z hlediska algebraické manipulace s nimi (např. $+/-$).

Základy modulární aritmetiky (1)

Definice kongruence

Nechť $a, b, m \in \mathbb{Z}$, kde $m > 1$. Pokud $m | (b - a)$, říkáme, že b je kongruentní k a modulo m a píšeme

$$b \equiv a \pmod{m}.$$

Pokud $m \nmid (b - a)$, říkáme, že b není kongruentní k a modulo m a píšeme

$$b \not\equiv a \pmod{m}.$$

Pokud používáme celočíselnou aritmetiku a výsledky redukujeme modulem m, říkáme, že používáme tzv. *jedno-modulovou aritmetiku kódů zbytkových tříd (single-modulus residue arithmetic)*. Celé číslo $m > 1$ nazýváme *modulem* aritmetického systému.

Typický příklad z běžného života – „hodinová aritmetika“
$23 \equiv 11 \pmod{12}$ – ? 11 hod. $\sim$ 23 hod. ?

Základy modulární aritmetiky (2)

Vlastnosti kongruencí

Nechť $a, b, c, d, x, y, m \in \mathbb{Z}$, kde $m > 1$.

1. Následující tři kongruence jsou ekvivalentní:
$$\begin{aligned} a &\equiv b \pmod{m}, \\ b &\equiv a \pmod{m}, \\ a - b &\equiv 0 \pmod{m}. \end{aligned}$$
2. Pokud $a \equiv b \pmod{m}$ a $b \equiv c \pmod{m}$ potom $a \equiv c \pmod{m}$.
3. Pokud $a \equiv b \pmod{m}$ a $c \equiv d \pmod{m}$ potom $ax + cy \equiv bx + dy \pmod{m}$.
4. Pokud $a \equiv b \pmod{m}$ a $c \equiv d \pmod{m}$, potom $ac \equiv bd \pmod{m}$.

Základy modulární aritmetiky (3)

V jedno-modulární reziduální aritmetice je každé celé číslo $b \in \mathbb{Z}$ zobrazeno do celého čísla $r \in \mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$.
Číslo r je *nejmenším nezáporným reziduem* b modulo m.

Definice zobrazení $|\cdot|_m$

$|\cdot|_m : \mathbb{Z} \to \mathbb{Z}_m$ je definováno zápisem $|b|_m = r$ tehdy a jen tehdy, když $0 \leq r < m$ a $b \equiv r \pmod{m}$.

$\mathbb{Z}$ je sjednocení m disjunktních podmnožin $\mathcal{R}_0, \mathcal{R}_1, \ldots, \mathcal{R}_{m-1}$ nazvaných *zbytkové třídy*, kde $\mathcal{R}_k = \{b \in \mathbb{Z} : |b|_m = k\}$.

Příklad: Když $m = 7$, potom $58 \in \mathcal{R}_2$ protože $|58|_7 = 2$. Říkáme, že 2 je nejmenší nezáporné reziduum čísla 58 modulo 7.

Základy modulární aritmetiky (4)

Vlastnosti zobrazení $|\cdot|_m$

Věta 1

Nechť $a, b, m \in \mathbb{Z}$, kde $m > 1$. Potom

$$|a|_m \quad \text{je jedinečné},$$

$$|a|_m = |b|_m \iff a \equiv b \pmod{m},$$

$$|km|_m = 0 \quad \text{pro všechna} \quad k \in \mathbb{Z}$$

a dále platí

$$|a+b|_m = \Big||a|_m + |b|_m\Big|_m = \Big||a|_m + b\Big|_m = \Big|a + |b|_m\Big|_m$$

$$|ab|_m = \Big||a|_m|b|_m\Big|_m = \Big||a|_m b\Big|_m = \Big|a|b|_m\Big|_m.$$

Z předcházejícího je zřejmé, že nezáleží na tom, kdy se provede redukce modulo m.

Základy modulární aritmetiky (5)

Věta 2

Množina $(\mathbb{Z}_m, +, \cdot)$, kde $+$ a $\cdot$ označuje sčítání modulo m a násobení modulo m tvoří konečný komutativní okruh s jednotkou.

Důkaz: Ověříme následující vlastnosti, které jsou platné pro každé $a, b, c, \in \mathbb{Z}_m$.

uzavřenost	$\lvert a+b\rvert_m \in \mathbb{Z}_m$	$\lvert ab\rvert_m \in \mathbb{Z}_m,$
komutativita	$\lvert a+b\rvert_m = \lvert b+a\rvert_m$	$\lvert ab\rvert_m = \lvert ba\rvert_m,$
asociativita	$\lvert a+(b+c)\rvert_m = \lvert (a+b)+c\rvert_m$	$\lvert a(bc)\rvert_m = \lvert (ab)c\rvert_m,$
neutrální prvek	$\lvert a+0\rvert_m = \lvert a\rvert_m$	$\lvert a\cdot 1\rvert_m = \lvert a\rvert_m,$
inv. prvek k +	$\lvert a+\underline{a}\rvert_m = 0$	$\cdots,$
distributivita	$\lvert a(b+c)\rvert_m = \lvert ab+ac\rvert_m,$	

kde *aditivní inverze modulo m* je

$$\begin{aligned}\underline{a} &\equiv \lvert -a\rvert_m \\ &= m-a.\end{aligned}$$

Základy modulární aritmetiky (6)

Můžeme definovat odčítání na okruhu $(\mathbb{Z}, +, \cdot)$ jako sčítání s aditivní inverzí modulo m

Definice odčítání na okruhu $(\mathbb{Z}, +, \cdot)$

$$|a - b|_m \equiv |a + \underline{b}|_m.$$

Modulární multiplikativní inverze určitého prvku $(\mathbb{Z}_m, +, \cdot)$ umožňuje provádět dělení tímto prvkem jako násobení jeho inverzí modulo m.

Problém: existence modulární multiplikativní inverze prvku z $(\mathbb{Z}_m, +, \cdot)$.

Věta 3

Konečný komutativní okruh $(\mathbb{Z}, +, \cdot)$ je konečným tělesem tehdy a jen tehdy, pokud m je prvočíslo.

Základy modulární aritmetiky (7)

Pokud m je prvočíslo, $(\mathbb{Z}_m, +, \cdot)$ je izomorfní k Galoisovu tělesu GF(p) a každý nenulový prvek $\mathbb{Z}_m$ má multiplikativní inverzi modulo m, která je definovaná následovně:

Věta 4 – definice

Když m je prvočíslo, $b \neq 0$ a $b \in \mathbb{Z}_m$, pak existuje jediné celé číslo $c \in \mathbb{Z}_m$, které vyhovuje rovnici

$$|cb|_m = |bc|_m = 1.$$

Číslu c říkáme *multiplikativní inverze b modulo m* a píšeme

$$c = b^{-1}(m)$$

nebo jednoduše b^{-1} pokud je modul znám.

Pokud m není prvočíslo, $(\mathbb{Z}_m, +, \cdot)$ není těleso a nenulové prvky nemusí mít multiplikativní inverzi.

Základy modulární aritmetiky (8)

Věta 5 o existenci inverze

Nechť $b \in \mathbb{Z}$. Potom existuje jediné celé číslo $c \in \mathbb{Z}_m$, které vyhovuje rovnici

$$|cb|_m = |bc|_m = 1 \Leftrightarrow |b|_m \neq 0 \wedge \gcd(b, m) = 1.$$

Důsledek: Když $b \in \mathbb{Z}_m, b \neq 0 \Rightarrow$ existuje právě jedno $b^{-1}(m) \in \mathbb{Z}_m$ $\iff$ b a m jsou vzájemně nesoudělná.

Příklady:

- $m = 10$ a $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ tak jen čísla 1,3,7 a 9 mají multiplikativní inverzi modulo 10.
- $m = 5$ (prvočíslo) a $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ tak všechny nenulové prvky (tj. 1,2,3,4) mají multiplikativní inverzi modulo 5.

$(\mathbb{Z}_m, +, \cdot)$ je vždy konečný komutativní okruh. Když m je prvočíslo $\Rightarrow$ $(\mathbb{Z}_m, +, \cdot)$ je konečné těleso izomorfní ke Galoisovu tělesu GF(m).

Definice dělení na konečném tělese

Když b^{-1} existuje $\Rightarrow$ definujeme dělení modulo m jako

$$\left|\frac{a}{b}\right|_m = |ab^{-1}|_m.$$

Pozor!

Podíl dvou celých čísel v jedno-modulární aritmetice, pokud existuje, je vždy celé číslo a to i v případě, že a nedělí b.

Příklad:

$$\begin{aligned} |7/9|_{11} &= |7 \cdot 9^{-1}|_{11} \\ &= |7 \cdot 5|_{11} \\ &= 2\,. \end{aligned}$$

Základy modulární aritmetiky (10)

$|b|_m$ je definováno jako nezáporné rezidum (zbytek) b modulo m. Tímto způsobem jsou výpočty v jedno-modulární aritmetice prováděny s nezápornými celými čísly z množiny $(\mathbb{Z}_m, +, \cdot)$.

V případě použití množiny záporných čísel, uvažujeme množinu *symetrických reziduí* modulo m.

$$\mathbb{S}_m = \left\{-\frac{m-1}{2}, \ldots, -2, -1, 0, 1, 2, \ldots, \frac{m-1}{2}\right\},$$

Pro symetrii vzhledem k nule, m musí být liché číslo.

Množina $\mathbb{S}_m$ zobrazuje každé celé číslo $b \in \mathbb{Z}$ do celého čísla $s \in \mathbb{S}_m$ podle následujícího zobrazení.

Definice symetrického rezidua b modulo $m \rightarrow /b/_m$

$$/\cdot/_m \colon \mathbb{Z} \rightarrow \mathbb{S}_m \wedge /b/_m = s \quad \Leftrightarrow \quad b \equiv s \pmod{m} \wedge -\tfrac{m}{2} < s < \tfrac{m}{2}$$

Základy modulární aritmetiky (11)

Vlastnosti zobrazení $/\cdot/_m$

- $(\mathbb{S}_m, +, \cdot)$ je konečný komutativní okruh,
- Když m je prvočíslo $\Rightarrow$ $(\mathbb{S}_m, +, \cdot)$ je konečné těleso,
- $(\mathbb{S}_m, +, \cdot)$ je izomorfní k $(\mathbb{Z}_m, +, \cdot)$.

Uvažujme případ, že data popisující řešený problém jsou z $\mathbb{S}_m$ $\Rightarrow$

1. zobrazíme daná data z $\mathbb{S}_m$ do $\mathbb{Z}_m$,
2. vykonáváme operace v $\mathbb{Z}_m$,
3. výsledky převedeme do $\mathbb{S}_m$.

Zobrazovací funkce z $/\cdot/_m$ do $|\cdot|_m$ a obráceně jsou následující:

$$|a|_m = \begin{cases} /a/_m, & \text{když } 0 \leq /a/_m < \frac{m}{2} \\ /a/_m + m & \text{jinak}, \end{cases}$$

$$/a/_m = \begin{cases} |a|_m, & \text{když } 0 \leq |a|_m < \frac{m}{2} \\ |a|_m - m & \text{jinak}, \end{cases}$$

Příklad:

$$\begin{aligned} |x|_{103} &= |48/12 + (-24)|_{103} \\ &= \left| |48 \cdot 12^{-1}|_{103} + 79 \right|_{103} \\ &= \left| |48 \cdot 43|_{103} + 79 \right|_{103} \\ &= |4 + 79|_{103} \\ &= 83. \end{aligned}$$

Tento výsledek zobrazíme zpět do $\mathbb{S}_{103}$ a získáme:

$$/x/_{103} = -20.$$

Poznámka: Je důležité vybrat tak velké m, aby $\mathbb{S}_m$ obsahovalo jak hodnoty popisující řešený problém, tak také hodnoty výsledku řešení problému.
Výsledek může být nesprávný, ale je kongruentní se správným výsledkem $\Rightarrow$ nastalo *pseudo-přetečení (pseudo-overflow)*.

Základy teorie čísel (1)

Definice – Největší společný dělitel (greatest common divisor — GCD)

Největší společný dělitel dvou celých nenulových čísel a a b je největší kladné číslo d, pro které platí: $d|a$ a $d|b$. Největší společný dělitel a a b je označen jako $\gcd(a,b)$. Také definujeme $\gcd(0,0)=0$. Z této definice dále plyne:

$$\begin{aligned}\gcd(a,a) &= |a|,\\ \gcd(a,1) &= 1,\\ \gcd(a,b)|a \quad &\text{a současně} \quad \gcd(a,b)|b.\end{aligned}$$

Definice – Nesoudělnost

Celá čísla a a b jsou nesoudělná (relatively prime) když a a b mají největší společný dělitel $\gcd(a,b)=1$.

Příklad: Čísla 25 a 42 jsou nesoudělná protože $\gcd(25,42)=1$.

Základy teorie čísel (2)

Věta 6

Když $a, b, c \in \mathbb{Z}$ a dále když platí, že $a|b$ a $b|c$, potom $a|c$.

Důkaz: Protože $a|b$ a $b|c \Rightarrow$ existují taková celá čísla e a f, pro která platí $ae = b$ a $bf = c$. Z toho vyplývá, že $c = bf = (ae)f = a(ef)$ a $a|c$.

Příklad: $5|15, 15|45 \Rightarrow 5|45$.

Věta 7

Když $a, b, m, n \in \mathbb{Z}$ a dále když platí, že $c|a$ a $c|b$, potom $c|(ma + nb)$.

Důkaz: Když $c|a$ a $c|b \Rightarrow$ existují e a $f \in \mathbb{Z}$, pro která platí $a = ce$ a $b = cf \Rightarrow ma + mb = mce + ncf = c(me + nf)$ a potom $c|(ma + nb)$.

Příklad: $3|6, 3|15 \Rightarrow 3|(6m + 15n) \equiv 3|(3(2m + 5n))$.

Základy teorie čísel (3)

Věta 8

Nechť $a, b, c, d \in \mathbb{Z}$, pro která platí $\gcd(a, b) = d$, $\Rightarrow$

1. $\gcd(a/d, b/d) = 1$
2. $\gcd(a + cb, b) = \gcd(a, b)$

Důkaz:

1. Platí $\gcd(a, b) = d \Rightarrow$ ukážeme, že a/d a b/d nemají společný kladný dělitel jiný než 1. Nechť $e \in \mathbb{Z}$, $e > 0$ a platí $e|(a/d)$ a $e|(b/d) \Rightarrow$ existují taková $k, l \in \mathbb{Z}$, pro která platí $a/d = ke$ a $b/d = le$ a tedy $a = dek$ a $b = del \Rightarrow de$ je společným dělitelem a a b. Protože d je největší společný dělitel a a b platí $de \leq d$ a z toho plyne, že $e = 1$ a tedy také $\gcd(a/d, b/d) = 1$.
2. Když nějaké celé číslo e dělí jak a, tak také $b \Rightarrow e|(a + cb)$. Společní dělitelé b a $(a + cb)$ jsou stejná čísla jako společní dělitelé a a $b \Rightarrow$??? $\Rightarrow \gcd(a + cb, b) = \gcd(a, b)$.

Základy teorie čísel (4)

Dále si ukážeme, že největší společný dělitel celých nenulových čísel a a b je vyjádřen součtem $ma + nb$, kde m a n jsou celá čísla.

Definice – Lineární kombinace

Když $a, b \in \mathbb{Z}$, potom **lineární kombinace** nenulových čísel a a b je vyjádřena vztahem $ma + nb$, kde $m, n \in \mathbb{Z}$.

Věta 9

Největší společný dělitel celých nenulových čísel a a b je nejmenší kladné celé číslo, které je lineární kombinací a a b.

Důkaz (1): Nechť d je nejmenší kladné číslo, které je lineární kombinací a a b. (Minimálně jedno takové kladné číslo existuje, protože jedna ze dvou lineárních kombinací $1a + 0b$ a $(-1)a + 0b$, kde $a \neq 0$, je kladná.) Pak píšeme

$$d = ma + nb,$$

kde m a n jsou celá čísla.

Základy teorie čísel (5)

Důkaz (2): Ukážeme, že $d|a$ a $d|b$. Z algoritmu pro dělení plyne

$$a = dq + r, \quad 0 \leq r < d.$$

Z předchozích dvou rovnic dostáváme rovnici

$$r = a - dq = a - q(ma + nb) = (1 - qm)a - qnb.$$

Z toho plyne, že r je lineární kombinací a a b. Protože $0 \leq r < d$ a d je nejmenší kladná lineární kombinace a a b platí, že $r = 0$ a odtud $d|a$. Podobným způsobem můžeme ukázat, že platí $d|b$.
Dále si dokážeme, že d je největší společný dělitelem a i b. Toto tvrzení platí, pokud existuje nějaký společný dělitel c čísel a a b, který dělí také d. Protože $d = ma + nb$ a z předpokladu $c|a$ a $c|b$ potom podle Věty 7 $c|d$. Pokud $d|a$ a $d|b$, a to jsme dokázali, $\Rightarrow$ $\gcd(a, b) = d$.

Základy teorie čísel (6)

Vývojem algoritmu pro nalezení GCD dvou kladných celých čísel se zabýval řecký matematik Euklides narozen cca 350 let pnl. Metoda, kterou Euklides vyvinul/zapsal pro výpočet GCD je známa jako Euklidův algoritmus (EA).

Věta 10 – Euklidův algoritmus

Nechť $r_0 = a$ a $r_1 = b$ jsou celá čísla, pro která platí $a \geq b > 0$. Pokud je dělící algoritmus postupně použit k získání $r_j = r_{j+1} q_{j+1} + r_{j+2}$, při platnosti podmínek $0 < r_{j+2} < r_{j+1}$ pro $j = 0, 1, 2, \ldots, n-2$ a $r_{n+1} = 0$, potom $\gcd(a, b) = r_n$ je poslední nenulový zbytek.

Jinak: $\gcd(a, b)$ je poslední nenulový zbytek r_n v sekvenci rovnic generovaných s postupným použitím dělícího algoritmu prováděného tak dlouho, dokud není zbytek rovný nule. V každém dalším kroku algoritmu je dělenec a dělitel zaměněn za menší čísla a to za dělitele a zbytek kroku předchozího.

Důkaz (1): Nechť $r_0 = a$ a $r_1 = b$ jsou kladná celá čísla, pro která platí $a \geq b$. Postupným prováděním dělícího algoritmu dostáváme posloupnost rovnic a podmínek pro výpočet zbytků $r_2, r_3, \ldots, r_{n-1}$

$$
\begin{array}{lcll}
r_0 & = & r_1 q_1 + r_2 & 0 \leq r_2 < r_1 \\
r_1 & = & r_2 q_2 + r_3 & 0 \leq r_3 < r_2 \\
 & \vdots & & \\
r_{j-2} & = & r_{j-1} q_{j-1} + r_j & 0 \leq r_j < r_{j-1} \\
 & \vdots & & \\
r_{n-3} & = & r_{n-2} q_{n-2} + r_{n-1} & 0 \leq r_{n-1} < r_{n-2} \\
r_{n-2} & = & r_{n-1} q_{n-1} + r_n & 0 \leq r_n < r_{n-1} \\
r_{n-1} & = & r_n q_n &
\end{array}
$$

Můžeme předpokládat, že pro získání zbytku, který je roven nule, potřebujeme konečný počet dělení a to nejvíce a protože platí $a = r_0 > r_1 > r_2 > \cdots \geq 0$.

Základy teorie čísel (8)

Důkaz (2): S použitím pomocné věty Věta 8 (2.) dále platí, že $\gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \gcd(r_2, r_3) = \cdots = \gcd(r_{n-3}, r_{n-2}) = \gcd(r_{n-2}, r_{n-1}) = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n \Rightarrow \gcd(a, b) = r_n$, kde r_n je poslední nenulový zbytek.

Příklad: $\gcd(254, 158) = ?$

$$
\begin{aligned}
254 &= 1 \cdot 158 + 96 \\
158 &= 1 \cdot 96 + 62 \\
96 &= 1 \cdot 62 + 34 \\
62 &= 1 \cdot 34 + 28 \\
34 &= 1 \cdot 28 + 6 \\
28 &= 4 \cdot 6 + 4 \\
6 &= 1 \cdot 4 + 2 \\
4 &= 2 \cdot 2\,.
\end{aligned}
$$

$\gcd(254, 158) = 2.$

Základní věta aritmetiky (1)

Množinu všech kladných nenulových čísel (přirozených čísel) rozdělujeme do tří skupin:

1. Číslo 1, které kromě sebe není dělitelné žádným jiným číslem.
2. Prvočísla, které kromě sebe jsou dělitelné jen číslem 1.
3. A ostatní čísla, která se nazývají složená.

Věta 11 - pomocná

Když $a|bc$ a $\gcd(a, b) = 1$ potom $a|c$.

Důkaz: Z podmínky $\gcd(a, b) = 1$ plyne podle Věty 9, že existují taková celá čísla x a y, že $1 = ax + by$. Vynásobme uvedenou rovnici číslem c:

$$c = cax + cby.$$

Podle předpokladu $a|bc$ a Věty 7 je tedy pravá strana poslední rovnosti dělitelná číslem a, a proto musí být dělitelná také levá tj. číslem c.

Základní věta aritmetiky (2)

Věta 12

Nechť p je prvočíslo a nechť $p|(a_1 \cdot a_2 \cdot \dots \cdot a_k)$, kde a_i, k jsou přirozená čísla. Potom buď $p|a_1$ nebo $p|a_2$ ... nebo $p|a_k$. Slovy: Když prvočíslo je dělitelem součinu, potom je dělitelem alespoň jednoho činitele.

Důkaz: Důkaz provedeme indukcí.
Větu dokážeme nejdříve pro $k = 2$. Pokud p je prvočíslo, mohou nastat dva případy, buď $p|a_1$, a v tom případě nemáme co dokazovat, nebo $\gcd(p, a_1) = 1$. Ve druhém případě z pomocné Věty 11 a ze vztahu $p|(a_1 \cdot a_2)$ plyne $p|a_2$.
Nyní si označme $A = a_1 \cdot a_2 \cdots a_{k-1}$. Předpokládejme, že věta platí pro $k - 1$ činitelů a dokážeme, že platí také pro k činitelů. Podle předpokladů věty platí $p|(A \cdot a_k)$. Opět rozlišujeme dva případy: buď $p|A$, a potom podle indukčního předpokladu je naše tvrzení pravdivé, neboť $p|a_k$.

Základní věta aritmetiky (3)

Věta 13

Každé složené číslo můžeme psát ve tvaru součinu prvočísel.

Důkaz: Důkaz provedeme indukcí.
Nejmenší složené číslo je 4, pro které platí $4 = 2 \cdot 2$, a tedy tvrzení je správné. Předpokládejme, že tvrzení je pravdivé pro všechna složená čísla menší než n. Nechť n je složené číslo a můžeme ho napsat ve tvaru $n = a \cdot b$, kde $1 < a < n$, $1 < b < n$. Číslo a je buď prvočíslo, nebo složené číslo menší než n, a tak podle indukčního předpokladu je ho možné napsat ve tvaru součinu prvočísel. To samé platí také pro b, a proto také n můžeme zapsat ve tvaru součinu prvočísel, protože n je součinem a a b.

Základní věta aritmetiky ukazuje, že prvočísla jsou základními "stavebními prvky" přirozených čísel.

Základní věta aritmetiky (4)

Věta 14 – Základní věta aritmetiky

Každé kladné celé číslo n se dá vyjádřit jediným způsobem ve tvaru, který se nazývá **kanonickým rozkladem** čísla n nebo **prvočíselnou mocninnou faktorizací** čísla n

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

kde $p_1 < p_2 < \cdots < p_k$ jsou prvočísla a $\alpha_1, \ldots, \alpha_k$ jsou přirozená čísla.

Slovně: Každé složené číslo může být jednoznačně zapsáno jako součin prvočísel, kde prvočíselné součinitele jsou seřazeny do neklesající posloupnosti.

Důkaz (1): Vyjádření složených čísel ve tvaru součinů prvočísel bylo již uvedeno ve Větě 13. Když n je prvočíslo, pak stačí, když $k = 1$, $p_1 = n$ a $\alpha_1 = 1$.
Zbývá ještě dokázat, že pro každé přirozené číslo existuje jediné takové vyjádření.

Základní věta aritmetiky (5)

Důkaz (2): Předpokládejme, že pro nějaké n existují dvě vyjádření v kanonickém tvaru

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

$$n = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdots q_s^{\beta_s},$$

kde $p_1 < p_2 < \cdots < p_k$, $q_1 < q_2 < \cdots < q_s$, jsou prvočísla a $\alpha_1, \ldots, \alpha_k$ a $\beta_1, \ldots, \beta_s$ jsou přirozená čísla. Potom

$$p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k} = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdots q_k^{\beta_s}.$$

Pro každé i tedy platí

$$p_i | (q_1^{\beta_1} \cdot q_2^{\beta_2} \cdots q_s^{\beta_s}).$$

Na základě Věty 12 z toho plyne, že $p_i | q_j^{\beta_j}$ pro některá j. Stačí opět aplikovat Větu 12, abychom dostali $p_i | q_i$, a to je možné jen tehdy, když $p_i = q_i$, protože obě jsou prvočísla. Z toho dále plyne, že na pravé straně rovnice $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k} = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdots q_k^{\beta_s}$ je alespoň tolik prvočísel, jako na levé, tj. $k \leq s$. Protože p_i a q_i jsou uspořádané podle velikosti $\Rightarrow p_1 = q_1, \ldots, p_k = q_k$.

Základní věta aritmetiky (6)

Důkaz (3): Zbývá ještě dokázat, že $\alpha_i = \beta_i$ pro $i = 1, 2, \ldots, k$. Tento důkaz provedeme nepřímo. Předpokládejme, že $\alpha_i > \beta_i$. Potom z rovnosti $s = k$ po vydělení rovnice $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k} = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdots q_k^{\beta_s}$ číslem $p_i^{\beta_i}$ dostaneme rovnost

$$p_1^{\alpha_1} \cdots p_{i-1}^{\alpha_{i-1}} \cdot p_i^{\alpha_i - \beta_i} \cdot p_{i+1}^{\alpha_{i+1}} \cdots p_k^{\alpha_k} = p_1^{\beta_1} \cdots p_{i-1}^{\beta_{i-1}} \cdot p_{i+1}^{\beta_{i+1}} \cdots p_k^{\beta_k}.$$

$\alpha_i - \beta_i > 0$, a proto levá strana předchozí rovnosti je dělitelná prvočíslem p_i, ale pravá ne, a to je spor. Podobně postupujeme v případě $\beta_i > \alpha_i$, takže pro všechny $i = 1, \ldots, k$ platí $\alpha_i = \beta_i$. Z toho ale vyplývá, že každé dvě vyjádření čísla n v kanonickém tvaru jsou totožná, a proto libovolné n můžeme vyjádřit v kanonickém tvaru jen jediným způsobem.

Příklad: Kladná čísla 240, 289 a 1001 můžeme vyjádřit následovně:

$$\begin{aligned} 240 &= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 = 2^4 \cdot 3 \cdot 5 \\ 289 &= 17 \cdot 17 = 17^2 \\ 1001 &= 7 \cdot 11 \cdot 13 \end{aligned}$$

Základní věta aritmetiky (7)

Dále si uvedeme, jakým způsobem lze využít prvočíselnou faktorizaci pro popis největšího společného dělitele – GCD dvou celých čísel a a b $\gcd(a, b)$. Dále označení $\min(a, b)$ vyjadřuje menší nebo minimum dvou čísel a a b.

Nechť prvočíselná faktorizace dvou čísel a a b je vyjádřena

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \quad b = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdots q_k^{\beta_k},$$

kde každý exponent je celé nezáporné číslo, a kde všechna prvočísla vyskytující se v prvočíselné faktorizaci a a b jsou obsažena v obou součinech a také s nulovým exponentem $\Rightarrow$ to nejsou kanonické rozklady. Potom

$$\gcd(a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdot p_2^{\min(\alpha_2, \beta_2)} \cdots p_k^{\min(\alpha_k, \beta_k)},$$

protože čísla a a b sdílejí právě $\min(\alpha_i, \beta_i)$ násobků prvočísla p_i.

Základní věta aritmetiky (8)

Prvočíselný rozklad může být také použit pro nalezení nejmenšího celého čísla, které je násobkem dvou kladných celých čísel.

Definice – Nejmenší společný násobek (least common multiple – LCM)

Nejmenší společný násobek dvou kladných čísel a a b je nejmenší kladné celé číslo, které je dělitelné čísly a i b.
Nejmenší společný násobek čísel a a b je označován zápisem $[a, b]$.

Pokud prvočíselné rozklady čísel a a b jsou známe, lehce můžeme najít $[a, b]$. Nechť opět platí

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \quad b = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdots q_k^{\beta_k},$$

a také každý exponent je celé nezáporné číslo, a kde všechna prvočísla vyskytující se v prvočíselné faktorizaci a a b jsou obsažena v obou součinech.

Základní věta aritmetiky (9)

Pro celé číslo, které dělí jak a, tak také b platí, že jeho prvočíselný rozklad je vytvořený prvočísly p_i umocněný minimálně mocninou většího ze dvou čísel α_i a $\beta_i \Rightarrow [a, b]$, nejmenší kladné celé číslo dělitelné a a b je

$$[a, b] = p_1^{\max(\alpha_1, \beta_1)} \cdot p_2^{\max(\alpha_2, \beta_2)} \cdots p_k^{\max(\alpha_k, \beta_k)},$$

kde $\max(x, y)$ označuje větší číslo z čísel x, y.

- Prvočíselný rozklad velkých celých čísel je časově náročná operace $\Rightarrow$
- nalezení nejmenšího společného násobku dvou celých čísel využíváme GCD daných čísel.
- GCD lze lehce nalezt podle Euklidova algoritmu.

Věta 15 – pomocná

Když x a y jsou reálná čísla, potom $\min(x, y) + \max(x, y) = x + y$.

Základní věta aritmetiky (10)

Věta 16

Když a a b jsou dvě kladná celá čísla, potom $[a, b] = \dfrac{a \cdot b}{\gcd(a, b)}$.

Důkaz: Nechť a a b mají prvočíselný rozklad $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_k^{\beta_k}$, kde exponenty $\alpha_i \geq 0$ $\beta_i \geq 0$ jsou celá čísla. Označme $M_i = \max(\alpha_i, \beta_i)$ a $m_i = \min(\alpha_i, \beta_i)$. Potom

$$
\begin{aligned}
[a, b] \cdot \gcd(a, b) &= p_1^{M_1} \cdot p_2^{M_2} \cdots p_k^{M_k} \cdot p_1^{m_1} \cdot p_2^{m_2} \cdots p_k^{m_k}, \\
&= p_1^{M_1 + m_1} \cdot p_2^{M_2 + m_2} \cdots p_k^{M_k + m_k}, \\
&= p_1^{\alpha_1 + \beta_1} \cdot p_2^{\alpha_2 + \beta_2} \cdots p_k^{\alpha_k + \beta_k}, \\
&= p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k} \cdot p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_k^{\beta_k}, \\
&= a \cdot b\,.
\end{aligned}
$$

Využili jsme rovnosti $M_i + m_i = \max(\alpha_i, \beta_i) + \min(\alpha_i, \beta_i) = \alpha_i + \beta_i$, jejíž platnost plyne z pomocné Věty 15.