Diskrétní matematika – 3. týden
Elementární teorie čísel – Eulerova věta, řád prvku

Jan Slovák

Masarykova univerzita
Fakulta informatiky

jaro 2015

Obsah přednášky

Doporučené zdroje

- Jan Slovák, Martin Panák, Michal Bulant **Matematika drsně a svižně**, *e*-text na `www.math.muni.cz/Matematika_drsne_svizne`.
- Michal Bulant, výukový text k přednášce **Elementární teorie čísel**, `http://is.muni.cz/el/1431/podzim2012/M6520/um/main-print.pdf`
- Jiří Herman, Radan Kučera, Jaromír Šimša, **Metody řešení matematických úloh**. MU Brno, 2001.
- William Stein, **Elementary Number Theory: Primes, Congruences, and Secrets**, Springer, 2008. Dostupné na `http://wstein.org/ent/ent.pdf`
- Radan Kučera, výukový text k přednášce **Algoritmy teorie čísel**, `http://www.math.muni.cz/~kucera/texty/ATC10.pdf`

Aritmetické funkce

Aritmetickou funkcí zde rozumíme funkci, jejímž definičním oborem je množina přirozených čísel.

Definice

Rozložme přirozené číslo n na prvočísla: $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Hodnotu *Möbiovy funkce* $\mu(n)$ definujeme rovnu 0, pokud pro některé i platí $\alpha_i > 1$ a rovnu $(-1)^k$ v opačném případě. Dále definujeme $\mu(1) = 1$.

Příklad

$\mu(4) = \mu(2^2) = 0, \mu(6) = \mu(2 \cdot 3) = (-1)^2, \mu(2) = \mu(3) = -1.$

Dokážeme nyní několik důležitých vlastností Möbiovy funkce, zejména tzv. *Möbiovu inverzní formuli*.

Lemma

Pro $n \in \mathbb{N} \setminus \{1\}$ *platí* $\sum_{d|n} \mu(d) = 0$.

Důkaz.

Zapíšeme-li n ve tvaru $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, pak všechny dělitele d čísla n jsou tvaru $d = p_1^{\beta_1} \cdots p_k^{\beta_k}$, kde $0 \leq \beta_i \leq \alpha_i$ pro všechna $i \in \{1, \ldots, k\}$. Proto

$$\begin{aligned}
\sum_{d|n} \mu(d) &= \sum_{\substack{(\beta_1,\ldots,\beta_k)\in(\mathbb{N}\cup\{0\})^k \\ 0\leq\beta_i\leq\alpha_i}} \mu(p_1^{\beta_1} \cdots p_k^{\beta_k}) = \\
&= \sum_{(\beta_1,\ldots,\beta_k)\in\{0,1\}^k} \mu(p_1^{\beta_1} \cdots p_k^{\beta_k}) \\
&= \binom{k}{0} + \binom{k}{1} \cdot (-1) + \binom{k}{2} \cdot (-1)^2 + \cdots + \binom{k}{k} \cdot (-1)^k \\
&= \big(1 + (-1)\big)^k = 0.
\end{aligned}$$

S Möbiovou funkcí úzce souvisí pojem *Dirichletův součin* (konvoluce):

Definice

Buďte f, g aritmetické funkce. Jejich *Dirichletův součin* je definován předpisem

$$(f \circ g)(n) = \sum_{d|n} f(d) \cdot g\left(\tfrac{n}{d}\right) = \sum_{d_1 d_2 = n} f(d_1) \cdot g(d_2).$$

Lemma

Dirichletův součin je asociativní.

Důkaz.

$$((f \circ g) \circ h)(n) = \sum_{d_1 d_2 d_3 = n} f(d_1) \cdot g(d_2) \cdot h(d_3) = (f \circ (g \circ h))(n)$$

□

Příklad

Definujme dvě pomocné funkce $\mathbb{I}$ a I předpisem $\mathbb{I}(1) = 1$, $\mathbb{I}(n) = 0$ pro všechna $n > 1$, resp. $I(n) = 1$ pro všechna $n \in \mathbb{N}$. Pak pro každou aritmetickou funkci f platí:

$$f \circ \mathbb{I} = \mathbb{I} \circ f = f \quad \text{a} \quad (I \circ f)(n) = (f \circ I)(n) = \sum_{d|n} f(d).$$

Dále platí $I \circ \mu = \mu \circ I = \mathbb{I}$, neboť

$$(I \circ \mu)(n) = \sum_{d|n} I(d)\mu(\tfrac{n}{d}) = \sum_{d|n} I(\tfrac{n}{d})\mu(d) =$$
$$= \sum_{d|n} \mu(d) = 0 \quad \text{pro všechna } n > 1$$

podle lemmatu za definicí Möbiovy funkce (pro $n = 1$ je tvrzení zřejmé).

Věta (Möbiova inverzní formule)

Nechť je aritmetická funkce F definovaná pomocí aritmetické funkce f předpisem $F(n) = \sum_{d|n} f(d)$. Pak lze funkci f vyjádřit ve tvaru

$$f(n) = \sum_{d|n} \mu(\tfrac{n}{d}) \cdot F(d).$$

Důkaz.

Vztah $F(n) = \sum_{d|n} f(d)$ lze jiným způsobem zapsat jako $F = f \circ I$. Proto $F \circ \mu = (f \circ I) \circ \mu = f \circ (I \circ \mu) = f \circ \mathbb{I} = f$, což je tvrzení věty. □

Definice

Multiplikativní funkcí přirozených čísel rozumíme takovou aritmetickou funkci, která splňuje, že pro všechny dvojice **nesoudělných** čísel $a, b \in \mathbb{N}$ platí

$$f(a \cdot b) = f(a) \cdot f(b).$$

Příklad

Multiplikativními funkcemi jsou např. funkce $f(n) = \sigma(n)$, $f(n) = \tau(n)$, či $f(n) = \mu(n)$ nebo, jak brzy dokážeme i tzv. Eulerova funkce $f(n) = \varphi(n)$.

Eulerova funkce

Definice

Nechť $n \in \mathbb{N}$. Definujme Eulerovu funkci φ předpisem

$$\varphi(n) = |\{a \in \mathbb{N} \,|\, 0 < a \leq n, (a, n) = 1\}|$$

Příklad

$\varphi(1) = 1, \varphi(5) = 4, \varphi(6) = 2$, je-li p prvočíslo, je zřejmě $\varphi(p) = p - 1$.

Nyní dokážeme několik důležitých tvrzení o funkci φ:

Lemma

Nechť $n \in \mathbb{N}$. Pak $\sum_{d|n} \varphi(d) = n$.

Důkaz.

Uvažme n zlomků

$$\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \ldots, \frac{n-1}{n}, \frac{n}{n}.$$

Zkrátíme-li zlomky na základní tvar a seskupíme podle jmenovatelů, snadno dostaneme právě uvedené tvrzení. □

Věta

Nechť $n \in \mathbb{N}$, jehož rozklad je tvaru $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Pak

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

Důkaz.

S využitím předchozího lemmatu a Möbiovy inverzní formule dostáváme

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d} = n - \frac{n}{p_1} - \cdots - \frac{n}{p_k} + \cdots + (-1)^k \frac{n}{p_1 \cdots p_k} =$$

$$= n \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

□

Poznámka

Předchozí výsledek lze obdržet i bez použití Möbiovy inverzní formule pomocí principu inkluze a exkluze na základě zjištění počtu čísel soudělných s n v určitém intervalu.

Důsledek

Nechť $a, b \in \mathbb{N}$, $(a, b) = 1$. *Pak*

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b).$$

Poznámka

Rovněž toto tvrzení lze odvodit nezávisle na základě poznatku $(n, ab) = 1 \iff (n, a) = 1 \wedge (n, b) = 1$. Spolu se snadno odvoditelným výsledkem

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

pak lze odvodit vztah pro výpočet φ již třetím způsobem.

Příklad

Vypočtěte $\varphi(72)$.

Řešení

$72 = 2^3 \cdot 3^2 \implies \varphi(72) = 72 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{3}) = 24$, alternativně $\varphi(72) = \varphi(8) \cdot \varphi(9) = 4 \cdot 6 = 24$. □

Příklad

Dokažte, že $\forall n \in \mathbb{N} : \varphi(4n + 2) = \varphi(2n + 1)$.

Řešení

$\varphi(4n + 2) = \varphi(2 \cdot (2n + 1)) = \varphi(2) \cdot \varphi(2n + 1) = \varphi(2n + 1)$. □

Malá Fermatova věta

Tato tvrzení patří mezi nejdůležitější výsledky elementární teorie čísel.

Věta (Fermatova, Malá Fermatova)

Nechť $a \in \mathbb{Z}$, p prvočíslo, $p \nmid a$. Pak

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

Důkaz.

Tvrzení vyplyne jako snadný důsledek Eulerovy věty. Dá se ale dokázat i přímo (např. matematickou indukcí nebo kombinatoricky) □

Důsledek

Nechť $a \in \mathbb{Z}$, p prvočíslo. Pak

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

Úplná a redukovaná soustava zbytků

Definice

Úplná soustava zbytků modulo m je libovolná m-tice čísel po dvou nekongruentních modulo m (nejčastěji $0, 1, \ldots, m-1$).
Redukovaná soustava zbytků modulo m je libovolná $\varphi(m)$-tice čísel nesoudělných s m a po dvou nekongruentních modulo m.

Lemma

Nechť $x_1, x_2, \ldots, x_{\varphi(m)}$ tvoří redukovanou soustavu zbytků modulo m. Je-li $a \in \mathbb{Z}$, $(a, m) = 1$ pak i čísla $a \cdot x_1, \ldots, a \cdot x_{\varphi(m)}$ tvoří redukovanou soustavu zbytků modulo m.

Důkaz.

Protože $(a, m) = 1$ a $(x_i, m) = 1$, platí $(a \cdot x_i, m) = 1$. Kdyby pro nějaká i, j platilo $a \cdot x_i \equiv a \cdot x_j \pmod{m}$, po vydělení obou stran kongruence číslem a nesoudělným s m dostaneme $x_i \equiv x_j \pmod{m}$. □

Eulerova věta

Věta (Eulerova)

Nechť $a \in \mathbb{Z}$, $m \in \mathbb{N}$, $(a, m) = 1$. *Pak*

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

Důkaz.

Buď $x_1, x_2, \ldots, x_{\varphi(m)}$ libovolná redukovaná soustava zbytků modulo m. Podle předchozího lemmatu je i $a \cdot x_1, \ldots, a \cdot x_{\varphi(m)}$ redukovaná soustava zbytků modulo m. Platí tedy, že pro každé i existuje j ($i, j \in \{1, 2, \ldots, \varphi(m)\}$) tak, že $a \cdot x_i \equiv x_j \pmod{m}$. Vynásobením dostáváme
$(a \cdot x_1) \cdot (a \cdot x_2) \cdots (a \cdot x_{\varphi(m)}) \equiv x_1 \cdot x_2 \cdots x_{\varphi(m)} \pmod{m}$. Po úpravě

$$a^{\varphi(m)} \cdot x_1 \cdot x_2 \cdots x_{\varphi(m)} \equiv x_1 \cdot x_2 \cdots x_{\varphi(m)} \pmod{m}$$

vydělení číslem $x_1 \cdot x_2 \cdots x_{\varphi(m)}$ dostaneme požadované. □

Řád čísla

S Eulerovou funkcí a Eulerovou větou úzce souvisí důležitý pojem *řád čísla modulo m*:

Definice

Nechť $a \in \mathbb{Z}$, $m \in \mathbb{N}$ $(a, m) = 1$. *Řádem čísla a modulo m* rozumíme nejmenší přirozené číslo n splňující

$$a^n \equiv 1 \pmod{m}.$$

Poznámka

To, že je řád definován, plyne z Eulerovy věty – pro každé číslo nesoudělné s modulem je totiž jistě jeho řád nejvýše roven $\varphi(m)$. Jak později uvidíme, velmi důležitá jsou právě ta čísla, jejichž **řád je roven právě** $\varphi(m)$ – tato čísla nazýváme primitivními kořeny modulo m a hrají důležitou roli mj. při řešení binomických kongruencí.

Příklad

Pro libovolné $m \in \mathbb{N}$ má číslo 1 modulo m řád 1. Číslo -1 má řád

- 1 pro $m = 1$ nebo $m = 2$
- 2 pro $m > 2$

Příklad

Určete řád čísla 2 modulo 7.

Řešení

$$2^1 = 2 \not\equiv 1 \pmod 7$$
$$2^2 = 4 \not\equiv 1 \pmod 7$$
$$2^3 = 8 \equiv 1 \pmod 7$$

Řád čísla 2 modulo 7 je tedy roven 3. □

Uveďme nyní několik zásadních tvrzení udávajících vlastnosti řádu čísla modulo m:

Lemma

Nechť $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$, $(a, m) = (b, m) = 1$. *Jestliže* $a \equiv b \pmod{m}$, *pak obě čísla* a, b *mají stejný řád modulo* m.

Důkaz.

Umocněním kongruence $a \equiv b \pmod{m}$ na n-tou dostaneme $a^n \equiv b^n \pmod{m}$, tedy $a^n \equiv 1 \pmod{m} \iff b^n \equiv 1 \pmod{m}$. □

Lemma

Nechť $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. Je-li řád čísla a modulo m roven $r \cdot s$, (kde $r, s \in \mathbb{N}$), pak řád čísla a^r modulo m je roven s.

Důkaz.

Protože žádné z čísel $a, a^2, a^3, \ldots, a^{rs-1}$ není kongruentní s 1 modulo m, není ani žádné z čísel $a^r, a^{2r}, a^{3r}, \ldots, a^{(s-1)r}$ kongruentní s 1. Platí ale $(a^r)^s \equiv 1 \pmod{m}$, proto je řád a^r modulo m roven s. □

Poznámka

Opak obecně neplatí – z toho, že řád čísla a^r modulo m je roven s ještě neplyne, že řád čísla a modulo m je $r \cdot s$.

Např pro $m = 13$ máme:

$a = 3$, $a^2 = 9 \pmod{13}$, $a^3 = 27 \equiv 1 \pmod{13} \Rightarrow 3$ má řád 3 mod 13.

$b = -4$, $b^2 = 16 \not\equiv 1 \pmod{13}$, $b^3 = -64 \equiv 1 \pmod{13} \Rightarrow -4$ má řád 3 mod 13.

Přitom $(-4)^2 = 16 \equiv 3 \pmod{13}$ má stejný řád 3 jako číslo 3, ale číslo -4 nemá řád $2 \cdot 3$.

Přesný popis závislosti řádu na exponentu dávají následující 2 věty:

Věta

Nechť $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. Označme r řád čísla a modulo m. Pak pro libovolná $t, s \in \mathbb{N} \cup \{0\}$ platí

$$a^t \equiv a^s \pmod{m} \iff t \equiv s \pmod{r}.$$

Důkaz.

Bez újmy na obecnosti lze předpokládat, že $t \geq s$. Vydělíme-li číslo $t - s$ číslem r se zbytkem, dostaneme $t - s = q \cdot r + z$, kde $q, z \in \mathbb{N}_0, 0 \leq z < r$.

"$\Leftarrow$" Protože $t \equiv s \pmod{r}$, máme $z = 0$, a tedy $a^{t-s} = a^{qr} = (a^r)^q \equiv 1^q \pmod{m}$. Vynásobením obou stran kongruence číslem a^s dostaneme tvrzení.

"$\Rightarrow$" Z $a^t \equiv a^s \pmod{m}$ plyne $a^s \cdot a^{qr+z} \equiv a^s \pmod{m}$. Protože je $a^r \equiv 1 \pmod{m}$, je rovněž $a^{qr+z} \equiv a^z \pmod{m}$. Celkem po vydělení obou stran kongruence číslem a^s (které je nesoudělné s modulem), dostáváme $a^z \equiv 1 \pmod{m}$. Protože $z < r$, plyne z definice řádu, že $z = 0$, a tedy $r \mid t - s$. □

Zřejmým důsledkem předchozí věty a Eulerovy věty je následující tvrzení

Důsledek

Nechť $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. Označme r řád čísla a modulo m.

1. *Pro libovolné $n \in \mathbb{N} \cup \{0\}$ platí*

$$a^n \equiv 1 \pmod{m} \iff r \mid n.$$

2. $r \mid \varphi(m)$

Následující věta je zobecněním předchozího Lemmatu.

Věta

Nechť $m, n \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. *Je-li řád čísla* a *modulo* m *roven* $r \in \mathbb{N}$, *je řád čísla* a^n *modulo* m *roven* $\frac{r}{(n,r)}$.

Důkaz.

Protože $\frac{r \cdot n}{(r,n)} = [r, n]$, což je zřejmě násobek r, máme

$$(a^n)^{\frac{r}{(r,n)}} = a^{[r,n]} \equiv 1 \pmod{m}$$

(plyne z předchozího Důsledku, neboť $r \mid [r, n]$). Na druhou stranu, je-li $k \in \mathbb{N}$ libovolné takové, že $(a^n)^k = a^{n \cdot k} \equiv 1 \pmod{m}$, dostáváme ($r$ je řád a), že $r \mid n \cdot k$ a dále víme, že $\frac{r}{(n,r)} \mid \frac{n}{(n,r)} \cdot k$ a díky nesoudělnosti čísel $\frac{r}{(n,r)}$ a $\frac{n}{(n,r)}$ dostáváme $\frac{r}{(n,r)} \mid k$. Proto je $\frac{r}{(n,r)}$ řádem čísla a^n modulo m. □

Poslední z této řady tvrzení dává do souvislosti řády dvou čísel a řád jejich součinu:

Lemma

Nechť $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$, $(a, m) = (b, m) = 1$. Jestliže a je řádu r a b je řádu s modulo m, kde $(r, s) = 1$, pak číslo $a \cdot b$ je řádu $r \cdot s$ modulo m.

Důkaz.

Označme δ řád čísla $a \cdot b$. Pak $(ab)^\delta \equiv 1 \pmod{m}$ a umocněním obou stran kongruence dostaneme $a^{r\delta} b^{r\delta} \equiv 1 \pmod{m}$. Protože je r řádem čísla a, je $a^r \equiv 1 \pmod{m}$, tj. $b^{r\delta} \equiv 1 \pmod{m}$, a proto $s \mid r\delta$. Z nesoudělnosti r a s plyne $s \mid \delta$. Analogicky dostaneme i $r \mid \delta$, a tedy (opět s využitím nesoudělnosti r, s) $r \cdot s \mid \delta$. Obráceně zřejmě platí $(ab)^{rs} \equiv 1 \pmod{m}$, proto $\delta \mid rs$. Celkem tedy $\delta = rs$. □

Kongruence o jedné neznámé

Definice

Nechť $m \in \mathbb{N}$, $f(x), g(x) \in \mathbb{Z}[x]$. Zápis

$$f(x) \equiv g(x) \pmod{m}$$

nazýváme *kongruencí o jedné neznámé* x a rozumíme jím úkol nalézt *množinu řešení*, tj. množinu všech takových čísel $c \in \mathbb{Z}$, pro která $f(c) \equiv g(c) \pmod{m}$.
Dvě kongruence o jedné neznámé nazveme *ekvivalentní*, mají-li stejnou množinu řešení.
Uvedená kongruence je ekvivalentní s kongruencí

$$\underbrace{f(x) - g(x)}_{\in \mathbb{Z}[x]} \equiv 0 \pmod{m}.$$

Hledání řešení výčtem všech možností

Věta

Nechť $m \in \mathbb{N}$, $f(x) \in \mathbb{Z}[x]$. Pro libovolná $a, b \in \mathbb{Z}$ platí

$$a \equiv b \pmod{m} \implies f(a) \equiv f(b) \pmod{m}.$$

Důkaz.

Nechť je $f(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0$, kde $c_0, c_1, \ldots, c_n \in \mathbb{Z}$. Protože $a \equiv b \pmod{m}$, pro každé $i = 1, 2, \ldots, n$ platí $c_i a^i \equiv c_i b^i \pmod{m}$, a tedy sečtením těchto kongruencí pro $i = 1, 2, \ldots, n$ a kongruence $c_0 \equiv c_0 \pmod{m}$ dostaneme

$$c_n a^n + \cdots + c_1 a + c_0 \equiv c_n b^n + \cdots + c_1 b + c_0 \pmod{m},$$

tj. $f(a) \equiv f(b) \pmod{m}$. □

Počet řešení kongruence

Důsledek

Množina řešení libovolné kongruence modulo m je sjednocením některých zbytkových tříd modulo m.

Definice

Počtem řešení kongruence o jedné neznámé modulo m rozumíme počet zbytkových tříd modulo m obsahujících řešení této kongruence.

Příklad

1. Kongruence $2x \equiv 3 \pmod 3$ má jedno řešení (modulo 3).
2. Kongruence $10x \equiv 15 \pmod{15}$ má pět řešení (modulo 15).
3. Kongruence z příkladu (1) a (2) jsou ekvivalentní.

Věta

Nechť $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Označme $d = (a, m)$. Pak kongruence

$$ax \equiv b \pmod{m}$$

(o jedné neznámé x) má řešení právě tehdy, když $d \mid b$.
Pokud platí $d \mid b$, má tato kongruence právě d řešení (modulo m).

Důkaz.

Dokážeme nejprve, že uvedená podmínka je nutná. Je-li celé číslo c řešením této kongruence, pak nutně $m \mid a \cdot c - b$. Pokud přitom $d = (a, m)$, pak protože $d \mid m$ i $d \mid a \cdot c - b$ a
$d \mid a \cdot c - (a \cdot c - b) = b$.

Dokončení důkazu.

Obráceně dokážeme, že pokud $d \mid b$, pak má daná kongruence právě d řešení modulo m. Označme $a_1, b_1 \in \mathbb{Z}$ a $m_1 \in \mathbb{N}$ tak, že $a = d \cdot a_1$, $b = d \cdot b_1$ a $m = d \cdot m_1$. Řešená kongruence je tedy ekvivalentní s kongruencí

$$a_1 \cdot x \equiv b_1 \pmod{m_1},$$

kde $(a_1, m_1) = 1$. Tuto kongruenci můžeme vynásobit číslem $a_1^{\varphi(m_1)-1}$ a díky Eulerově větě obdržíme

$$x \equiv b_1 \cdot a_1^{\varphi(m_1)-1} \pmod{m_1}.$$

Tato kongruence má jediné řešení modulo m_1 a tedy $d = m/m_1$ řešení modulo m. □

Následující příklad ukáže, že postup uvedený v důkazu věty obvykle není tím nejefektivnějším – s výhodou lze použít jak Bezoutovu větu, tak ekvivalentní úpravy řešené kongruence.

Příklad

Řešte $39x \equiv 41 \pmod{47}$

1. Nejprve využijeme Eulerovu větu, stejně jako v důkazu předchozí věty.
2. Další možností je využít Bezoutovu větu.
3. Obvykle nejrychlejším, ale nejhůře algoritmizovatelným způsobem řešení je metoda takových úprav kongruence, které zachovávají množinu řešení.

$$\begin{aligned} 39x \equiv 41 \pmod{47} &\iff -8x \equiv -6 \pmod{47} \iff \\ 4x \equiv 3 \pmod{47} &\iff 4x \equiv -44 \pmod{47} \iff \\ x \equiv -11 \pmod{47} &\iff x \equiv 36 \pmod{47} \end{aligned}$$

Wilsonova věta

Pomocí věty o řešitelnosti lineárních kongruencí lze dokázat mj. významnou Wilsonovu větu udávající nutnou (i postačující) podmínku prvočíselnosti. Takové podmínky jsou velmi významné ve výpočetní teorii čísel, kdy je třeba efektivně poznat, je-li dané velké číslo prvočíslem. Bohužel dosud není známo, jak rychle vypočítat modulární faktoriál velkého čísla, proto není v praxi Wilsonova věta k tomuto účelu používána.

Věta (Wilsonova)

Přirozené číslo $n > 1$ je prvočíslo, právě když

$$(n-1)! \equiv -1 \pmod{n}$$

Vcelku přímočarý důkaz je v učebnici.

Soustavy lineárních kongruencí

Máme-li soustavu lineárních kongruencí o téže neznámé, můžeme podle předchozí věty rozhodnout o řešitelnosti každé z nich.
V případě, kdy aspoň jedna z kongruencí nemá řešení, nemá řešení ani celá soustava. Naopak, jestliže každá z kongruencí řešení má, upravíme ji do tvaru $x \equiv c_i \pmod{m_i}$. Dostaneme tak soustavu kongruencí

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ &\vdots \\ x &\equiv c_k \pmod{m_k} \end{aligned}$$

Zřejmě stačí vyřešit případ $k = 2$, řešení soustavy více kongruencí snadno obdržíme opakovaným řešením soustav dvou kongruencí.

Věta

Nechť c_1, c_2 jsou celá čísla, m_1, m_2 přirozená. Označme $d = (m_1, m_2)$. Soustava dvou kongruencí

$$x \equiv c_1 \pmod{m_1}$$
$$x \equiv c_2 \pmod{m_2}$$

v případě $c_1 \not\equiv c_2 \pmod{d}$ nemá řešení. Jestliže naopak $c_1 \equiv c_2 \pmod{d}$, pak existuje celé číslo c tak, že $x \in \mathbb{Z}$ vyhovuje soustavě, právě když vyhovuje kongruenci

$$x \equiv c \pmod{[m_1, m_2]}.$$

Důkaz.

Má-li soustava nějaké řešení $x \in \mathbb{Z}$, platí nutně $x \equiv c_1 \pmod{d}$, $x \equiv c_2 \pmod{d}$, a tedy i $c_1 \equiv c_2 \pmod{d}$. Odtud plyne, že v případě $c_1 \not\equiv c_2 \pmod{d}$ soustava nemůže mít řešení.

Dokončení důkazu.

Předpokládejme dále $c_1 \equiv c_2 \pmod{d}$. První kongruenci řešené soustavy vyhovují všechna celá čísla x tvaru $x = c_1 + tm_1$, kde $t \in \mathbb{Z}$ je libovolné. Toto x bude vyhovovat i druhé kongruenci soustavy, právě když bude platit $c_1 + tm_1 \equiv c_2 \pmod{m_2}$, tj. $tm_1 \equiv c_2 - c_1 \pmod{m_2}$. Podle věty o řešitelnosti lineárních kongruencí má tato kongruence (vzhledem k t) řešení, neboť $d = (m_1, m_2)$ dělí $c_2 - c_1$, a $t \in \mathbb{Z}$ splňuje tuto kongruenci právě když

$$t \equiv \frac{c_2 - c_1}{d} \cdot \left(\frac{m_1}{d}\right)^{\varphi(\frac{m_2}{d})-1} \left(\mathrm{mod}\ \frac{m_2}{d}\right),$$

tj. právě když

$$x = c_1 + tm_1 = c_1 + (c_2 - c_1) \cdot \left(\tfrac{m_1}{d}\right)^{\varphi(\frac{m_2}{d})} + r\frac{m_1 m_2}{d} = c + r \cdot [m_1, m_2],$$

kde $r \in \mathbb{Z}$ je libovolné a $c = c_1 + (c_2 - c_1) \cdot (m_1/d)^{\varphi(m_2/d)}$, neboť $m_1 m_2 = d \cdot [m_1, m_2]$. Našli jsme tedy takové $c \in \mathbb{Z}$, že libovolné $x \in \mathbb{Z}$ splňuje soustavu, právě když $x \equiv c \pmod{[m_1, m_2]}$, což jsme chtěli dokázat. □

Všimněme si, že důkaz této věty je konstruktivní, tj. udává vzorec, jak číslo c najít. Věta nám tedy dává metodu, jak pomocí jediné kongruence zachytit podmínku, že x vyhovuje této soustavě . Podstatné je, že tato nová kongruence je téhož tvaru jako obě původní. Můžeme proto tuto metodu aplikovat i na soustavu – nejprve z první a druhé kongruence vytvoříme kongruenci jedinou, které vyhovují právě ta x, která vyhovovala původním dvěma kongruencím, pak z nově vzniklé a z třetí kongruence vytvoříme další atd. Při každém kroku se nám počet kongruencí soustavy sníží o 1, po $k-1$ krocích tedy dostaneme kongruenci jedinou, která nám bude popisovat všechna řešení dané soustavy.

Čínská zbytková věta (CRT)

Ve čtvrtém století se čínský matematik Sun Ze (Sun Tsu) ptal na číslo, které při dělení třemi dává zbytek 2, při dělení pěti zbytek 3 a při dělení sedmi je zbytek opět 2.

Důsledek (Čínská zbytková věta)

Nechť $m_1, , \ldots, m_k \in \mathbb{N}$ *jsou po dvou nesoudělná,* $a_1, \ldots, a_k \in \mathbb{Z}$. *Pak platí: soustava*

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

má jediné řešení modulo $m_1 \cdot m_2 \cdots m_k$.

Důkaz.

Jde o jednoduchý důsledek předchozího tvrzení, který lze ale rovněž elegantně dokázat přímo. □

Uvědomme si, že jde o docela silné tvrzení (které ve skutečnosti platí v podstatně obecnějších algebraických strukturách), umožňující nám při předepsání libovolných zbytků podle zvolených (po dvou nesoudělných) modulů garantovat, že existuje číslo s těmito předpsanými zbytky.

Příklad

Řešte systém kongruencí

$$\begin{aligned} x &\equiv 1 \pmod{10} \\ x &\equiv 5 \pmod{18} \\ x &\equiv -4 \pmod{25}. \end{aligned}$$

Řešení

Výsledkem je $x \equiv 221 \pmod{450}$.

Čínskou zbytkovou větu můžeme použít také „v opačném směru“.

Příklad

Řešte kongruenci $23\,941x \equiv 915 \pmod{3564}$.

Řešení

Rozložme $3564 = 2^2 \cdot 3^4 \cdot 11$. Protože ani 2, ani 3, ani 11 nedělí číslo 23 941, platí $(23\,941, 3564) = 1$ a má tedy kongruence řešení. Protože $\varphi(3564) = 2 \cdot (3^3 \cdot 2) \cdot 10 = 1080$, je řešení tvaru $x \equiv 915 \cdot 23\,941^{1079} \pmod{3564}$. Úprava čísla stojícího na pravé straně by však vyžádala značné úsilí. Proto budeme kongruenci řešit poněkud jinak.

Řešení

Víme, že $x \in \mathbb{Z}$ řešením dané kongruence, právě když je řešením soustavy

$$\begin{aligned} 23941x &\equiv 915 \pmod{2^2} \\ 23941x &\equiv 915 \pmod{3^4} \\ 23941x &\equiv 915 \pmod{11}. \end{aligned}$$

Vyřešíme-li postupně každou z kongruencí soustavy, dostaneme ekvivalentní soustavu

$$\begin{aligned} x &\equiv 3 \pmod{4} \\ x &\equiv -3 \pmod{81} \\ x &\equiv -4 \pmod{11}, \end{aligned}$$

odkud snadno postupem pro řešení soustav kongruencí dostaneme $x \equiv -1137 \pmod{3564}$, což je také řešení zadané kongruence.

Modulární reprezentace čísel

Při počítání s velkými čísly je někdy výhodnější než s dekadickým či binárním zápisem čísel pracovat s tzv. *modulární reprezentací* (též *residue number system*), která umožňuje snadnou paralelizaci výpočtů s velkými čísly. Takový systém je určen k-ticí modulů (obvykle po dvou nesoudělných) a každé číslo menší než jejich součin je pak jednoznačně reprezentováno k-ticí zbytků (jejichž hodnoty nepřevyšují příslušné moduly) – viz např. `http://goo.gl/oM25m`.

Příklad

Pětice modulů $3, 5, 7, 11, 13$ nám umožní jednoznačně reprezentovat čísla menší než 15015 a efektivně provádět (v případě potřeby distribuovaně) běžné aritmetické operace. Vypočtěme např. součin čísel 1234 a 5678, v této modulární soustavě reprezentovaných pěticemi $[1, 4, 2, 2, 12]$ a $[2, 3, 1, 2, 10]$. Součin provedeme po složkách a dostaneme $[2, 2, 2, 4, 3]$, což na závěr pomocí CRT převedeme zpět na 9662, což je modulo 15015 totéž jako $1234 \cdot 5678$.