Diskrétní matematika B – 3. týden
Elementární teorie čísel – Primitivní kořeny, řešení kongruencí

Michal Bulant

Masarykova univerzita
Fakulta informatiky

jaro 2019

Obsah přednášky

Doporučené zdroje

- Jan Slovák, Martin Panák, Michal Bulant, *Matematika drsně a svižně*, MU Brno, 2013, 774 s. (též jako e-text).
- *Předmětové záložky v IS MU*
- Michal Bulant, výukový text k přednášce **Elementární teorie čísel**, `http://is.muni.cz/el/1431/podzim2015/M6520/um/main-print.pdf`
- 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/ATC2014.pdf`

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. Tento pojem je přitom jen jiným názvem pro generátor grupy $(\mathbb{Z}_m^\times, \cdot)$ (viz algebraická část později).

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

$$\begin{aligned} 2^1 &= 2 \not\equiv 1 \pmod{7} \\ 2^2 &= 4 \not\equiv 1 \pmod{7} \\ 2^3 &= 8 \equiv 1 \pmod{7} \end{aligned}$$

Řád čísla 2 modulo 7 je tedy roven 3. □

Kryptografická motivace

Důležitou aplikací primitivních kořenů je protokol pro výměnu klíčů.

Diffie-Hellman key exchange

Whitfield Diffie, Martin Hellman (1976; M. Williamson, GCHQ - 1974)
Popis pro laiky – viz `http://goo.gl/QBNXP`, motivace pro nezasvěcené – viz `http://goo.gl/Z0tMP`.
Výměna klíčů pro symetrickou kryptografii bez předchozího kontaktu (tj. náhrada jednorázových klíčů, kurýrů s kufříky, ...).

- Dohoda stran na **prvočísle** p a primitivním kořenu g modulo p (veřejné)
- Alice vybere náhodné a a pošle $g^a \pmod p$
- Bob vybere náhodné b a pošle $g^b \pmod p$
- Společným klíčem pro komunikaci je $g^{ab} \pmod p$.

Poznámka

- Problém diskrétního logaritmu (DLP)
- Nezbytná autentizace (*man in the middle attack*)
- Z protokolu DH na výměnu klíčů odvozen šifrovací algoritmus ElGamal

Vlastnosti řádu

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

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 $r \mid t - s$. $\square$

Zřejmým důsledkem předchozí věty a Eulerovy věty je následující tvrzení (jehož druhá část je přeformulováním Lagrangeovy věty z Algebry pro naši situaci):

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. $\square$

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 $\delta = rs$. □

Primitivní kořeny

Definice

Nechť $m \in \mathbb{N}$. Celé číslo $g \in \mathbb{Z}$, $(g, m) = 1$ nazveme *primitivním kořenem* modulo m, pokud je jeho řád modulo m roven $\varphi(m)$.

Lemma

Je-li g primitivní kořen modulo m, pak pro každé číslo $a \in \mathbb{Z}$, $(a, m) = 1$ existuje jediné $x_a \in \mathbb{Z}$, $0 \le x_a < \varphi(m)$ s vlastností $g^{x_a} \equiv a \pmod{m}$. Funkce $a \mapsto x_a$ se nazývá **diskrétní logaritmus**, *příp. index čísla x (vzhledem k danému m a zafixovanému primitivnímu kořeni g) a je bijekcí mezi množinami $\{a \in \mathbb{Z}; (a, m) = 1, 0 < a < m\}$ a $\{x \in \mathbb{Z}; 0 \le x < \varphi(m)\}$.*

Důkaz.

Předpokládejme, že pro $x, y \in \mathbb{Z}$, $0 \le x, y < \varphi(m)$ je $g^x \equiv g^y \pmod{m}$. Z vlastností řádu pak $x \equiv y \pmod{\varphi(m)}$, tj. $x = y$, proto je zobrazení injektivní, a tedy i surjektivní. $\square$

Existence primitivních kořenů

Věta

Buď $m \in \mathbb{N}$, $m > 1$. Primitivní kořeny modulo m existují právě tehdy, když m splňuje některou z následujících podmínek:

- *$m = 4$ nebo m je prvočíslo,*
- *m je mocnina lichého prvočísla,*
- *m je dvojnásobek mocniny lichého prvočísla.*

Dokážeme pouze část tohoto tvrzení, se kterou ve většině případů vystačíme:

Tvrzení

Nechť p je liché prvočíslo. Pak existují primitivní kořeny modulo p.

Existence primitivního kořene.

Označme $r_1, r_2, \dots, r_{p-1}$ řády čísel $1, 2, \dots, p-1$ modulo p. Buď $\delta = [r_1, r_2, \dots, r_{p-1}]$ nejmenší společný násobek těchto řádů. Ukážeme, že mezi čisly $1, 2, \dots, p-1$ existuje číslo řádu δ a že $\delta = p - 1$.
Nechť $\delta = q_1^{\alpha_1} \cdots q_k^{\alpha_k}$ je rozklad δ na prvočísla. Pro libovolné $s \in \{1, \dots k\}$ existuje $c \in \{1, \dots, p-1\}$ tak, že $q_s^{\alpha_s} \mid r_c$ (jinak by existoval menší společný násobek čísel $r_1, r_2, \dots, r_{p-1}$ než je δ), tj. ex. $b \in \mathbb{Z}$ tak, že $r_c = b \cdot q_s^{\alpha_s}$. Protože c má řád r_c, má číslo $g_s := c^b$ podle tvrzení o řádech mocnin řád roven $q_s^{\alpha_s}$.
Provedením předchozí úvahy pro libovolné $s \in \{1, \dots k\}$ dostaneme $g_1, \dots, g_k$ a můžeme položit $g := g_1 \cdots g_k$. Z vlastností řádu součinu dostáváme, že řád g je roven součinu řádů čísel $g_1, \dots, g_k$, tj. číslu $q_1^{\alpha_1} \cdots q_k^{\alpha_k} = \delta$.

Dokončení.

Nyní dokážeme, že $\delta = p - 1$. Protože řády čísel $1, 2, \dots, p - 1$ dělí δ, dostáváme pro libovolné $x \in \{1, 2, \dots, p - 1\}$ vztah $x^\delta \equiv 1 \pmod{p}$. Kongruence stupně δ modulo prvočíslo p má nejvýše δ řešení (jde vlastně o hledání kořenů polynomů nad tělesem, kterých, jak uvidíme v algebraické části, je nejvýše tolik, kolik je stupeň polynomu). Podle předchozího má však kongruence $p - 1$ řešení, proto nutně $\delta \geq p - 1$. Přitom $\delta \mid p - 1$ (jakožto řád čísla g), proto zejména $\delta \leq p - 1$, a celkem $\delta = p - 1$. $\square$

Hledání primitivních kořenů

Obecně je pro daný modul nalezení primitivního kořene velmi výpočetně náročná operace. Následující věta nám udává ekvivalentní podmínku pro to, aby zkoumané číslo bylo primitivním kořenem, jejíž ověření je o něco snažší než přímý výpočet řádu tohoto čísla.

Věta

Buď m takové, že modulo m existují primitivní kořeny. Zapišme $\varphi(m) = q_1^{\alpha_1} \cdots q_k^{\alpha_k}$. Pak pro libovolné $g \in \mathbb{Z}$, $(g, m) = 1$ platí, že g je primitivní kořen modulo m, právě když

$$g^{\frac{\varphi(m)}{q_1}} \not\equiv 1 \pmod{m}, \ldots, g^{\frac{\varphi(m)}{q_k}} \not\equiv 1 \pmod{m}.$$

Důkaz.

Pokud by platila některá z uvedených kongruencí, znamenalo by to, že řád g je menší než $\varphi(m)$.
Obráceně, pokud g není primitivní kořen, pak existuje $d \in \mathbb{N}$, $d \mid \varphi(m)$, kde $d < \varphi(m)$ a $g^d \equiv 1 \pmod{m}$. Je-li $u = \frac{\varphi(m)}{d} > 1$, nutně existuje $i \in \{1, \ldots, k\}$ tak, že $q_i \mid u$. Pak ale

$$g^{\frac{\varphi(m)}{q_i}} = g^{d \cdot \frac{u}{q_i}} \equiv 1 \pmod{m}.$$

$\square$

Příklad

Určíme primitivní kořeny modulo 41.

Řešení

Protože $\varphi(41) = 40 = 2^3 \cdot 5$, je libovolné celé číslo g, které je s 41 nesoudělné, primitivním kořenem modulo 41 právě tehdy, když $g^{20} \not\equiv 1 \pmod{41} \wedge\ g^8 \not\equiv 1 \pmod{41}$.

$$
\begin{aligned}
g = 2: \quad & 2^8 = 2^5 \cdot 2^3 \equiv -9 \cdot 8 \equiv 10 \pmod{41} \\
& 2^{20} = (2^5)^4 \equiv (-9)^4 = 81^2 \equiv (-1)^2 = 1 \pmod{41} \\
g = 3: \quad & 3^8 = (3^4)^2 \equiv (-1)^2 = 1 \pmod{41} \\
g = 4: \quad & \text{řád } 4 = 2^2 \text{ vždy dělí řád } 2 \\
g = 5: \quad & 5^8 = (5^2)^4 \equiv (-2^4)^4 = 2^{16} = (2^8)^2 \equiv 10^2 \equiv 18 \pmod{41} \\
& 5^{20} = (5^2)^{10} \equiv (-2^4)^{10} = 2^{40} = (2^{20})^2 \equiv 1 \pmod{41} \\
g = 6: \quad & 6^8 = 2^8 \cdot 3^8 \equiv 10 \cdot 1 = 10 \pmod{41} \\
& 6^{20} = 2^{20} \cdot (3^8)^2 \cdot 3^4 \equiv 1 \cdot 1 \cdot (-1) = -1 \pmod{41}
\end{aligned}
$$

Řešení (Dokončení.)

Dokázali jsme tak, že 6 je (nejmenší kladný) primitivní kořen modulo 41 (pokud by nás zajímaly i ostatní primitivní kořeny modulo 41, tak bychom je dostali umocněním 6 na všechna čísla od 1 do 40, která jsou se 40 nesoudělná – je jich právě $\varphi(40) = \varphi(2^3 \cdot 5) = 16$ a jsou jimi tyto zbytky modulo 41: $\pm 6, \pm 7, \pm 11, \pm 12, \pm 13, \pm 15, \pm 17, \pm 19$.

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

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. $\square$

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

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

Důkaz.

Dokážeme nejprve, že pro libovolné složené číslo $n > 4$ platí $n \mid (n-1)!$, tj. $(n-1)! \equiv 0 \pmod{n}$. Nechť $1 < d < n$ je netriviální dělitel n. Je-li $d \neq n/d$, pak protože $1 < d, n/d \leq n-1$, je $n = d \cdot n/d \mid (n-1)!$. Pokud $d = n/d$, tj. $n = d^2$, pak protože je $n > 4$, je i $d > 2$ a $n \mid (d \cdot 2d) \mid (n-1)!$. Pro $n = 4$ snadno dostáváme $(4-1)! \equiv 2 \not\equiv -1 \pmod{4}$.

Nechť je nyní p prvočíslo. Čísla z množiny $\{2, 3, \dots, p-2\}$ seskupíme do dvojic vzájemně inverzních čísel modulo p, resp. dvojic čísel, jejichž součin dává zbytek 1 po dělení p. Pro dané číslo a z této množiny existuje podle předchozí věty jediné řešení kongruence $a \cdot x \equiv 1 \pmod{p}$. Protože $a \neq 0, 1, p-1$, je zřejmé, že rovněž pro řešení c této kongruence platí $c \not\equiv 0, 1, -1 \pmod{p}$. Číslo a nemůže být ve dvojici samo se sebou; kdyby totiž $a \cdot a \equiv 1 \pmod{p}$, pak nutně $a \equiv \pm 1 \pmod{p}$. Součin všech čísel uvedené množiny je tedy tvořen součinem $(p-3)/2$ dvojic (jejichž součin je vždy kongruentní s 1 modulo p). Proto máme $(p-1)! \equiv 1^{(p-3)/2} \cdot (p-1) \equiv -1 \pmod{p}$.

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

$$
\begin{aligned}
x &\equiv c_1 \pmod{m_1} \\
x &\equiv c_2 \pmod{m_2}
\end{aligned}
$$

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

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

tj. právě když

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

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.

Řešení

Odpověď je (prý) ukryta v následující písni:

孫子歌 Sunzi Ge

三人同行七十里
五樹梅花廿一枝
七子團圓正月半
一百零五轉回起

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.

Čínská zbytková věta – přímý důkaz

Označme $M := m_1 m_2 \cdots m_r$ a $n_i = M/m_i$ pro každé i, $1 \leq i \leq r$. Potom pro libovolné i je m_i nesoudělné s n_i, existuje proto nějaké $b_i \in \{1, \dots, m_i - 1\}$ tak, že $b_i n_i \equiv 1 \pmod{m_i}$. Všimněme si, že $b_i n_i$ je dělitelné všemi m_j, $1 \leq j \leq r$, $i \neq j$. Proto je hledaným řešením soustavy číslo

$$x = a_1 b_1 n_1 + a_2 b_2 n_2 + \cdots + a_r b_r n_r$$

a snadno je vidět, že jeho zbytek modulo M je jednoznačně určen.

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).

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 $1234 \cdot 5678$.

Binomické kongruence

V této části se zaměříme na řešení speciálních typů polynomiálních kongruencí vyššího stupně, tzv. *binomických kongruencí*. Jde o analogii binomických rovnic, kdy polynomem $f(x)$ je dvojčlen $x^n - a$. Snadno se ukáže, že se můžeme omezit na případ, kdy je a nesoudělné s modulem kongruence – v opačném případě totiž vždy můžeme pomocí ekvivalentních úprav kongruenci na tento případ převést nebo rozhodnout, že kongruence není řešitelná.

Příklad

Řešte kongruenci

$$x^3 \equiv 3 \pmod{18}.$$

Řešení

Protože je $(3, 18) = 3$, nutně $3 \mid x$. Užijeme-li substituci $x = 3 \cdot x_1$, dostáváme kongruenci $27x_1^3 \equiv 3 \pmod{18}$, která zřejmě nemá řešení, protože $(27, 18) \nmid 3$.

Mocninné zbytky

Definice

Nechť $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. Číslo a nazveme *n-tým mocninným zbytkem modulo m*, pokud je kongruence

$$x^n \equiv a \pmod{m}$$

řešitelná. V opačném případě nazveme a *n-tým mocninným nezbytkem modulo m*.
Pro $n = 2, 3, 4$ používáme termíny kvadratický, kubický a bikvadratický zbytek, resp. nezbytek modulo m.

Ukážeme, jakým způsobem řešit binomické kongruence modulo m, pokud modulo m existují primitivní kořeny (tedy zejména, je-li modul liché prvočíslo nebo jeho mocnina).

Řešení binomických kongruencí

Věta

Buď $m \in \mathbb{N}$ takové, že modulo m existují primitivní kořeny. Dále nechť $a \in \mathbb{Z}$, $(a, m) = 1$. Pak kongruence $x^n \equiv a \pmod{m}$ je řešitelná (tj. a je n-tý mocninný zbytek modulo m), právě když $a^{\varphi(m)/d} \equiv 1 \pmod{m}$, kde $d = (n, \varphi(m))$.
Přitom, je-li tato kongruence řešitelná, má právě d řešení.

Důkaz.

Nechť g je primitivní kořen modulo m. Pak podle předchozího Lemmatu existuje pro libovolné x nesoudělné s m jediné $y \in \mathbb{Z}$; $0 \le y < \varphi(m)$ tak, že $x \equiv g^y \pmod{m}$, podobně pro dané a existuje jediné $b \in \mathbb{Z}$; $0 \le b < \varphi(m)$ tak, že $a \equiv g^b \pmod{m}$. Řešená binomická kongruence je tedy po této substituci ekvivalentní s kongruencí $(g^y)^n \equiv g^b \pmod{m}$ a s využitím dříve dokázaného tvrzení i s lineární kongruencí $n \cdot y \equiv b \pmod{\varphi(m)}$.

Dokončení důkazu.

Tato kongruence

$$n \cdot y \equiv b \pmod{\varphi(m)}$$

je řešitelná, právě když $d = (n, \varphi(m)) \mid b$ (a je-li řešitelná, pak má d řešení).

Zbývá dokázat, že $d \mid b$, právě když $a^{\varphi(m)/d} \equiv 1 \pmod{m}$.

Kongruence $1 \equiv a^{\varphi(m)/d} \equiv g^{b\varphi(m)/d}$ platí, právě když $\varphi(m) \mid \frac{b\varphi(m)}{d}$, a to platí právě když $d \mid b$.

$\square$

Důsledek

Za předpokladů předchozí věty, je-li navíc $(n, \varphi(m)) = 1$, má kongruence $x^n \equiv a \pmod{m}$ vždy řešení, a to jediné. Jinými slovy, umocňování na n-tou (kde n je nesoudělné s $\varphi(m)$) je bijekce na množině $\mathbb{Z}_m^\times$ invertibilních zbytkových tříd modulo m.