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

Michal Bulant

Masarykova univerzita
Fakulta informatiky

jaro 2013

Obsah přednášky

Doporučené zdroje

- Martin Panák, Jan Slovák, **Drsná matematika**, průběžně připravovaný *e*-text.
- *Předmětové záložky v IS MU*
- 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` a `http://wstein.org/edu/2007/spring/ent/`
- Radan Kučera, výukový text k přednášce **Algoritmy teorie čísel**, `http://www.math.muni.cz/~kucera/texty/ATC10.pdf`

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 $x_1, x_2, \dots, x_{\varphi(m)}$ libovolná redukovaná soustava zbytků modulo m. Podle předchozího lemmatu je i $a \cdot x_1, \dots, a \cdot x_{\varphi(m)}$ redukovaná soustava zbytků modulo m. Platí tedy, že pro každé i existuje j ($i, j \in \{1, 2, \dots, \varphi(m)\}$) 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. $\square$

Poznámka

Eulerova věta je rovněž důsledkem Lagrangeovy věty uplatněným na grupu $(\mathbb{Z}_m^\times, \cdot)$. S Lagrangeovou větou se seznámíme o něco později, v části věnované algebře.

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 $(\mathbb{Z}_m^\times, \cdot)$ (opět viz algebraická část).

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. $\square$

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 $\delta = rs$. $\square$

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 $x_a \in \mathbb{Z}$, $0 \leq x_a < \varphi(m)$ 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 $\{x \in \mathbb{Z}; 0 \leq x < \varphi(m)\}$.*

Důkaz.

Předpokládejme, že pro $x, y \in \mathbb{Z}$, $0 \leq x, y < \varphi(m)$ 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:

- *$m = 2$ nebo $m = 4$,*
- *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.

Důkaz.

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 $g^{20} \not\equiv 1 \pmod{41} \wedge g^8 \not\equiv 1 \pmod{41}$.

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

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: $\pm 6, \pm 7, \pm 11, \pm 12, \pm 13, \pm 15, \pm 17, \pm 19$.

RSA

Ron Rivest, Adi Shamir, Leonard Adleman (1977; C. Cocks,GCHQ – 1973)

- každý účastník A potřebuje dvojici klíčů – veřejný V_A a soukromý S_A
- generování klíčů: zvolí dvě velká prvočísla p, q, vypočte $n = pq$, $\varphi(n) = (p-1)(q-1)$ [n je veřejné, ale $\varphi(n)$ nelze snadno spočítat]
- zvolí **veřejný klíč** e a ověří, že $(e, \varphi(n)) = 1$
- např. pomocí Euklidova algoritmu spočítá **tajný klíč** d tak, aby $e \cdot d \equiv 1 \pmod{\varphi(n)}$
- zašifrování numerického *kódu* zprávy M: $C = C_e(M) \equiv M^e \pmod{n}$
- dešifrování šifry C: $OT = D_d(C) \equiv C^d \pmod{n}$

Důkaz.

Fermatova, resp. Eulerova věta. $\square$

Poznámka

- Korektní naprogramování bez postranních kanálů není triviální (viz např. PKCS#1, RFC 3447).
- Analogicky podepisování (hashů) zpráv (viz např. DSA)
- Viz RSA factoring challenge (např. rozklad 212 ciferného čísla RSA-704 vynese 30 000 USD).

Příklad

- **Generování klíče.** Alice vybere prvočísla $p = 2357, q = 2551$ a vypočte $n = p \cdot q = 6012707$ a $\varphi(n) = (p-1)(q-1) = 6007800$. Alice zvolí $e = 3674911$ a pomocí Euklidova algoritmu vypočte $d = 422191$ ($e \cdot d \equiv 1 \pmod{\varphi(n)}$). Soukromý klíč Alice je d, veřejný pak (n, e).
- Chce-li Bob poslat Alici zprávu $m = 5234673$, pomocí modulárního umocňování vypočte

  $$c \equiv m^e \equiv 5234673^{3674911} \equiv 3650502 \pmod{n},$$

  a tu odešle Alici.
- Alice zprávu dešifruje díky výpočtu

  $$c^d \equiv 3650502^{422191} \equiv 5234673.$$

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

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. □

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 $\{2, 3, \ldots, p-2\}$ 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
$(p-1)! \equiv 1^{(p-3)/2} \cdot (p-1) \equiv -1 \pmod{p}$.