Diskrétní matematika B – 4. týden
Elementární teorie čísel – Řešení kongruencí

Michal Bulant

Masarykova univerzita
Fakulta informatiky

jaro 2014

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/podzim2012/M6520/um/main-print.pdf`
- 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/`

Doporučené zdroje – algoritmy

- Radan Kučera, výukový text k přednášce **Algoritmy teorie čísel**, `http://www.math.muni.cz/~kucera/texty/ATC10.pdf`
- Donald E. Knuth, **The Art Of Computer Programming**.
- Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein. **Introduction to Algorithms**, MIT Press, 2009.
- Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, **Handbook of Applied Cryptography**, CRC Press, 2001. (též jako *e*-text).

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 $y \in \mathbb{Z}$; $0 \leq y < \varphi(m)$ tak, že $x \equiv g^y \pmod{m}$, podobně pro dané a existuje jediné $b \in \mathbb{Z}$; $0 \leq b < \varphi(m)$ 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 $d \mid b$.

□

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.

Obecnější typy kongruencí

Při řešení obecné polynomiální kongruence $f(x) \equiv 0 \pmod{m}$ stačí zjistit, pro která celá čísla a, $0 \leq a < m$, platí $f(a) \equiv 0 \pmod{m}$. Nevýhodou této metody je její pracnost, která se zvyšuje se zvětšující se hodnotou m. Je-li m složené, $m = p_1^{n_1} \dots p_k^{n_k}$, kde $p_1, \dots, p_k$ jsou různá prvočísla, a je-li navíc $k > 1$, můžeme nahradit tuto kongruenci soustavou kongruencí

$$f(x) \equiv 0 \pmod{p_1^{n_1}}$$
$$\vdots$$
$$f(x) \equiv 0 \pmod{p_k^{n_k}},$$

která má stejnou množinu řešení, a řešit každou kongruenci této soustavy zvlášť. Tím získáme obecně několik soustav lineárních kongruencí, které už umíme řešit. Výhoda této metody spočívá v tom, že moduly kongruencí soustavy jsou menší než modul původní kongruence (a navíc je možné, jak brzy ukážeme, tyto kongruence ještě zjednodušit).

Příklad

Řešte kongruenci $x^5 + 1 \equiv 0 \pmod{11}$.

Příklad

Řešte kongruenci $x^3 - 3x + 5 \equiv 0 \pmod{105}$.

Řešení

Kdybychom postupovali obdobně jako dříve pro $m = 105$, museli bychom spočítat pro $f(x) = x^3 - 3x + 5$ sto pět hodnot $f(0)$, $f(1)$, $\ldots$, $f(104)$. Proto raději rozložíme $105 = 3 \cdot 5 \cdot 7$ a budeme řešit kongruence $f(x) \equiv 0$ postupně pro moduly $3, 5, 7$ a z řešení soustavy těchto kongruencí zrekonstruujeme řešení kongruence původní.

Kongruence modulo mocnina prvočísla

Postup pro řešení kongruencí modulo mocnina prvočísla udává důkaz následující věty.

Věta (Henselovo lemma)

Nechť p je prvočíslo, $f(x) \in \mathbb{Z}[x]$, $a \in \mathbb{Z}$ je takové, že $p \mid f(a), p \nmid f'(a)$. Pak platí: pro každé $n \in \mathbb{N}$ má soustava

$$x \equiv a \pmod{p}$$
$$f(x) \equiv 0 \pmod{p^n}$$

právě jedno řešení modulo p^n.

Náznak důkazu

Důkaz.

Indukcí vzhledem k n: pro $n = 1$ platí díky předpokladu věty. Nechť dále $n > 1$ a věta platí pro $n - 1$. Buď x řešení soustavy pro n, tedy i pro $n - 1$. Označme jedno z řešení soustavy pro $n - 1$ jako c_{n-1} a hledejme řešení pro n ve tvaru $x = c_{n-1} + k \cdot p^{n-1}$. Je třeba zjistit, pro která k platí $f\left(c_{n-1} + k \cdot p^{n-1}\right) \equiv 0 \pmod{p^n}$. Víme, že $p^{n-1} \mid f\left(c_{n-1} + k \cdot p^{n-1}\right)$ a užijme binomickou větu pro $f(x) = a_m x^m + \cdots + a_1 x + a_0$. Odtud

$$f\left(c_{n-1} + k \cdot p^{n-1}\right) \equiv 0 \pmod{p^n} \iff$$
$$\iff 0 \equiv \frac{f(c_{n-1})}{p^{n-1}} + k \cdot f'(c_{n-1}) \pmod{p}.$$

Přitom $f'(c_{n-1}) \equiv f'(a) \not\equiv 0 \pmod{p}$ a odtud vidíme, že existuje právě jedno řešení k této kongruence, a je tedy číslo $c_{n-1} + k \cdot p^{n-1}$ jediným řešením dané soustavy modulo p^n. □

Příklad

Řešte kongruenci $x^4 + 7x + 4 \equiv 0 \pmod{27}$.

Řešení

Řešme nejprve tuto kongruenci modulo 3 (např. dosazením) – snadno zjistíme, že řešení je $x \equiv 1 \pmod{3}$. Zapišme řešení ve tvaru $x = 1 + 3t$, kde $t \in \mathbb{Z}$ a řešme kongruenci modulo 9.

$$\begin{aligned} x^4 + 7x + 4 &\equiv 0 \pmod{9} \\ (1+3t)^4 + 7(1+3t) + 4 &\equiv 0 \pmod{9} \\ 1 + 4 \cdot 3t + 7 + 7 \cdot 3t + 4 &\equiv 0 \pmod{9} \\ 33t &\equiv -12 \pmod{9} \\ 11t &\equiv -4 \pmod{3} \\ t &\equiv 1 \pmod{3} \end{aligned}$$

Zapsáním $t = 1 + 3s$, kde $s \in \mathbb{Z}$ dostaneme $x = 4 + 9s$.

Řešení

Po dosazení

$$\begin{aligned}
(4+9s)^4 + 7(4+9s) + 4 &\equiv 0 \pmod{27} \\
4^4 + 4 \cdot 4^3 \cdot 9s + 28 + 63s + 4 &\equiv 0 \pmod{27} \\
256 \cdot 9s + 63s &\equiv -288 \pmod{27} \\
256s + 7s &\equiv -32 \pmod{3} \\
2s &\equiv 1 \pmod{3} \\
s &\equiv 2 \pmod{3}
\end{aligned}$$

Celkem dostáváme řešení $x = 4 + 9s = 4 + 9(2 + 3r) = 22 + 27r$, kde $r \in \mathbb{Z}$, neboli $x \equiv 22 \pmod{27}$. □

Kvadratické kongruence

Naším úkolem bude najít jednodušší podmínku, jak zjistit, jestli je řešitelná (a případně, kolik má řešení) kvadratická kongruence

$$ax^2 + bx + c \equiv 0 \pmod{m}.$$

Z teorie, uvedené dříve, je snadné vidět, že k rozhodnutí, je-li tato kongruence řešitelná, stačí určit, je-li řešitelná (binomická) kongruence

$$x^2 \equiv a \pmod{p},$$

kde p je liché prvočíslo a a číslo s ním nesoudělné.
Pro určení řešitelnosti kongruence můžeme samozřejmě využít Větu o řešitelnosti binomické kongruence, její využití ale často naráží na výpočetní složitost, proto se (nejen) v kvadratickém případě snažíme najít kritérium jednodušší na výpočet.

Příklad

Určete počet řešení kongruence $x^2 \equiv 219 \pmod{383}$.

Řešení

Protože 383 je prvočíslo a $(2, \varphi(383)) = 2$, z věty plyne, že daná kongruence je řešitelná (a má 2 řešení), právě tehdy, když $219^{\frac{383}{2}} = 219^{191} \equiv 1 \pmod{383}$. Ověření platnosti není bez použití výpočetní techniky snadné (i když je to pořád ještě „na papíře“ vyčíslitelné). Ukážeme, jak tuto podmínku ověřit s pomocí Legendreova symbolu daleko snadněji.

Legendreův symbol

Definice

Nechť je p liché prvočíslo. *Legendreův symbol* definujeme předpisem

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & p \nmid a,\ a \text{ je kvadratický zbytek modulo } p, \\ 0 & p \mid a, \\ -1 & p \nmid a,\ a \text{ je kvadratický nezbytek modulo } p. \end{cases}$$

Příklad

Protože je kongruence $x^2 \equiv 1 \pmod{p}$ řešitelná pro libovolné liché prvočíslo p, je $(1/p) = 1$.
$(-1/5) = 1$, protože kongruence $x^2 \equiv -1 \pmod{5}$ je ekvivalentní s kongruencí $x^2 \equiv 4 \pmod{5}$, jejímiž řešeními jsou $x \equiv \pm 2 \pmod{5}$.

Lemma

Nechť p je liché prvočíslo, $a, b \in \mathbb{Z}$ libovolná. Pak platí:

1. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
3. $a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Důkaz.

ad 1. Pro $p \mid a$ je tvrzení zřejmé; pokud je a kvadratický zbytek modulo p, pak tvrzení plyne z Věty o řešitelnosti binomických kongruencí. Z téže věty plyne, že v případě kvadratického nezbytku je $a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$. Pak ale, protože $p \mid a^{p-1} - 1 = (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1)$ nutně $p \mid a^{\frac{p-1}{2}} + 1$, tj. $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

ad 2. Plyne z 1.

ad 3. Zřejmé z definice.

□

Důsledek

1. *V libovolné redukované soustavě zbytků modulo p je stejný počet kvadratických zbytků a nezbytků.*
2. *Součin dvou kvadratických zbytků je zbytek, součin dvou nezbytků je zbytek, součin zbytku a nezbytku je nezbytek.*
3. $(-1/p) = (-1)^{\frac{p-1}{2}}$, *tj. kongruence* $x^2 \equiv -1 \pmod{p}$ *je řešitelná právě tehdy, když* $p \equiv 1 \pmod{4}$.

Nekonečnost počtu prvočísel tvaru $4k + 1$

Již s využitím těchto základních tvrzení o hodnotách Legendreova symbolu jsme schopni dokázat větu o nekonečnosti počtu prvočísel tvaru $4k + 1$.

Tvrzení

Prvočísel tvaru $4k + 1$ je nekonečně mnoho.

Důkaz.

Sporem. Předpokládejme, že $p_1, p_2, \ldots, p_\ell$ jsou všechna prvočísla tvaru $4k + 1$ a uvažme číslo $N = (2p_1 \cdots p_\ell)^2 + 1$. Toto číslo je opět tvaru $4k + 1$. Pokud je N prvočíslo, jsme hotovi (protože je jistě větší než kterékoli z $p_1, p_2, \ldots, p_\ell$), pokud je složené, musí existovat prvočíslo p, dělící N. Zřejmě přitom žádné z prvočísel $2, p_1, p_2, \ldots, p_\ell$ není dělitelem N, proto stačí dokázat, že p je rovněž tvaru $4k + 1$. Protože ale $(2p_1 \cdots p_\ell)^2 \equiv -1 \pmod{p}$, dostáváme, že $(-1/p) = 1$, a to platí právě tehdy, je-li $p \equiv 1 \pmod{4}$. □

Zákon kvadratické reciprocity

Nejdůležitější tvrzení, umožňující efektivně určit hodnotu Legendreova symbolu (a tak rozhodnout o řešitelnosti kvadratické kongruence), je tzv. Zákon kvadratické reciprocity.

Věta

Nechť p, q jsou lichá prvočísla. Pak

1. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
2. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$
3. $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \cdot (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

Důkaz.

Viz literatura, důkazů je celá řada (v roce 2010 uváděl F. Lemmermeyer 233 důkazů), obvykle ovšem využívajících (zejména u těch stručnějších z nich) hlubších znalostí z algebraické teorie čísel. □

Věta se v tomto tvaru uvádí zejména proto, že pomocí těchto tří vztahů a základních pravidel pro úpravy Legendreova symbolu jsme schopni vypočítat hodnotu (a/p) pro libovolné celé číslo a.

Důsledek

1. -1 *je kvadratický zbytek pro prvočísla* p *splňující* $p \equiv 1 \pmod 4$ *a nezbytek pro prvočísla splňující* $p \equiv 3 \pmod 4$.
2. 2 *je kvadratický zbytek pro prvočísla* p *splňující* $p \equiv \pm 1 \pmod 8$ *a nezbytek pro prvočísla splňující* $p \equiv \pm 3 \pmod 8$.
3. *Je-li* $p \equiv 1 \pmod 4$ *nebo* $q \equiv 1 \pmod 4$, *je* $(p/q) = (q/p)$, *pro ostatní lichá* p, q *je* $(p/q) = -(q/p)$.

Příklad

Určete $\left(\frac{79}{101}\right)$.

Řešení

$$\left(\frac{79}{101}\right) = \left(\frac{101}{79}\right) \qquad \textit{101 dává po dělení 4 zbytek 1}$$

$$= \left(\frac{22}{79}\right)$$

$$= \left(\frac{2}{79}\right) \cdot \left(\frac{11}{79}\right)$$

$$= \left(\frac{11}{79}\right) \qquad \textit{79 dává pod dělení 8 zbytek -1}$$

$$= (-1)\left(\frac{79}{11}\right) \qquad \textit{11 i 79 dávají pod dělení 4 zbytek 3}$$

$$= (-1)\left(\frac{2}{11}\right) = 1 \qquad \textit{11 dává pod dělení 8 zbytek 3}$$

Jacobiho symbol

Vyčíslení Legendreova symbolu (jak jsme viděli i v předchozím příkladu) umožňuje používat zákon kvadratické reciprocity jen na prvočísla a nutí nás tak provádět faktorizaci čísel na prvočísla, což je výpočetně velmi náročná operace. Toto lze obejít rozšířením definice Legendreova symbolu na tzv. *Jacobiho symbol* s podobnými vlastnostmi.

Definice

Nechť $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $2 \nmid b$. Nechť $b = p_1 p_2 \cdots p_k$ je rozklad b na (lichá) prvočísla (výjimečně neseskupujeme stejná prvočísla do mocniny, ale vypisujeme každé zvlášť, např. $135 = 3 \cdot 3 \cdot 3 \cdot 5$). Symbol

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right) \cdot \left(\frac{a}{p_2}\right) \cdots \left(\frac{a}{p_k}\right)$$

se nazývá *Jacobiho symbol*.

Dále ukážeme, že Jacobiho symbol má podobné vlastnosti jako Legendreův symbol (s jednou podstatnou odchylkou). Neplatí totiž obecně, že z $(a/b) = 1$ plyne řešitelnost kongruence $x^2 \equiv a \pmod{b}$.

Příklad

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right) = (-1) \cdot (-1) = 1$$

a přitom kongruence

$$x^2 \equiv 2 \pmod{15}$$

není řešitelná (není totiž řešitelná kongruence $x^2 \equiv 2 \pmod{3}$ a není ani řešitelná kongruence $x^2 \equiv 2 \pmod{5}$).

Věta (Kvadratická reciprocita pro Jacobiho symbol)

Nechť $a, b \in \mathbb{N}$ jsou lichá. Pak

1. $\left(\frac{-1}{a}\right) = (-1)^{\frac{a-1}{2}}$
2. $\left(\frac{2}{a}\right) = (-1)^{\frac{a^2-1}{8}}$
3. $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}$

Příklad

Rozhodněte o řešitelnosti kongruence $x^2 \equiv 219 \pmod{383}$.

Řešení

383 je prvočíslo, proto bude kongruence řešitelná, bude-li Legendreův symbol $(219/383) = 1$.

$$\left(\frac{219}{383}\right) = -\left(\frac{383}{219}\right) \quad \textit{(Jacobi) 383 i 219 dávají po dělení 4 zbytek 3}$$

$$= -\left(\frac{164}{219}\right) = -\left(\frac{41}{219}\right) \qquad 164 = 2^2 \cdot 41$$

$$= -\left(\frac{219}{41}\right) \quad \textit{(Jacobi) 41 dává po dělení 4 zbytek 1}$$

$$= -\left(\frac{14}{41}\right) = -\left(\frac{2}{41}\right)\left(\frac{7}{41}\right)$$

$$= -\left(\frac{7}{41}\right) \quad \textit{41 dává po dělení 8 zbytek 1}$$

$$= -\left(\frac{41}{7}\right) \quad \textit{41 dává po dělení 4 zbytek 1}$$

$$= -\left(\frac{-1}{7}\right) = 1 \quad \textit{7 dává po dělení 4 zbytek 3.}$$

Rabinův kryptosystém

Prvním veřejným kryptosystémem, k jehož prolomení je prokazatelně potřeba faktorizovat modul, je **Rabinův kryptosystém**, který si uvedeme ve zjednodušené verzi:

- každý účastník A potřebuje dvojici klíčů – veřejný V_A a soukromý S_A
- generování klíčů: A zvolí dvě podobně velká prvočísla $p, q \equiv 3 \pmod 4$, vypočte $n = pq$.
- $V_A = n$, $S_A = (p, q)$
- zašifrování numerického *kódu* zprávy M: $C = C_e(M) \equiv M^2 \pmod n$
- dešifrování šifry C: vypočtou se (čtyři) odmocniny z C modulo n a snadno se otestuje, která z nich byla původní zprávou.

Výpočet druhé odmocniny z C modulo $n = pq$, kde $p \equiv q \equiv 3 \pmod 4$

- vypočti $r = C^{(p+1)/4} \pmod p$ a $s = C^{(q+1)/4} \pmod q$
- vypočti a, b tak, že $ap + bq = 1$
- polož[a] $x = (aps + bqr) \pmod n$, $y = (aps - bqr) \pmod n$
- druhými odmocninami z C modulo n jsou $\pm x$, $\pm y$.

[a] Uvědomte si, že jde vlastně o aplikaci Čínské zbytkové věty!

Příklad

V Rabinově kryptosystému Alice zvolila za svůj soukromý klíč $p = 23, q = 31$, veřejným klíčem je pak $n = pq = 713$. Zašifrujte zprávu $m = 327$ pro Alici a ukažte, jak bude Alice tuto zprávu dešifrovat.

Řešení

$c = 692$, kandidáti původní zprávy jsou $\pm 4 \cdot 23 \cdot 14 \pm 3 \cdot 31 \cdot 18 \pmod{713}$.