Diskrétní matematika – 4. týden
Elementární teorie čísel – Primitivní kořeny

Lukáš Vokřínek

Masarykova univerzita
Fakulta informatiky

podzim 2020

Obsah přednášky

Doporučené zdroje

- Jan Slovák, Martin Panák, Michal Bulant
Matematika drsně a svižně, *e*-text na
`www.math.muni.cz/Matematika_drsne_svizne`.

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

Plán přednášky

Minule

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.

Minule

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 $\delta = rs$. $a^{rs} b^{rs} = 1$, $a^r = 1$, $b^s = 1$ $\square$

Minule

Důsledek

Nechť $m \in \mathbb{N}$ a r je nejmenší společný násobek všech řádů modulo m. Pak existuje číslo řádu r modulo m.

Minule

Důsledek

Nechť $m \in \mathbb{N}$ a r je nejmenší společný násobek všech řádů modulo m. Pak existuje číslo řádu r modulo m.

Důkaz.

Stačí pro a řádu s, b řádu t najít prvek řádu $[s, t]$. Nechť $d = (s, t)$, pak tímto prvkem je $a^d \cdot b$. □

Minule

Důsledek

Nechť $m \in \mathbb{N}$ a r je nejmenší společný násobek všech řádů modulo m. Pak existuje číslo řádu r modulo m.

Důkaz.

Stačí pro a řádu s, b řádu t najít prvek řádu $[s, t]$. Nechť $d = (s, t)$, pak tímto prvkem je $a^d \cdot b$. □

Pak všechna $(a, m) = 1$ splňují $a^r \equiv 1 \pmod{m}$, tj. jsou to řešení kongruence

$$x^r \equiv 1 \pmod{m}$$

Zejména nás budou zajímat tzv. primitivní kořeny, tj. čísla mající řád přesně $\varphi(m)$ – to je přesně počet řešení této rovnice.

Primitivní kořeny modulo součin

Příklad

Nechť $m = 35$ a nechť $(a, m) = 1$. Pak podle Eulerovy věty

$$(\cdot)^3 \quad a^4 \equiv 1 \pmod 5, \quad (\cdot)^2 \quad a^6 \equiv 1 \pmod 7$$

$$a^{12} \equiv 1 \pmod 5, \quad a^{12} \equiv 1 \pmod 7 \quad \Rightarrow \quad a^{12} \equiv 1 \pmod{35}.$$

Je tedy každé číslo řádu 12 (případně menšího, ale to vyloučíme časem).

Primitivní kořeny modulo součin

Příklad

Nechť $m = 35$ a nechť $(a, m) = 1$. Pak podle Eulerovy věty

$$a^4 \equiv 1 \pmod 5, \quad a^6 \equiv 1 \pmod 7$$
$$a^{12} \equiv 1 \pmod 5, \; a^{12} \equiv 1 \pmod 7 \quad \Rightarrow \quad a^{12} \equiv 1 \pmod{35}.$$

Je tedy každé číslo řádu 12 (případně menšího, ale to vyloučíme časem).
Tedy kongruence $x^{12} \equiv 1 \pmod{35}$ stupně 12 má $\varphi(35) = 4 \cdot 6 = 24$ řešení.

$\varphi(5 \cdot 7) = \underbrace{4}_{\varphi(5)} \cdot \underbrace{6}_{\varphi(7)} = 24$

Primitivní kořeny modulo součin

Příklad

Nechť $m = 35$ a nechť $(a, m) = 1$. Pak podle Eulerovy věty

$$a^4 \equiv 1 \pmod 5, \quad a^6 \equiv 1 \pmod 7$$
$$a^{12} \equiv 1 \pmod 5, \quad a^{12} \equiv 1 \pmod 7 \quad \Rightarrow \quad a^{12} \equiv 1 \pmod{35}.$$

Je tedy každé číslo řádu 12 (případně menšího, ale to vyloučíme časem). $\Rightarrow$ prim. kořen ~~max~~

prvek řádu $\varphi(m) = 24$

Tedy kongruence $x^{12} \equiv 1 \pmod{35}$ stupně 12 má $\varphi(35) = 4 \cdot 6 = 24$ řešení.

Věta

Pokud je m dělitelné aspoň dvěma lichými prvočísly, primitivní kořen modulo m neexistuje.

$m = p \cdot q \Rightarrow a^{\frac{(p-1)(q-1)}{2}} \equiv 1 \ (m)$

Polynomiální kongruence modulo prvočíslo

polynom ... $f(a) \equiv 0 \pmod p$ „kořen mod p“

Uvažme $f(x) \equiv 0 \pmod p$ a vydělme $f(x)$ se zbytkem kořenovým činitelem $(x - a)$:

st. 0 -- číslo $f(a)$

$$f(x) = (x - a) \cdot g(x) + r \qquad \Rightarrow \qquad r = f(a)$$

Polynomiální kongruence modulo prvočíslo

Uvažme $f(x) \equiv 0 \pmod p$ a vydělme $f(x)$ se zbytkem kořenovým činitelem $(x-a)$:

stupně o 1 menšího než f

$$f(x) = (x-a)\cdot g(x) + r \qquad \Rightarrow \qquad r = f(a) \equiv 0$$

Pokud je a kořenem kongruence, dostaneme

$f(b) \equiv 0 \iff b-a \equiv 0$ nebo $g(b) \equiv 0$

$b \equiv a$

$$f(x) \equiv (x-a)\cdot g(x) \pmod p.$$

Protože je p prvočíslo, jsou kořeny $f(x)$ právě a a kořeny $g(x)$, který je stupně o jedna menšího. Protože konstantní polynomy nemají kořeny, má $f(x)$ maximálně tolik kořenů, kolik je jeho stupeň (bacha na $f(x) \equiv 0$).

$px^2 + p \equiv 0$ kořenem vše (!): p kořen

Polynomiální kongruence modulo prvočíslo

Uvažme $f(x) \equiv 0 \pmod{p}$ a vydělme $f(x)$ se zbytkem kořenovým činitelem $(x - a)$:

$$f(x) = (x - a) \cdot g(x) + r \qquad \Rightarrow \qquad r = f(a)$$

Pokud je a kořenem kongruence, dostaneme

$$f(x) \equiv (x - a) \cdot g(x) \pmod{p}.$$

Protože je p prvočíslo, jsou kořeny $f(x)$ právě a a kořeny $g(x)$, který je stupně o jedna menšího. Protože konstantní polynomy nemají kořeny, má $f(x)$ maximálně tolik kořenů, kolik je jeho stupeň (bacha na $f(x) \equiv 0$).

$p=2$ ... jeden kořen

Důsledek

$x^2 \equiv 1 \pmod{p}$ *má kořeny právě* ± 1.

$x^2-1 \equiv (x-1)(x+1)$ (p)

Věta

Nechť $p \in \mathbb{N}$ je prvočíslo. Pak existuje primitivní kořen modulo p.

Věta

Nechť $p \in \mathbb{N}$ je prvočíslo. Pak existuje primitivní kořen modulo p.

= nejm. spol. násobek všech řádů

Důkaz.

Nechť r je maximální řád, podle Eulerovy věty $r \mid p - 1$. Pak všech $p - 1$ nenulových zbytkových tříd jsou kořeny

$x^{p-1} \equiv 1 \Rightarrow r \mid p-1$

nesoudělných

$$x^r \equiv 1 \pmod{p}$$

a podle předchozího $p - 1 \leq r$. $r = p-1$ $\square$

ex prvek řádu $p-1 = \varphi(p)$ = prim. kořen

Věta

Nechť $p \in \mathbb{N}$ je prvočíslo. Pak existuje primitivní kořen modulo p^k.

Věta

Nechť $p \in \mathbb{N}$ je prvočíslo. Pak existuje primitivní kořen modulo p^k.

Důkaz.

Platí $\varphi(p^k) = \underline{p^{k-1}} \cdot (\underline{p-1})$ a tito činitelé jsou nesoudělní.

Věta

Nechť $p \in \mathbb{N}$ je prvočíslo. Pak existuje primitivní kořen modulo p^k.

Důkaz.

Platí $\varphi(p^k) = p^{k-1} \cdot (p-1)$ a tito činitelé jsou nesoudělní. Nechť $g \pmod{p}$ je primitivní kořen, tj. prvek řádu $p-1$. Pak řád $g \pmod{p^k}$ bude násobkem $p-1$.

$g^r \equiv 1 \quad (p^k)$

$\Downarrow$

$g^r \equiv 1 \quad (p)$

$p-1 \mid r$

Věta

Nechť $p \in \mathbb{N}$ je prvočíslo. Pak existuje primitivní kořen modulo p^k.

Důkaz.

Platí $\varphi(p^k) = p^{k-1} \cdot (p-1)$ a tito činitelé jsou nesoudělní. Nechť $g \pmod{p}$ je primitivní kořen, tj. prvek řádu $p-1$. Pak řád $g \pmod{p^k}$ bude násobkem $p-1$. Stačí najít prvek řádu p^{k-1}. Ukážeme, že je jím $1+p$; indukcí vzhledem ke $k = 1, 2, \ldots$; konkrétně ukážeme:

$$(1+p)^{p^{k-2}} \equiv 1 + p^{k-1} \not\equiv 1 \pmod{p^k}$$

Věta

Nechť $p \in \mathbb{N}$ je prvočíslo. Pak existuje primitivní kořen modulo p^k.

Důkaz.

Platí $\varphi(p^k) = p^{k-1} \cdot (p-1)$ a tito činitelé jsou nesoudělní. Nechť $g \pmod{p}$ je primitivní kořen, tj. prvek řádu $p-1$. Pak řád $g \pmod{p^k}$ bude násobkem $p-1$. Stačí najít prvek řádu p^{k-1}. Ukážeme, že je jím $1+p$; indukcí vzhledem ke $k = 1, 2, \ldots$; konkrétně ukážeme:

$k+1 \to k$

$$(1+p)^{p^{k-2}} \equiv 1 + p^{k-1} \not\equiv 1 \pmod{p^k}$$

(instance pro $k+1$ dá $(1+p)^{p^{k-1}} \equiv 1 + p^k \pmod{p^{k+1}}$).

Věta

Nechť $p \in \mathbb{N}$ je prvočíslo. Pak existuje primitivní kořen modulo p^k.

Důkaz.

Platí $\varphi(p^k) = p^{k-1} \cdot (p-1)$ a tito činitelé jsou nesoudělní. Nechť $g \pmod{p}$ je primitivní kořen, tj. prvek řádu $p-1$. Pak řád $g \pmod{p^k}$ bude násobkem $p-1$. Stačí najít prvek řádu p^{k-1}. Ukážeme, že je jím $1+p$; indukcí vzhledem ke $k = 1, 2, \ldots$; konkrétně ukážeme:

$$(1+p)^{p^{k-2}} \equiv 1 + p^{k-1} \not\equiv 1 \pmod{p^k}$$

(instance pro $k+1$ dá $(1+p)^{p^{k-1}} \equiv 1 + p^k \pmod{p^k}$).

Věta

Nechť $p \in \mathbb{N}$ je prvočíslo. Pak existuje primitivní kořen modulo p^k.

Důkaz.

Platí $\varphi(p^k) = p^{k-1} \cdot (p-1)$ a tito činitelé jsou nesoudělní. Nechť $g \pmod{p}$ je primitivní kořen, tj. prvek řádu $p-1$. Pak řád $g \pmod{p^k}$ bude násobkem $p-1$. Stačí najít prvek řádu p^{k-1}. Ukážeme, že je jím $1+p$; indukcí vzhledem ke $k = 1, 2, \ldots$; konkrétně ukážeme:

$$\underline{(1+p)^{p^{k-2}} \equiv 1 + p^{k-1}} \not\equiv 1 \pmod{p^k}$$

(instance pro $k+1$ dá $(1+p)^{p^{k-1}} \equiv 1 + p^k \equiv 1 \pmod{p^k}$). $\square$

Věta

Nechť $p \in \mathbb{N}$ je prvočíslo. Pak existuje primitivní kořen modulo p^k.

Důkaz.

Platí $\varphi(p^k) = p^{k-1} \cdot (p-1)$ a tito činitelé jsou nesoudělní. Nechť $g \pmod{p}$ je primitivní kořen, tj. prvek řádu $p-1$. Pak řád $g \pmod{p^k}$ bude násobkem $p-1$. Stačí najít prvek řádu p^{k-1}. Ukážeme, že je jím $1+p$; indukcí vzhledem ke $k = 1, 2, \ldots$; konkrétně ukážeme:

$$(1+p)^{p^{k-2}} \equiv 1 + p^{k-1} \not\equiv 1 \pmod{p^k}$$

(instance pro $k+1$ dá $(1+p)^{p^{k-1}} \equiv 1 + p^k \equiv 1 \pmod{p^k}$). $\square$

Lemma

$$a \equiv b \pmod{p^k} \qquad \Rightarrow \qquad a^p \equiv b^p \pmod{p^{k+1}}.$$

Lemma. $a \equiv b \quad (p^k) \implies \underline{\underline{a^p \equiv b^p}} \quad (p^{k+1})$

$\Rightarrow a \equiv b \quad (p)$

Dk. $a^p - b^p = \underbrace{(a-b)}_{\text{děl. } p^k} \underbrace{(a^{p-1} + a^{p-2}b + \dots + ab^{p-2} + b^{p-1})}_{\text{? děl } p.}$

děl. p^{k+1}

$a^{p-1} + a^{p-2}b + \dots + ab^{p-2} + b^{p-1}$

$\equiv a^{p-1} + a^{p-2}a + \dots + aa^{p-2} + a^{p-1} \quad (p)$

$\equiv p \cdot a^{p-1} \equiv 0 \quad (p)$

$(1+p)^{p^{k-2}} \equiv 1 + p^{k-1} \pmod{p^k}$

$k=2$: $(1+p)^1 \overset{?}{\equiv} 1+p^1 \pmod{p^2}$

$(\;)^p$ $\Rightarrow$ $\left((1+p)^{p^{k-2}}\right)^p \equiv (1+p^{k-1})^p \pmod{p^{k+1}}$

$1+p^k$

$(1+p)^{p^{k-1}} \equiv \underline{1 + \binom{p}{1} p^{k-1}} + \binom{p}{2}(p^{k-1})^2 + \dots$

Hledání primitivního kořene

Sofistikovaná metoda se zatím nezná. Zkoušením po nějaké době uspějeme: Kolik je primitivních kořenů modulo prvočíslo?

Hledání primitivního kořene

Sofistikovaná metoda se zatím nezná. Zkoušením po nějaké době uspějeme: Kolik je primitivních kořenů modulo prvočíslo? Jsou to právě $g^a \pmod p$, kde $(a, \varphi(p)) = 1$, tedy jich je $\varphi(\varphi(p))$. Přitom platí

g... prim. kořen

$$p/\varphi(\varphi(p)) \in O(\log\log p),$$

$(g^a)^r \equiv 1$

$\Leftrightarrow \underline{a \cdot r \equiv 0 \ (\varphi(p}$

$r \equiv 0 \ (\varphi(p$

takže pravděpodobnost, že náhodné číslo bude primitivním kořenem je zhruba

$$1/\log\log p$$

$$\frac{\varphi(\varphi(p))}{p} \approx \frac{1}{\log\log p}$$

Hledání primitivního kořene

Sofistikovaná metoda se zatím nezná. Zkoušením po nějaké době uspějeme: Kolik je primitivních kořenů modulo prvočíslo? Jsou to právě $g^a \pmod p$, kde $(a, \varphi p) = 1$, tedy jich je $\varphi(\varphi(p))$. Přitom platí

$$p/\varphi(\varphi(p)) \in O(\log\log p),$$

takže pravděpodobnost, že náhodné číslo bude primitivním kořenem je zhruba

$$1/\log\log p$$

a počet pokusů potřebných k nalezení primitivního kořene s předem danou pravděpodobností je úměrný $\log\log p$, tedy logaritmický vzhledem k délce vstupu

INPUT: prvočíslo p
OUTPUT: prim. kořen mod p

Hledání primitivního kořene

Sofistikovaná metoda se zatím nezná. Zkoušením po nějaké době uspějeme: Kolik je primitivních kořenů modulo prvočíslo? Jsou to právě $g^a \pmod p$, kde $(a, \varphi p) = 1$, tedy jich je $\varphi(\varphi(p))$. Přitom platí

$$p/\varphi(\varphi(p)) \in O(\log \log p),$$

takže pravděpodobnost, že náhodné číslo bude primitivním kořenem je zhruba

$$1/\log \log p$$

a počet pokusů potřebných k nalezení primitivního kořene s předem danou pravděpodobností je úměrný $\log \log p$, tedy logaritmický vzhledem k délce vstupu (ověření toho, zda se vskutku jedná o primitivní kořen trvá déle, viz příště).

Plán přednášky

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 $\varphi(m)$.

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 $g^{x_a} \equiv a \pmod{m}$.

$1, g, g^2, \dots, g^{\varphi(m)-1}$ jsou právě všechna $(a, m) = 1$

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

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. $\square$

Plán přednášky

Kvadratické kongruence modulo prvočíslo

Věta

Nechť p je liché prvočíslo a $(a, p) = 1$. Kongruence $x^2 \equiv a \pmod{p}$ má řešení, právě když $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

$x^2 \equiv a \quad (p)$ ... a je kvadratický zbytek

Kvadratické kongruence modulo prvočíslo

Věta

Nechť p je liché prvočíslo a $(a, p) = 1$. Kongruence $x^2 \equiv a \pmod{p}$ má řešení, právě když $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Důkaz.

Použijeme primitivní kořen g a vyjádříme $x^2 \equiv a \pmod{p}$ pomocí něj: nechť $x \equiv g^{\xi}$, $a \equiv g^{\alpha}$, pak kongruence je ekvivalentní

$g^{2\xi}$ $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \varphi(p)$

$$(g^{\xi})^2 \equiv g^{\alpha} \pmod{p} \quad \Leftrightarrow \quad 2\xi \equiv \underline{\alpha} \pmod{p-1}.$$

Protože je $p-1$ sudé, řešení existuje, právě když α je sudé:

$$\alpha \equiv 0 \pmod{2} \quad \Leftrightarrow \quad \frac{p-1}{2} \cdot \alpha \equiv 0 \pmod{p-1}.$$

$$\Leftrightarrow \quad a^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}\cdot\alpha} \equiv g^0 \equiv 1 \pmod{p}. \qquad \square$$

Legendreův symbol

Věta

Nechť p je liché prvočíslo a $(a,p)=1$. Kongruence $x^2 \equiv a \pmod p$ má řešení, právě když $a^{\frac{p-1}{2}} \equiv 1 \pmod p$.

Legendreův symbol

Věta

Nechť p je liché prvočíslo a $(a,p)=1$. Kongruence $x^2 \equiv a \pmod p$ má řešení, právě když $a^{\frac{p-1}{2}} \equiv 1 \pmod p$.

Definice

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

- $x^2 \equiv a$ nemá řešení

Legendreův symbol a vzhledem k p

Legendreův symbol

Věta

Nechť p je liché prvočíslo a $(a,p)=1$. Kongruence $x^2 \equiv a \pmod p$ má řešení, právě když $a^{\frac{p-1}{2}} \equiv 1 \pmod p$.

Definice

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

Jednoduchým důsledkem věty dostáváme $\boxed{\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p}$: protože $(a^{\frac{p-1}{2}})^2 \equiv a^{p-1} \equiv 1$, je $a^{\frac{p-1}{2}}$ rovno ± 1.

i pro $a \equiv 0$ (p)

Legendreův symbol

Důsledek

$\left(\frac{-1}{p}\right) = +1$, *resp.* -1, *pokud* $p \equiv 1 \pmod 4$, *resp.* $p \equiv 3 \pmod 4$.
Tedy kongruence $x^2 \equiv -1 \pmod p$ *má řešení, právě když* p *dává po dělení čtyřmi zbytek 1.*

$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

$p \equiv 1 \ (4)$

$\frac{p-1}{2} \equiv 0 \ (2)$

$p \equiv 3 \ (4)$

$\frac{p-1}{2} \equiv 1 \ (2)$

Legendreův symbol

Důsledek

$\left(\frac{-1}{p}\right) = +1$, resp. -1, pokud $p \equiv 1 \pmod 4$, resp. $p \equiv 3 \pmod 4$. Tedy kongruence $x^2 \equiv -1 \pmod p$ má řešení, právě když p dává po dělení čtyřmi zbytek 1.

Počítání Legendreova symbolu je jednoduché s následujícími pravidly:

- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$,
- $a \equiv b \pmod p \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$,
- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$,
- $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \cdot (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \ (p)$

$p \equiv 1 \ (4)$ složitější

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

$\left(\frac{5}{11}\right) = ? \equiv 5^{\frac{11-1}{2}} \quad (11)$

Gaussovo lemma

zbytek

-1
-2
-3
-4
-5

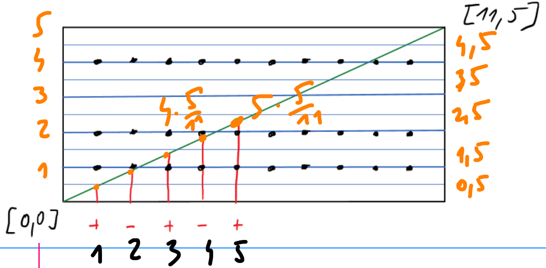
zb. po dël. 11 menší než 11/2

$$\begin{cases} 1\cdot 5 \equiv +5 \\ 2\cdot 5 \equiv -1 \\ 3\cdot 5 \equiv +4 \\ 4\cdot 5 \equiv -2 \\ 5\cdot 5 \equiv +3 \end{cases}$$

$$5!\cdot 5^{\frac{11-1}{2}} \equiv \pm 5!$$

$$\text{sign} \equiv 5^{\frac{11-1}{2}} \equiv \left(\frac{5}{11}\right) \quad (11)$$

$+1$



$1 \cdot 5 \equiv 5$

$2 \cdot 5 \equiv -1$

$3 \cdot 5 \equiv 4$

$4 \cdot 5 \equiv -2$

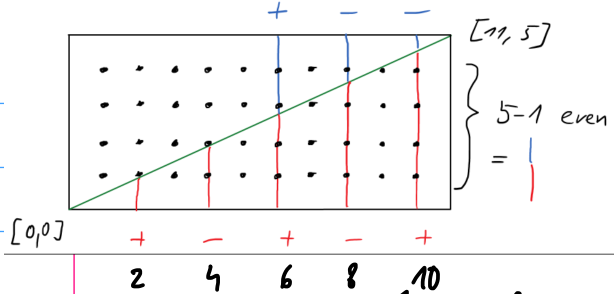
$5 \cdot 5 \equiv 3$

$\frac{1 \cdot 5}{11} =$ celé číslo $+ \frac{5}{11}$

$\frac{2 \cdot 5}{11} = \qquad - \frac{1}{11}$

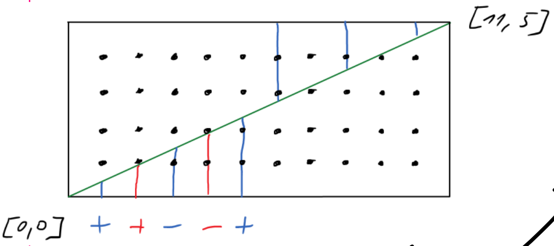
$\frac{3 \cdot 5}{11} = \qquad + \frac{4}{11}$

$\vdots$



$$\left(\frac{5}{11}\right) = (-1)^{\text{počet bodů v diagramu}}$$

5 liché:



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

5 liché !

liché

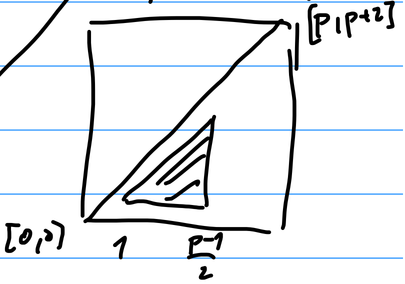
$$\left(\frac{2}{p}\right) = \left(\frac{p+2}{p}\right)$$

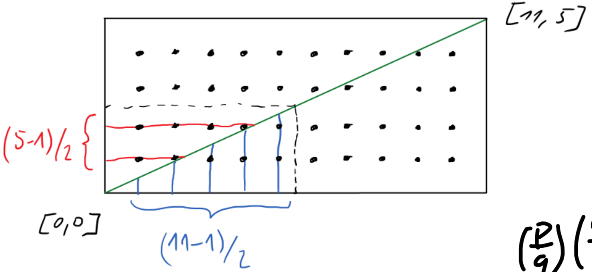
$$= (-1)^{1+2+\dots+\frac{p-1}{2}}$$

$$= (-1)^{\frac{p-1}{2}\cdot\frac{p+1}{4}} = (-1)^{\frac{p^2-1}{8}}$$

počet   prům. člen

p liché prvoč.





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

$$\left(\frac{5}{11}\right) = (-1)^{\text{počet pod}}$$

$$\left(\frac{11}{5}\right) = (-1)^{\text{počet vlevo}}$$

$$\left(\frac{5}{11}\right)\cdot\left(\frac{11}{5}\right) = (-1)^{\text{počet pod a vlevo}} = (-1)^{\frac{11-1}{2}\cdot\frac{5-1}{2}}$$

Jacobiho symbol: n liché, a jakékoliv

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_k}\right) \quad \text{kde } n = p_1 \cdots p_k$$

$a \equiv b \ (n) \Rightarrow$

Platí ty samé vztahy $\Rightarrow \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$$

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}} \quad n, m \text{ liché}$$

<u>Příklad</u>. $\left(\frac{219}{383}\right) = (-1)\cdot\left(\frac{383}{219}\right) = (-1)\left(\frac{164}{219}\right)$

$$= (-1)\cdot\underbrace{\left(\frac{2}{219}\right)\left(\frac{2}{219}\right)}_{1}\left(\frac{41}{219}\right) = (-1)\cdot\left(\frac{219}{41}\right) = (-1)\left(\frac{14}{41}\right) =$$

$$= (-1)\left(\frac{2}{41}\right)\left(\frac{7}{41}\right) = (-1)\left(\frac{41}{7}\right) = (-1)\left(\frac{6}{7}\right) = (-1)\left(\frac{2}{7}\right)\left(\frac{3}{7}\right)$$

$$(-1)\left(\frac{2}{7}\right)\left(\frac{3}{7}\right) = (-1)\underbrace{(-1)^{\frac{3-1}{4}\cdot\frac{7-1}{4}}}_{-1}\cdot\left(\frac{7}{3}\right)$$

$$\left(\frac{2}{7}\right) = (-1)^{\frac{7^2-1}{8}} = (-1)^6 = +1$$

$$= \left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = \underline{\underline{+1}}$$

$\left(\frac{219}{383}\right) = +1$ tj. (383 je prvočíslo)

$x^2 \equiv 219 \pmod{383}$ má řešení

$$\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{p}{3}\right) & p \equiv 1\ (4) \\ -\left(\frac{p}{3}\right) & p \equiv 3\ (4) \end{cases}$$

$p \equiv 1\ (4)$: $p\equiv 1\ (3)$: $\left(\frac{1}{3}\right) = 1$ $\quad p \equiv 1\ (12)$

$p \equiv 1\ (4)$: $p\equiv 2\ (3)$: $\left(\frac{2}{3}\right) = -1$ $\quad p \equiv 5\ (12)$

$p \equiv 3\ (4)$: $p\equiv 1\ (3)$: $-\left(\frac{1}{3}\right) = -1$ $\quad p \equiv 7\ (12)$

$p \equiv 3\ (4)$: $p\equiv 2\ (3)$: $-\left(\frac{2}{3}\right) = 1$ $\quad p \equiv 11\ (12)$

3 je kvadr. zb. mod $p \iff p \equiv 1, 11$ modulo 12.

Jak najít x t. ž. $x^2 \equiv a \pmod p$

Pro $p \equiv 3 \pmod 4$ $\iff$ $\left(\frac{-1}{p}\right) = -1$

-1 není kvadr. zbytek

$\left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = -\left(\frac{a}{p}\right)$

Tvrzení: nechť $\left(\frac{a}{p}\right) = 1$, $p \equiv 3 \pmod 4$.

potom $\pm a^{\frac{p+1}{4}}$ jsou odmocniny z a.

Důkaz. $\left(\pm a^{\frac{p+1}{4}}\right)^2 \equiv a^{\frac{p+1}{2}} \equiv a^{\frac{p-1}{2}} \cdot a$

$\equiv \left(\frac{a}{p}\right) \cdot a \equiv a$.

$x^2 - a = \left(x - a^{\frac{p+1}{4}}\right)\left(x + a^{\frac{p+1}{4}}\right)$ (a není kv. zb. $\Rightarrow \pm a^{\frac{p+1}{4}} = \sqrt{-a}$)

Plán přednášky

Základní úlohy výpočetní teorie čísel

V mnoha praktických úlohách využívajících výsledky teorie čísel je zapotřebí umět rychle provést jeden či více z následujících výpočtů:

1. běžné aritmetické operace (součet, součin, dělení se zbytkem) na celých číslech,

Základní úlohy výpočetní teorie čísel

i pro velká čísla

V mnoha praktických úlohách využívajících výsledky teorie čísel je zapotřebí umět rychle provést jeden či více z následujících výpočtů:

1. běžné aritmetické operace (součet, součin, dělení se zbytkem) na celých číslech,
2. zbytek mocniny celého čísla a na přirozené číslo n po dělení daným m.

Základní úlohy výpočetní teorie čísel

V mnoha praktických úlohách využívajících výsledky teorie čísel je zapotřebí umět rychle provést jeden či více z následujících výpočtů:

1. běžné aritmetické operace (součet, součin, dělení se zbytkem) na celých číslech,
2. zbytek mocniny celého čísla a na přirozené číslo n po dělení daným m.
3. inverzi celého čísla a modulo $m \in \mathbb{N}$,

Základní úlohy výpočetní teorie čísel

V mnoha praktických úlohách využívajících výsledky teorie čísel je zapotřebí umět rychle provést jeden či více z následujících výpočtů:

1. běžné aritmetické operace (součet, součin, dělení se zbytkem) na celých číslech,
2. zbytek mocniny celého čísla a na přirozené číslo n po dělení daným m.
3. inverzi celého čísla a modulo $m \in \mathbb{N}$,
4. největší společný dělitel dvou celých čísel (a případně koeficienty do Bezoutovy rovnosti),

Základní úlohy výpočetní teorie čísel

V mnoha praktických úlohách využívajících výsledky teorie čísel je zapotřebí umět rychle provést jeden či více z následujících výpočtů:

1. běžné aritmetické operace (součet, součin, dělení se zbytkem) na celých číslech,
2. zbytek mocniny celého čísla a na přirozené číslo n po dělení daným m.
3. inverzi celého čísla a modulo $m \in \mathbb{N}$,
4. největší společný dělitel dvou celých čísel (a případně koeficienty do Bezoutovy rovnosti),
5. rozhodnout o daném čísle, je-li prvočíslo nebo složené,

Základní úlohy výpočetní teorie čísel

V mnoha praktických úlohách využívajících výsledky teorie čísel je zapotřebí umět rychle provést jeden či více z následujících výpočtů:

ok

1. běžné aritmetické operace (součet, součin, dělení se zbytkem) na celých číslech,
2. zbytek mocniny celého čísla a na přirozené číslo n po dělení daným m.
3. inverzi celého čísla a modulo $m \in \mathbb{N}$,
4. největší společný dělitel dvou celých čísel (a případně koeficienty do Bezoutovy rovnosti),

těžké

5. rozhodnout o daném čísle, je-li prvočíslo nebo složené,
6. v případě složenosti rozložit dané číslo na součin prvočísel.

Základní aritmetické operace

Základní aritmetické operace se i na velkých číslech obvykle provádějí obdobně jako jsme se to učili na základní a střední škole, kdy umíme sčítat v *lineárním*, násobit a dělit se zbytkem v *kvadratickém* čase.

Základní aritmetické operace

Základní aritmetické operace se i na velkých číslech obvykle provádějí obdobně jako jsme se to učili na základní a střední škole, kdy umíme sčítat v *lineárním*, násobit a dělit se zbytkem v *kvadratickém* čase. Pro **násobení**, které je základem mnoha dalších operací, existují asymptoticky rychlejší algoritmy (typu *rozděl a panuj*) - např. první takový Karatsubův (1960) časové náročnosti $\Theta(n^{\log_2 3})$

Základní aritmetické operace

Základní aritmetické operace se i na velkých číslech obvykle provádějí obdobně jako jsme se to učili na základní a střední škole, kdy umíme sčítat v *lineárním*, násobit a dělit se zbytkem v *kvadratickém* čase. Pro **násobení**, které je základem mnoha dalších operací, existují asymptoticky rychlejší algoritmy (typu *rozděl a panuj*) - např. první takový Karatsubův (1960) časové náročnosti $\Theta(n^{\log_2 3})$ nebo algoritmus Schönhage-Strassenův (1971) časové náročnosti $\Theta(n \log n \log \log n)$, který využívá tzv. Fast Fourier Transform. Ten je ale přes svou asymptotickou převahu výhodný až pro násobení čísel majících alespoň desítky tisíc cifer (a používá se tak např. v GIMPS).

Základní aritmetické operace

Základní aritmetické operace se i na velkých číslech obvykle provádějí obdobně jako jsme se to učili na základní a střední škole, kdy umíme sčítat v *lineárním*, násobit a dělit se zbytkem v *kvadratickém* čase. Pro **násobení**, které je základem mnoha dalších operací, existují asymptoticky rychlejší algoritmy (typu *rozděl a panuj*) - např. první takový Karatsubův (1960) časové náročnosti $\Theta(n^{\log_2 3})$ nebo algoritmus Schönhage-Strassenův (1971) časové náročnosti $\Theta(n \log n \log \log n)$, který využívá tzv. Fast Fourier Transform. Ten je ale přes svou asymptotickou převahu výhodný až pro násobení čísel majících alespoň desítky tisíc cifer (a používá se tak např. v GIMPS).
Pěkný přehled je např. na `http://en.wikipedia.org/wiki/Computational_complexity_of_mathematical_operations`

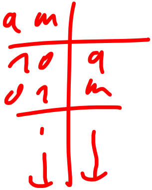
GCD a modulární inverze

Jak už jsme ukazovali dříve, výpočet řešení kongruence $a \cdot x \equiv 1 \pmod{m}$ s neznámou x lze snadno (díky Bezoutově větě) převést na výpočet největšího společného dělitele čísel a a m a na hledání koeficientů k, l do Bezoutovy rovnosti $k \cdot a + l \cdot m = 1$ (nalezené k je pak onou hledanou inverzí a modulo m).

GCD a modulární inverze

Jak už jsme ukazovali dříve, výpočet řešení kongruence $a \cdot x \equiv 1 \pmod{m}$ s neznámou x lze snadno (díky Bezoutově větě) převést na výpočet největšího společného dělitele čísel a a m a na hledání koeficientů k, l do Bezoutovy rovnosti $k \cdot a + l \cdot m = 1$ (nalezené k je pak onou hledanou inverzí a modulo m).

```
function extended_gcd(a, m)
    if m == 0
        return (1, 0)
    else
        (q, r) := divide (a, m)
        (k, l) := extended_gcd(m, r)
        return (l, k − q ∗ l)
```



Podrobná analýza (viz např. `[Knuth]` nebo `[Wiki]`) ukazuje, že tento algoritmus je **kvadratické** časové složitosti.

Modulární umocňování

Modulární umocňování je, jak jsme již viděli dříve, velmi využívaná operace mj. při ověřování, zda je dané číslo prvočíslo nebo číslo složené. Jedním z efektivních algoritmů je tzv. **modulární umocňování zprava doleva**:

Modulární umocňování

Modulární umocňování je, jak jsme již viděli dříve, velmi využívaná operace mj. při ověřování, zda je dané číslo prvočíslo nebo číslo složené. Jedním z efektivních algoritmů je tzv. **modulární umocňování zprava doleva**:

```
function modular_pow(base, exponent, modulus)
    result := 1
    while exponent > 0
      if (exponent mod 2 == 1):
        result := (result * base) mod modulus
      exponent := exponent >> 1
      base = (base * base) mod modulus
    return result
```

Algoritmus modulárního umocňování je založen na myšlence, že např. při počítání $2^{64} \pmod{1000}$

- není třeba nejprve počítat 2^{64} a poté jej vydělit se zbytkem číslem 1000, ale lépe je postupně násobit „dvojky“ a kdykoliv je výsledek větší než 1000, provést redukci modulo 1000, Algoritmus modulárního umocňování je založen na myšlence, že např. při počítání $2^{64} \pmod{1000}$

- není třeba nejprve počítat 2^{64} a poté jej vydělit se zbytkem číslem 1000, ale lépe je postupně násobit „dvojky“ a kdykoliv je výsledek větší než 1000, provést redukci modulo 1000,
- ale zejména, že není třeba provádět takové množství násobení (v tomto případě 63 naivních násobení je možné nahradit pouze šesti umocněními na druhou, neboť

$$2^{64} = (((((2^2)^2)^2)^2)^2)^2.$$

Příklad (Ukázka průběhu algoritmu)

Vypočtěme $2^{560} \pmod{561}$.

Příklad (Ukázka průběhu algoritmu)

Vypočtěme $2^{560} \pmod{561}$. Protože $560 = (1000110000)_2$, dostaneme uvedeným algoritmem

$2^{560} = (2^2)^{280} = 4^{280}$

exponent	base	result	exp's last digit
560	2	1	0
280	4	1	0
140	16	1	0
70	256	1	0
35	460	1	1
17	103	460	1
8	511	256	0
4	256	256	0
2	460	256	0
1	103	256	1
0	511	1	0

$1 \cdot 2^{560}$
$1 \cdot 4^{280}$
$1 \cdot 16^{140}$
$1 \cdot 256^{70}$
$1 \cdot 460^{35}$
$460 \cdot 103^{17}$
$256 \cdot 511^{8}$
$256 \cdot 256^{4}$
$256 \cdot 460^{2}$
$256 \cdot 103^{1}$
$511 \cdot 1^{0}$

počet kroků = délka exponentu

$460^{35} = 460 \cdot 460^{34} = 460 \cdot (256)^{17}$

Příklad (Ukázka průběhu algoritmu)

Vypočtěme $2^{560} \pmod{561}$. Protože $560 = (1000110000)_2$, dostaneme uvedeným algoritmem

exponent	base	result	exp's last digit
560	2	1	0
280	4	1	0
140	16	1	0
70	256	1	0
35	460	1	1
17	103	460	1
8	511	256	0
4	256	256	0
2	460	256	0
1	103	256	1
0	511	1	0

A tedy $2^{560} \equiv 1 \pmod{561}$. ← není Eulerova věta (561 není prvočíslo)

Efektivita modulárního umocňování

V průběhu algoritmu se pro každou binární číslici exponentu provede umocnění základu na druhou modulo n (což je operace proveditelná v nejhůře kvadratickém čase), a pro každou „jedničku" v binárním zápisu navíc provede jedno násobení. Celkově jsme tedy schopni provést modulární umocňování nejhůře v **kubickém** čase.

Je p prvočíslo?

musí být $a^{p-1} \equiv 1 \pmod p$

$\rightsquigarrow$ <u>test</u>: zvolíme a, spočítáme $a^{p-1} \pmod p$

$p = 35$ zvolíme $a = 2$

$$2^{34} \equiv 1 \cdot 2^{34} \equiv 1 \cdot 4^{17} \quad 17 = 1 + 2 \cdot 8$$

$$\equiv 4 \cdot 16^{8} \equiv 4 \cdot 11^{4}$$

$$\equiv 4 \cdot 16^{2} \equiv 4 \cdot 11^{1} \equiv 9 \quad (35)$$

$\Rightarrow$ 35 není prvočíslo, protože

$$2^{34} \not\equiv 1 \pmod{35}$$

561 projde --- $a^{560} \equiv 1 \pmod{561}$
pokud $(a, 561) = 1$

složitější test: $a^{\frac{p-1}{2}} \equiv \sqrt{a^{p-1}} \equiv \sqrt{1} \equiv \pm 1$
$\pmod p$

$\rightsquigarrow$ $p = 561$ $\quad a = 2$: $2^{280} \equiv 1$

$a = 5$: $5^{280} \not\equiv 1$

$\Rightarrow$ 561 není prvočíslo

ještě složitější test: $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$

$\rightsquigarrow$ $p = 1729$ $\quad a = 11$: $11^{864} \equiv 1 \not\equiv \left(\frac{11}{865}\right)$

$$\left(\frac{11}{865}\right) \equiv \left(\frac{865}{11}\right) \equiv \left(\frac{7}{11}\right) \equiv (-1)\left(\frac{11}{7}\right) = (-1)\left(\frac{4}{7}\right) \equiv -1$$

$\left(\frac{2}{7}\right)^2 \equiv 1$