Věta: Primitivní kořeny mod m existují, právě když

- $m = 2$ *nebo* $m = 4$,
- m *je mocnina lichého prvočísla*
- m *je dvojnásobek mocniny lichého prvočísla.*

Poznámka. Pokud pro přirozené číslo existují primitivní kořeny, tak jich mezi čísly $1, 2, \ldots, m$ existuje právě $\varphi(\varphi(m))$. Je-li totiž g primitivní kořen a $a \in \{1, 2, \ldots, \varphi(m)\}$ libovolné, pak g^a je podle Věty 19 řádu $\frac{\varphi(m)}{(a,\varphi(m))}$, což je rovno $\varphi(m)$ právě tehdy, je-li $(a, \varphi(m)) = 1$. Takových a je v množině $\{1, 2, \ldots, \varphi(m)\}$ právě $\varphi(\varphi(m))$.

Důkaz Věty provedeme v několika krocích. Snadno je vidět, že primitivní kořen modulo 2 je 1 a modulo 4 je 3. Dále ukážeme, že primitivní kořeny existují modulo libovolné liché prvočíslo (pro ty, kdo si pamatují základy algebry, tak vlastně jiným způsobem dokážeme, že grupa $(\mathbb{Z}_m^\times, \cdot)$ invertibilních zbytkových tříd modulo prvočíselné m je cyklická.

Tvrzení 4.1. *Nechť p je liché prvočíslo. Pak existují primitivní kořeny modulo p.*

Důkaz. Označme $r_1, r_2, \ldots, r_{p-1}$ řády čísel $1, 2, \ldots, p-1$ modulo p. Buď $\delta = [r_1, r_2, \ldots, r_{p-1}]$ nejmenší společný násobek těchto řádů. Ukážeme, že mezi čisly $1, 2, \ldots, p-1$ 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 $s \in \{1, \ldots k\}$ existuje $c \in \{1, \ldots, p-1\}$ tak, že $q_s^{\alpha_s} \mid r_c$ (jinak by existoval menší společný násobek čísel $r_1, r_2, \ldots, r_{p-1}$ 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 Věty 19 řád $q_s^{\alpha_s}$.

Provedením předchozí úvahy pro libovolné $s \in \{1, \ldots k\}$ dostaneme $g_1, \ldots, g_k$ a můžeme položit $g := g_1 \cdots g_k$. Podle Lemmatu za Větou 19 dostáváme, že řád g je roven součinu řádů čísel $g_1, \ldots, g_k$, tj. číslu $q_1^{\alpha_1} \cdots q_k^{\alpha_k} = \delta$.

Nyní dokážeme, že $\delta = p - 1$. Protože řády čísel $1, 2, \ldots, p-1$ dělí δ, dostáváme pro libovolné $x \in \{1, 2, \ldots, p-1\}$ vztah $x^\delta \equiv 1 \pmod p$. Kongruence stupně δ modulo p má podle Věty 26 nejvýše δ řešení (a podle předchozího má $p-1$ řešení), proto nutně $\delta \geq p - 1$. Přitom $\delta \mid p - 1$ (jakožto řád čísla g), proto zejména $\delta \leq p - 1$, a celkem $\delta = p - 1$. □

Nyní ukážeme, že primitivní kořeny existují dokonce modulo mocniny lichých prvočísel. K tomuto budeme potřebovat dvě pomocná tvrzení.

Lemma. *Buď p liché prvočíslo, $l \geq 2$ libovolné. Pak pro libovolné $a \in \mathbb{Z}$ platí*

$$(1 + ap)^{p^{l-2}} \equiv 1 + ap^{l-1} \pmod{p^l}.$$

I. $l = 2$: $(1+ap)^{p^0} \equiv 1 + ap^1$

Důkaz. Plyne snadno z binomické věty s využitím matematické indukce.
I. Pro $l = 2$ tvrzení zřejmě platí.
II. Nechť tvrzení platí pro l, dokážeme jej i pro $l+1$. S využitím Lemmatu na str. 23 tak umocněním na p-tou tvrzení pro l (s navýšením modulu) dostaneme

$$(1+ap)^{p^{l-1}} \equiv (1+ap^{l-1})^p \pmod{p^{l+1}}.$$

Z binomické věty přitom plyne

$$(1+ap^{l-1})^p = 1 + p\cdot a\cdot p^{l-1} + \sum_{k=2}^{p} \binom{p}{k} a^k p^{(l-1)k}$$

a vzhledem k tomu, že pro $1 < k < p$ platí $p \mid \binom{p}{k}$, stačí ukázat $p^{l+1} \mid p^{(l-1)k}$, což je ekvivalentní s $1 \le (k-1)(l-1)$. Rovněž pro $k = p$ dostáváme díky $l \ge 3$ vztah $p^{l+1} \mid p^{(l-1)p}$. □

Lemma. *Buď p liché prvočíslo, $l \ge 2$ libovolné. Pak pro libovolné $a \in \mathbb{Z}$, splňující $p \nmid a$ platí, že řád čísla $1+ap$ modulo p^l je roven p^{l-1}.*

Důkaz. Podle předchozího Lemmatu je

$$(1+ap)^{p^{l-1}} \equiv 1 + ap^l \pmod{p^{l+1}},$$

a uvážíme-li tuto kongruenci modulo p^l, dostaneme $(1+ap)^{p^{l-1}} \equiv 1 \pmod{p^l}$. Přitom přímo z předchozího Lemmatu a faktu $p \nmid a$ plyne $(1+ap)^{p^{l-2}} \not\equiv 1 \pmod{p^l}$, což dává požadované. □

Tvrzení 4.2. *Buď p liché prvočíslo. Pak pro každé $l \in \mathbb{N}$ existuje primitivní kořen modulo p^l.*

Důkaz. Nechť g je primitivní kořen modulo p. Ukážeme, že pokud $g^{p-1} \not\equiv 1 \pmod{p^2}$, je g dokonce primitivním kořenem modulo p^l pro libovolné $l \in \mathbb{N}$. (Pokud by platilo $g^{p-1} \equiv 1 \pmod{p^2}$, pak $(g+p)^{p-1} \equiv 1 + (p-1)g^{p-2}p \not\equiv 1 \pmod{p^2}$, a tedy místo g můžeme volit za původní primitivní kořen číslo $g+p$.) Nechť tedy g splňuje $g^{p-1} \not\equiv 1 \pmod{p^2}$. Pak existuje $a \in \mathbb{Z}$, $p \nmid a$ tak, že $g^{p-1} = 1 + p\cdot a$. Ukážeme, že g je modulo p^l řádu $\varphi(p^l) = (p-1)p^{l-1}$. Buď $n \in \mathbb{N}$ nejmenší číslo, splňující $g^n \equiv 1 \pmod{p^l}$. Podle předchozího Lemmatu je g^{p-1} modulo p^l řádu p^{l-1}. Pak ale

$$(g^{p-1})^n = (g^n)^{p-1} \equiv 1 \pmod{p^l} \Longrightarrow p^{l-1} \mid n.$$

Zároveň z $g^n \equiv 1 \pmod{p}$ plyne $p-1 \mid n$. Protože jsou čísla $p-1$ a p^{l-1} nesoudělná, dostáváme $(p-1)p^{l-1} \mid n$. Proto $n = \varphi(p^l)$ a g je tedy primitivní kořen modulo p^l. □

Tvrzení 4.3. *Buď p liché prvočíslo a g primitivní kořen modulo p^l pro $l \in \mathbb{N}$. Pak liché z čísel $g, g+p^l$ je primitivním kořenem modulo $2p^l$.*

Důkaz. Nechť c je liché přirozené číslo. Pak pro libovolné $n \in \mathbb{N}$ platí $c^n \equiv 1 \pmod{p^l}$, právě když $c^n \equiv 1 \pmod{2p^l}$. Protože $\varphi(2p^l) = \varphi(p^l)$, je každý lichý primitivní kořen modulo p^l rovněž primitivním kořenem modulo $2p^l$. □

Další tvrzení popisuje případ mocnin sudého prvočísla. K tomu využijeme obdobných pomocných tvrzení jako v případě lichých prvočísel.

Lemma. *Buď $l \in \mathbb{N}$, $l \geq 3$. Pak $5^{2^{l-3}} \equiv 1 + 2^{l-1} \pmod{2^l}$.*

Důkaz. Obdobně jako výše pro $2 \nmid p$. □

Lemma. *Buď $l \in \mathbb{N}$, $l \geq 3$. Pak řád čísla 5 modulo 2^l je 2^{l-2}.*

Důkaz. Snadný z předchozího Lemmatu. □

Tvrzení 4.4. *Nechť $l \in \mathbb{N}$. Primitivní kořeny existují modulo 2^l právě tehdy, když $l \leq 2$.*

Důkaz. Buď $l \geq 3$. Pak množina

$$S = \{(-1)^a \cdot 5^b; a \in \{0,1\}, 0 \leq b < 2^{l-2}; b \in \mathbb{Z}\}$$

tvoří redukovanou soustavu zbytků modulo 2^l (má totiž $\varphi(2^l)$ prvků o kterých se snadno ukáže, že jsou po dvou nekongruentní modulo 2^l).

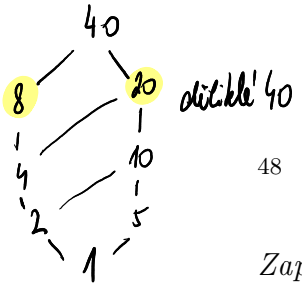
Přitom zřejmě (s využitím předchozího Lemmatu) řád každého prvku S dělí 2^{l-2}, proto v této (a tedy ani v žádné jiné) redukované soustavě nemůže existovat prvek řádu $\varphi(2^l) = 2^{l-1}$. □

Posledním kamínkem do mozaiky tvrzení, která společně dokazují Větu 30, je tvrzení popisující neexistenci primitivních kořenů pro složená čísla, která nejsou mocninou prvočísla (ani jejím dvojnásobkem).

Tvrzení 4.5. *Nechť $m \in \mathbb{N}$ je dělitelné alespoň 2 prvočísly a není dvojnásobkem mocniny lichého prvočísla. Pak modulo m neexistují primitivní kořeny.*

Důkaz. Buď rozklad m na prvočísla tvaru $2^\alpha p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, kde $\alpha \in \mathbb{N}_0, \alpha_i \in \mathbb{N}, 2 \nmid p_i$ a buď platí $k \geq 2$ nebo $k \geq 1$ a $\alpha \geq 2$. Označíme-li $\delta = [\varphi(2^\alpha), \varphi(p_1^{\alpha_1}), \ldots, \varphi(p_k^{\alpha_k})]$, pak se snadno vidí, že $\delta < \varphi(2^\alpha) \cdot \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k}) = \varphi(m)$ a že pro libovolné $a \in \mathbb{Z}$, $(a, m) = 1$ platí $a^\delta \equiv 1 \pmod{m}$. Proto modulo m neexistují primitivní kořeny. □

Nyní máme dokázáno tvrzení přesně charakterizující ty moduly, pro které existují primitivní kořeny. Obecně je ale 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 31. *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

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

□

Příklad. Postupně určíme primitivní kořeny modulo $41, 41^2$ a $2 \cdot 41^2$.

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

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

$g = 2$: $2^8 = 2^5 \cdot 2^3 \equiv -9 \cdot 8 \equiv 10 \not\equiv 1 \pmod{41}$

$2^{20} = (2^5)^4 \equiv (-9)^4 = 81^2 \equiv (-1)^2 = 1 \pmod{41}$ 2 není p.k.

$g = 3$: $3^8 = (3^4)^2 \equiv (-1)^2 = 1 \pmod{41}$ 3 není p.k.

$g = 4$: řád $4 = 2^2$ vždy dělí řád 2 obecně, řád q je $\frac{r}{(r,2)} = \frac{r}{2}$, pro sudé r, kde r je řád 2

$g = 5$: $5^8 = (5^2)^4 \equiv (-2^4)^4 = 2^{16} = (2^8)^2 \equiv 10^2 \equiv 18 \pmod{41}$

$5^{20} = (5^2)^{10} \equiv (-2^4)^{10} = 2^{40} = (2^{20})^2 \equiv 1 \pmod{41}$ 5 není p.k.

$g = 6$: $6^8 = 2^8 \cdot 3^8 \equiv 10 \cdot 1 = 10 \pmod{41}$

$6^{20} = 2^{20} \cdot 3^{20} \equiv 2^{20} \cdot (3^8)^2 \cdot 3^4 \equiv 1 \cdot 1 \cdot (-1) = -1 \pmod{41}$

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

Dokážeme-li nyní, že $6^{40} \not\equiv 1 \pmod{41^2}$, budeme vědět, že 6 je i primitivním kořenem modulo libovolná mocnina 41 (pokud bychom „měli smůlu“ a $6^{40} \equiv 1 \pmod{41^2}$, pak by primitivním kořenem modulo 41^2 bylo číslo $47 = 6 + 41$). Při ověření podmínky si vypomůžeme několika triky (tzv. modulární reprezentace čísel), abychom se obešli bez manipulace s velkými čísly.

Nejprve vypočtěme zbytek po dělení 6^8 číslem 41^2; k tomu se nám bude hodit vypočítat zbytek po dělení čísel 2^8 a 3^8:

$$2^8 = 256 = 6 \cdot 41 + 10$$
$$3^8 = (3^4)^2 = (2 \cdot 41 - 1)^2 \equiv -4 \cdot 41 + 1 \pmod{41^2}$$
$$\text{Pak } 6^8 = 2^8 \cdot 3^8 \equiv (6 \cdot 41 + 10)(-4 \cdot 41 + 1) \equiv$$
$$\equiv -34 \cdot 41 + 10 \equiv 7 \cdot 41 + 10 \pmod{41^2}$$
$$\text{a } 6^{40} = (6^8)^5 \equiv (7 \cdot 41 + 10)^5 \equiv (10^5 + 5 \cdot 7 \cdot 41 \cdot 10^4) =$$
$$= 10^4(10 + 35 \cdot 41) \equiv (-2 \cdot 41 - 4)(-6 \cdot 41 + 10) \equiv$$
$$\equiv (4 \cdot 41 - 40) = 124 \not\equiv 1 \pmod{41^2}.$$

$-34 \equiv 7 \pmod{41}$ ⇓ $-35 \cdot 41 \equiv 7 \cdot 41 \pmod{41^2}$

$\Rightarrow$ 6 je p.k. mod 41^2

Přitom jsme využili toho, že $10^4 = 6 \cdot 41^2 - 86$, tj. $10^4 \equiv -2 \cdot 41 - 4 \pmod{41^2}$.

Je tedy 6 primitivním kořenem modulo 41^2 a protože je to sudé číslo, je primitivním kořenem modulo $2 \cdot 41^2$ číslo $1687 = 6 + 41^2$ (nejmenším kladným primitivním kořenem modulo $2 \cdot 41^2$ je přitom číslo 7). $\Leftarrow 7^{40} \not\equiv 1 \pmod{41^2}$

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

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

[ležádlr :]

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

$$x^2 \equiv a \pmod{p}, \tag{27}$$

kde p je liché prvočíslo a a číslo s ním nesoudělné.

$m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

$ax^2+bx+c \equiv 0 \pmod{m}$ ⇙ ⇘

$ax^2+bx+c \equiv 0 \pmod{p_i^{\alpha_i}}$ ⇓ Hensel

$ax^2+bx+c \equiv 0 \pmod{p_i}$ | $\cdot u$ kde $a \cdot a \equiv 1 \pmod{p}$

$x^2+Bx+C \equiv 0 \pmod{p}$ ($p \neq 2$)

$\left(x+\frac{B}{2}\right)^2 - A \equiv 0 \pmod{p}$

pro sudé B (B liché $\Rightarrow B \equiv B+p$)

$y^2 \equiv A \pmod{p}$

Tato je vyřešitelná ⇓

$A^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

Pro určení řešitelnosti kongruence (27) můžeme samozřejmě využít Větu 27, její využití ale často naráží na výpočetní složitost, proto se 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 27 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). Závěrem této části tuto podmínku ověříme s pomocí Legendreova symbolu daleko snadněji.

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

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

$\left(\frac{219}{383}\right)$ „219 vzhledem k 383“

$a^{\frac{\varphi(m)}{d}} \equiv 1 \pmod{m}$,

kde $d = (n, \varphi(m)) = (2, p-1) = 2$

$n = 2,\ m < p$