Věta 26. *Buď $p$ prvočíslo, $f(x) \in \mathbb{Z}[x]$. Má-li kongruence $f(x) \equiv 0 \pmod{p}$ více než $\mathrm{st}(f)$ řešení, pak jsou všechny koeficienty polynomu $f$ násobkem $p$.*

Důkaz. V jazyce algebry jde vlastně o počet kořenů nenulového polynomu nad (konečným) tělesem $\mathbb{Z}_p$, kterých je nejvýše $\mathrm{st}(f)$. □

Důsledek. *(Jiný důkaz Wilsonovy věty) Pro každé prvočíslo $p$ platí*

$$(p-1)! \equiv -1 \pmod{p}.$$

Důkaz. Pro $p = 2$ je tvrzení zřejmé, dále uvažujme jen lichá prvočísla $p$. Řešením kongruence

$$(x-1)(x-2)\cdots(x-(p-1)) - (x^{p-1}-1) \equiv 0 \pmod{p}$$

je podle Malé Fermatovy věty libovolné $a \in \mathbb{Z}$, které není násobkem $p$, tj. kongruence má $p-1$ řešení. Přitom je ale její stupeň menší než $p-1$, proto jsou podle předchozí věty všechny koeficienty polynomu na levé straně kongruence násobkem $p$, speciálně absolutní člen, kterým je $(p-1)!+1$. Tím je Wilsonova věta dokázána. □

**4.5. Binomické kongruence a primitivní kořeny.** 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

$$x^2 \equiv 18 \pmod{63}.$$

Řešení. Protože je $(18, 63) = 9$, musí platit $9 \mid x^2$, tj. $3 \mid x$. Položíme-li $x = 3x_1$, $x_1 \in \mathbb{Z}$, dostáváme ekvivalentní kongruenci $x_1^2 \equiv 2 \pmod{7}$, která již splňuje omezení na nesoudělnost modulu a pravé strany kongruence. Podle Věty 26 víme, že má nejvýše 2 řešení a snadno se vidí, že jimi jsou $x_1 \equiv \pm 3 \pmod{7}$, tj. $x_1 \equiv \pm 3, \pm 10, \pm 17, \pm 24, \pm 31, \pm 38, \pm 45, \pm 52, \pm 59 \pmod{63}$. Řešeními původní kongruence jsou tedy $x \equiv 3 \cdot x_1 \pmod{63}$, tj. $x \equiv \pm 9, \pm 12, \pm 30 \pmod{63}$.

Příklad. Řešte kongruenci

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

Řešení. Protože je $(3, 18) = 3$, nutně $3 \mid x$. Užijeme-li, podobně jako výše, substituci $x = 3 \cdot x_1$, dostáváme kongruenci

$$27x_1^3 \equiv 3 \pmod{18},$$

která zřejmě nemá řešení, protože $(27, 18) \nmid 3$.

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 $m$.

V tomto odstavci ukážeme, jakým způsobem řešit binomické kongruence modulo $m$, pokud modulo $m$ existují tzv. primitivní kořeny.

DEFINICE. Nechť $m \in \mathbb{N}$. Celé číslo $a \in \mathbb{Z}$, $(a, m) = 1$ 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 $a \to x_a$ se nazývá diskrétní logaritmus, příp. index čísla $x$ (vzhledem k danému $m$ a zafixovanému primitivnímu kořeni $g$) a je bijekcí mezi množinami*
$\{a \in \mathbb{Z};\, (a, m) = 1, 0 < a \leq m\}$ *a* $\{x \in \mathbb{Z};\, 0 \leq x < \varphi(m)\}$.

DŮKAZ. Stačí ukázat tvrzení o bijekci a protože obě množiny mají stejný počet prvků, stačí dokázat injektivitu uvedeného zobrazení. Předpokládejme, že pro $x, y \in \mathbb{Z}$, $0 \leq x, y < \varphi(m)$ je $g^x \equiv g^y \pmod{m}$. Podle Věty 18 pak $x \equiv y \pmod{\varphi(m)}$, tj. $x = y$. □

Později ukážeme, že primitivní kořeny existují „dostatečně často“ na to, aby následující věta řešila všechny potřebné případy.

VĚTA 27. *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 Věty 18 i s lineární kongruencí

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

Tato kongruence 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* $m$.

Důkaz. Zřejmý. □

Následující věty nám dávají obecnou informaci o počtu řešení kongruencí podle modulu, kterým je mocnina prvočísla. Jde o speciální případy Henselova lemmatu pro případ binomických kongruencí.

Věta 28. *Buď* $p$ *prvočíslo,* $a \in \mathbb{Z}$, $n \in \mathbb{N}, p \nmid a$, $p \nmid n$. *Je-li kongruence* $x^n \equiv a \pmod{p}$ *řešitelná, je řešitelná i kongruence* $x^n \equiv a \pmod{p^\alpha}$ *pro libovolné přirozené číslo* $\alpha$ *a má stejný počet řešení jako kongruence modulo* $p$.

Důkaz. Plyne z Henselova lemmatu pro kongruenci $f(x) \equiv 0 \pmod{p}$, kde $f(x) = x^n - a$. Pak totiž $f'(x) = n \cdot x^{n-1}$ a pokud $b \in \mathbb{Z}$ splňuje $f(b) \equiv 0 \pmod{p}$, pak jistě $p \nmid b$, a proto $p \nmid f'(b)$.

□

Věta 29. *Buď* $n \in \mathbb{N}$, $a \in \mathbb{Z}$, $2 \nmid a$. *Označme dále* $l \in \mathbb{N}_0$ *největší takové, že* $2^l \mid n$. *Je-li kongruence* $x^n \equiv a \pmod{2^{2l+1}}$ *řešitelná, je řešitelná i kongruence* $x^n \equiv a \pmod{2^\alpha}$ *pro libovolné* $\alpha \in \mathbb{N}$, $\alpha \geq 2l+1$ *a má stejný počet řešení jako kongruence modulo* $2^{2l+1}$.

Důkaz. Prozatím neuveden. □

Poznámka. Uvážíme-li v předchozí větě přirozené číslo $n \equiv 2 \pmod{4}$, pak je $l = 1$. Pro liché $a$ je kongruence $x^n \equiv a \pmod{8}$ řešitelná právě když je $a \equiv 1 \pmod{8}$ (a má 4 řešení). Díky přechozí větě víme, že pro $a \equiv 1 \pmod{8}$ má řešení libovolná kongruence tvaru $x^n \equiv a \pmod{2^\alpha}$ pro $\alpha \geq 3$ a má 4 řešení.

V předchozích odstavcích jsme se zabývali řešitelností binomických kongruencí podle modulů, pro které existuje primitivní kořen. Ve zbytku této části se budeme zabývat tím, pro která čísla primitivní kořeny existují. Postupně dokážeme následující větu:

Věta 30. *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.*

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 $\delta$ a že $\delta = p-1$.

Nechť $\delta = q_1^{\alpha_1} \cdots q_k^{\alpha_k}$ je rozklad $\delta$ 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 $\delta$), 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 $\delta$, dostáváme pro libovolné $x \in \{1, 2, \ldots, p-1\}$ vztah $x^\delta \equiv 1 \pmod{p}$. Kongruence stupně $\delta$ modulo $p$ má podle Věty 26 nejvýše $\delta$ 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*

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