Z druhé kongruence dostáváme, že $x = -3 + 81t$, kde $t \in \mathbb{Z}$. Dosazením do třetí kongruence soustavy (23) dostaneme

$$-3 + 81t \equiv -4 \pmod{11},$$

tedy $81t \equiv -1 \pmod{11}$, tj. $4t \equiv 32 \pmod{11}$, odkud $t \equiv 8 \pmod{11}$, a proto $t = -3 + 11s$, kde $s \in \mathbb{Z}$. Dosazením $x = -3 + 81(-3 + 11s) = -3 - 3 \cdot 81 + 11 \cdot 81s$ do první kongruence soustavy (23) dostaneme

$$-3 - 3 \cdot 81 + 11 \cdot 81s \equiv 3 \pmod{4},$$

tedy

$$1 + 1 \cdot 1 + (-1) \cdot 1s \equiv 3 \pmod{4},$$

tj. $-s \equiv 1 \pmod{4}$ a proto $s = -1 + 4r$, kde $r \in \mathbb{Z}$. Je tedy

$$x = -3-3\cdot81+11\cdot81(-1+4r) = -3-14\cdot81+4\cdot11\cdot81r = -1137+3564r,$$

neboli $x \equiv -1137 \pmod{3564}$, což je také řešení zadané kongruence. □

4.3. Kongruence vyšších stupňů. Vraťme se k obecnějšímu případu, kdy na obou stranách kongruence stojí mnohočleny téže proměnné x s celočíselnými koeficienty. Snadno můžeme tuto kongruenci odečtením upravit na tvar

$$F(x) \equiv 0 \pmod{m}, \tag{24}$$

kde $F(x)$ je mnohočlen s celočíselnými koeficienty a $m \in \mathbb{N}$. Věta 20 nám poskytuje sice pracnou, ale univerzální metodu řešení této kongruence. Při řešení kongruence (24) totiž stačí zjistit, pro která celá čísla a, $0 \le a < m$, 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 kongruenci (24) soustavou kongruencí

$$\begin{aligned} F(x) &\equiv 0 \pmod{p_1^{n_1}} \\ &\vdots \\ F(x) &\equiv 0 \pmod{p_k^{n_k}}, \end{aligned} \tag{25}$$

která má stejnou množinu řešení, a řešit každou kongruenci této soustavy zvlášť. Tím získáme obecně několik soustav kongruencí (19), které už umíme řešit. Výhoda této metody spočívá v tom, že moduly kongruencí soustavy (25) jsou menší než modul původní kongruence (24).

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

Řešení. Označme $F(x) = x^5 + 1$. Pak platí $F(0) = 1$, $F(1) = 2$ a dále platí

$$\begin{aligned}
F(2) &= 33 \equiv 0 \pmod{11},\\
F(3) &= 3^5 + 1 = 9 \cdot 9 \cdot 3 + 1 \equiv (-2)^2 \cdot 3 + 1 = 12 + 1 \equiv 2 \pmod{11},\\
F(4) &= 4^5 + 1 = 2^{10} + 1 \equiv 1 + 1 = 2 \pmod{11},
\end{aligned}$$

kde jsme využili Fermatovu větu 16, podle které $2^{10} \equiv 1 \pmod{11}$. Podobně dále

$$\begin{aligned}
F(5) &= 5^5 + 1 \equiv 16^5 + 1 = 4^{10} + 1 \equiv 1 + 1 = 2 \pmod{11},\\
F(6) &= 6^5 + 1 \equiv (-5)^5 + 1 \equiv -16^5 + 1 \equiv -4^{10} + 1 \equiv 0 \pmod{11},\\
F(7) &= 7^5 + 1 \equiv (-4)^5 + 1 = -2^{10} + 1 \equiv -1 + 1 = 0 \pmod{11},\\
F(8) &= 8^5 + 1 \equiv 2^5 \cdot 2^{10} + 1 \equiv 32 + 1 \equiv 0 \pmod{11},\\
F(9) &= 9^5 + 1 = 3^{10} + 1 \equiv 1 + 1 = 2 \pmod{11},\\
F(10) &= 10^5 + 1 \equiv (-1)^5 + 1 = 0 \pmod{11},
\end{aligned}$$

a tedy řešením kongruence $x^5 + 1 \equiv 0 \pmod{11}$ jsou právě všechna x, vyhovující některé z kongruencí $x \equiv 2 \pmod{11}$, $x \equiv 6 \pmod{11}$, $x \equiv 7 \pmod{11}$, $x \equiv 8 \pmod{11}$, $x \equiv 10 \pmod{11}$. □

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. Platí $F(0) = 5$, $F(1) = 3$, $F(2) = 7$, $F(3) = 23$, $F(-1) = 7$, $F(-2) = 3$, $F(-3) = -13$ (pro snadnější výpočty jsme počítali například $F(-1)$ místo $F(6)$ – využijeme toho, že $F(6) \equiv F(-1) \pmod{7}$ podle předchozího Tvrzení a podobně). Kongruence $F(x) \equiv 0 \pmod{3}$ má tedy řešení $x \equiv 1 \pmod{3}$; kongruence $F(x) \equiv 0 \pmod{5}$ má řešení $x \equiv 0 \pmod{5}$; řešením kongruence $F(x) \equiv 0 \pmod{7}$ jsou $x \in \mathbb{Z}$ splňující $x \equiv 2 \pmod{7}$ nebo $x \equiv -1 \pmod{7}$. Zbývá tedy vyřešit dvě soustavy kongruencí:

$$\begin{aligned}
x &\equiv 1 \pmod{3},\\
x &\equiv 0 \pmod{5},\\
x &\equiv 2 \pmod{7}
\end{aligned}
\qquad \text{a} \qquad
\begin{aligned}
x &\equiv 1 \pmod{3},\\
x &\equiv 0 \pmod{5},\\
x &\equiv -1 \pmod{7}.
\end{aligned}$$

Protože první dvě kongruence jsou u obou soustav stejné, budeme se nejprve zabývat jimi. Ze druhé kongruence dostáváme $x = 5t$ pro $t \in \mathbb{Z}$, dosazením do první

$$5t \equiv 1 \pmod{3},$$

tedy $-t \equiv 1 \pmod 3$, odkud $t = -1 + 3s$ pro $s \in \mathbb{Z}$, odkud $x = -5 + 15s$. Dosaďme nejprve do třetí kongruence první soustavy:

$$-5 + 15s \equiv 2 \pmod 7,$$

odkud $s \equiv 0 \pmod 7$, tj. $s = 7r$ pro $r \in \mathbb{Z}$ a proto $x = -5 + 105r$. Dosadíme-li $x = -5 + 15s$ do třetí kongruence druhé soustavy, dostaneme

$$-5 + 15s \equiv -1 \pmod 7,$$

odkud $s \equiv 4 \pmod 7$, tj. $s = 4 + 7r$ pro $r \in \mathbb{Z}$, a proto $x = -5 + 15(4 + 7r) = 55 + 105r$. Celkem jsou tedy řešením dané kongruence $F(x) \equiv 0 \pmod{105}$ všechna celá čísla x, splňující $x \equiv -5 \pmod{105}$ nebo $x \equiv 55 \pmod{105}$. □

Postup pro řešení kongruencí, kde modulem je mocnina prvočísla, udává důkaz následující věty.

VĚTA 24 (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*

$$\begin{aligned} x &\equiv a \pmod p \\ f(x) &\equiv 0 \pmod{p^n} \end{aligned} \tag{26}$$

právě jedno řešení modulo p^n.

DŮKAZ. Indukcí vzhledem k n. Případ $n = 1$ je zřejmý. Nechť dále $n > 1$ a věta platí pro $n - 1$. Je-li x řešením (26) pro n, je řešením (26) i pro $n - 1$. Libovolné řešení (26) pro n je tedy tvaru

$$x = c_{n-1} + k \cdot p^{n-1}, \quad \text{kde } k \in \mathbb{Z}.$$

Je třeba zjistit, zda $f(c_{n-1} + k \cdot p^{n-1}) \equiv 0 \pmod{p^n}$. Víme, že $p^{n-1} \mid f(c_{n-1} + k \cdot p^{n-1})$ a užijme binomickou větu pro $f(x) = a_m x^m + \cdots + a_1 x + a_0$, kde $a_0, \ldots, a_m \in \mathbb{Z}$. Pak

$$(c_{n-1} + k \cdot p^{n-1})^i \equiv c_{n-1}^i + i \cdot c_{n-1}^{i-1} \cdot k p^{n-1} \pmod{p^n}.$$

Platí tedy

$$f(c_{n-1} + k \cdot p^{n-1}) \equiv f(c_{n-1}) + k \cdot p^{n-1} f'(c_{n-1}),$$

tj.

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

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

Protože $c_{n-1} \equiv a \pmod p$, dostaneme $f'(c_{n-1}) \equiv f'(a) \not\equiv 0 \pmod p$, tedy $(f'(c_{n-1}), p) = 1$. Užitím Věty 21 o řešitelnosti lineárních kongruencí dostáváme, že existuje právě jedno řešení $k \pmod p$ této kongruence a protože c_{n-1} bylo podle indukčního předpokladu jediné řešení modulo p^{n-1}, je číslo $c_{n-1} + k \cdot p^{n-1}$ jediným řešením (26) 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 $x = 4 + 9s$ a 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 $x \equiv 22 \pmod{27}$. □

Řešení obecných kongruencí vyššího stupně jsme tedy převedli na řešení kongruencí modulo prvočíslo. Ukazuje se, že zde je největší „kámen úrazu“, protože pro tyto kongruence žádný obecný postup (s výjimkou postupu podle Věty 20, tj. vyzkoušení všech možností) není znám. Uvedeme alespoň několik obecných tvrzení ohledně řešitelnosti a počtu řešení takových kongruencí a v dalších částech skript podrobnější výsledky v některých speciálních případech.

4.4. Kongruence s prvočíselným modulem.

VĚTA 25. *Buď p prvočíslo, $f(x) \in \mathbb{Z}[x]$. Libovolná kongruence $f(x) \equiv 0 \pmod p$ je ekvivalentní s kongruencí stupně nejvýše $p - 1$.*

DŮKAZ. Protože pro libovolné $a \in \mathbb{Z}$ platí $p \mid a^p - a$ (důsledek Malé Fermatovy věty), jsou řešením kongruence $x^p - x \equiv 0 \pmod p$ všechna celá čísla. Vydělíme-li polynom $f(x)$ se zbytkem polynomem $x^p - x$, dostaneme

$$f(x) = q(x) \cdot (x^p - x) + r(x)$$

pro vhodné $f(x), r(x) \in \mathbb{Z}$, kde stupeň $r(x)$ je menší než stupeň dělitele tedy než p. Dostáváme tak, že kongruence $r(x) \equiv 0 \pmod p$ je ekvivalentní kongruenci $f(x) \equiv 0 \pmod p$ a je přitom stupně nejvýše $p - 1$. □

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 $(27, 18) \nmid 3$.