Algebra — cvičení 3, řešení

2. (a) Spočtěte $3^{3^{3^{3^3}}} \mod 28$. Jelikož $\mathrm{NSD}(3, 28) = 1$, lze užít Eulerovu větu. Máme $\varphi(28) = \varphi(4)\varphi(7) = 2 \cdot 6 = 12$. Zbývá určit, kolik je $3^{3^{3^3}} \mod 12$. Nyní již ovšem nelze užít Eulerovu větu. Všimněme si ale, že $3 \cdot 3 \equiv -3 \,(\mathrm{mod}\, 12)$. V $\mathbb{Z}_{12}$ proto máme $3^k = (-1)^{k+1}3$ pro libovolné $k > 0$. Jelikož mocnina trojky je liché číslo, dostaneme $3^{3^{3^3}} \mod 12 = 3$. Dohromady tedy

$$3^{3^{3^{3^3}}} \mod 28 = 3^3 \mod 28 = 27.$$

2. (b) Spočtěte $3^{5^{7^{9^{11^{13}}}}} \mod 28$. Podobně jako v předchozím případu zjišťujeme, kolik je $5^{7^{9^{11^{13}}}} \mod 12$. Nyní už lze užít Eulerovu větu znovu, jelikož $\mathrm{NSD}(5, 12) = 1$. Nebo si můžeme všimnout, že $5 \cdot 5 \mod 12 = 1$, pročež $5^{\text{„liché číslo“}} \mod 12 = 5$. Dostáváme

$$3^{5^{7^{9^{11^{13}}}}} \mod 28 = 3^5 \mod 28 = (-1)3^2 \mod 28 = 19.$$

3. (b) Najděte všechna $x \in \mathbb{Z}$ splňující $2x + 1 \equiv 2 \pmod 3$, $3x + 2 \equiv 3 \pmod 4$ a $4x + 3 \equiv 2 \pmod 5$. Všimneme si, že $3, 4, 5$ jsou po dvou nesoudělná. Budeme tedy moci použít Čínskou zbytkovou větu poté, co si kongruence malinko upravíme, abychom měli vyjádřené x. Dostaneme po řadě $x \equiv 2 \,(\mathrm{mod}\, 3)$, $x \equiv 3 \,(\mathrm{mod}\, 4)$ a $x \equiv 1 \,(\mathrm{mod}\, 5)$. Řešíme jako vzorový příklad on-line minulý týden. V $\mathbb{Z}_{60}$ dostaneme jediné řešení, a to 11. Množina všech řešení dané soustavy kongruencí potom je $\{60m + 11;\, m \in \mathbb{Z}\}$.

3. (c) Najděte všechna $x \in \mathbb{Z}$ splňující $10x \equiv 6 \pmod{32}$ a $3x \equiv 1 \pmod 5$. Nejprve upravíme na ekvivalentní soustavu kongruencí: $5x \equiv 3 \,(\mathrm{mod}\, 16)$ a $x \equiv 2 \,(\mathrm{mod}\, 5)$. První z nich se dále ještě ekvivalentně upraví (vynásobením třinácti) na $x \equiv 7 \,(\mathrm{mod}\, 16)$. Řešením obou dvou kongruencí je tedy 7. Z Čínské zbytkové věty pak plyne, že jde o jediné řešení v $\mathbb{Z}_{80}$. Soustavu proto řeší právě všechna celá čísla tvaru $80k + 7$, kde $k \in \mathbb{Z}$.

4. (a) Najděte všechna $x \in \mathbb{Z}$ splňující $x^2 \equiv 1 \pmod 3$ a $x^2 \equiv 1 \pmod 7$. První kongruence je ekvivalentní disjunkci $x \equiv 1 \pmod 3$ *nebo* $x \equiv 2 \pmod 3$. To lze hezky kompaktně zapsat jako $3 \nmid x$. Druhá kongruence je ekvivalentní $x \equiv \pm 1 \pmod 7$. Všechna řešení v $\mathbb{Z}_{21}$ tedy jsou $1, 8, 13, 20$. Množina všech celočíselných řešení proto je

$$\{21m + n;\, m \in \mathbb{Z}, n \in \{1, 8, 13, 20\}\}.$$

4. (b) Najděte všechna $x \in \mathbb{Z}$ splňující $x^2 \equiv -1 \pmod{65}$. Pamatujete si na důkaz ČZV? Jeho důsledkem v našem specifickém případě je, že zobrazení $f : \mathbb{Z}_{65} \to \mathbb{Z}_5 \times \mathbb{Z}_{13}$ definované vztahem $f(a) = (a \mod 5, a \mod 13)$ je bijekce (dokonce izomorfismus okruhů). Ekvivalentně proto můžeme řešit soustavu kongruencí $x^2 \equiv -1 \pmod 5$ a $x^2 \equiv -1 \pmod{13}$. Polynom $x^2 + 1$ má v tělese $\mathbb{Z}_5$ kořeny 2 a $-2 = 3$; naproti tomu v $\mathbb{Z}_{13}$ jde o kořeny 5 a $-5 = 8$. Tím dostáváme všechna řešení v $\mathbb{Z}_{65}$ jakožto $f^{-1}(2, 5), f^{-1}(2, 8), f^{-1}(3, 5), f^{-1}(3, 8)$. Konkrétně jde o čísla $57, 47, -47 = 18, -57 = 8$. Všechna celočíselná řešení pak mají tvar $65m + n$, kde $m \in \mathbb{Z}$ a $n \in \{8, 18, 47, 57\}$.

5. Najděte všechna $x \in \mathbb{Z}$ splňující $x^{11} \equiv 2 \pmod 5$ a $x^8 \equiv 1 \pmod 7$. Jistě nesmí být $5 \mid x$, ani $7 \mid x$. Ve všech ostatních případech můžeme použít Eulerovu větu. Jelikož

$\varphi(5) = 4$ a $\varphi(7) = 6$, Eulerova věta říká, že $x^4 \equiv 1 \pmod 5$ a $x^6 \equiv 1 \pmod 7$. Takže vynásobíme-li obě strany první kongruence x, dostaneme $1 \equiv 2x \pmod 5$, ekvivalentně $x \equiv 3 \pmod 5$. U druhé kongruence potom obdržíme $x^2 \equiv 1 \pmod 7$, což dává $x \equiv \pm 1 \pmod 7$. Dostáváme, že všechna řešení v $\mathbb{Z}_{35}$ jsou $8, 13$; všechna celočíselná potom tvaru $35m + n$, kde $m \in \mathbb{Z}$ a $n \in \{8, 13\}$.

7. Najděte všechna $x, y \in \mathbb{Z}$ splňující $x^6 + x + xy \equiv 1 \pmod 7$. Předně jistě $7 \nmid x$. Eulerova věta potom říká, že $x^6 \equiv 1 \pmod 7$. Tím se nám původní kongruence upraví na $7 \mid x(1 + y)$. Víme ale, že $7 \nmid x$, pročež $7 \mid 1 + y$, ekvivalentně $y \equiv 6 \pmod 7$. Množina všech řešení je tedy rovna $\{(x, y) \in \mathbb{Z}^2;\ 7 \nmid x \ \&\ y \equiv 6 \pmod 7\}$.

8. Určete poslední tři cifry čísla 249^{19}. Potřebujeme spočítat $249^{19} \mod 1000$. Sice máme $\mathrm{NSD}(249, 1000) = 1$, takže lze užít Eulerovu větu, ale vzhledem k tomu, že $\varphi(1000) = 16 \cdot 25 = 400$, moc si při výpočtu nepomůžeme. Řešením je zapojit navíc ČZV. Napíšeme si $1000 = 8 \cdot 125$ a budeme počítat $249^{19} \mod 8$ a $249^{19} \mod 125$. V prvním případě dostaneme $1^{19} = 1$ a ve druhém $(-1)^{19} \mod 125 = 124$. Hledaným řešením je proto právě takové $x \in \mathbb{Z}_{1000}$, pro něž $x \equiv 1 \pmod 8$ a $x \equiv -1 \pmod{125}$. Tyto vlastnosti má (čirou náhodou) číslo 249.

9. Najděte všechna $x \in \mathbb{Z}_{77}$ taková, že (v $\mathbb{Z}_{77}$) platí $x^2 + 8x = 62$. Přičtením 16 k oběma stranám dostaneme $(x + 4)^2 = 78 = 1$. Po substituci $y = x + 4$ tedy hledáme kořeny polynomu $y^2 - 1$ v $\mathbb{Z}_{77}$. Tím jsme se dostali do analogické situace jako v **4 (b)**. Řešením jsou taková $y \in \mathbb{Z}_{77}$, pro něž $y \equiv \pm 1 \pmod 7$ a $y \equiv \pm 1 \pmod{11}$. Konkrétně tedy $y \in \{1, 34, -34 = 43, -1 = 76\}$. Hledanými x jsou proto $-3 = 74, 30, 39, 72$.

10. Spočtěte $130^{9^{3^{2021^{123}}}} \mod 221$. Jelikož $\mathrm{NSD}(130, 221) = 13$, nelze užít Eulerovu větu. Označme $h = 130^{9^{3^{2021^{123}}}}$. Jelikož $221 = 13 \cdot 17$, budeme počítat $h \bmod 13$ a $h \bmod 17$. V prvním případě dostáváme ihned $h \bmod 13 = 0$. V druhém už můžeme použít Eulerovu větu. Jest $\varphi(17) = 16$, bude nás tedy zajímat $9^{3^{2021^{123}}} \mod 16$. Při další eulerovské iteraci pak $3^{2021^{123}} \bmod 8 = 3^{\text{„liché číslo“}} \bmod 8 = 3$. Při backtrackingu posléze obdržíme $9^{3^{2021^{123}}} \bmod 16 = 9^3 \bmod 16 = 9$.

Máme $h \bmod 17 = 130^9 \bmod 17 = 11^9 \bmod 17 = (-6)^9 \bmod 17 = (-6)2^4 \bmod 17 = 6$. Hledáme tedy $x \in \mathbb{Z}_{221}$ takové, že $x \equiv 0 \,(\mathrm{mod}\, 13)$ a $x \equiv 6 \,(\mathrm{mod}\, 17)$. Z ČZV víme, že je takové x právě jedno. Konkrétně se jedná o $x = 91$.

11. (a) Pro $\{p, q\} = \{2, 3\}$ nic takového samozřejmě nedokážete. V zadání by mělo správně být, že se jedná o dvě lichá prvočísla. Pak je $x \in \mathbb{Z}_{pq}$ kořenem právě tehdy, když $pq \mid x(x + 1)(x + 2)$. To je dále ekvivalentní tomu, že existují ne nutně různá $u, v \in \{x, x+1, x+2\}$ taková, že $p \mid u$ a $q \mid v$. Z ČZV máme právě jedno řešení x poslední dvojice podmínek pro každou volbu $u, v \in \{x, x + 1, x + 2\}$. Tím, že jsou obě prvočísla lichá, je toto přiřazení prosté, tj. různé dvojice (u, v) dávají různá x. Navíc různých dvojic (u, v) je 9, což jsme chtěli dokázat.

11. (b) Neexistují. Předpokládejme, že by existovala nějaká taková volba a, b. Označme $x^2 + ax + b = (x - c)(x - d)$, kde $c, d \in \mathbb{Z}_{pq}$. To lze, neboť tento polynom má v $\mathbb{Z}_{pq}$ nějaký kořen c a d je jím ihned jednoznačně určeno. Opět víme, že $x \in \mathbb{Z}_{pq}$ je kořenem právě tehdy, když $pq \mid (x - c)(x - d)$. Podobným argumentem jako v předchozím případě se ukáže, že možnosti pro dvojice (u, v) jsou tentokrát čtyři. Tyto dávají čtyři různé kořeny

x, pokud je $c \not\equiv d \pmod{p}$ a současně $c \not\equiv d \pmod{q}$. V opačném případě jsou nejvýše dva kořeny. Když totiž například platí $c \equiv d \pmod{q}$, pak $q \mid x - c \iff q \mid x - d$.

12. Dokažte, že $\lim_{n\to\infty} \varphi(n) = \infty$. Z hodnoty Eulerovy funkce v prvočíslech (a z toho, že prvočísel je nekonečně mnoho) dostáváme snadno, že $\limsup_{n\to\infty} \varphi(n) = \infty$. Zajímavější je ukázat totéž pro limes inferior.

K tomu si stačí uvědomit, jak vypadá vzorec pro výpočet φ a že $(p-1)^2 > p$ pro libovolné liché prvočíslo. V důsledku pak platí pro liché n, že $\varphi(n)^2 \geq n$. Je-li $n = 2^z$ pro $z \in \mathbb{N}$, potom $\varphi(n) = n/2$. Dohromady pak pro libovolné $n \in \mathbb{N}$ platí odhad $\varphi(n)^2 \geq n/2$, takže

$$\varphi(n) \geq \sqrt{\frac{n}{2}}.$$