27.2.

1 Pollardova ρ-metoda

1.1. Určete periodu a preperiodu posloupnosti $\{s_n\}_{n\geq 0}$ určené polynomiálním zobrazením $f(x) = ax + b \in \mathbb{Z}_p$ pro $x \in \mathbb{Z}_p$, kde $p \in \mathbb{P}$, tj. $s_0 \in \mathbb{Z}_p$ a $s_{n+1} = f(s_n)$, pokud

(a) $a = 1$, $b \in \mathbb{Z}_p$,

(b) $a \in \mathbb{Z}_p^*$, $b = 0$.

(a) Nejprve vyjádříme přímo hodnotu $s_n = s_0 + nb$. Pro $b = 0$ je posloupnost konstantní, a proto má preperiodu $m = 0$ a periodu $t = 1$.

Pokud $b \neq 0$, máme $ib \neq 0$ pro $i = 1, \ldots, p-1$ a $pb = 0$, což znamená, že má posloupnost preperiodu $m = 0$ a periodu $t = p$.

Pollardova ρ-metoda bude v případě $b = 0$ úspěšná, jen tehdy, kdy $b = 0$ vzniklo modulením nenulové hodnoty $B \in \mathbb{Z}_N$, tedy když jsme uhodli násobek vlastního dělitele $p \mid N$, což se nedá očekávat často. V případě $b \neq 0$ je součet $t + m = p$, tedy v případech obou algoritmů musíme provést maximální možný počet iterací (p vně)

(b) Opět snadno určíme nerekurentní vzorec $s_n = a^n s_0$.Je-li $s_0 = 0$, posloupnost je konstantně nulová, tedy posloupnost s preperiodou $m = 0$ a periodou $t = 1$.

Pokud $s_0 \neq 0$, vidíme, že preperioda posloupnosti je nulová, neboť $a^{p-1} = 1$ a že nejmenší přirozené číslo t splňující $s_0 = s_0 a^t$, tedy perioda posloupnosti, je rovno právě řádu $o_{\mathbb{Z}_p^*}(a)$.

Všimněme si, že například pro bezpečné prvočíslo $p = 2q + 1$, kde $q \in \mathbb{P}$ obsahuje grupa $\mathbb{Z}_p^*$ jeden prvek řádu 1 a jeden prvek řádu 2, které pro Pollardovu ρ-metodu nejsou dobře použitelné a pak $(q-1)$ prvků řádu q a stejný pročet prvků řádu $2q$, které říkají, že procházka po různých číslech posloupnosti v Pollardových algoritmech by byla opět příliš dlouhá. □

6.3.

1.2. Označme $f_{a,b} : \mathbb{Z}_p \to \mathbb{Z}_p$ afinní transformace daná vztahem $f_{a,b}(x) = ax + b$ a $\mathrm{Aff}(\mathbb{Z}_p) = \{f_{a,b} \mid a \in \mathbb{Z}_p^*, b \in \mathbb{Z}_p\}$. Dokažte $\mathrm{Aff}(\mathbb{Z}_p)$ je podgrupou symetrické grupy $S(\mathbb{Z}_p)$ pro $p \in \mathbb{P}$, tedy grupa.

Stačí si rozmyslet, že

$$f_{1,0} = \mathrm{id}, \quad f_{a,b} f_{c,d} = f_{ac,ad+b}, \quad f_{a,b}^{-1} = f_{a^{-1},-a^{-1}b}$$

odkud plyne, že $f_{a,b}$ je invertibilní, tedy permutace na $\mathbb{Z}_p$ a množina $\mathrm{Aff}(\mathbb{Z}_p)$ je uzavřená na operace skládání a invertování a jedná s etudíž o podgrupu. □

1.3. Určete periodu a preperiodu posloupnosti $\{s_n\}_{n\geq 0}$ dané polynomiálním zobrazením $f : \mathbb{Z}_p \to \mathbb{Z}_p$ pro $p \in \mathbb{P}$, pokud

(a) $f(x) = ax + b$, $a, b \in \mathbb{Z}_p^*$ a $a \neq 1$.

(b) $f(x) = x^2$.

(a) S využitím předchozí úlohy najdeme c tak, aby $f_{1,c} f_{a,b} f_{1,c}^{-1} = f_{u,0}$. Nejprve spočteme

$$f_{1,c} f_{a,b} f_{1,c}^{-1} = f_{1,c} f_{a,b} f_{1,-c} = f_{a,b+c} f_{1,-c} = f_{a,-ac+b+c},$$

z podmínky $-ac + b + c = 0$ plyne, že $c = b(a-1)^{-1}$.

Označme $g = f_{1,c}$, $f = f_{a,b}$ a $h = gfg^{-1}$. Protože $s_n = f^n(s_0) = g^{-1}h^n(g(s_0))$, vidíme, že $s_i = s_j$, právě když $h^i(g(s_0)) = h^j(g(s_0))$, tedy perioda i preperioda posloupností $\{s_n\}_{n\geq 0}$ a $\{h^n(g(s_0))\}_{n\geq 0}$ je stejná. Nyní zbývá využít 1.1, která říká, že pro $s_0 = -c$ jsou obě posloupnosti konstantní , tedy mají preperiodu $m = 0$ a periodu $t = 1$ a pro $s_0 \neq -c$ mají obě posloupnosti opět preperiodu $m = 0$ a periodu $t = o_{\mathbb{Z}_p^*}(a)$.

(b) Nejprve si uvědomíme, že ze vztahu $s_{n+1} = s_n^2$ okamžitě plyne nerekurentní vzoreček $s_n = s_0^{2^n}$. Dále si všimneme, že pro $s_0 = 0, 1$ je získaní posloupnost konstantní, tedy s preperiodou 0 a periodou 1 a můžeme se tak omezit na na hledáme nejmenšího i a nejmenšího $j > i$, pro která platí , že $s_i = s_j$ za předpokladu, že $s_0 \neq 0, 1$. Najdeme-li je, pak i bude právě preperioda a $j - i$ perioda této posloupnosti. Uvážíme řadu ekvivalentních překladů podmínky v grupě $\mathbb{Z}_p^*$

$$s_i = s_j \Leftrightarrow s_0^{2^i} = s_0^{2^j} \Leftrightarrow s_0^{2^j - 2^i} = 1 \Leftrightarrow s_0^{2^i(2^{j-i}-1)} = 1 \Leftrightarrow o_{\mathbb{Z}_p^*}(s_0) \mid 2^i(2^{j-i} - 1),$$

kde poslední ekvivalence plyne z faktu, že exponentem prvku jsou právě násobky řádu prvku. Nyní vyjádříme $o_{\mathbb{Z}_p^*}(s_0) = 2^e m$ pomocí $e = v_2(o_{\mathbb{Z}_p^*}(s_0))$, kde m je liché. Potom dostáváme ekvivalence

$$o_{\mathbb{Z}_p^*}(s_0) \mid 2^i(2^{j-i} - 1) \Leftrightarrow i \geq e,\ m \mid 2^{j-i} \Leftrightarrow i \geq e,\ 2^{j-i} \equiv 1 \pmod{m}.$$

Minimálních hodnot tedy dosahujeme pro preperiodu $i = e$ a periodu $j - i = o_{\mathbb{Z}_m^*}(2)$. □

13.3.

2 B-mocná čísla

2.1. Určete hodnotu e_B a spočítejte všechna čísla, která jsou B-mocná, pokud (a) $B = 4$, (b) $B = 10$.

(a) Vidíme, že právě prvočísla $2, 3$ jsou menší nebo rovna než 4, proto

$$e_4 = 2^{\lfloor \log_2(4) \rfloor} 3^{\lfloor \log_3(4) \rfloor} = 2^2 \cdot 3^1 = 12.$$

Z přednášky víme, že B-mocná čísla dělí e_B a snadno nahlédneme, že každý dělitěl e_B je B-mocný. Proto množina $\{2^i \cdot 3^j \mid i \in \mathbb{Z}_3, j \in \mathbb{Z}_2\}$ obsahuje právě všechna 4-mocná čísla, kterých je $3 \cdot 2 = 6$.

(b) Podobně jako v (a) nahlédnme, že právě prvočísla $2, 3, 5, 7 \leq 10$ a

$$e_{10} = 2^{\lfloor \log_2(10) \rfloor} 3^{\lfloor \log_3(10) \rfloor} 5^{\lfloor \log_5(10) \rfloor} 7^{\lfloor \log_7(10) \rfloor} = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520.$$

Dále množina všech 10-mocných čísla $\{2^i \cdot 3^j \cdot 5^k \cdot 7^l \mid i \in \mathbb{Z}_4, j \in \mathbb{Z}_3, k, l \in \mathbb{Z}_2\}$ obsahuje $48 = 4 \cdot 3 \cdot 2^2$ různých hodnot. □

2.2. Pro (a) $B = 4$, (b) $B = 10$ najděte všechna prvočísla $p \leq 20$, pro která jsou B-mocná čísla $p - 1$.

(a) Hledáme prvočísla $p \leq 20$, pro něž $p - 1 \mid 12$. Vidíme, že jde právě o prvočísla

$$1 + 1 = 2,\ 2 + 1 = 3,\ 4 + 1 = 5,\ 6 + 1 = 7,\ 12 + 1 = 13.$$

(b) Kromě všech hodnot z (a) ještě máme prvočísla

$$10 + 1 = 1,\ 18 + 1 = 19.$$

□

2.3. Pro (a) $B = 4$, (b) $B = 10$ najděte všechna prvočísla $p \leq 20$, pro která jsou B-mocná čísla $p + 1$.

(a) Tentokrát hledáme prvočísla $p \leq 20$, pro něž $p + 1 \mid 12$, jimž jsou

$$3 - 1 = 2,\ 4 - 1 = 3,\ 6 - 1 = 5,\ 12 - 1 = 11.$$

(b) Opět k prvočíslům z (a) přidáme prvočísla

$$8 - 1 = 7,\ 18 - 1 = 17,\ 20 - 1 = 19.$$

□

Připomeňme, že číslo $F_n = 2^{2^n} + 1$ se nazývá Fermatovo, zjevně $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ jsou prvočísla.

2.4. Dokažte, že F_4 je prvočíslo.

Protože $F_4 - 1 = 2^{16} \equiv -1 \pmod{F_4}$, snadno uvážíme, že prvočíselný dělitel $p > 2$ čísla F_4 splňuje kongruence

$$2^{16} \equiv -1 \pmod{p} \quad \text{a} \quad 2^{32} \equiv 1 \pmod{p},$$

což znamená, že řád prvku 2 je v grupě $\mathbb{Z}_p^*$ právě 32. O každém prvku grupy $\mathbb{Z}_p^*$ dále z Lagrangeovy věty víme, že je exponentu $p-1$, proto $32 \mid p-1$, tedy $p = 32k + 1$ pro nějaké k. Případný vlastní dělitel čísla F_4 musí být nejvýše $\sqrt{F_4} < 2^8 + 1 = F_3 = 257$, proto stačí uvážit prvočísla z hodnot $32k + 1$ pro $k = 1, \ldots 7$, jimiž jsou, jak snadno spočítáme, pouze hodnoty 97 a 193. U obou snadno spočítáme, že nejde o dělitele čísla F_4, proto je F_4 prvočíslo. □

2.5. Ukažte pomocí vhodné varianty Pollardovy $p - 1$-metody, že je F_5 složené.

Protože známe prvočíselný faktor 641 čísla F_5, můžeme si uvědomit, že $641 - 1 = 2^7 \cdot 5$ je exponent každého prvku $\mathbb{Z}_{641}^*$, tedy $a^{640} \equiv 1 \pmod{641}$ pro každé $a \in \mathbb{Z}_{F_5}^*$. Zvolíme tedy hodnotu $B = 2^7 = 128$ a upravíme 2.variantu Pollardovy $p - 1$-metody tak, že místo hodnoty e_{128} pracující se součinem příliš mnoha pročísel uvážíme hodnotu $\hat{e}_{128} = 2^7 \cdot 3^4 \cdot 5^3$, o níž víme, že $640 \mid \hat{e}_{128}$.

Zároveň si vzpomeňme , že $2^{64} \equiv 1 \pmod{F_5}$, což znamená, že

$$2^{\hat{e}_{128}} \equiv (2^{64})^{2 \cdot 81 \cdot 125} \equiv 1 \pmod{F_4}.$$

Protože $2^{\hat{e}_{128}} \equiv 1 \pmod{640}$ bude $\gcd(2^{\hat{e}_{128}} - 1, F_5) = F_5$, tudíž pomocí $a = 2$ prvočíselný dělitel 641 nenajdeme. Proto zvolíme $a = 3$ a počítáme

$$a_1 = (3^{81}) \bmod F_5 = 1918862017, \quad a_2 = (a_1) \bmod F_5 = 4292273029.$$

Nyní budeme testovat největší společné dělitele $\gcd(a_i - 1, F_5)$ a počítat $a_{i+1} = (a_i^2) \bmod F_5$:

$$\begin{aligned}
\gcd(a_2 - 1, F_5) = 1, &\quad a_3 = (a_2^2) \bmod F_5 = 585323894, \\
\gcd(a_3 - 1, F_5) = 1, &\quad a_4 = (a_3^2) \bmod F_5 = 4278871505, \\
\gcd(a_4 - 1, F_5) = 1, &\quad a_5 = (a_4^2) \bmod F_5 = 2092752224, \\
\gcd(a_5 - 1, F_5) = 1, &\quad a_6 = (a_5^2) \bmod F_5 = 2812764726, \\
\gcd(a_6 - 1, F_5) = 1, &\quad a_7 = (a_6^2) \bmod F_5 = 1314231249, \\
\gcd(a_7 - 1, F_5) = 1, &\quad a_8 = (a_7^2) \bmod F_5 = 3257626099, \\
\gcd(a_8 - 1, F_5) = 1, &\quad a_9 = (a_8^2) \bmod F_5 = 3616864936.
\end{aligned}$$

Nyní už dostáváme, že $\gcd(3^{\hat{e}_{128}} - 1, F_5) = \gcd(a_9 - 1, F_5) = 641$, čímž jsme ověřili, že je F_5 složené číslo. □

2.6. Nechť $P = (0, 1)$. Víte-li, že $|E_{1,1}(\mathbb{Z}_7)| = 5$ a $|E_{1,1}(\mathbb{Z}_{11})| = 14$,

(a) určete řád prvku P v grupách $E_{1,1}(\mathbb{Z}_7)$ a $E_{1,1}(\mathbb{Z}_{11})$

(b) spočítejte velikost množiny $|E_{1,1}(\mathbb{Z}_{77})|$,

(c) spočítejte hodnoty nebo najděte kolizi při výpočtu $Q = P \oplus P$, $R = Q \oplus Q$, $S = R \oplus P$ v ECM na množině $|E_{1,1}(\mathbb{Z}_{77})|$,

(d) určete, co je výsledkem výpočtu z (c) v grupách $|E_{1,1}(\mathbb{Z}_7)|$ a $|E_{1,1}(\mathbb{Z}_{11})|$.

(a) Protože $P \neq o$ a grupa $E_{1,1}(\mathbb{Z}_7)$ je prvočíselného řádu 5, musí být prvek P generátor, tedy je řádu 5.

V grupě $E_{1,1}(\mathbb{Z}_{11})$ řádu 14 mohou být prvky řádu 1, 2, 7 a 14 (i v tomto případě se jedná o cyklickou grupu), proto stačí spočítat $[2]P$ a $[7]P$, abychom řád určili. Označíme-li $(\gamma_1, \gamma_2) = [2]P$, pak

$$\gamma_1 = \lambda^2 - 2 \cdot 0 = 5^2 - 2 \cdot 0 = 3, \text{ protože } \lambda = \frac{3 \cdot 0^2 + 1}{2 \cdot 1} = -5,$$

$$\gamma_2 = \lambda(0 - \gamma_1) - 1 = -5(0 - 3) - 1 = 3, \text{ tudíž } [2]P = (3, 3).$$

Dále pro $(\gamma_1, \gamma_2) = [4]P = [2](3, 3)$ dostáváme $\lambda = \frac{3 \cdot 3^2 + 1}{2 \cdot 3} = 1$,

$$\gamma_1 = \lambda^2 - 2 \cdot 3 = 1^2 - 6 = -5, \ \gamma_2 = \lambda(3 - \gamma_1) - 3 = 1(3 + 5) - 3 = 5,$$

proto $[4]P = (-5, 5)$.

Nyní spočítáme $(\gamma_1, \gamma_2) = [3]P = P \oplus [2]P = (0, 1) \oplus (3, 3)$:

$$\gamma_1 = \lambda^2 - 0 - 3 = 3^2 - 3 = -5, \text{ protože } \lambda = \frac{1 - 3}{0 - 3} = -3,$$

$$\gamma_2 = \lambda(0 - \gamma_1) + 5 = -3(0 + 5) - 1 = -5, \text{ a proto } [3]P = (-5, -5).$$

Nyní vidíme, že $[4]P = \ominus[3]P$, což znamená, že $[7]P = o$, a protože jsme už zjistili, že $P \neq o$ a $P \neq \ominus P$, má prvek P v grupě $E_{1,1}(\mathbb{Z}_{11})$ řád 7.

(b) Uvědomíme si, že nám zobrazení

$$\Psi : \{(x, y) \in \mathbb{Z}_{77}^2 \mid y^2 \equiv x^3 + x + 1 \pmod{77}\} \to$$

$$\{(x, y) \in \mathbb{Z}_7^2 \mid y^2 \equiv x^3 + x + 1 \pmod{7}\} \times \{(x, y) \in \mathbb{Z}_{11}^2 \mid y^2 \equiv x^3 + x + 1 \pmod{11}\}$$

dané předpisem $\Psi(x, y) = ((x) \bmod 7, (y) \bmod 7), (x) \bmod 11, (y) \bmod 11))$ díky čínské větě o zbytcích dává bijekci. Uvědomíme-li si, že vlevo máme

množinu $E_{1,1}(\mathbb{Z}_{77}) \setminus \{o\}$ a vpravo kartézský součin množin $E_{1,1}(\mathbb{Z}_{77}) \setminus \{o\}$ a $E_{1,1}(\mathbb{Z}_{11}) \setminus \{o\}$ dostáváme

$$|E_{1,1}(\mathbb{Z}_{77})| = |(E_{1,1}(\mathbb{Z}_{77}) \setminus \{o\}) \times (E_{1,1}(\mathbb{Z}_{11}) \setminus \{o\})| + 1 = 4 \cdot 13 + 1 = 53.$$

(c) Budeme postupovat jako v úloze (a). Nejprve pro dublování $(\gamma_1, \gamma_2) = [2]P$ na $E_{1,1}(\mathbb{Z}_{77})$ spočítáme $\lambda = \frac{3 \cdot 0^2 + 1}{2 \cdot 1} = 2^1 = -38$ a poté určíme

$$\gamma_1 = \lambda^2 - 2 \cdot 0 = 38^2 - 2 \cdot 0 = -19, \ \gamma_2 = \lambda(0 - \gamma_1) - 1 = -38(0 + 19) - 1 = -30.$$

Našli jsme tedy $Q = (-19, -30)$. Opět dublujeme $(\gamma_1, \gamma_2) = R = [2]Q$, tedy spočteme směrnici příslušné tečny $\lambda = \frac{3 \cdot 19^2 + 1}{2 \cdot (-30)} = \frac{6}{-60} = \frac{-8}{80} = \frac{69}{3} = 23$ a poté

$$\gamma_1 = 23^2 - 2 \cdot (-19) = 28, \ \gamma_2 = 23(-19 - 28) + 30 = 27,$$

tedy $R = (28, 27)$ a konečně hledáme-li $P \oplus R$ pak při pokusu o spočtení sečného λ vidíme, že $\gcd(28, 77) = 7$, tedy jsme dostali kolizi výpočtu a vlastní dělitel 7 čísla 77.

(d) Protože v $|E_{1,1}(\mathbb{Z}_7)|$ i v $|E_{1,1}(\mathbb{Z}_{11})|$ při výpočtu $Q = P \oplus P$, $S = Q \oplus Q$, $R = S \oplus P$ využíváme tentýž vzorec při jiném modulu, který dělí pvodní modul 77, stačí výsledek upravit příslušnám modulem. Tedy $E_{1,1}(\mathbb{Z}_7)$ dostáváme

$$Q = ((-19)) \bmod 7, (-30) \bmod 7) = (2, -2)$$
$$R = ((28)) \bmod 7, (27) \bmod 7) = (0, -1)$$

a okamžitě vidíme, že $R = \ominus P$, proto $S = R \oplus P = [5]P = o$, což je v souladu se zjištěním o řádu prvku P z úlohy (a).

Hodnoty Q a R v $E_{1,1}(\mathbb{Z}_{11})$ už jsem určili ve výpočtu (a), tedy zopakujme, že máme

$$Q = ((-19)) \bmod 11, (-30) \bmod 11) = (3, 3)$$
$$R = ((28)) \bmod 11, (27) \bmod 11) = (-5, 5)$$

a zbývá nám buď standardním postupem spočítat $(\gamma_1, \gamma_2) = S = R \oplus P = [5]P$, kdy směrnice sečny je $\lambda = \frac{5-1}{-5-0} = \frac{2}{3} = -3$ a

$$\gamma_1 = 3^2 + 5 - 0 = 3, \quad \gamma_2 = -3(0 - 3) - 1 = -3,$$

nebo si uvědomíme, že ze znalosti řádu prvku P a hodnoty $[2]P = (3, 3)$, které jsme zjistili v (a) plyne, že $[5]P = \ominus[2]P = \ominus(3, 3) = (3, -3)$. □

2.7. Víte-li, že $|E_{1,1}(\mathbb{Z}_{199})| = 218$, $|E_{1,1}(\mathbb{Z}_{269})| = 294$ a $53531 = 199 \cdot 269$, vysvětlete, proč pro e_{49} a $P = (0, 1) \in E_{1,1}(\mathbb{Z}_{53531})$ můžeme očekávat, že ECM nalezne netriviání dělitel čísla 53531.

□

3 Odmocniny modulo n

3.1. Nechť $p \in \mathbb{P}$ liché splňuje $p \equiv 3 \pmod 4$ a $a \in \mathbb{Z}_p^*$. Pokud pro $a \in \mathbb{Z}_p^*$ existuje řešení rovnice $x^2 = a$, ověřte, že je právě tvaru $x = \pm a^{\frac{p+1}{4}}$.

Uvědomíme si, že $4 \mid p+1$ a že řešení rovnice $x^2 = a$ existuje, právě když $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = 1$. Proto

$$(a^{\frac{p+1}{4}})^2 = a^{\frac{p+1}{2}} = a,$$

proto $x = \pm a^{\frac{p+1}{4}}$. □

3.2. Nechť $p = 8k + 5 \in \mathbb{P}$ pro $k \in \mathbb{N}$ (tedy $p \equiv 5 \pmod 8$). a $a \in \mathbb{Z}_p^*$. Dokažte, že pokud existuje řešení rovnice $x^2 = a \in \mathbb{Z}_p^*$, je právě buď tvaru $x = \pm a^{k+1}$ nebo $x = \pm 2^{2k+1} a^{k+1}$.

Je-li a kvadratický zbytek modulo p, pak opět pro $\frac{p-1}{2} = 4k + 2$ platí, že $a^{4k+2} = 1$, tudíž a^{2k+1} je prvek exponentu 2, a proto $a^{2k+1} = \pm 1$.

Pokud $a^{2k+1} = 1$, pak $a^{2k+2} = a$, a proto je řešením naší rovnice $x = \pm a^{k+1}$.

Jestliže $a^{2k+1} = -1$, vzpomeneme si, že $2^{4k+2} = \left(\frac{2}{p}\right) = -1$, neboť 2 je kvadratický zbytek modulo prvočíslo p, právě když $p \equiv \pm 1 \pmod 8$, což znamená, že $2^{4k+2} a^{2k+1} = 1$, proto $2^{4k+2} a^{2k+2} = a$ a $x = \pm 2^{2k+1} a^{k+1}$ je hledaným řešením.

□

3.3. Najděte všechna řešení rovnice $x^2 = a$ pro $a \in \mathbb{Z}_p^*$ pro

(a) $p = 31$, $a = 20$,

(b) $p = 31$, $a = 11$,

(c) $p = 101$, $a = 24$,

(d) $p = 101$, $a = 70$.

Protože $31 \equiv 3 \pmod 4$ stačí v příkladech (a), (b) využít výsledek úlohy 3.1, spočítat $x = \pm a^{k+1}$ a ověřit, zda opravdu $x^2 = a$ (nebo předem zjistit, zda je a kvadratický zbytek):

(a) $x = 20^{\frac{32}{4}} = (-11)^8 = \pm(-3)^4 = 12$ a $x^2 = 20$, proto $x = \pm 12$.

(b) $x = \pm 11^{\frac{32}{4}} = \pm(-3)^4 = \pm 12$ a $x^2 \neq 11$, tedy rovnice nemá řešení.

V úlohách (c) a (d) využijeme analogicky k předchozím řešením výsledku 3.2, neboť $101 \equiv 5 \pmod 8$ a $101 = 8k + 5$ pro $k = 12$. Nejprve v $\mathbb{Z}_{101}$ spočteme $2^{2k+1} = 2^{25} = 10$, poté spočítáme $y = a^{k+1}$. Pokud $y^2 = a$, budeme mít řešení $\pm y$. V opačném případě zjistíme, zda $-y^2 = a$, tedy zda $(2^{25}y)^2 = (10y) = a$, a pokud ano, bude řešním úlohy $\pm 10y$, jinak úloha řešení mít nebude.

(c) Počítáme $y = 24^{k+1} = 24^{13} = -23$, a protože $y^2 = 24$, máme řešení $x = \pm 23$.

(d) Nyní $y = 70^{13} = 43$, a protože $y^2 = 31 = -70$, vidíme, že řešení existuje a je nutně tvaru $x = \pm 10 \cdot 43 = \pm 26$. □

3.4. Najděte v tělese $\mathbb{Z}_{101}$ všechny kořeny polynomu $3x^2 + 7x - 27$.

Nejprve spočítáme determinant polynomu $7^2 + 4 \cdot 3 \cdot 27 = 70$. V úloze 3.3(d) už jsme našli $\sqrt{70} = \pm 26$, nyní zbývá využít klasický vzoreček

$$x = -\frac{7}{6} \pm \frac{26}{6} = -7 \cdot 17 \pm 26 \cdot 17 = -18 \pm 38.$$

Zjistili jsme, že polynom $3x^2 + 7x - 27$ má v $\mathbb{Z}_{101}$ kořeny 20 a 45. □