ALGEBRAICKÉ A ČÍSELNĚ TEORETICKÉ POZADÍ ELIPTICKÉ KRYPTOGRAFIE S VYBRANÝMI ALGORITMY, ZEJMÉNA PRO URČENÍ ŘÁDU ELIPTICKÉ KŘIVKY

MIROSLAV KUREŠ

Abstrakt. Článek přináší především přehled vybraných výsledků z algebry (a částečně i z teorie čísel), které jsou nezbytné pro studium eliptických křivek nad konečnými poli. Motivací pro takové studium je kryptografie založená na eliptických křivkách (stručněji eliptická kryptografie nebo jen ECC), která se v posledních letech bouřlivě rozvíjí. Obsah článku vychází z autorových přednášek na Semináři z aplikované geometrie Ústavu matematiky FSI VUT v Brně v prvním pololetí roku 2007, které pak byly dále upraveny a znovu předneseny studentům navštěvující nepovinný předmět Aplikovaná algebra pro inženýry (opět na FSI VUT v Brně). Článek obsahuje i vybrané algoritmy, zejména pro určení řádu eliptické křivky.

Úvod

Základními pojmy teorie eliptických křivek a jejich aplikací v kryptografii s veřejným klíčem se zabýval již autorův článek [2]; proto je zde připomeneme jen stručně. *Eliptickou křivkou* $\mathcal{E}$ nad polem $\mathbb{F}$ rozumíme algebraickou křivku třetího stupně s rovnicí $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, kde $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}$ a kde tzv. *diskriminant* Δ eliptické křivky $\mathcal{E}$ je nenulový. Přitom $\Delta = -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6$, kde $d_2 = a_1^2 + 4a_2$, $d_4 = 2a_4 + a_1a_3$, $d_6 = a_3^2 + 4a_6$, $d_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 + a_4^2$. Je-li $\mathbb{F}_q = \mathbb{F}_{p^n}$ (p prvočíslo, $n \in \mathbb{N}$ konečné pole s charakteristikou různou od 2 a 3), pak vhodnou změnou souřadnic lze Weierstrassovu rovnici transformovat na rovnici $y^2 = x^3 + ax + b$, podobných zjednodušení lze dosáhnout i pro charakteristiky 2 a 3. *Bodem eliptické křivky* $\mathcal{E}$ rozumíme každý bod $[x, y]$ se souřadnicemi $x, y \in \mathbb{F}$ splňujícími její rovnici a dále bod ∞. Nad body eliptické křivky (nadále již bereme $\infty \in \mathcal{E}$) lze zavést binární operaci značenou + (podrobněji v [2]), s touto operací pak křivka tvoří grupu. *Řádem eliptické křivky* $\mathcal{E}$ pak rozumíme řád této grupy čili počet bodů $\mathcal{E}$; značíme ho $\#\mathcal{E}$. Je-li $\mathcal{E}$ eliptická křivka nad konečným polem $\mathbb{F}_q$, pro její řád $\#\mathcal{E}(\mathbb{F}_q)$ platí $q+1-2\sqrt{q} \le \#\mathcal{E}(\mathbb{F}_q) \le q+1+2\sqrt{q}$, tzn. řád je prvkem intervalu zvaného *Hasseho interval*. *Řád bodu P eliptické křivky* pak je obvyklý řád prvku z teorie grup čili nejmenší $n \in \mathbb{N}$ takové, že $nP = \infty$. Budeme ho značit $|P|$.

U čtenáře předpokládáme jen znalosti základů teorie grup (opakovaně mj. využíváme Lagrangeův teorém, tedy že řád prvku dělí řád grupy). Uvádíme zde tedy

2010 *MSC.* Primární 94A60, 11T71; Sekundární 14H52.

Klíčová slova. Kryptografie založená na eliptických křivkách, algoritmy pro určení řádu eliptické křivky.

i některé dobře známé výsledky, jako Malou Fermatovu větu a Čínskou zbytkovou věty v kontextu, v jakém je potřebujeme.

Článku je ponechána původní struktura přednášky s členěním na číslované odstavce. Text je doplněn řadou ilustrativních příkladů.

1. Vybraná tvrzení z algebry a teorie čísel z pohledu ECC

1 Pokud jde o generování náhodného bodu eliptické křivky $\mathcal{E}$, můžeme vzít náhodný prvek $\mathbb{F}_q$, dosadit ho za x nebo za y a druhou souřadnici dopočítat z rovnice eliptické křivky.[1] Pokud neexistuje řešení pro druhou souřadnici, vezmeme jiný prvek $\mathbb{F}_q$. Toto se pokusíme zefektivnit (pro prvočíselná pole), a to i s ohledem na nalezení řádu $\mathcal{E}$.

2 Je-li $n \in \mathbb{N}$ a existuje-li pro $0 \neq m < n$ řešení rovnice

$$y^2 \equiv m \pmod{n}$$

(pro neznámou y), řekneme, že m je *kvadratickým reziduem* (modulo n). Pro eliptickou křivku $\mathcal{E}(\mathbb{F}_p)$ s rovnicí

$$y^2 = x^3 + ax + b$$

musí pro každou nenulovou x-ovou souřadnici jejího bodu být výraz $x^3 + ax + b$ *kvadratickým reziduem* (modulo p).

3 Kvadratická rezidua se pro přirozená n tabelují. Uvádíme přehled kvadratických reziduí modulo $n = 2, \ldots, 20$ (a zvýrazňujeme prvočísla):

$$\begin{aligned}
n = \mathbf{2}: &\quad 1\\
n = \mathbf{3}: &\quad 1\\
n = 4: &\quad 1\\
n = \mathbf{5}: &\quad 1, 4\\
n = 6: &\quad 1, 3, 4\\
n = \mathbf{7}: &\quad 1, 2, 4\\
n = 8: &\quad 1, 4\\
n = 9: &\quad 1, 4, 7\\
n = 10: &\quad 1, 4, 5, 6, 9\\
n = \mathbf{11}: &\quad 1, 3, 4, 5, 9\\
n = 12: &\quad 1, 4, 9\\
n = \mathbf{13}: &\quad 1, 3, 4, 9, 10, 12\\
n = 14: &\quad 1, 2, 4, 7, 8, 9, 11\\
n = 15: &\quad 1, 4, 6, 9, 10\\
n = 16: &\quad 1, 4, 9\\
n = \mathbf{17}: &\quad 1, 2, 4, 8, 9, 13, 15, 16\\
n = 18: &\quad 1, 4, 7, 9, 10, 13, 16
\end{aligned}$$

[1] pochopitelně je výhodnější dosazování za x, neboť dosazení za y vede na kubickou rovnici

$$n = \mathbf{19}: \qquad 1, 4, 5, 6, 7, 9, 11, 16, 17$$
$$n = 20: \qquad 1, 4, 5, 9, 16$$

a dále máme např.

$$n = \mathbf{2357}: \qquad 1, 4, 6, 9, \ldots 2346, 2347, 2348, 2351, 2353, 2356$$

(celkem 1178 reziduí můžeme najít např. pomocí [3]).

4 Je-li m kvadratickým reziduem, pak vyhovující y, pro něž

$$y^2 \equiv m \pmod{n},$$

nazýváme *odmocninou* m (modulo n).

5 Pro eliptickou křivku $\mathcal{E}(\mathbb{F}_p)$ s rovnicí $y^2 = x^3 + ax + b$ náhodně vybereme x a ověříme, zda $x^3 + ax + b$ je kvadratickým reziduem.[2] Pokud ano, spočteme y jako odmocninu x^3+ax+b. Najdeme-li vyhovující y, je také $-y$ odmocninou x^3+ax+b. (Pro $p > 2$ a pro $y \neq 0$ je $-y$ prvek různý od y.) Dále, předpokládejme, že také z je odmocninou $x^3 + ax + b$. To znamená

$$y^2 \equiv z^2 \pmod{p},$$

z čehož

$$y^2 - z^2 = (y + z)(y - z) \equiv 0 \pmod{p}$$

a vidíme, že $z = y$ nebo $z = -y$.

Z uvedeného plyne, že je-li $x^3 + ax + b$ kvadratickým reziduem a y jeho odmocninou, je jedinou další odmocninou téhož rezidua $-y$.

6 Pro $p > 2$ dávají nenulové prvky y a $-y$ totéž kvadratické reziduum y^2 (a žádný jiný prvek již toto reziduum nedává). Takových dvojic $(y, -y)$ v $\mathbb{F}_p$ ovšem je $\frac{p-1}{2}$, tedy také počet kvadratických reziduí v $\mathbb{F}_p$ je roven

$$\frac{p-1}{2}.$$

Při náhodné volbě prvku $\mathbb{F}_p$ máme tedy téměř padesátiprocentní pravděpodobnost, že jde o kvadratické reziduum.

7 *Eulerovo kritérium.* Pro prvočíselné pole s $p > 2$ platí: m je nenulovým kvadratickým reziduem (modulo p) právě tehdy, když

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

a m je kvadratickým *nereziduem*[3] (modulo p) právě tehdy, když

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

(Důkaz bude později.)

---

[2] ovšem totéž kvadratické reziduum může vyjít pro různá x, některá kvadratická rezidua nemusíme obdržet a také x^3+ax+b kvadratickým reziduem být nemusí – proto z počtu kvadratických reziduí řád eliptické křivky jednoduše odhadnout nelze

[3] tzn. je nenulové a není kvadratickým reziduem

8 Nyní z Eulerova kritéria plyne, že součin dvou kvadratických reziduí je kvadratické reziduum, součin dvou nereziduí je reziduum, avšak součin rezidua a nerezidua je nereziduum.

9 *Legendrův symbol* $\left(\frac{m}{n}\right)$ se zavede následovně:

$$\left(\frac{m}{n}\right) = \begin{cases} 1 & \text{je-li } m \text{ kvadratickým reziduem (modulo } n), \\ 0 & \text{je-li } m \text{ nula (modulo } n), \\ -1 & \text{je-li } m \text{ kvadratickým nereziduem (modulo } n). \end{cases}$$

Potom řád eliptické křivky pomocí t a Legendrova symbolu vyjádříme takto:

$$t = -\sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax + b}{p}\right).$$

Přímé užití tohoto vztahu se někdy nazývá *naivní algoritmus* pro určení řádu eliptické křivky.

10 *Malá Fermatova věta.* Pro libovolné $0 \neq y \in \mathbb{F}_p$ platí

$$y^{p-1} \equiv 1 \pmod{p}.$$

Důkaz. $\mathbb{F}_p - \{0\}$ spolu s operací násobení tvoří grupu. Tato grupa má $p-1$ prvků čili řád $p-1$. Ovšem řád prvku m dělí řád grupy; tedy existuje $k \in \mathbb{N}$ takové, že $y^k \equiv 1 \pmod{p}$, $k | p-1$. Pak ovšem také $y^{p-1} \equiv 1 \pmod{p}$.

11 *Wilsonova věta.* V $\mathbb{F}_p$ platí

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

Důkaz. Nejdříve zjistíme, která $y \in \mathbb{F}_p$ splňují

$$y^2 \equiv 1 \pmod{p}.$$

Převedeme-li jedničku na levou stranu a provedeme-li rozklad rozdílu čtverců, máme

$$(y+1)(y-1) \equiv 0 \pmod{p}$$

a z toho máme $y = 1$ nebo $y = -1 \equiv p-1$. Tedy 1 a $p-1$ jsou jediné dva prvky rovné své multiplikativní inverzi. Všechny ostatní prvky sdružíme do dvojic tak, aby v dvojici byly právě k sobě inverzní prvky (pro násobení). Těchto dvojic je $\frac{p-3}{2}$ a součin každé z nich je 1. Stačí tedy přeměnit pořadí činitelů v $(p-1)!$ takto

$$(p-1)! = (p-1) \cdot 1 \cdot \underbrace{(\text{součin první dvojice})}_{1} \cdot \underbrace{(\text{součin } \frac{p-3}{2}\text{-té dvojice})}_{1},$$

abychom viděli, že[4]

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

[4] například pro $\mathbb{F}_7$ máme $6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 6 \cdot 1 \cdot (2 \cdot 4) \cdot (3 \cdot 5) = 6 \cdot 1 \cdot 1 \cdot 1 = 6 \equiv -1 \pmod{7}$

12 *Důkaz Eulerova kritéria.* Především si uvědomme, že pro dané $m \in \mathbb{F}_p$ existuje pro každé $0 \neq y \in \mathbb{F}_p$ takové $z \in \mathbb{F}_p$, že

$$yz \equiv m \pmod{p}.$$

(Skutečně, $z = y^{-1}m$.) Předpokládejme nejprve, že m není kvadratickým reziduem, tedy rovnice

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

nemá řešení pro žádné $y \in \mathbb{F}_p$. To znamená, že všech $p-1$ prvků $\mathbb{F}_p$ je sdruženo do dvojic a součin každé takové dvojice je roven m. Současně součin všech součinů těchto $\frac{p-1}{2}$ dvojic je roven $(p-1)!$, tzn.

$$(p-1)! = m^{\frac{p-1}{2}}$$

a levá strana je rovna -1 (modulo p) podle Wilsonovy věty. Je-li m kvadratickým reziduem, pak $m = y^2$ pro nějaké $y \in \mathbb{F}_p$, máme potom

$$m^{\frac{p-1}{2}} = (y^2)^{\frac{p-1}{2}} = y^{p-1}$$

a tento výraz je roven 1 (modulo p) podle Malé Fermatovy věty.

13 Výpočet odmocniny v $\mathbb{F}_q = \mathbb{F}_{p^n}$, $p > 2$, provedeme pomocí tzv. *Smartova algoritmu*[5].
VSTUP: Kvadratické reziduum $x \in \mathbb{F}_q$.
1. KROK: Vyjádříme $\frac{q-1}{2}$ ve tvaru

$$\frac{q-1}{2} = 2^T s,$$

kde T je nezáporné celé číslo a s je liché přirozené číslo.
2. KROK: Vezmeme libovolné kvadratické nereziduum $y \in \mathbb{F}_q$ a spočteme $A = y^s$.
3. KROK: Spočteme $B = x^{\frac{s-1}{2}}$ a položíme $t_0 = 0$, $k = 0$.
4. KROK: Nyní pro $k = 0, \ldots, T-1$ počítáme

$$t_{k+1} = t_k + 2^k C_k,$$

kde

$$C_k = \begin{cases} 0 & \text{jestliže } \left((A^{t_k}B)^2 x\right)^{2^{T-1-k}} = 1, \\ 1 & \text{jestliže } \left((A^{t_k}B)^2 x\right)^{2^{T-1-k}} = -1. \end{cases}$$

5. KROK: Položíme

$$\sqrt{x} = (A^{t_T}B)x.$$

VÝSTUP: Odmocnina $\sqrt{x} \in \mathbb{F}_q$.

(Poznamenejme, že čísla s, T a A mohou být připravena již při inicializaci pole $\mathbb{F}_q$.)

14 *Příklad.* V prvočíselném poli $\mathbb{F}_{2357}$ je $x = 525$ kvadratickým reziduem a $y = 2$ nereziduem. (Dále počítáme samozřejmě modulo 2357). Pak $\frac{q-1}{2} = \frac{p-1}{2} = \frac{2357-1}{2} = 1178 = 2^1 \cdot 589$. Máme $s = 589$, $T = 1$ a $A = 2^{589} = 633$. Spočteme $B = 525^{\frac{589-1}{2}} = 525^{294} = 1828$. Nyní $t_0 = 0$ a protože

$$(633^0 \cdot 1828)^2 \cdot 525)^{2^{1-1-0}} = 1,$$

[5]efektivnější algoritmus než Smartův je anoncován např. v [6]

což je kvadratické reziduum, máme $C_0 = 0$. Odtud $t_1 = 0$. V závěrečném kroku vypočteme

$$\sqrt{x} = 633^0 \cdot 1828 \cdot 525 = 401.$$

Dalším řešením je $-401 = 1956$.

2. Řád eliptických křivek nad prvočíselnými poli

15 Známe-li některé body na křivce a jejich řády, může to postačit k určení řádu křivky. Najdeme-li totiž nejmenší společný násobek L řádů jednotlivých bodů, je řád křivky určitě jeho násobkem. Podaří-li se, aby pouze jediný násobek L ležel v Hasseho intervalu, je řád křivky nalezen. (Musíme ovšem mít efektivní metodu pro zjištění řádu bodu.)

16 Uvedeme *Shanksův algoritmus*, který vychází z 15 a řeší problém hledání řádu bodů eliptické křivky.
Vstup: $\mathcal{L} = \lfloor q + 1 - 2\sqrt{q} \rfloor$, $\mathcal{H} = \lceil q + 1 + 2\sqrt{q} \rceil$, $d = \lceil \sqrt{\mathcal{H} - \mathcal{L}} \rceil$.
1. krok: Náhodně vybereme bod $P \in (\mathbb{F}_q)$.
2. krok: Spočteme $P, 2P, \ldots, (d-1)P$. Je-li $iP = \infty$ pro nějaké $i \leq d$, jdeme na 1. krok. Jinak vytvoříme posloupnost $BS = \{\infty, P, 2P, \ldots, (d-1)P\}$. (Prohledali jsme několik nejmenších násobků bodu P, udělali jsme tzv. *baby step*.)
3. krok: Položíme $Q = dP$ a počítáme $H_j = \mathcal{L}P + jQ$ pro $j = 1, 2, \ldots, d$. Z bodů H_j vytvoříme posloupnost HS. (Nyní hledáme „velké“ násobky bodu P s krokem d, to je tzv. *giant step*.)
4. krok: Je-li jediné H_j prvkem BS[6], vezmeme odpovídající dvojici indexů[7] i, j, položíme $\#\mathcal{E}(\mathbb{F}_q) = \mathcal{L} + jd - i$ a jdeme na Výstup. Je-li více (řekněme M) prvků HS prvkem BS, uspořádáme dvojice indexů (i_k, j_k), $k = 1, \ldots, M$ tak, aby $j_1 > \cdots > j_M$; potom vezmeme dvojici (i_1, j_1), (i_2, j_2) a položíme $|P| = (j_1 - j_2)d - (i_1 - i_2)$.
5. krok: Je-li $|P| < \sqrt{q} - 1$, jdeme zpět na 1. krok.
6. krok: Náhodně vybereme bod $R \in \mathcal{E}(\mathbb{F}_q)$.
7. krok: Opakujeme 2. krok, 3. krok a 4. krok (pro bod R), spočte-li se $\#\mathcal{E}(\mathbb{F}_q)$, jdeme na Výstup, jinak jdeme na 8. krok.
8. krok: Stejně jako ve 4. kroku pro bod P, určíme nyní řád $|R|$. Dále určíme nejmenšího dělitele s řádu $|R|$ tak, že sR je násobkem P. Je-li $s|P| < 4\sqrt{q}$, jdeme zpět na 5. krok.
9. krok: Určíme n takové, že $ns|P|$ leží v Hasseho intervalu[8]. Položíme $\#\mathcal{E}(\mathbb{F}_q) = ns|P|$.
Výstup: $\#\mathcal{E}(\mathbb{F}_q)$.

17 *Příklad.* Pro prvočíselné pole $\mathbb{F}_{2357}$ uvažujme eliptickou křivku

$$\mathcal{E}\colon y^2 = x^3 + 2006x + 1.$$

[6] alespoň jedno H_j prvkem BS být musí, plyne to z Lagrangeova teorému: povšimněme si totiž, že pomocí BS a HS efektivně hledáme, jaký násobek bodu P je roven ∞

[7] v BS je index $i = 0, 1, \ldots, d-1$, v HS index $j = 1, 2, \ldots, d$

[8] takové n je jediné

Hasseho interval zde je

$$2358 - 2\sqrt{2357} \leq \#\mathcal{E}(\mathbb{F}_{2357}) \leq 2358 + 2\sqrt{2357},$$

což prakticky znamená

$$2261 \leq \#\mathcal{E}(\mathbb{F}_{2357}) \leq 2455.$$

18 *Příklad.* Vezmeme-li bod $P = [0, 1]$ s řádem 1200, s přihlédnutím k Hasseho intervalu máme okamžitě spočten řád eliptické křivky; pouze jediný násobek 1200, a sice 2400, leží v Hasseho intervalu. Vezměme si proto nyní o něco méně pohodlnou situaci: předpokládejme, že známe bod $P = [1471, 41]$, jehož řád je roven 50 a bod $R = [2326, 48]$ s řádem 30. Nejmenší společný násobek L řádů bodů Q a R je 150 a tedy řád eliptické křivky je nějaký násobek 150; v Hasseho intervalu je toto číslo opět jediné: 2400.

19 *Příklad.* Vstupem pro Shanksův algoritmus v tomoto příkladě jsou čísla $\mathcal{L} = 2260$, $\mathcal{H} = 2456$, $d = 14$. Vybereme bod $P = [0, 1]$. Pak dostaneme

$$BS =$$
$$\{\infty, [0, 1], [1927, 2315], [595, 1118], [161, 1721], [171, 983], [1046, 2028],$$
$$[1725, 61], [1601, 1419], [589, 1110], [1271, 211], [325, 153], [651, 1950], [2129, 2300]\}$$

a

$$HS =$$
$$\{[565, 332], [154, 1835], [1595, 625], [1574, 258], [380, 2275], [1753, 547], [833, 376],$$
$$[966, 1274], [2212, 481], \infty, [2212, 1876], [966, 1083], [833, 1981], [1753, 1810]\}.$$

Zde je $i = 0$, $j = 10$ a odtud

$$\#\mathcal{E}(\mathbb{F}_{2357}) = 2260 + 10 \cdot 14 - 0 = 2400.$$

20 *Příklad.* Pro další prověření Shanksova algoritmu se nabízí zvolit jiný počáteční bod P. Zkusme například $P = [1471, 41]$. Pak dostaneme

$$BS =$$
$$\{\infty, [1471, 41], [590, 67], [1309, 1629], [1844, 1753], [310, 915], [1633, 1835],$$
$$[989, 670], [353, 1659], [192, 56], [2003, 1727], [856, 127], [2110, 1727], [2219, 1958]\}$$

a

$$HS =$$
$$\{[1974, 1093], [2110, 630], [590, 67], [1697, 1458], [1363, 916], [1633, 522], [353, 1659],$$
$$[601, 630], [1530, 2086], \infty, [1530, 271], [601, 1727], [353, 698], [1633, 1835]\}.$$

Máme $i_1 = 6$, $j_1 = 14$, dále $i_2 = 0$, $j_2 = 10$; $i_3 = 8$, $j_3 = 7$; $i_4 = 2$, $j_4 = 3$. Potom řád $|P| = (14 - 10) \cdot 14 - (6 - 0) = 50$. Volíme náhodně další bod $\mathcal{E}$, vezměme tedy $R = [2326, 48]$. Pro tento bod dostaneme

$$BS =$$
$$\{\infty, [2326, 48], [1752, 360], [1453, 1391], [1535, 2191], [1395, 2248], [1363, 1441],$$

$$[262, 858], [985, 1447], [2102, 279], [73, 1827], [647, 2179], [2003, 630], [1477, 1363]\}$$

a

$$HS =$$
$$\{[1363, 916], [985, 1447], [985, 910], [1363, 1441], [73, 530], [1535, 2191], [2003, 1727],$$
$$[1752, 360], [1458, 579], \infty, [1458, 1778], [1752, 1997], [2003, 630], [1535, 166]\}.$$

Máme $i_1 = 12$, $j_1 = 13$, dále $i_2 = 0$, $j_2 = 10$; $i_3 = 2$, $j_3 = 8$; $i_4 = 4$, $j_4 = 6$; $i_5 = 6$, $j_5 = 4$; $i_6 = 8$, $j_6 = 2$; řád $|R| = (13 - 10) \cdot 14 - (12 - 0) = 30$. Dělitelé $|R|$ jsou 1, 2, 3, 5, 6, 10, 15 a 30. Zatímco R, $2R$, $3R$ a $5R$ nejsou žádným násobkem P, $6R = 20P$ a tedy $s = 6$; $s|P| > 4\sqrt{q}$ a určíme $n = 8$. Jako výsledek obdržíme $\#\mathcal{E}(\mathbb{F}_q) = ns|P| = 8 \cdot 6 \cdot 50 = 2400$.

22 Množina $\{0, 1, \ldots, n-1\}$ s operací sčítání modulo n představuje grupu, kterou značíme $\mathbb{Z}_n$. Dále, kartézský součin $\{0, 1, \ldots, n_1 - 1\} \times \{0, 1, \ldots, n_2 - 1\}$ s operací indukovanou sčítáním modulo n_1 v první a modulo n_2 v druhé složce je grupou, kterou značíme $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$. Grupa $\mathcal{E}(\mathbb{F}_q)$ je vždy izomorfní grupě $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$, přičemž n_2 dělí jak n_1, tak $q - 1$ (a n_1, n_2 jsou takto určeny jednoznačně). Pak ovšem $\#\mathcal{E}(\mathbb{F}_q) = n_1 n_2$. V grupě $\mathcal{E}(\mathbb{F}_q)$ musí také existovat bod řádu n_1.

23 Je-li $n_2 = 1$ (v předchozím vyjádření $\#\mathcal{E}(\mathbb{F}_q) = n_1 n_2$), je grupa $\mathcal{E}(\mathbb{F}_q)$ *cyklická*. Je-li $n_2 > 1$ malé přirozené číslo $(2, 3, 4, \ldots)$, říkáme, že grupa $\mathcal{E}(\mathbb{F}_q)$ je *téměř cyklická*. V cyklické grupě existuje bod, jehož řád je roven již přímo $\#\mathcal{E}(\mathbb{F}_q)$. Výhodné ale už také je, je-li grupa téměř cyklická, neboť v ní existují body dostatečně vysokého řádu, jejichž (patrně) jediný násobek patří do Hasseho intervalu.

24 Pro dané a, b uvažujme všechny eliptické křivky

$$y^2 = x^3 + ad^2x + bd^3, \qquad 0 \neq d \in \mathbb{F}_p.$$

Platí: všechny křivky s $\left(\frac{d}{p}\right) = 1$ jsou vzájemně izomorfní (a tudíž mají týž řád)[9]; také ale všechny křivky s $\left(\frac{d}{p}\right) = -1$ jsou vzájemně izomorfní (a s tímž řádem). Tohoto výsledku užil dále Mestre a odvodil následující tvrzení.

25 Předpokládejme, že máme dvě eliptické křivky $\mathcal{E}$, $\bar{\mathcal{E}}$ vyjádřené pro nějaká $d, \bar{d}$ ve tvaru

$$\begin{aligned} \mathcal{E}\colon \quad y^2 &= x^3 + ad^2x + bd^3 \\ \bar{\mathcal{E}}\colon \quad y^2 &= x^3 + a\bar{d}^2x + b\bar{d}^3, \end{aligned}$$

přičemž $\left(\frac{d}{p}\right) = 1$ a $\left(\frac{\bar{d}}{p}\right) = -1$. Předpokládejme dále, že grupa $\mathcal{E}$ je izomorfní grupě $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ a n_2 dělí n_1 a grupa $\bar{\mathcal{E}}$ je izomorfní grupě $\mathbb{Z}_{\bar{n}_1} \oplus \mathbb{Z}_{\bar{n}_2}$ a $\bar{n}_2$ dělí $\bar{n}_1$. Pak pro $p > 457$ platí

$$\max\{n_1, \bar{n}_1\} > 4\sqrt{p}.$$

Tento výsledek znamená, že alespoň jedna z křivek $\mathcal{E}$, $\bar{\mathcal{E}}$ má bod řádu většího než $4\sqrt{p}$.

[9] a protože vždy $\left(\frac{1}{p}\right) = 1$, jsou především izomorfní s křivkou s $d = 1$

26 Další důležitý Mestreho výsledek o řádu křivek $\mathcal{E}(\mathbb{F}_p)$ a $\bar{\mathcal{E}}(\mathbb{F}_p)$ je

$$\#\mathcal{E}(\mathbb{F}_p) + \#\bar{\mathcal{E}}(\mathbb{F}_p) = 2p + 2.$$

27 Nabízí se tedy hledat bod (za předpokladu $p > 457$) dostatečně vysokého řádu dle 24 na jedné z křivek $\mathcal{E}$, $\bar{\mathcal{E}}$ a pomocí první části Shanksova algoritmu spočítat jeho řád. Provedeme tzv. *Mestreho smyčku.*
VSTUP: p, $\mathcal{E}(\mathbb{F}_p)$, $\bar{\mathcal{E}}(\mathbb{F}_p)$.
1. KROK: Vybereme náhodně $x \in \mathbb{F}_p$.
2. KROK: Spočteme $\sigma = \left(\ \right)$. Je-li $\sigma = 0$, jdeme zpět na 1. KROK. Je-li $\sigma = 1$, budeme pracovat s křivkou $\mathcal{E}_w = \mathcal{E}$ a souřadnicí $x_w = x$, jinak $\mathcal{E}_w = \bar{\mathcal{E}}$ a $x_w = dx$.
3. KROK: Dopočteme bod $P = [x_w, y_w]$ na $\mathcal{E}_w$ (tedy najdeme y_w). Pro tento bod provedeme 2. KROK, 3. KROK a 4. KROK Shanksova algoritmu. Pokud se ale ve 4. KROKU Shanksova algoritmu nespočte přímo $\#\mathcal{E}_w$[10], jdeme na 1. KROK této (Mestreho) smyčky.
4. KROK: Je-li $\mathcal{E}_w = \mathcal{E}$, klademe $\#\mathcal{E} = \#\mathcal{E}_w$, jinak $\#\mathcal{E} = 2p + 2 - \#\mathcal{E}_w$.
VÝSTUP: $\#\mathcal{E}(\mathbb{F}_p)$.

28 Poznamenejme, že podstata oprávněnosti případného „přepnutí“ na křivku $\bar{\mathcal{E}}$ a náhradu souřadnice x souřadnicí dx tkví v tom, že

$$(dx)^3 + ad^2 \cdot (dx) + bd^3 = d^3(x^3 + ax + b)$$

je kvadratickým reziduem z důvodu popsaného v 8.

29 *Příklad.* Pro $\mathbb{F}_{2357}$ a křivku $\mathcal{E}$ s rovnicí $y^2 = x^3 + 2006x + 1$ při volbě $x = 14$ spočteme $x^3 + 2006x + 1 = 188$ a 188 je kvadratickým reziduem, protože podle Eulerova kritéria máme $188^{1178} \equiv 1 \pmod{2357}$. Odmocninou 188 modulo 2357 je 138, dále $-138 \equiv 2219 \pmod{2357}$, tedy $[14, 138], [14, 2219] \in \mathcal{E}$. Totéž kvadratické reziduum 188 dostaneme i při volbách $x = 1040$ a $x = 1303$. Proto také $[1040, 138], [1040, 2219], [1303, 138], [1303, 2219] \in \mathcal{E}$.

30 *Příklad.* Protože 4 je kvadratickým reziduem modulo 2357, je křivka s rovnicí

$$y^2 = x^3 + 2006 \cdot 4^2 \cdot x + 1 \cdot 4^3 = x^3 + 1455x + 64$$

izomorfní s křivkou $\mathcal{E}\colon y^2 = x^3 + 2006x + 1$. Naopak, 2 není kvadratickým reziduem modulo 2357 a tedy křivku s rovnicí

$$y^2 = x^3 + 2006 \cdot 2^2 \cdot x + 1 \cdot 2^3 = x^3 + 953x + 8$$

bereme dále jako $\bar{\mathcal{E}}$. Náhodně vyberme $x = 2$; potom $2^3 + 2006 \cdot 2 + 1 = 1664$ není kvadratickým reziduem modulo 2357 čili $\sigma = \left(\frac{1664}{2357}\right) = -1$. Tudíž naši křivkou $\mathcal{E}_w$ je křivka

$$\mathcal{E}_w = \bar{\mathcal{E}}\colon y^2 = x^3 + 953x + 8$$

a $x_w = 2 \cdot 2 = 4$ a vezmeme například $P = [4, 79]$. Pro tento bod dá Shanksův algoritmus $\#\mathcal{E}_w = 2316$ a odtud $\#\mathcal{E} = 2 \cdot 2357 + 2 - 2316 = 2400$.

[10] tedy je-li více prvků HS prvkem BS

3. Algebraický uzávěr konečného pole, Frobeniův endomorfismus a torzní grupy

31 Jsou-li F a G pole, pak každý okruhový homomorfismus $h\colon F \to G$ je injektivní. Jsou-li F a G pole a existuje-li okruhový homomorfismus $h\colon F \to G$, pak G nazveme *rozšířením* pole F. Podpole $h(F)$ v G pak obvykle ztotožňujeme s F.

32 Rozšíření G pole F nazveme *algebraické*, jestliže G obsahuje pouze kořeny polynomů nad F.[11]

33 Uvažujme algebru polynomů v jedné neurčité $F[x]$ nad polem F. Jestliže nekonstantní polynom $P \in F[x]$ jde vyjádřit jako součin (lineárních) kořenových součinitelů z $F[x]$, tj.

$$P = \prod_{i=1}^{\deg P} (x - r_i)$$

($r_i \in F$ jsou kořeny P), řekneme, že P je *úplně rozložitelný* v $F[x]$.

Jinými slovy, je-li polynom P stupně $m \in \mathbb{N}$ úplně rozložitelný v $F[x]$, má m kořenů F (včetně násobnosti).

34 *Steinitzova věta.* Pro každé pole F existuje jediné jeho algebraické rozšíření G takové, že každý polynom $P \in F[x]$ je úplně rozložitelný v $G[x]$ a G je nejmenší pole s touto vlastností.

Pole G se pak nazývá *algebraický uzávěr* F; píšeme $G = \bar{F}$. Pole, pro něž platí $F = \bar{F}$ se nazývá *algebraicky uzavřené.*[12]

35 Algebraický uzávěr $\bar{\mathbb{F}}_q$ libovolného konečného pole $\mathbb{F}_q$ má nekonečně mnoho prvků[13]. Pole $\bar{\mathbb{F}}_q = \bar{\mathbb{F}}_{p^n}$ je pole charakteristiky p a kardinality $\aleph_0$.

36 Jako ilustraci si stačí uvědomit, že např. nad polem $\mathbb{F}_2$ je polynom

$$x^2 + x + 1$$

nerozložitelný. Označíme-li jeho kořen j, dostaneme rozšíření $\mathbb{F}_2$ o čtyřech prvcích: $0, 1, j, j+1$. Toto pole je izomorfní[14] s $\mathbb{F}_4$, s nímž ho dále ztotožníme. Nerozložitelný polynom je ovšem i nad $\mathbb{F}_4$ a dostáváme nekonečnou posloupnost rozšíření

$$\mathbb{F}_2 \subset \mathbb{F}_4 \subset \mathbb{F}_8 \subset \mathbb{F}_{16} \subset \dots,$$

přičemž žádné z konečných polí není algebraicky uzavřené. Tato konečná pole ovšem mají týž algebraický uzávěr, tedy

$$\bar{\mathbb{F}}_2 = \bar{\mathbb{F}}_4 = \bar{\mathbb{F}}_8 = \bar{\mathbb{F}}_{16} = \dots.$$

---

[11] je třeba dobře známo, že $\mathbb{C}$ je algebraickým rozšířením $\mathbb{R}$, avšak $\mathbb{R}$ není algebraickým rozšířením $\mathbb{Q}$, neboť $\mathbb{R}$ obsahuje i čísla, která nejsou kořeny polynomů nad $\mathbb{Q}$ (čísla *transcedentní* vzhledem k $\mathbb{Q}$)

[12] příkladem algebraicky uzavřeného pole je $\mathbb{C}$

[13] nad konečným polem vždy existují nerozložitelné polynomy

[14] dle Galoisova teorému

37 Nad polem F charakteristiky p (máme tedy na mysli buď $\mathbb{F}_{p^n} = \mathbb{F}_q$ nebo $\bar{\mathbb{F}}_q$) definujme *jednoduchý Frobeniův endomorfismus*

$$\phi\colon F \to F$$

předpisem

$$\phi(x) = x^p.$$

38 Vlastnosti jednoduchého Frobeniova endomorfismu:

$$\phi(xy) = \phi(x)\phi(y)$$

(zřejmé);

$$\phi(x+y) = \phi(x) + \phi(y)$$

(rozepíšeme $\phi(x+y) = (x+y)^p = x^p + \binom{p}{1}x^{p-1}y = \ldots \binom{p}{p-1}xy^{p-1} + y^p$, pro pole charakteristiky p ale máme $\binom{p}{1} = \cdots = \binom{p}{p-1} = 0$).

39 Pro pole $\mathbb{F}_p$ je přímým důsledkem malé Fermatovy věty vlastnost

$$x^p = x \quad \text{pro všechna } x \in \mathbb{F}_p.$$

To znamená, že $\mathbb{F}_p$ s prvky $0, 1, \ldots, p-1$ představuje množinu pevných bodů jednoduchého Frobeniova endomorfismu $\phi\colon F \to F$. Pevných bodů není více, protože polynom

$$x^p - x$$

může mít nejvýše p kořenů.

40 Aplikujeme-li dvakrát po sobě jednoduchý Frobeniův endomorfismus, dostaneme zobrazení

$$\phi^2 = \phi(\phi)\colon F \to F,$$

pro něž

$$\phi^2(x) = x^{p^2}.$$

Pak množinou pevných bodů pro ϕ^2 je $\mathbb{F}_{p^2}$. Obecně, iterací dostaneme

$$\phi^n\colon F \to F,$$

kde

$$\phi^n(x) = x^{p^n}$$

a množinou pevných bodů je $\mathbb{F}_{p^n}$. Pro n z vyjádření $q = p^n$ pak zobrazení ϕ^n označíme novým symbolem π a budeme ho nazývat *Frobeniův endomorfismus.*

41 Označme $\bar{\mathcal{E}}$ eliptickou křivku na algebraickém uzávěru $\bar{\mathbb{F}}_q$ pole $\mathbb{F}_q$, která má stejnou rovnici $y^2 = x^3 + ax + b$ jako $\mathcal{E}$. Na bod $P = [x, y] \in \bar{\mathcal{E}}$ aplikujme Frobeniův endomorfismus takto:

$$\pi(P) = [\pi(x), \pi(y)] = [x^q, y^q].$$

42 Nyní platí:

(i) je-li $P \in \bar{\mathcal{E}}$, pak také $\pi(P) \in \bar{\mathcal{E}}$,
(ii) pro $P \in \bar{\mathcal{E}}$ nastane $\pi(P) = P$ právě tehdy, když $P \in \mathcal{E}$,
(iii) pro $P, Q \in \bar{\mathcal{E}}$ je $\pi(P+Q) = \pi(P) + \pi(Q)$.

(Vlastnost (i) není samozřejmá a zasluhuje důkaz. Vlastnost (ii) již dokázána byla, jde o výše uvedený popis pevných bodů Frobeniova endomorfismu. Vlastnost (iii) plyne z „příjemných“ vlastností Frobeniova endomorfismu, srv. [38].)

43 Na $\mathcal{E}$ je Frobeniův endomorfismus π identickým zobrazením, což vyjádříme jeho charakteristickou rovnicí $\pi - 1 = 0$. Otázkou nyní je, jakou charakteristickou rovnici má Frobeniův endomorfismus π pro $\bar{\mathcal{E}}$. Odpoveď je tato: charakteristická rovnice π pro $\bar{\mathcal{E}}$ je

$$\pi^2 - t\pi + q = 0,$$

kde

$$t = q + 1 - \#\mathcal{E}(\mathbb{F}_q).$$

Přesněji, pro π platí

$$\pi(\pi([x, y])) - t\pi([x, y]) + q[x, y] = 0,$$

tzn.

$$[x^{q^2}, y^{q^2}] + q[x, y] = t[x^q, y^q].$$

44 Bod P křivky $\bar{\mathcal{E}}$ splňující

$$nP = \infty$$

nazýváme *n-tý torzní bod*. Množina všech n-tých torzních bodů se značí $\bar{\mathcal{E}}[n]$, je podgrupou grupy $\bar{\mathcal{E}}$, kterou nazýváme *n-tá torzní grupa*. (Evidentně $\bar{\mathcal{E}}[1]$ je triviální grupa obsahující jen bod ∞.)

45 Pro body druhé torzní grupy platí $P + P = \infty$, což je možné jen pro nulovou y-ovou souřadnici bodu P. Tedy jde o to, zda existuje kořen rovnice $x^3 + ax + b = 0$ (v $\mathbb{F}_q$). Pokud ano, potom je řád $\#\mathcal{E}(\mathbb{F}_q)$ sudý a tedy t je sudé čili $t \equiv 0 (\bmod 2)$. Neexistuje-li kořen $x^3 + ax + b = 0$ (v $\mathbb{F}_q$), je $t \equiv 1 (\bmod 2)$.

Proveďme výpočet

$$\gcd(x^3 + ax + b, x^q - x).$$

Je-li tento největší společný dělitel roven 1, tedy $x^3 + ax + b$ a $x^q - x$ jsou nesoudělné polynomy, kořen rovnice $x^3 + ax + b = 0$ v $\mathbb{F}_q$) neexistuje, v opačném případě pak ano. Zdůvodnění této skutečnosti je následující: rovnice $x^3 + ax + b = 0$ má samozřejmě kořen v $\bar{\mathbb{F}}_q$ (dle definice algebraického uzávěru): ovšem $\mathbb{F}_q = \{x \in \bar{\mathbb{F}}_q; x = x^q\}$,[15] tedy splňuje-li kořen v $\bar{\mathbb{F}}_q$ také rovnici $x^q - x = 0$, je kořen prvkem $\mathbb{F}_q$.

46 Je zřejmé, že je-li n libovolným násobkem řádu bodu P, pak $P \in \bar{\mathcal{E}}[n]$.

47 *Příklad.* Pro popis všech torzních grup křivky $\bar{\mathcal{E}}$ $y^2 = x^3 + 2006x + 1$ nad $\bar{\mathbb{F}}_{2357}$ nyní můžeme využít spočteného řádu $\#\mathcal{E} = 2400$. Číslo 2400 má dělitele 1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 20, 24, 25, 30, 32, 40, 48, 50, 60, 75, 80, 96, 100, 120, 150, 160, 200, 240, 300, 400, 480, 600, 800, 1200, 2400. Například $\bar{\mathcal{E}}[7]$ bude proto podobně jako $\bar{\mathcal{E}}[1]$ triviální grupou.

[15] viz [39], [40]

4. Schoofův algoritmus (využití Čínské zbytkové věty)

48 Schoofův algoritmus publikovaný v roce 1985 počítá řád eliptické křivky v polynomiálním čase. Nechť $q = p^n, p > 3$. Protože je řád $\#\mathcal{E}(\mathbb{F}_q)$ číslo z (Hasseho) intervalu délky $4\sqrt{q}$, stačí pro určení $\#\mathcal{E}(\mathbb{F}_q)$ znát číslo

$$\#_N\mathcal{E}(\mathbb{F}_q) \;=\; \#\mathcal{E}(\mathbb{F}_q) \bmod N,$$

kde $N > 4\sqrt{q}$.

49 Nyní N vyjádřeme pomocí prvočíselného rozkladu

$$N = l_1 \cdot \cdots \cdot l_r = \prod_{i=1}^{r} l_i > 4\sqrt{q}$$

(l_i prvočísla — předpokládejme, že jsou malá, navzájem různá, různá od 2 i od p [16]); pokud známe všechna $\#_{l_i}\mathcal{E}(\mathbb{F}_q)$, $i = 1, \ldots, r$, můžeme toho využít k výpočtu $\#_N\mathcal{E}(\mathbb{F}_q)$. Aplikujeme přitom následující větu.

50 *Čínská zbytková věta.* Jsou-li čísla $l_1, \ldots, l_r$ po dvou nesoudělná, má soustava

$$\begin{aligned} x &\equiv c_1 \pmod{l_1},\\ x &\equiv c_2 \pmod{l_2},\\ &\cdots\\ x &\equiv c_r \pmod{l_r} \end{aligned}$$

jediné řešení modulo $N = l_1 \ldots l_r$. Toto řešení x můžeme spočíst jako

$$x = \sum_{i=1}^{r} c_i N_i M_i,$$

kde $N_i = \frac{N}{l_i}$ a $M_i = N_i^{-1} \bmod l_i$ (tzv. *Gaussův algoritmus*).

51 Pro eliptickou křivku $\mathcal{E}$ s rovnicí $y^2 = x^3 + ax + b$ nad polem s charakteristikou různou od 2 definujme rekurentně posloupnost polynomů dvou proměnných takto:

$$\begin{aligned} \psi_0 &= 0,\\ \psi_1 &= 1,\\ \psi_2 &= 2y,\\ \psi_3 &= 3x^4 + 6ax^2 + 12bx - a^2,\\ \psi_4 &= 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3),\\ &\cdots\\ \psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \quad \text{pro } m \geq 2,\\ \psi_{2m} &= \frac{\psi_m}{2y}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \quad \text{pro } m > 2. \end{aligned}$$

Polynom ψ_n se nazývá *n-tý dělící polynom.* Budeme počítat $l_r + 2$ dělících polynomů (l_r je největší prvočíslo z rozkladu 49).

[16] obvykle se začíná od 2 a berou se postupně různá prvočísla, až součin překročí $4\sqrt{q}$; případ $l = 2$ jsme ale zmínili v 45 a pro zjednodušení ho v tuto chvíli zde vypouštíme

52 Základní vlastnost dělících polynomů je tato:
Dělící polynom ψ_n je polynom dvou neurčitých x, y nad $\mathbb{F}_q$, splňující pro každý bod $\infty \neq P = [x, y] \in \bar{\mathcal{E}}[n]$

$$\psi_n(x, y) = 0.$$

53 S využitím rovnice eliptické křivky $y^2 = x^3 + ax + b$ můžeme dělící polynomy upravit tak, aby pro liché n byl ψ_n polynomem jediné proměnné x (tento polynom je stupně $\frac{n^2-1}{2}$) a pro sudé n měl ψ_n tvar součinu y s polynomem proměnné x (tento polynom je stupně $\frac{n^2-4}{2}$). Pak lze ψ_n^2 rovněž vyjádřit pro každé n jako polynom jedné proměnné x. Nakonec si uvědomme, že i $\psi_{n-1}\psi_{n+1}$ je (opět s využitím rovnice eliptické křivky $y^2 = x^3+ax+b$) také pro každé n polynom proměnné x.

54 Je-li $P = [x, y]$ bod $\bar{\mathcal{E}}$, lze jeho n-násobek a $-n$-násobek (n kladné) vyjádřit pomocí dělících polynomů:

$$nP = \left[x - \frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2}, \frac{\psi_{2n}}{2\psi_n^4}\right],$$

$$-nP = \left[x - \frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2}, -\frac{\psi_{2n}}{2\psi_n^4}\right].$$

Nyní tedy vidíme, že pomocí uvedeného vztahu je první souřadnice nP (resp. $-nP$) vyjádřena jako racionální funkce souřadnice x a druhá souřadnice pak jako násobek souřadnice y a opět racionální funkce souřadnice x.

55 Uvažujme v **53** zmíněné polynomy proměnné x, tzn. pro liché n přímo $f_n = \psi_n$ a pro sudé n $f_n = \frac{\psi_n}{y}$. Lze ukázat, že tyto polynomy nemají vícenásobné kořeny. Z toho pak plyne, že pro liché prvočíslo l má f_l, který je stupně $\frac{l^2-1}{2}$, v $\bar{\mathbb{F}}_q$ právě $\frac{l^2-1}{2}$ kořenů, představujících x-ové souřadnice bodu torzní grupy $\bar{\mathcal{E}}[l]$ a ke každé x-ové souřadnice lze najít dvě různé souřadnice y-ové (pracujeme nad algebraicky uzavřeným polem). Po započtení bodu ∞, který rovněž patří do $\bar{\mathcal{E}}[l]$, zjišťujeme, že počet bodů $\bar{\mathcal{E}}[l]$ je l^2.

56 Pro prvočíslo l nyní vezměme číslo $\bar{q}$ takto:

$$\begin{aligned} \bar{q} &\equiv q \pmod{l}, \\ |\bar{q}| &< \frac{l}{2} \end{aligned}$$

($\bar{q}$ může být i záporné); podle předchozího nyní můžeme vyjádřit násobek $\bar{q}P = \bar{q}[x, y]$.

57 Nyní nepůjde o nic jiného než o aplikaci charakteristické rovnice Frobeniova endomorfismu uvedené v **43**. Platí totiž: je-li $P = [x, y] \in \bar{\mathcal{E}}[l]$, pak $q[x, y] = \bar{q}[x, y]$. Označíme-li dále

$$\bar{t} = t \mod l,$$

potom také $t[x^q, y^q] = \bar{t}[x^q, y^q]$. Charakteristickou rovnici máme pro $[x, y] \in \bar{\mathcal{E}}[l]$ ve tvaru

$$[x^{q^2}, y^{q^2}] + \bar{q}[x, y] = \bar{t}[x^q, y^q].$$

58 Poté, co vyjádříme x-ovou souřadnici $\bar{q}[x,y] = \bar{q}P$ pomocí dělících polynomů, provedeme součet: x-ovou souřadnici součtu $[x^{q^2}, y^{q^2}] + \bar{q}[x,y]$ označíme x' a spočteme ji pomocí vzorce pro součet dvou bodů (pro něj je více variant[17]).

59 Nyní tedy máme rovnici $x' = \bar{t}x^q$ neboli $x' - \bar{t}x^q = 0$, kterou vyřešíme pro neznámou $\bar{t}$.[18] Hledané t_l může nabývat hodnoty $\bar{t}$ nebo $-\bar{t}$. Na všechna nalezená t_l aplikujeme 50, abychom obdrželi t.

60 Pro určení $\#\mathcal{E}(\mathbb{F}_{2357})$ stačí tedy znát číslo $\#_N\mathcal{E}(\mathbb{F}_{2357})$, kde $N > 154$. Nabízí se zvolit například

$$N = 165 = 3 \cdot 5 \cdot 11 = l_1 \cdot l_2 \cdot l_3.$$

Budeme proto nejdříve počítat číslo $\#_3\mathcal{E}(\mathbb{F}_{2357})$; l je tedy nejprve rovno 3.

61 *Příklad.* Pro prvočíselné pole $\mathbb{F}_{2357}$ uvažujme eliptickou křivku

$$\mathcal{E}\colon y^2 = x^3 + 2006x + 1.$$

Dělící polynomy jsou

$$\begin{aligned}
\psi_1 &= 1,\\
\psi_2 &= 2y,\\
\psi_3 &= 3x^4 + 251x^2 + 12x + 1720,\\
\psi_4 &= 4x^6y + 51x^4y + 80x^3y + 1402x^2y + 902xy + 1013y,\\
\psi_5 &= 2330x^{12} + 294x^{10} + 2033x^9 + 1728x^8 + 2352x^7 + 32x^6y^4 + 992x^6\\
&\quad +284x^5 + 408x^4y^4 + 770x^4 + 640x^3y^4 + 905x^3 + 1788x^2y^4 + 339x^2\\
&\quad +145xy^4 + 1002x + 1033y^4 + 1519.
\end{aligned}$$

Pomocí rovnice $y^2 = x^3+2006x+1$ jdou ψ_1, ψ_3 a ψ_5 vyjádřit jako funkce proměnné x, totéž platí pro ψ_2^2 a ψ_4^2.

$$\begin{aligned}
\psi_1 &= 1,\\
\psi_2^2 &= 4x^4 + 953x + 4,\\
\psi_3 &= 3x^4 + 251x^2 + 12x + 1720,\\
\psi_5 &= 5x^{12} + 1808x^{10} + 380x^9 + 1468x^8 + 612x^7 + 354x^6 + 2121x^5 +\\
&\quad 1333x^4 + 444x^3 + 2106x^2 + 1937x + 195,
\end{aligned}$$

$$\begin{aligned}
t &= q + 1 - \#\mathcal{E}(\mathbb{F}_q),\\
t &= 2357 + 1 - 2400 = -42.
\end{aligned}$$

[17] zde se musíme rozhodovat, zda jde o obecný případ dvou různých bodů nebo o různé body se stejnou první souřadnicí nebo zda jde o týž bod

[18] řešení této rovnice je ovšem třeba nějak efektivně (!) zvládnout; např. v [4] je uvedena metoda tzv. postupného umocňování

Reference

[1] D. Hankerson, A. Menezes, S. Vanstone: *Guide to Elliptic Curve Cryptography*, Springer, 2004.
[2] M. Kureš: *Weilovo párování na eliptických křivkách v kryptosystémech založených na totožnosti a kryptograficky randomizované odpovídací techniky*, Kvaternion **2012**, 103–111.
[3] Výpočet kvadratických reziduí on-line, `http://www.math.mtu.edu/mathlab/COURSES/holt/dnt/quadratic4.html`
[4] G. Musiker: *Schoof's algorithm for counting points on* $E(\mathbb{F}_q)$, 2005, `http://math.ucsd.edu/~gmusiker/schoof.pdf`
[5] S. Sundriyal: *Independent Study Report: Point Counting on Elliptic Curves over Finite Fields*, `http://www.cs.rit.edu/~scs7015/indepent_study/ec.pdf`
[6] F. Wang, Y. Nogami, Y. Morikawa: *A high-speed square root computation in finite fields with application to elliptic curve cryptosystem*, Memoirs of the Faculty of Engineering, Okayama University **39** (2005), 82–92.
[7] E. V. York, *Elliptic Curves Over Finite Fields*, Thesis, George Mason University, 1992, `http://www.math.uiuc.edu/~handuong/crypto/york.pdf`.

Miroslav Kureš, Ústav matematiky, Fakulta strojního inženýrství, Vysoké učení technické v Brně, Technická 2, 61669 Brno, Česká republika,
e-mail: `kures@fme.vutbr.cz`