FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Název:	Kryptograficky slabé eliptické křivky a specializované útoky na ECDLP
Student:	Jiří Soukup
Vedoucí:	Ing. Ivo Petr, Ph.D.
Studijní program:	Informatika
Studijní obor:	Bezpečnost a informační technologie
Katedra:	Katedra počítačových systémů
Platnost zadání:	Do konce letního semestru 2020/21

Pokyny pro vypracování

Pro jisté třídy tzv. "kryptograficky slabých" eliptických křivek (EC) existují metody umožňující řešit problém diskrétního logaritmu (ECDLP) v subexponenciálním či dokonce polynomiálním počtu kroků. Cílem práce je prostudovat současný stav problematiky a identifikovat EC, kterým je třeba se z bezpečnostních důvodů vyhnout.

- Seznamte se s aparátem kryptografie eliptických křivek, identifikujte třídy kryptograficky slabých EC (např. anomální křivky).
- Popište a implementujte algoritmy umožňující generovat kryptograficky slabé EC.
- Důkladně popište a ve vhodně zvoleném programovacím jazyce implementujte algoritmy umožňující efektivní řešení ECDLP na těchto křivkách (např. pro anomální křivky Smartův útok používající zdvih do p-adických čísel).
- Na náhodně generovaných instancích ECDLP porovnejte složitost specializovaných algoritmů se složitostí generických algoritmů užívaných pro řešení ECDLP (jako Pollardova Rho metoda či Babystep-Giantstep).

Seznam odborné literatury

[1] "Weak Curves In Elliptic Curve Cryptography" - Peter Novotney
[2] "The Discrete Logarithm Problem on Elliptic Curves of Trace One" - Nigel P. Smart

prof. Ing. Pavel Tvrdík, CSc.
vedoucí katedry

doc. RNDr. Ing. Marcel Jiřina, Ph.D.
děkan

V Praze dne 10. února 2020

FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

Bakalářská práce

Kryptograficky slabé eliptické křivky a specializované útoky na ECDLP

Jiří Soukup

Katedra počítačových systémů
Vedoucí práce: Ing. Ivo Petr, Ph.D.

4. června 2020

Poděkování

Na tomto místě bych rád poděkoval své rodině za všestrannou a bezvýhradnou podporu při studiu. Současně patří poděkování Ing. Ivu Petrovi, Ph.D. za cenné rady, vstřícnost a ochotu při vedení mé bakalářské práce.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principu při přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisu, zejména skutečnost, že České vysoké učení technické v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 citovaného zákona.

V Praze dne 4. června 2020 . . . . . .

České vysoké učení technické v Praze
Fakulta informačních technologií
© 2020 Jiří Soukup. Všechna práva vyhrazena.
Tato práce vznikla jako školní dílo na Českém vysokém učení technickém v Praze, Fakultě informačních technologií. Práce je chráněna právními předpisy a mezinárodními úmluvami o právu autorském a právech souvisejících s právem autorským. K jejímu užití, s výjimkou bezúplatných zákonných licencí a nad rámec oprávnění uvedených v Prohlášení na předchozí straně, je nezbytný souhlas autora.

Odkaz na tuto práci

Soukup, Jiří. *Kryptograficky slabé eliptické křivky a specializované útoky na ECDLP*. Bakalářská práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2020.

Abstrakt

Problém diskrétního logaritmu je základem pro množství kryptografických systémů současnosti. Není totiž znám algoritmus schopný řešit ho efektivně v libovolné grupě. Body eliptické křivky nad konečným tělesem jsou často využívány jako grupa, v níž je tento problém implementován. Smartův útok nabízí jeho řešení sice jen na anomálních eliptických křivkách, ale za to s lineární časovou složitostí.

V této práci rozebereme proč a jak Smartův útok funguje, implementujeme ho v jazyce SAGE a měřením ověříme jeho časovou složitost v porovnání se složitostí algoritmů Baby-step giant-step a Pollard's rho, které lze použít v libovolné grupě.

Klíčová slova anomální eliptická křivka, problém diskrétního logaritmu, Smartův útok, p-adická čísla, SAGE

Abstract

Many of today's cryptosystems are based on the discrete logarithm problem. There is no known algorithm that is able to solve it quickly in an arbitrary group. Often a group of points of an elliptic curve is used to implement the problem in. Although it works only for anomalous elliptic curves, Smart's attack solves the problem with linear time complexity.

In this thesis we describe how Smart's attack works and we implement it in SAGE software. In the end we present a measurement comparing its time complexity to time complexity of Baby-step giant-step and Pollard's Rho – algorithms that can solve the discrete logarithm problem in an arbitrary group.

Keywords anomalous elliptic curve, discrete logarithm problem, Smart's attack, p-adic numbers, SAGE

Obsah

Seznam obrázků

Úvod

Jedním z principů, na nichž stojí kryptografické systémy zajišťující ustanovení společného klíče nebo realizaci elektronického podpisu, je problém diskrétního logaritmu. Bezpečnost těchto systémů je dána tím, že není znám algoritmus fungující na libovolné grupě, který by byl schopen problém diskrétního logaritmu vyřešit rozumně rychle.

V praxi často používanou grupou, na níž je problém diskrétního logaritmu implementován, je grupa bodů eliptické křivky nad konečným tělesem. Určitá podmnožina eliptických křivek nad konečným tělesem – anomální eliptické křivky – je ale pro takové využití velmi problematická. Existuje totiž způsob, jak na těchto křivkách řešit problém diskrétního logaritmu s lineární časovou složitostí. Jedná se o takzvaný Smartův útok. Tato možnost rychlého řešení problému diskrétního logaritmu má značný přesah do praxe, kde naprosto vylučuje použití anomálních eliptických křivek ve výše popsaných systémech. V této práci se budeme zabývat zejména právě Smartovým útokem.

V kapitole 1 představíme základní matematické znalosti potřebné pro chápání způsobu, jakým Smartův útok funguje. Věnovat se budeme především eliptickým křivkám a problému diskrétního logaritmu. Zmíníme i některé poznatky k problematice projektivní geometrie.

V kapitole 2 se budeme zabývat obecnými algoritmy schopnými řešit problém diskrétního logaritmu na libovolné grupě. Popíšeme princip, na kterém pracují, a jejich časovou a paměťovou složitost.

Kapitola 3 je věnována Smartovu útoku samotnému. V ní krok po kroku rozebereme, proč tento algoritmus vůbec funguje.

Na závěr v kapitole 4 ukážeme, jak lze Smartův útok implementovat. Implementujeme také algoritmus pro generování anomálních eliptických křivek. Pro implementaci obou algoritmů využijeme software SAGE. Na anomálních eliptických křivkách získaných prezentovaným algoritmem následně provedeme měření časové složitosti Smartova útoku a dvou algoritmů schopných řešit problém diskrétního logaritmu na libovolné grupě – Baby-step giant-step

a Pollard's Rho. Tyto výsledky pak porovnáme se složitostmi, jakých by měřené algoritmy měly dosahovat dle teorie.

Kapitola 1

Matematický základ

Abychom se mohli blíže podívat na problematiku kryptograficky slabých eliptických křivek, musíme nejprve řádně zavést pojmy, s nimiž budeme pracovat. V této kapitole si proto řekneme, co je eliptická křivka nad obecným tělesem, jaké má vlastnosti a co se stane, budeme-li ji uvažovat nad tělesem konečným. Dále popíšeme problém diskrétního logaritmu, a to jak v obecné podobě, tak v případě eliptických křivek.

1.1 Eliptické křivky

Nebude-li řečeno jinak, definice a tvrzení této sekce budou vycházet z [1] (kapitola 3.1).

Definice 1.1. *Eliptická křivka* E nad tělesem K je dána rovnicí

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1.1}$$

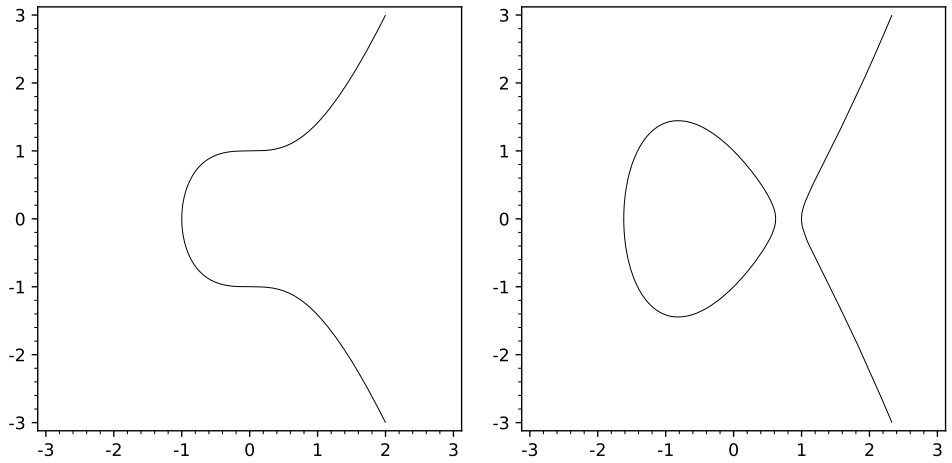
kde $a_1, a_2, a_3, a_4, a_6 \in K$ a $\Delta \neq 0$, přičemž Δ je *diskriminant* E definovaný následovně:

$$\begin{aligned}
\Delta &= -{d_2}^2 d_8 - 8{d_4}^3 - 27{d_6}^2 + 9d_2d_4d_6,\\
d_2 &= {a_1}^2 + 4a_2,\\
d_4 &= 2a_4 + a_1a_3,\\
d_6 &= {a_3}^2 + 4a_6,\\
d_8 &= {a_1}^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2{a_3}^2 - {a_4}^2.
\end{aligned}$$

Je-li L nadtělesem K, pak množina L-racionálních bodů na E je tvaru

$$E(L) = \{(x, y) \in L \times L : y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0\} \cup \{\mathcal{O}\},$$

kde $\mathcal{O}$ je *bod v nekonečnu*.



(a) $E : y^2 = x^3 + 1$ (b) $E : y^2 = x^3 - 2x + 1$

Obrázek 1.1: Eliptické křivky nad $\mathbb{R}$

Poznámka 1.2.

a) Rovnice (1.1) je označována jako *Weierstrassova rovnice*.

b) Je-li eliptická křivka E definována nad tělesem K, je zároveň definována nad kterýmkoli nadtělesem tělesa K. Toho bude využito v první fázi Smartova útoku (zdvihu eliptické křivky z $\mathbb{F}_p$ do $\mathbb{Q}_p$).

c) Podmínka $\Delta \neq 0$ u eliptické křivky nad $\mathbb{R}$ zajišťuje, že tato křivka je „hladká“, tedy že má v každém bodě právě jednu tečnu. Tato vlastnost je důležitá pro zavedení grupové operace sčítání na eliptické křivce.

d) Více k zavedení bodu $\mathcal{O}$ je k nalezení v [1] (sekce 3.2).

e) L-racionální body na eliptické křivce E jsou body (x, y), které splňují rovnici udávající E a které jsou prvky L. Bod v nekonečnu je považován za L-racionální bod pro všechna nadtělesa L tělesa K.

Definice 1.3. Mějme eliptickou křivku E nad tělesem K a ať $\mathrm{char}(K) \notin \{2, 3\}$. Pak každou E můžeme popsat *zjednodušenou Weierstrassovou rovnicí*

$$y^2 = x^3 + ax + b, \tag{1.2}$$

kde $a, b \in K$. Diskriminant takové křivky je $\Delta = -16(4a^3 + 27b^2)$.

Poznámka 1.4. Jak bude dále v této práci patrné, případy, kdy charakteristika tělesa K je 2 nebo 3, nejsou z hlediska tématu práce zajímavé. Všechny eliptické křivky, s nimiž budeme pracovat, tak bude možné popsat rovnicí (1.2).

Definice 1.5. Mějme eliptickou křivku E danou rovnicí (1.2). *j-invariant* křivky E definujeme jako [2]

$$j = 1728 * \frac{4a^3}{4a^3 + 27b^2}. \tag{1.3}$$

Poznámka 1.6.

a) Všimněme si, že jmenovatel z pravé strany rovnice (1.3) bude vždy různý od nuly. Pokud by platilo $4a^3 + 27b^2 = 0$, byl by diskriminant křivky E nulový, což z definice 1.1 nemůže nastat.

b) j je j-invariantem eliptické křivky dané rovnicí

$$y^2 = x^3 + \frac{3j}{1728 - j}x + \frac{2j}{1728 - j} \tag{1.4}$$

za předpokladu, že $j \notin \{0, 1728\}$ [2].

c) j-invariantu bude využito při generování *anomálních* eliptických křivek. Tato podkategorie eliptických křivek bude zavedena v sekci 2.2.

Definice 1.7. Mějme prvočíslo p, eliptickou křivku E nad $\mathbb{F}_p$ danou rovnicí (1.2) a $u \in \mathbb{Z}$ takové, že u není čtverec modulo p. Pak definujeme *kvadratický twist* $\tilde{E}$ eliptické křivky E jako eliptickou křivku nad $\mathbb{F}_p$ danou rovnicí [3]

$$uy^2 = x^3 + ax + b.$$

Poznámka 1.8. j-invariant E je roven j-invariantu kvadratického twistu $\tilde{E}$ [3].

Definice 1.9. Mějme eliptickou křivku E nad tělesem K. *Řádem křivky E* nazveme počet jejích K-racionálních bodů, je-li tento počet konečný. Tuto hodnotu budeme značit $\#E(K)$.

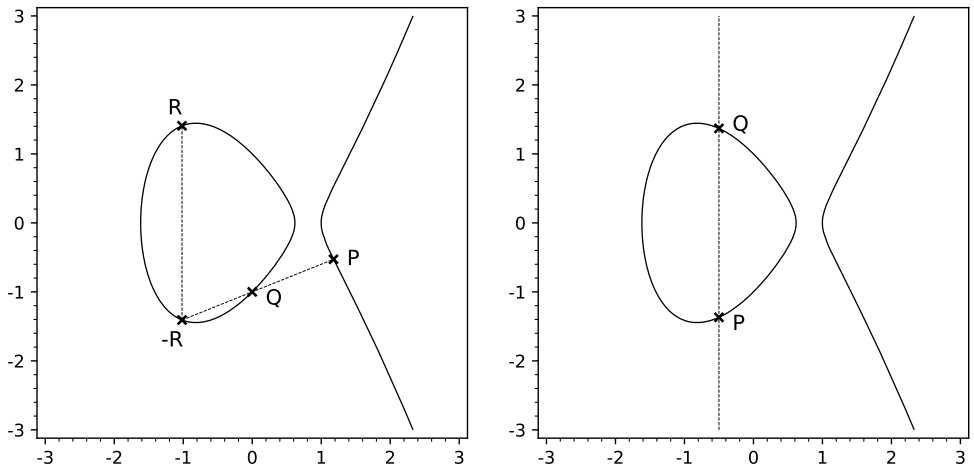
1.1.1 Eliptická křivka jako grupa

Na eliptické křivce E nad tělesem K dané rovnicí (1.2) lze zavést operaci sčítání jejích bodů tak, že $E(K)$ spolu s touto operací tvoří komutativní grupu. Mějme body $P, Q \in E(K)$. Vyjdeme z geometrického přístupu v $\mathbb{R}$.

1. Je-li $Q = \mathcal{O}$, zavedeme $P + Q = P$. Pro $P = \mathcal{O}$ zavedeme $P + Q = Q$.

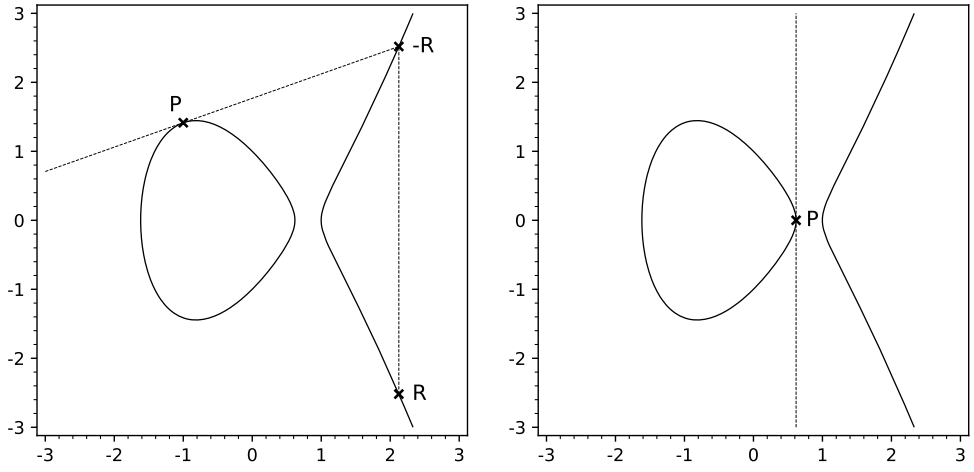
2. Opačným prvkem bodu $P = (x_p, y_p)$ vzhledem ke sčítání zvolíme $-P = (x_p, -y_p)$. Jedná se o bod souměrný s P podle osy x, který na E také leží. Pokud $P = \mathcal{O}$, položíme $-P = \mathcal{O}$.

3. Mějme body P, Q takové, že $P \neq Q$, $P \neq \mathcal{O}$, $Q \neq \mathcal{O}$.



(a) $P + Q = R$ (b) $P + Q = \mathcal{O}$

Obrázek 1.2: Součet bodů eliptické křivky



(a) $P + P = R$ (b) $P + P = \mathcal{O}$

Obrázek 1.3: Součet bodu eliptické křivky se sebou samým

a) Je-li zároveň $Q \neq -P$, přímka daná body P a Q protne křivku E právě v jednom dalším bodě $-R$. Potom zavedeme $P + Q = R$ (vizte obrázek 1.2a).

b) Pokud $Q = -P$, přímka daná body P a Q protne křivku E „v nekonečnu“. Z toho důvodu položíme $P+Q = \mathcal{O}$ (vizte obrázek 1.2b).

4. Pro $P = (x_p, y_p) = Q \neq \mathcal{O}$, uvážíme tečnu křivky E v bodě P.

a) Je-li $y_p \neq 0$, protne uvažovaná tečna křivku E právě v jednom dalším bodě $-R$. Analogicky s případem 3a zavedeme $P + Q = R$ (vizte obrázek 1.3a).

b) Pokud $y_p = 0$, protne uvažovaná tečna křivku E „v nekonečnu“. Z toho důvodu položíme $P + Q = \mathcal{O}$ (vizte obrázek 1.3b).

Případ 3a, sečtení dvou bodů $P = (x_p, y_p)$, $Q = (x_q, y_q)$, $P \neq \pm Q$ můžeme analyticky vyjádřit následujícím způsobem:

$$P + Q = (x, y), \text{ kde} \tag{1.5}$$

$$x = \left(\frac{y_q - y_p}{x_q - x_p}\right)^2 - x_p - x_q, \tag{1.6}$$

$$y = \left(\frac{y_q - y_p}{x_q - x_p}\right)(x_p - x) - y_p. \tag{1.7}$$

Případ 4a, sečtení bodu $P = (x_p, y_p)$ sama se sebou, lze za podmínky $P \neq -P$ popsat následovně:

$$P + P = (x, y), \text{ kde} \tag{1.8}$$

$$x = \left(\frac{3{x_p}^2 + a}{2y_p}\right)^2 - 2x_p, \tag{1.9}$$

$$y = \left(\frac{3{x_p}^2 + a}{2y_p}\right)(x_p - x) - y_p. \tag{1.10}$$

Přičemž a z rovnice (1.9) a (1.10) je koeficientem ze zjednodušené Weierstrassovy rovnice křivky E.

Vztahy (1.6), (1.7), (1.9) a (1.10) lze použít v libovolném tělese K. $E(K)$ spolu s operací sčítání definovanou rovnicemi (1.5)–(1.10) tvoří komutativní grupu. Pro důkaz vizte například [2](sekce 2.2).

Definice 1.10. Mějme eliptickou křivku E nad tělesem K, bod $P \in E(K)$ a $n \in \mathbb{N}$. Výrazem nP budeme rozumět $\underbrace{P + P + \ldots + P}_{n}$.

Definice 1.11. Mějme eliptickou křivku E nad tělesem K a bod $P \in E(K)$. Nejmenší číslo $n \in \mathbb{N}$ takové, že

$$nP = \mathcal{O},$$

nazveme *řádem bodu* P.

Uvažme situaci, kdy chceme získat bod nP pro eliptickou křivku E nad tělesem K, $P \in E(K)$, $n \in \mathbb{N}$. Počítat postupně body $2P$, $3P$, ..., nP není ani zdaleka optimální. Výpočetně přívětivější variantou je algoritmus *Double-and-add* nebo další algoritmy z něj vycházející.

Algoritmus 1.12. Mějme eliptickou křivku E nad tělesem K, $P \in E(K)$, $n \in \mathbb{N}$. Algoritmus *Double-and-add* spočte bod nP následovně:

1. Začni s $a = n$, $B = \mathcal{O}$, $C = P$.
2. Pokud a je sudé, ať $a = a/2$, $B = B$, $C = 2C$.
3. Pokud a je liché, ať $a = a - 1$, $B = B + C$, $C = C$.
4. Pokud $a \neq 0$, pokračuj krokem 2.
5. Vrať B.

Vrácené B je rovno nP [2] (sekce 2.2).

Poznámka 1.13.

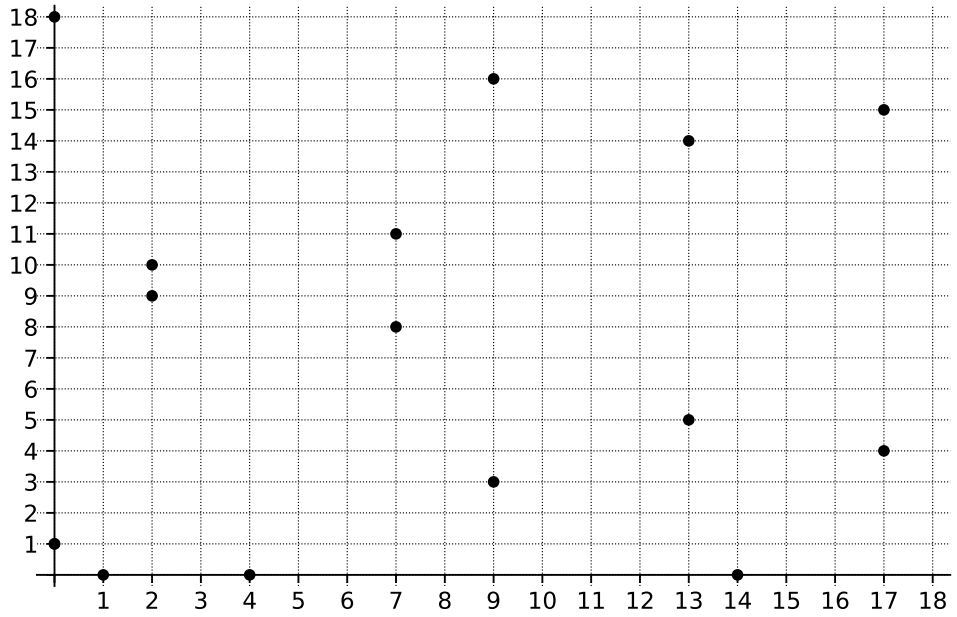
a) Je vidět, že jsou zapotřebí nejvýše dvě sečtení bodů eliptické křivky, aby se délka binárního zápisu proměnné a z algoritmu 1.12 o jedna zkrátila. V okamžiku, kdy je $a = 0$, algoritmus skončí. Časová složitost tohoto algoritmu je tedy $O(\log(n))$.

b) Měřítkem, které jsme zvolili pro vyjádření časové složitosti algoritmu 1.12 je počet grupových operací. A i dále, nebude-li řečeno jinak, budeme používat toto měřítko.

Příklad 1.14. Vezměme $n = 19$ a bod $P \in E(K)$. Hledá-li bod nP, algoritmus *Double-and-add* bude postupně počítat body $2P$, $4P$, $8P$, $16P$ a výsledek získá jako součet $16P + 2P + P$.

1.1.2 Eliptické křivky nad konečným tělesem

Dále v této práci se budeme věnovat zejména případu, kdy těleso, nad kterým danou eliptickou křivku uvažujeme, má konečný počet prvků. Ona eliptická křivka pak zákonitě bude mít jen konečně mnoho bodů (vizte obrázek 1.4). Určitý odhad počtu bodů eliptické křivky nad konečným tělesem nabízí *Hasseho věta*.



Obrázek 1.4: Eliptická křivka $E : y^2 = x^3 - 2x + 1$ nad $\mathbb{F}_{19}$

Věta 1.15. *(Hasse)*
Ať E je eliptická křivka nad konečným tělesem $\mathbb{F}_q$. Pak pro řád E platí

$$|q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}.$$

Pro důkaz vizte [2] (sekce 4.2).

Pro sčítání bodů eliptické křivky nad konečným tělesem již není dost dobře možné využít geometrického přístupu. Musíme si vystačit s analytickým vyjádřením, které jsme zachytili v rovnicích (1.5)–(1.10).

1.2 Homogenní souřadnice

Důležitou vlastností *projektivních prostorů*, kterou euklidovské prostory nesdílí, je možnost reprezentovat „body v nekonečnu“ přímo jako body daného prostoru. Umožněno je to zavedením *homogenních souřadnic*.

V těchto souřadnicích je bod (x, y, z) bodem v nekonečnu právě tehdy, když $z = 0$. Z rovnice (1.1) zapsané v homogenních souřadnicích,

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3,$$

je pak vidět, že jediným bodem v nekonečnu na eliptické křivce je bod $(0, 1, 0)$ [1]. Zvolíme-li totiž $z = 0$, je nutně $x = 0$, přičemž zároveň platí, že libovolný

nenulový násobek homogenních souřadnic reprezentuje stejný bod euklidovského prostoru.

Zobrazení převádějící bod S eliptické křivky v euklidovském prostoru do projektivního prostoru je tak dáno předpisem

$$S \longmapsto \begin{cases} (zx, zy, z), \text{ pro } S = (x, y) \neq \mathcal{O} \text{ a } z \neq 0; \\ (0, 1, 0), \text{ pro } S = \mathcal{O}. \end{cases}$$

Zobrazení bodu eliptické křivky opačným směrem, tedy z projektivního prostoru do euklidovského prostoru, určuje předpis

$$(x, y, z) \longmapsto \begin{cases} (\frac{x}{z}, \frac{y}{z}), \text{ pro } z \neq 0; \\ \mathcal{O}, \text{ pro } z = 0. \end{cases}$$

Další informace k problematice projektivní geometrie lze nalézt v [4].

1.3 Problém diskrétního logaritmu

Definice 1.16. Mějme grupu G (v multiplikativní notaci). Pro $g \in G$ ať $\langle g \rangle$ je cyklická podgrupa generovaná g. Je-li dáno $g \in G$ a $a \in \langle g \rangle$, pak úlohu nalezení $x \in \mathbb{N}$ takového, že $g^x = a$, nazveme *problém diskrétního logaritmu* na grupě G [5].

Poznámka 1.17.

a) Číslo x označujeme jako diskrétní logaritmus a o základu g.

b) Zapisujeme-li grupu v aditivní notaci, což je i případ eliptických křivek, je rovnost z definice výše tvaru $xg = a$.

Náročnost problému diskrétního logaritmu se přímo odvíjí od grupy, na níž ho řešíme. Je-li grupa vhodně zvolená, může nám problém diskrétního logaritmu poskytnout v kryptografii tolik žádanou „jednosměrnou funkci“.

Příklad 1.18. Ať p je prvočíslo a g generátor multiplikativní grupy $\mathbb{F}_p^*$. Pak můžeme definovat funkci $f : \{1, \ldots, p-1\} \to \mathbb{F}_p^*$ předpisem

$$f(x) = g^x \bmod p.$$

Hodnota této funkce v bodě x může být spočtena relativně snadno za použití binárního rozkladu

$$x = \sum_{i=0}^{k} e_i 2^i,$$

kde $e_i \in \{0, 1\}$ (algoritmus *Square-and-multiply*). Takový výpočet bude vyžadovat nejvýše $2k$ násobení modulo p. Abychom ale byli schopni invertovat funkci f, musíme umět řešit problém diskrétního logaritmu na $\mathbb{F}_p^*$. Ten je pro velká p považován za obtížně řešitelný, díky čemuž je funkce f dobrým kandidátem na „jednosměrnou funkci“ [5].

Příklad 1.19. Jedním z kryptosystémů stavějících na problému diskrétního logaritmu je *Diffieho-Hellmanův protokol ustanovení společného klíče*. Ten ve své původní podobě zahrnuje dvě strany A a B komunikující veřejným kanálem tak, že

1. A a B si dohodnou prvočíslo p a generátor g grupy $\mathbb{F}_p^*$,
2. A zvolí tajné $X_\mathrm{A} \in \mathbb{F}_p^*$, B zvolí tajné $X_\mathrm{B} \in \mathbb{F}_p^*$,
3. A spočte $Y_\mathrm{A} = g^{X_\mathrm{A}} \bmod p$, B spočte $Y_\mathrm{B} = g^{X_\mathrm{B}} \bmod p$,
4. A a B si vymění hodnoty Y_A a Y_B,
5. A spočte společný klíč $K_\mathrm{AB} = g^{X_\mathrm{A}X_\mathrm{B}} = (Y_\mathrm{B})^{X_\mathrm{A}}$, B spočte společný klíč $K_\mathrm{AB} = g^{X_\mathrm{A}X_\mathrm{B}} = (Y_\mathrm{A})^{X_\mathrm{B}}$.

Pokud by bylo možné efektivně řešit problém diskrétního logaritmu na grupě $\mathbb{F}_p^*$, mohl by kdokoli, kdo monitoruje kanál, kterým A a B komunikují, z hodnot p, g, Y_A a Y_B určit tajné hodnoty X_A a X_B. S takovou znalostí pak lze dopočítat klíč K_AB, který A a B budou používat při další (symetricky šifrované) komunikaci [6].

1.4 Problém diskrétního logaritmu na eliptických křivkách

Definice 1.20. Ať E je eliptická křivka nad konečným tělesem K. Předpokládejme, že $P, Q \in E(K)$ jsou body takové, že $Q \in \langle P \rangle$. Úlohu nalezení $n \in \mathbb{N}$ splňujícího $Q = nP$ nazveme *problém diskrétního logaritmu na eliptické křivce* E.

Poznámka 1.21. Problém diskrétního logaritmu na eliptické křivce budeme dále označovat zkratkou ECDLP (z anglického Elliptic Curve Discrete Logarithm Problem).

Výhodou kryptosystémů postavených nad eliptickými křivkami je to, že umožňují použití klíčů o menší délce při zachování stejné úrovně zabezpečení, jakou nabízí kryptosystémy založené na problému diskrétního logaritmu v multiplikativní grupě $\mathbb{F}_p^*$ [7]. Z kratších klíčů pak logicky plynou menší nároky na hardware, což je zvlášť cenné, například pokud výpočet probíhá na čipové kartě.

Základní množina parametrů kryptosystému postaveného nad eliptickými křivkami sestává z prvočísla p, eliptické křivky E nad $\mathbb{F}_p$ a výchozího bodu $P \in E(\mathbb{F}_p)$ řádu $n \in \mathbb{N}$. Klíčem v takovém kryptosystému je pak dvojice (d, Q). Soukromý klíč d je náhodně zvolený z množiny $\{1, \ldots, n-1\}$. Pro veřejný klíč Q platí $Q = dP$. Bod Q je tedy náhodně zvoleným bodem grupy generované výchozím bodem P.

Tyto kryptosystémy jsou využívány zejména pro ustanovení společného klíče a realizaci elektronického podpisu.

Příklad 1.22. Ustanovení společného klíče za pomoci eliptických křivek vycházející z Diffieho-Hellmanova protokolu proběhne tak, že

1. A a B si dohodnou parametry p, $E(\mathbb{F}_p)$, P,
2. A vygeneruje klíč $(d_\mathrm{A}, Q_\mathrm{A})$, B vygeneruje klíč $(d_\mathrm{B}, Q_\mathrm{B})$,
3. A a B si vymění veřejné klíče Q_A a Q_B,
4. A a B spočtou bod $R = d_\mathrm{A}Q_\mathrm{B} = d_\mathrm{B}Q_\mathrm{A}$,
5. společný klíč je odvozen z R (typicky aplikováním pevně dané funkce na jeho souřadnici x) [8].

Kapitola 2

Řešení ECDLP

Na obtížnosti řešení problému diskrétního logaritmu závisí některé z nejrozšířenějších technologií současného internetu. Již zmíněné ustanovení společného klíče a elektronický podpis jsou využívány v protokolech a systémech, jako je transport layer security [9], secure shell [10] nebo třeba Bitcoin [11][8]. Jak oprávněný je ale předpoklad, že problém diskrétního logaritmu není efektivně řešitelný? Obsahem následující kapitoly bude náhled do fungování algoritmů, které jsou schopny problém diskrétního logaritmu – konkrétně ECDLP – řešit. Nejprve se budeme věnovat algoritmům fungujícím na obecných eliptických křivkách. V druhé části se zaměříme na konkrétní podkategorii eliptických křivek – *anomální* eliptické křivky.

2.1 Obecné eliptické křivky

Uvažujeme-li obecnou eliptickou křivku, nejlepšími známými algoritmy, které jsou schopny vyřešit na ní problém diskrétního logaritmu, jsou varianty deterministického *Baby-step giant-step* a pravděpodobnostního *Pollard's Rho* [12].

Mějme dánu eliptickou křivku E nad konečným tělesem $\mathbb{F}_q$, $\#E(\mathbb{F}_q) = n$, bod $P \in E(\mathbb{F}_q)$ řádu n a bod $Q \in \langle P \rangle$. Popíšeme princip, jak *Baby-step giant-step* a *Pollard's Rho* najdou $k \in \{0, \ldots, n-1\}$ takové, že $Q = kP$.

Algoritmus 2.1. (Pollard's Rho)

Zavedeme *iterační funkci* $f : \langle P \rangle \to \langle P \rangle$ takovou, aby bylo jednoduché spočíst $X' = f(X)$ a $c', d' \in \{0, \ldots, n-1\}$ splňující

$$X' = c'P + d'Q$$

pro dané $X = cP + dQ$. Pro výchozí bod $X_0 = c_0P + d_0Q$ s náhodně zvolenými $c_0, d_0 \in \{0, \ldots, n-1\}$ definujeme posloupnost $\{X_i\}$ předpisem

$$X_{i+1} = f(X_i)$$

pro $i \geq 0$. Jelikož $\langle P \rangle$ je konečná, v posloupnosti $\{X_i\}$ se dříve či později nějaký bod zopakuje – nastane kolize – a posloupnost se pak bude cyklicky opakovat. Kolize $X_i = X_j$, kde $i \neq j$, nám dává rovnici

$$c_i P + d_i Q = c_j P + d_j Q.$$

A jelikož je

$$(c_i - c_j)P = (d_j - d_i)Q = (d_j - d_i)kP,$$

můžeme určit řešení

$$k = (c_i - c_j) * (d_j - d_i)^{-1} \bmod n,$$

za předpokladu, že $d_j - d_i \in (\mathbb{Z}/n\mathbb{Z})^*$. Není tedy jisté, že nalezení kolize vede k nalezení řešení. Pravděpodobnost, že tomu tak bude, závisí na volbě iterační funkce f [13]. Více informací je k nalezení v [1] (sekce 4.1.2).

Algoritmus 2.2. (Baby-step giant-step)
Ať $m = \lceil \sqrt{n} \rceil$. Pak

$$k = k_0 + mk_1, \tag{2.1}$$

kde $0 \leq k_0 < m$ a $0 \leq k_1 < m$. Nejprve určíme $P' = mP$. Pak počítáme hodnoty $k_0 P$ pro $0 \leq k_0 < m$ (baby steps) a dvojice $(k_0 P, k_0)$ ukládáme do datové struktury snadno prohledatelné podle prvního prvku (např. setříděný seznam nebo binární strom). Následně pro $0 \leq k_1 < m$ kontrolujeme, jestli $Q - k_1 P'$ (giant step) je mezi uloženými hodnotami. Pokud najdeme shodu

$$k_0 P = Q - k_1 P',$$

je ECDLP vyřešen. Známe aktuální k_1, k_0 je uloženo spolu s $k_0 P$ a dle rovnice (2.1) získáme hledané k [12].

Ani jeden z uvedených algoritmů není vázán jen na eliptické křivky. Oba umí analogicky řešit problém diskrétního logaritmu na libovolné cyklické grupě [14, 12].

Pollard's Rho má časovou složitost $O(\sqrt{n})$. Jeho paměťová složitost je $O(1)$. Časová i paměťová složitost *Baby-step giant-step* je $O(\sqrt{n})$. Na rozdíl od *Pollard's Rho* se ale jedná o deterministický algoritmus [14, 12].

Není-li řád eliptické křivky prvočíselný, může být ke zrychlení řešení ECDLP na oné křivce použit *Pohligův-Hellmanův algoritmus*. Ten redukuje ECDLP z původní grupy do jejích podgrup, kde je k výpočtu ECDLP použit například některý ze dvou výše uvedených algoritmů. Dílčí výsledky z jednotlivých podgrup pak tvoří systém kongruencí, jehož řešení je i řešením původního ECDLP. Algoritmus je podrobně popsán v [15].

Pokryli jsme ty nejdůležitější algoritmy schopné pracovat na libovolné eliptické křivce. Existují ale určité druhy eliptických křivek, na kterých lze ECDLP vyřešit rychleji, než je tomu v obecném případě. Zde máme na mysli konkrétně *anomální* a *supersingulární* eliptické křivky. A právě prvním jmenovaným budeme dále věnovat veškerou pozornost. Pro více informací o řešení ECDLP na supersingulárních eliptických křivkách vizte [16].

2.2 Anomální eliptické křivky

Definice 2.3. Mějme prvočíslo p a eliptickou křivku E nad tělesem $\mathbb{F}_p$. Řekneme, že E je *anomální*, pokud

$$\#E(\mathbb{F}_p) = p.$$

Abychom tedy ověřili, že eliptická křivka, na níž chceme ECDLP vyřešit, je anomální, musíme najít počet jejích bodů. Algoritmus *SEA* (Schoof-Elkies-Atkin) je toho schopen v polynomiálním čase. Jedná se o algoritmus vycházející z původního Schoofova algoritmu. Ten navzdory polynomiální časové složitosti nedosahoval v praxi dobrých výsledků a byl vylepšen prací Elkiese a Atkina [17, 18].

Pokud by existoval algoritmus, který je na anomální eliptické křivce schopný vyřešit ECDLP s polynomiální časovou složitostí, celý proces ověření, že daná eliptická křivka je anomální, a řešení ECDLP by tuto složitost také nepřekročil. Existoval by tedy způsob, jak rychle řešit ECDLP na určité podmnožině eliptických křivek nad konečným tělesem. To by pak zákonitě mělo značný dopad na bezpečnost všude tam, kde se spoléhá na to, že ECDLP rychle řešit nelze.

Algoritmus řešící ECDLP na anomálních eliptických křivkách v polynomiálním čase skutečně existuje a je znám jako *Smartův útok*. Podrobně se mu budeme věnovat v následující kapitole.

Kapitola 3

Smartův útok

Smartův útok lze rozdělit do několika kroků a souvisejících tematických okruhů, které pro větší přehlednost nejprve rozebereme zvlášť. Na závěr pak všechny dosavadní poznatky spojíme do jednoho logického celku.

3.1 p-adická čísla

Definice 3.1. Mějme prvočíslo p. Pro libovolné nenulové $a \in \mathbb{Z}$ ať $\mathrm{ord}_p(a)$ je nejvyšší mocnina p, která dělí a. Pro $x \in \mathbb{Q}$, kde $x = a/b$, definujme $\mathrm{ord}_p(x)$ jako $\mathrm{ord}_p(a) - \mathrm{ord}_p(b)$. Dále definujme zobrazení $|\ |_p$ na $\mathbb{Q}$ následovně [19]:

$$|x|_p = \begin{cases} \frac{1}{p^{\mathrm{ord}_p(x)}}, \text{ pro } x \neq 0; \\ 0, \text{ pro } x = 0. \end{cases}$$

Zobrazení $|\ |_p$ je norma na $\mathbb{Q}$ [19]. Na jejím základě můžeme na $\mathbb{Q}$ zavést metriku.

Definice 3.2. Pro $x, y \in \mathbb{Q}$ ať $\mathrm{d}_p(x, y) = |x - y|_p$ [3].

Poznámka 3.3. Zobrazení d_p je metrika na $\mathbb{Q}$ [3].

Definice 3.4. Mějme metrický prostor (X, d) a ať $\{x_n\}_{n\in\mathbb{N}}$ je posloupnost prvků X. Řekneme, že $\{x_n\}_{n\in\mathbb{N}}$ je *konvergentní posloupnost*, pokud existuje $x \in X$ takové, že

$$\lim_{n\to\infty} \mathrm{d}(x_n, x) = 0,$$

tedy že pro každé $\epsilon > 0$ existuje $N \in \mathbb{N}$ takové, že

$$n \geq N \Rightarrow \mathrm{d}(x_n, x) < \epsilon.$$

V takovém případě řekneme, že $\{x_n\}_{n\in\mathbb{N}}$ *konverguje* k x neboli že x *je limitou* $\{x_n\}_{n\in\mathbb{N}}$ [20].

Definice 3.5. Mějme metrický prostor (X, d) a ať $\{x_n\}_{n\in\mathbb{N}}$ je posloupnost prvků X. Řekneme, že posloupnost $\{x_n\}_{n\in\mathbb{N}}$ je *cauchyovská*, pokud pro každé $\epsilon > 0$ existuje $N \in \mathbb{N}$ takové, že [20]

$$m, n \geq N \Rightarrow \mathrm{d}(x_m, x_n) < \epsilon.$$

Definice 3.6. Mějme metrický prostor (X, d). Pokud každá cauchyovská posloupnost v (X, d) konverguje k nějakému prvku X, řekneme, že (X, d) je *úplný* [20].

Definice 3.7. Vezměme množinu cauchyovských posloupností $\{a_i\}$ racionálních čísel. Dvě takové posloupnosti budeme považovat za ekvivalentní, pokud

$$\lim_{i\to\infty} \mathrm{d}_p(a_i, b_i) = 0.$$

Množinu *p-adických čísel* $\mathbb{Q}_p$ pak definujeme jako množinu tříd ekvivalence těchto posloupností [19].

Poznámka 3.8.

a) Metrický prostor $(\mathbb{Q}, \mathrm{d}_p)$ není úplný. Sestává z tříd ekvivalence obsahujících konstantní (a tedy cauchyovské) posloupnosti racionálních čísel [19].

b) Pro třídu ekvivalence $a \in \mathbb{Q}_p$ obsahující posloupnost $\{a_i\}$ můžeme definovat normu $|\ |_p$ jako
$$|a|_p = \lim_{i\to\infty} |a_i|_p.$$
Tato norma je pak zobecněním normy dané definicí 3.1 z $\mathbb{Q}$ na $\mathbb{Q}_p$. A pokud na jejím základě zavedeme na $\mathbb{Q}_p$ metriku d_p analogicky s definicí 3.2, je metrický prostor $(\mathbb{Q}_p, \mathrm{d}_p)$ zúplněním $(\mathbb{Q}, \mathrm{d}_p)$. Tedy $(\mathbb{Q}_p, \mathrm{d}_p)$ je úplný [19].

Příklad 3.9. Řekněme, že chceme určit vzdálenost 1 a $\frac{1}{25}$ v $\mathbb{Q}_5$. Zajímá nás tedy hodnota $\mathrm{d}_5(1, \frac{1}{25})$. Potom

$$\mathrm{d}_5\left(1, \frac{1}{25}\right) = \left|1 - \frac{1}{25}\right|_5 = \left|\frac{24}{25}\right|_5 = \frac{1}{5^{\mathrm{ord}_5(\frac{24}{25})}},$$

kde

$$\mathrm{ord}_5\left(\frac{24}{25}\right) = \mathrm{ord}_5(24) - \mathrm{ord}_5(25) = 0 - 2 = -2.$$

Ve výsledku je tedy $\mathrm{d}_5\left(1, \frac{1}{25}\right) = 25$.

Poznámka 3.10. Každé $x \in \mathbb{Q}_p$ může být zapsáno ve formě nekonečné řady

$$x = c_{-n}p^{-n} + \ldots + c_0 + c_1 p + \ldots + c_m p^m + \ldots,$$

kde $\forall i \in \mathbb{Z} : c_i \in \mathbb{Z}, 0 \leq c_i \leq p - 1$ [3].

Definice 3.11. Množinou *p-adických celých čísel* $\mathbb{Z}_p$ budeme rozumět všechna $x \in \mathbb{Q}_p$ splňující $|x|_p \leq 1$ [19].

Poznámka 3.12. Kterékoli $x \in \mathbb{Z}_p$ je tedy tvaru $c_0 + c_1 p + \ldots + c_m p^m + \ldots$

Příklad 3.13. Ukážeme, jak určit rozvoj z poznámky 3.10 pro $\frac{1}{35} \in \mathbb{Q}_p$. Vidíme, že $\frac{1}{35} = \frac{1}{5} * \frac{1}{7}$. Prozatím se budeme zabývat rozvojem $\frac{1}{7}$. Najdeme $k \in \{0, 1, 2, 3, 4\}$ takové, že

$$\frac{1}{7} = k + 5 * q$$

pro nějaké $q \in \mathbb{Z}_5$. Platí

$$\frac{1}{7} = 3 + 5\left(-\frac{4}{7}\right).$$

Dál hledáme analogické vyjádření vždy pro nově získané q:

$$\begin{array}{l|l} -\frac{4}{7} = 3 + 5\left(-\frac{5}{7}\right), & -\frac{3}{7} = 1 + 5\left(-\frac{2}{7}\right), \\ -\frac{5}{7} = 0 + 5\left(-\frac{1}{7}\right), & -\frac{2}{7} = 4 + 5\left(-\frac{6}{7}\right), \\ -\frac{1}{7} = 2 + 5\left(-\frac{3}{7}\right), & -\frac{6}{7} = 2 + 5\left(-\frac{4}{7}\right). \end{array}$$

Nyní jsme znovu získali $q = -\frac{4}{7}$. Hodnoty nalezené tímto postupem by se proto začaly periodicky opakovat. Dáme-li dohromady, co jsme doposud spočetli, máme

$$\begin{aligned} \frac{1}{7} &= 3 + 5\left(3 + 5\left(0 + 5\left(2 + 5\left(1 + 5\left(4 + 5\left(2 + 5\left(-\frac{4}{7}\right)\right)\right)\right)\right)\right)\right) \\ &= 3 + 3 * 5 + 0 * 5^2 + 2 * 5^3 + 1 * 5^4 + 4 * 5^5 + 2 * 5^6 + \ldots, \end{aligned}$$

přičemž víme, že další koeficienty budou dané periodicky se opakující posloupností $(3, 0, 2, 1, 4, 2)$. Teď již stačí zauvažovat $\frac{1}{5}$, kterou jsme na začátku vytkli, a získáme

$$\frac{1}{35} = \frac{1}{5} * \frac{1}{7} = 3 * 5^{-1} + 3 + 0 * 5 + 2 * 5^2 + 1 * 5^3 + 4 * 5^4 + 2 * 5^5 + \ldots,$$

kde další koeficienty se periodicky opakují, jak bylo popsáno výše.

Algoritmus provedení operací $+, -, *, /$ v $\mathbb{Q}_p$ je do značné míry analogický algoritmu odpovídajících operací v desítkové soustavě. Při sčítání a násobení zde probíhá přenos ke koeficientu u vyšší mocniny p, tak jako se v desítkové soustavě přenáší k vyšší mocnině 10. Podobně je tomu s „vypůjčením“ při odčítání. Dělení pak ze všeho nejvíce připomíná princip dělení polynomů.

Množina $\mathbb{Q}_p$ spolu s těmito operacemi tvoří těleso [19].

Příklad 3.14. Základní aritmetické operace v $\mathbb{Q}_7$ [19]:

$$\begin{array}{r} 5+3*7+0*7^2+1*7^3+\ldots \\ +\ 2+4*7+3*7^2+2*7^3+\ldots \\ \hline 0+1*7+4*7^2+3*7^3+\ldots \end{array}$$

$$\begin{array}{r} 2*7^{-1}+0+3*7+\ldots \\ -\ 4*7^{-1}+6+5*7+\ldots \\ \hline 5*7^{-1}+0+4*7+\ldots \end{array}$$

$$\begin{array}{r} 3+6*7+2*7^2+\ldots \\ *\ 4+5*7+1*7^2+\ldots \\ \hline 5+4*7+4*7^2+\ldots \\ 1*7+4*7^2+\ldots \\ 3*7^2+\ldots \\ \hline 5+5*7+4*7^2+\ldots \end{array}$$

$$\begin{array}{r} 1+2*7+4*7^2+\ldots \\ \underline{1+6*7+1*7^2+\ldots} \\ 3*7+2*7^2+\ldots \\ \underline{3*7+5*7^2+\ldots} \\ 4*7^2+\ldots \\ \underline{4*7^2+\ldots} \end{array} \quad / \ 3+5*7+1*7^2+\ldots \quad = 5+1*7+6*7^2+\ldots$$

3.2 Redukce modulo p

Odsud dále budeme předpokládat, že pro prvočíslo p vždy platí $p > 3$. Pro menší p bychom se totiž pohybovali na eliptických křivkách tak malého řádu, že by nebyl problém vyřešit na nich ECDLP téměř okamžitě i bez použití jakkoli sofistikovaného algoritmu.

Definice 3.15. Mějme eliptickou křivku nad $\mathbb{Q}_p$. Rovnice této křivky může být zapsána s koeficienty v $\mathbb{Z}_p$ [21]. Ať

$$E(\mathbb{Q}_p) : y^2 = x^3 + ax + b$$

je takový zápis. *Redukcí eliptické křivky E modulo p* budeme rozumět křivku

$$E'(\mathbb{F}_p) : y^2 = x^3 + cx + d, \text{ kde } c = a \bmod p \text{ a } d = b \bmod p.$$

Definice 3.16. Máme-li bod $S \in E(\mathbb{Q}_p)$, můžeme najít jeho homogenní souřadnice (x, y, w) takové, že $x, y, w \in \mathbb{Z}_p$, přičemž alespoň jedna ze souřadnic je v $\mathbb{Z}_p \setminus p\mathbb{Z}_p$ [21]. Potom bod $S' \in E'(\mathbb{F}_p)$, jehož homogenními souřadnicemi jsou $(x \bmod p, y \bmod p, w \bmod p)$, nazveme *redukcí bodu S modulo p*.

Poznámka 3.17. Zobrazení přiřazující bodu $S \in E(\mathbb{Q}_p)$ jeho redukci modulo p $S' \in E'(\mathbb{F}_p)$ budeme značit $\mathrm{red}_p()$.

3.3 Zdvih do $\mathbb{Q}_p$

Mějme eliptickou křivku $\bar{E}(\mathbb{F}_p)$ danou předpisem

$$Y^2 = X^3 + \bar{a}X + \bar{b}, \tag{3.1}$$

kde $\bar{a}, \bar{b} \in \mathbb{F}_p$, a její bod $\bar{S}$. Ukážeme, jak získat křivku $E(\mathbb{Q}_p)$ a na ní ležící bod S tak, že aplikujeme-li na $E(\mathbb{Q}_p)$ a S redukci modulo p, výsledkem bude původní $\bar{E}(\mathbb{F}_p)$ a $\bar{S}$.

3.3.1 Zdvih křivky

Zdvihem křivky $\bar{E}(\mathbb{F}_p)$ může být libovolná eliptická křivka $E(\mathbb{Q}_p)$ daná rovnicí tvaru

$$\begin{aligned} Y^2 &= X^3 + aX + b \\ &= X^3 + (\bar{a} + kp)X + (\bar{b} + lp), \end{aligned} \tag{3.2}$$

kde $k, l \in \mathbb{Z}_p$. Může se tedy jednat i o křivku danou původní rovnicí (3.1). Že se eliptická křivka daná rovnicí (3.2) redukuje na původní $\bar{E}$, je vidět přímo z definice 3.15.

3.3.2 Zdvih bodu

Mějme $\bar{S} = (\bar{x}, \bar{y}) \in \bar{E}(\mathbb{F}_p)$ a hledaný zdvih $S = (x, y) \in E(\mathbb{Q}_p)$. Zvolíme $x = \bar{x}$ a najdeme takové y, aby S (s ohledem na zvolené x) splňovalo rovnici určující $E(\mathbb{Q}_p)$, tj. rovnici (3.2) [3, 22]. Nyní ukážeme, jak toto y najít.

Hledané y je prvkem $\mathbb{Q}_p$, a je proto tvaru

$$y_{-n}p^{-n} + \ldots + y_0 + y_1 p + \ldots + y_m p^m + \ldots$$

Musíme tedy určit koeficienty $y_i \in \{0, \ldots, p-1\}$ (až do požadovaného stupně rozvoje). Označme

$$\begin{aligned} A &= \bar{x}^3 + a\bar{x} + b \in \mathbb{Z}, \\ f(y) &= y^2 - A. \end{aligned}$$

Věta 3.18. *(Henselovo lemma)*
Mějme polynom $f(X) \in \mathbb{Z}[X]$. Předpokládejme, že $x \in \mathbb{Z}$ je kořen f modulo p^s pro $s \geq 1$ a že $f'(x)$ je invertibilní modulo p. Pak existuje jednoznačně určený kořen $x' \in \mathbb{Z}/p^{s+1}\mathbb{Z}$ polynomu f modulo p^{s+1} splňující

$$x' \equiv x \pmod{p^s}.$$

Pro důkaz vizte [23].

Ověříme podmínky Henselova lemmatu pro polynom $f(y)$. Jeho kořen modulo p známe. Je jím $\bar{y}$, jelikož $\bar{S} \in \bar{E}(\mathbb{F}_p)$, neboli

$$\begin{aligned}\bar{y}^2 &\equiv \bar{x}^3 + \bar{a}\bar{x} + \bar{b} \pmod{p} \\ &\equiv \bar{x}^3 + a\bar{x} + b \pmod{p}.\end{aligned}$$

Zřejmě platí

$$f'(y) = 2y.$$

Druhým požadavkem je, aby $f'(\bar{y})$ bylo invertibilní modulo p, tj. aby $p \nmid 2\bar{y}$. Předpokládáme, že $p > 3$. Potom je třeba, aby $p \nmid \bar{y}$.

Uvažme situaci, kdy to tak není, tedy kdy $p \mid \bar{y}$. Pak

$$\bar{S} = (\bar{x}, 0) \in \bar{E}(\mathbb{F}_p)$$

pro nějaké $\bar{x} \in \mathbb{F}_p$. A vzhledem ke způsobu, jakým je zavedeno sčítání na eliptické křivce (případ 3b), je

$$2\bar{S} = \mathcal{O}.$$

Jinými slovy, bod $\bar{S}$ je řádu 2, respektive podgrupa generovaná bodem $\bar{S}$ je řádu 2. Dle *Lagrangeovy věty* (pro přesné znění a důkaz vizte [24]) potom platí $2 \mid \#\bar{E}(\mathbb{F}_p) = p$. p je prvočíslo, proto je pak nutně $p = 2$. To je ale spor s předpokladem $p > 3$. I druhá podmínka Henselova lemmatu je tedy splněna.

Označme $z_0 = \bar{y}$ (kořen $f(y)$ modulo p). Dle Henselova lemmatu $\exists z_1 \in \mathbb{Z}$:

$$\begin{aligned}f(z_1) &\equiv 0 \pmod{p^2}, \\ z_1 &\equiv z_0 \pmod{p}.\end{aligned}$$

Obecně řešíme problém, kdy pro známé z_i, $i \geq 0$ splňující

$$f(z_i) \equiv 0 \pmod{p^{i+1}}$$

hledáme z_{i+1} splňující

$$f(z_{i+1}) \equiv 0 \pmod{p^{i+2}},$$

přičemž z Henselova lemmatu víme, že takové z_{i+1} existuje a platí

$$z_{i+1} \equiv z_i \pmod{p^{i+1}}.$$

Potom $\exists t_{i+1} \in \mathbb{Z}$:

$$z_{i+1} = z_i + t_{i+1}p^{i+1}.$$

A tedy

$$\begin{aligned}f(z_{i+1}) = (z_i + t_{i+1}p^{i+1})^2 - A &\equiv 0 \pmod{p^{i+2}}, \\ {z_i}^2 + 2z_i t_{i+1}p^{i+1} + {t_{i+1}}^2 p^{2(i+1)} - A &\equiv 0 \pmod{p^{i+2}}, \\ 2z_i t_{i+1}p^{i+1} + {z_i}^2 - A &\equiv 0 \pmod{p^{i+2}},\end{aligned}$$

kde

$$z_i{}^2 - A \equiv 0 \pmod{p^{i+1}}.$$

Můžeme tedy označit

$$B = \frac{z_i{}^2 - A}{p^{i+1}} \in \mathbb{Z}$$

a pokračovat:

$$\begin{aligned} 2z_i t_{i+1} + B &\equiv 0 \pmod{p}, \\ t_{i+1} &\equiv (-B)2^{-1} z_i{}^{-1} \pmod{p}. \end{aligned}$$

Existence obou inverzí výše je dána předpokladem $p > 3$ a $p \nmid z_0$. Pro získané z_{i+1} pak platí

$$\begin{aligned} z_{i+1} &\equiv z_i \pmod{p^{i+1}}, \\ z_{i+1} &\equiv z_{i-1} + t_i p^i \pmod{p^{i+1}}, \\ z_{i+1} &\equiv z_{i-2} + t_{i-1} p^{i-1} + t_i p^i \pmod{p^{i+1}}, \\ &\vdots \\ z_{i+1} &\equiv z_0 + t_1 p + \ldots + t_{i-1} p^{i-1} + t_i p^i \pmod{p^{i+1}}. \end{aligned}$$

Což je přesně hledaný rozvoj y.

Zbývá ověřit, že redukce $S' = (x', y')$ takto získaného bodu $S = (x, y) \in E(\mathbb{Q}_p)$ je původní $\bar{S} = (\bar{x}, \bar{y}) \in E(\mathbb{F}_p)$. Zřejmě platí $\bar{x} = x = x'$. A jelikož

$$y \equiv \bar{y} + t_1 p + \ldots + t_i p^i \pmod{p^{i+1}},$$

je

$$y \equiv \bar{y} \pmod{p}.$$

Proto $y' = \bar{y}$, a tedy $S' = \bar{S}$.

Příklad 3.19. Mějme eliptickou křivku $\bar{E}$ danou rovnicí $y^2 = x^3 + 3x + 5$. To ať je zároveň i rovnice určující její zdvih E. Ukážeme, jak spočítat zdvih $P \in E(\mathbb{Q}_7)$ bodu $\bar{P} = (6, 6) \in \bar{E}(\mathbb{F}_7)$.

Souřadnici x bodu P zvolíme stejnou jako u $\bar{P}$, tj. 6. Dosadíme-li do rovnice křivky, máme

$$y^2 = 6^3 + 3 * 6 + 5 = 239.$$

Tato rovnice je modulo 7 určitě splněna pro souřadnici y bodu $\bar{P}$. Označíme tedy $z_0 = 6$ (budeme se držet stejného značení jako v obecném odvození výše). Z Henselova lemmatu víme, že $\exists z_1 \in \mathbb{Z}$:

$$\begin{aligned} z_1{}^2 &\equiv 239 \pmod{7^2}, \\ z_1 &\equiv z_0 \pmod{7}. \end{aligned} \tag{3.3}$$

Vyjádříme tedy z_1 jako $z_0 + 7t_1 = 6 + 7t_1$ a dosadíme zpět do rovnice (3.3):

$$\begin{aligned}(6+7t_1)^2 &\equiv 239 \pmod{7^2}\\ 36 + 12 * 7t_1 + 7^2{t_1}^2 &\equiv 43 \pmod{7^2}\\ 12 * 7t_1 &\equiv 7 \pmod{7^2}\\ 12t_1 &\equiv 1 \pmod 7\\ 5t_1 &\equiv 1 \pmod 7\\ t_1 &\equiv 3 \pmod 7.\end{aligned}$$

Odtud vidíme, že $z_1 = 6 + 3 * 7$. Nyní z Henselova lemmatu plynou vztahy

$$\begin{aligned}{z_2}^2 &\equiv 239 \pmod{7^3},\\ z_2 &\equiv z_1 \pmod{7^2}\end{aligned} \tag{3.4}$$

pro nějaké $z_2 \in \mathbb{Z}$. z_2 je tedy tvaru $z_1 + 7^2t_2 = 6 + 3 * 7 + 7^2t_2 = 27 + 7^2t_2$. Dosadíme do rovnice (3.4):

$$\begin{aligned}(27+7^2t_2)^2 &\equiv 239 \pmod{7^3}\\ 729 + 54 * 7^2t_2 + 7^4{t_2}^2 &\equiv 239 \pmod{7^3}\\ 54 * 7^2t_2 &\equiv 196 \pmod{7^3}\\ 54t_2 &\equiv 4 \pmod 7\\ 5t_2 &\equiv 4 \pmod 7\\ t_2 &\equiv 5 \pmod 7.\end{aligned}$$

Máme tedy $z_2 = 6 + 3 * 7 + 5 * 7^2$. Další členy rozvoje druhé souřadnice zdvihu $P = (6, 6 + 3 * 7 + 5 * 7^2 + \ldots)$ bychom spočetli naprosto analogicky.

Smartův útok staví mimo jiné na vztazích mezi některými podgrupami grupy $E(\mathbb{Q}_p)$ (tj. zdvihu původní křivky). Konkrétně se jedná o dva izomorfismy, které ve Smartově útoku hrají důležitou roli a které podrobněji rozebereme.

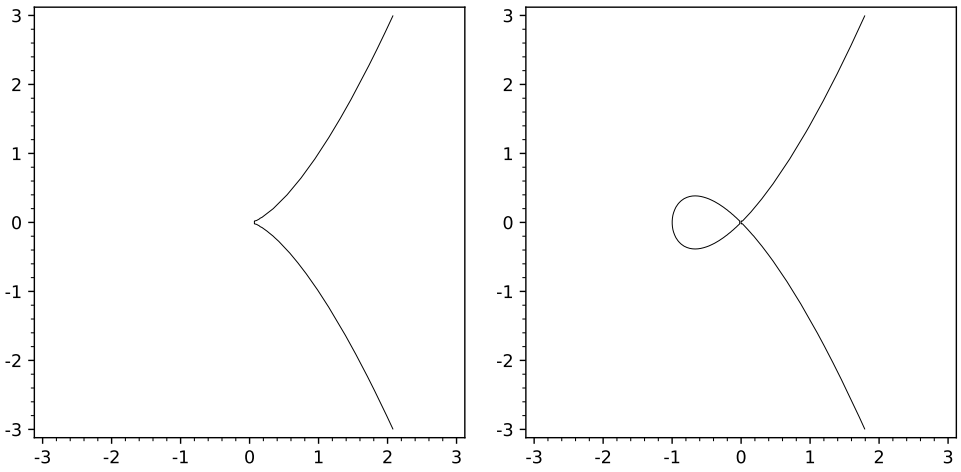
3.4 První izomorfismus

Definice 3.20. Mějme křivku E nad tělesem K danou Weierstrassovou rovnicí. Výrazem $E_{ns}(K)$ budeme značit množinu všech bodů křivky E, které nejsou singulární [21].

Poznámka 3.21.

a) *Singulární bod* je v principu takový bod, v němž se na křivce tvoří „hrot“ či „uzel“(vizte obrázky 3.1a, respektive 3.1b). Je-li

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$



(a) $y^2 = x^3$ (b) $y^2 = x^3 + x^2$

Obrázek 3.1: Singulární křivky

Weierstrassova rovnice udávající křivku E a P singulární bod na E, je

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0.$$

Přesný způsob zavedení singulárního bodu je k nalezení v [21] (kapitola 3).

b) V definici 3.20 se skutečně hovoří o libovolné křivce dané Weierstrassovou rovnicí. Nemusí se jednat o eliptickou křivku. Eliptická křivka dokonce žádné singulární body nikdy mít nebude, jelikož křivka daná Weierstrassovou rovnicí je singulární (tj. obsahuje singulární bod) právě tehdy, když je její diskriminant nulový [21], a diskriminant eliptické křivky je z definice různý od nuly.

c) Množina $E_{ns}(K)$ spolu s operací sčítání, jak byla zavedena v sekci 1.1.1, tvoří grupu [21].

Definice 3.22. Mějme eliptickou křivku E nad $\mathbb{Q}_p$ a její redukci modulo p E'. Množiny $E_0(\mathbb{Q}_p)$ a $E_1(\mathbb{Q}_p)$ definujeme následovně [21]:

$$E_0(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) : \mathrm{red}_p(P) \in E'_{ns}(\mathbb{F}_p)\},$$
$$E_1(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) : \mathrm{red}_p(P) = \mathcal{O} \in E'(\mathbb{F}_p)\}.$$

Definice 3.23. Mějme posloupnost

$$G_1 \xrightarrow{h_1} G_2 \xrightarrow{h_2} \dots \xrightarrow{h_n} G_{n+1},$$

kde $G_i, i \in \{1, \ldots, n+1\}$ jsou grupy a $h_i, i \in \{1, \ldots, n\}$ jsou homomorfismy z G_i do G_{i+1}. Řekneme, že tato posloupnost je *exaktní*, pokud

$$\forall i \in \{1, \ldots, n-1\} : \mathrm{im}(h_i) = \ker(h_{i+1}).$$

Poznámka 3.24. Máme-li exaktní posloupnost obsahující podposloupnost

$$\ldots \longrightarrow A \xrightarrow{g} B \xrightarrow{h} 0 \longrightarrow \ldots,$$

kde 0 značí triviální grupu, je g na B [25].

Věta 3.25. *Mějme homomorfismy $h_1 : \{\mathcal{O}\} \longrightarrow E_1(\mathbb{Q}_p)$, $h_2 : E_1(\mathbb{Q}_p) \longrightarrow E_0(\mathbb{Q}_p)$ a $h_4 : E'_{ns}(\mathbb{F}_p) \longrightarrow \{\mathcal{O}\}$. Pak posloupnost*

$$\{\mathcal{O}\} \xrightarrow{h_1} E_1(\mathbb{Q}_p) \xrightarrow{h_2} E_0(\mathbb{Q}_p) \xrightarrow{\mathrm{red}_p} E'_{ns}(\mathbb{F}_p) \xrightarrow{h_4} \{\mathcal{O}\}$$

je exaktní. Pro důkaz vizte [21].

Poznámka 3.26. V [21] autor nepracuje konkrétně s tělesy $\mathbb{Q}_p$ a $\mathbb{F}_p$. Věta odpovídající větě 3.25 a celá příslušná kapitola (kapitola 7) je zpracována obecněji. Tato kapitola kromě věty výše obsahuje další důležité poznatky osvětlující Smartův útok. Proto zde pro snazší orientaci uvádíme, jaká je konkrétní podoba obecných struktur používaných napříč kapitolou, dívá-li se na ni čtenář z pohledu Smartova útoku:

v – diskrétní valuace	ord_p,
K – lokální těleso, úplné vzhledem k v	$\mathbb{Q}_p$ (podmínky splněny dle [26]),
$R = \{x \in K : v(x) \geq 0\}$	$\mathbb{Z}_p$,
$R^* = \{x \in K : v(x) = 0\}$	$\mathbb{Z}_p \setminus p\mathbb{Z}_p$,
$\mathcal{M} = \{x \in K : v(x) > 0\}$	$p\mathbb{Z}_p$,
π – prvek R takový, že $\mathcal{M} = \pi R$	p,
$k = R/\mathcal{M}$	$\mathbb{F}_p$.

Věta 3.27. *(První věta o izomorfismu)*
Mějme grupy G a G'. θ ať je homomorfismus G na G'. Potom platí

$$G/\ker(\theta) \cong G'.$$

Pro důkaz vizte [27].

Vyjdeme z věty 3.25. Ta nám mimo jiné říká, že zobrazení red_p je homomorfismus z $E_0(\mathbb{Q}_p)$ do $E'_{ns}(\mathbb{F}_p)$. Zároveň z ní vidíme, že existuje podposloupnost exaktní posloupnosti tvaru

$$\ldots \longrightarrow E_0(\mathbb{Q}_p) \xrightarrow{\mathrm{red}_p} E'_{ns}(\mathbb{F}_p) \xrightarrow{h_4} \{\mathcal{O}\}.$$

Dle poznámky 3.24 je pak red_p na $E'_{ns}(\mathbb{F}_p)$. Díky tomu můžeme použít První větu o izomorfismu. Z té plyne

$$E_0(\mathbb{Q}_p)/\ker(\mathrm{red}_p) \cong E'_{ns}(\mathbb{F}_p). \tag{3.5}$$

Jak bylo popsáno v sekci 3.3, zdvih E původní křivky $\bar{E}$ je proveden tak, aby pro redukci modulo p E' zdvihu E platilo $E' = \bar{E}$. Víme, že $\bar{E}$ je eliptická křivka a jako taková není singulární. Proto ani E' není singulární, a tedy

$$E'_{ns}(\mathbb{F}_p) = E'(\mathbb{F}_p) = \bar{E}(\mathbb{F}_p). \tag{3.6}$$

Vrátíme-li se k definici 3.22, můžeme nyní psát

$$\begin{aligned} E_0(\mathbb{Q}_p) &= \{P \in E(\mathbb{Q}_p) : \mathrm{red}_p(P) \in E'_{ns}(\mathbb{F}_p)\} \\ &= \{P \in E(\mathbb{Q}_p) : \mathrm{red}_p(P) \in E'(\mathbb{F}_p)\} \\ &= E(\mathbb{Q}_p). \end{aligned} \tag{3.7}$$

Zároveň vidíme, že

$$\begin{aligned} E_1(\mathbb{Q}_p) &= \{P \in E(\mathbb{Q}_p) : \mathrm{red}_p(P) = \mathcal{O} \in E'(\mathbb{F}_p)\} \\ &= \ker(\mathrm{red}_p). \end{aligned} \tag{3.8}$$

Z rovnic (3.5), (3.6), (3.7) a (3.8) získáme první ze dvou zmíněných izomorfismů

$$E(\mathbb{Q}_p)/E_1(\mathbb{Q}_p) \cong \bar{E}(\mathbb{F}_p).$$

Nebude-li řečeno jinak, sekce 3.5 a 3.6 budou vycházet z [21].

3.5 Rozvoj v okolí $\mathcal{O}$

Mějme eliptickou křivku E nad tělesem K danou Weierstrassovou rovnicí

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Jak je vidět z homogenních souřadnic $(0, 1, 0)$ bodu $\mathcal{O}$, o $\mathcal{O}$ uvažujeme jako o bodu, který bychom získali, pokud bychom do nekonečna postupovali po přímce rovnoběžné s osou y. Provedeme-li tedy záměnu souřadnic

$$z = -\frac{x}{y} \quad \text{a} \quad w = -\frac{1}{y},$$

odpovídá $\mathcal{O}$ bodu $(z, w) = (0, 0)$. Zároveň rovnice (1.1) pak bude tvaru

$$w = z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2 + a_6w^3 = f(z, w).$$

Pokud tuto rovnici budeme rekurzivně dosazovat do sebe samotné, získáme vyjádření w jako mocninné řady v z:

$$\begin{aligned} w &= z^3 + (a_1 z + a_2 z^2)w + (a_3 + a_4 z)w^2 + a^6 w^3 \\ &= z^3 + (a_1 z + a_2 z^2)\left[z^3 + (a_1 z + a_2 z^2)w + (a_3 + a_4 z)w^2 + a_6 w^3\right] \\ &\quad + (a_3 + a_4 z)\left[z^3 + (a_1 z + a_2 z^2)w + (a_3 + a_4 z)w^2 + a_6 w^3\right]^2 \\ &\quad + a_6\left[z^3 + (a_1 z + a_2 z^2)w + (a_3 + a_4 z)w^2 + a_6 w^3\right] \\ &\vdots \\ &= z^3(1 + A_1 z + A_2 z^2 + \ldots). \end{aligned}$$

Kde pro A_n, $n \in \mathbb{N}$, platí $A_n \in \mathbb{Z}[a_1, \ldots, a_6]$. Tj. A_n jsou polynomy v koeficientech křivky E. Z tohoto vyjádření $w(z)$ pak můžeme odvodit

$$\begin{aligned} x(z) &= \frac{z}{w(z)} = \frac{1}{z^2} - \frac{a_1}{z} - a_2 - a_3 z - (a_4 + a_1 a_3)z^2 - \ldots, \\ y(z) &= -\frac{1}{w(z)} = -\frac{1}{z^3} + \frac{a_1}{z^2} + \frac{a_2}{z} + a_3 + (a_4 + a_1 a_3)z - \ldots \end{aligned}$$

Aby bod eliptické křivky mohl být popsán parametrem z, musí řada $x(z)$ konvergovat. Což je podmínka, která je pro $K = \mathbb{Q}_p$, $z \in p\mathbb{Z}_p$ a $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}_p$ splněna [3].

Máme-li body $(x(z_1), y(z_1))$, $(x(z_2), y(z_2))$ popsané parametry z_1, z_2, můžeme jejich součet popsat nekonečnou řadou

$$F(z_1, z_2) = z_1 + z_2 - a_1 z_1 z_2 - a_2({z_1}^2 z_2 + z_1 {z_2}^2) + \ldots$$

Definice 3.28. Pro $K = \mathbb{Q}_p$ definujeme grupu $\hat{E}(p\mathbb{Z}_p)$ jako množinu $p\mathbb{Z}_p$ s operací sčítání danou zobrazením F.

Poznámka 3.29.

a) Máme-li tedy $z_1, z_2 \in \hat{E}(p\mathbb{Z}_p)$, je $z_1 + z_2 = F(z_1, z_2)$.

b) Grupa $\hat{E}$ se označuje jako *formální grupa asociovaná s eliptickou křivkou* E.

Definice 3.30. Pro $z \in \hat{E}(p\mathbb{Z}_p)$ označme

$$v_p(z) = \left(\frac{z}{w(z)}, -\frac{1}{w(z)}\right).$$

Poznámka 3.31. Zobrazení v_p je izomorfismus $\hat{E}(p\mathbb{Z}_p)$ do $E_1(\mathbb{Q}_p)$.

Definice 3.32. Pro $n \in \mathbb{N}$ definujeme

$$E_n(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) : \mathrm{ord}_p(x(P)) \leq -2n\} \cup \{\mathcal{O}\},$$

kde $x(P)$ značí souřadnici x bodu P.

Poznámka 3.33.

a) $E_n(\mathbb{Q}_p)$ je podgrupou $E(\mathbb{Q}_p)$ [3].

b) Zobrazení v_p je izomorfismus $\hat{E}(p^n\mathbb{Z}_p)$ do $E_n(\mathbb{Q}_p)$, kde grupa $\hat{E}(p^n\mathbb{Z}_p)$ je množina $p^n\mathbb{Z}_p$ spolu s operací sčítání danou zobrazením F [3].

c) Všimněme si, že definice 3.32 se pro $n = 1$ překrývá s definicí 3.22. Vždy se ale jedná o stejnou grupu $E_1(\mathbb{Q}_p)$. Označme $E_1^1(\mathbb{Q}_p)$ grupu zavedenou definicí 3.22 a $E_1^2(\mathbb{Q}_p)$ grupu $E_1(\mathbb{Q}_p)$ zavedenou definicí 3.32. Mějme $A = (x, y) \in E_1^2(\mathbb{Q}_p)$. Jeho homogenní souřadnice jsou pak tvaru $(x, y, 1)$, kde

$$\mathrm{ord}_p(x) \leq -2.$$

Chceme-li na A aplikovat redukci modulo p, musí být každá z jeho homogenních souřadnic ze $\mathbb{Z}_p$ (vizte definici 3.16). Ekvivalentní homogenní souřadnice splňující tuto podmínku jsou tvaru $(p^i x, p^i y, p^i)$ pro $i \geq 2$. Takový bod se bude redukovat na $\mathcal{O} \in E'(\mathbb{F}_p)$ (vizte sekce 1.2 a 3.2) a je tedy v $E_1^1(\mathbb{Q}_p)$. Z toho plyne

$$E_1^2(\mathbb{Q}_p) \subset E_1^1(\mathbb{Q}_p). \tag{3.9}$$

Jak $E_1^1(\mathbb{Q}_p)$, tak $E_1^2(\mathbb{Q}_p)$ jsou izomorfní s $\hat{E}(p\mathbb{Z}_p)$ (poznámky 3.31 a 3.33b), a jsou tedy izomorfní navzájem. Z toho plyne, že jsou stejného řádu a spolu s inkluzí (3.9) že

$$E_1^1(\mathbb{Q}_p) = E_1^2(\mathbb{Q}_p).$$

3.6 Formální logaritmus

Formální logaritmus – $\log_{\mathcal{F}}$ – je funkce zobrazující formální grupu $\hat{E}(p\mathbb{Z}_p)$ do grupy $p\mathbb{Z}_p$ s běžným sčítáním p-adických čísel. Jedná se o izomorfismus daný předpisem

$$\log_{\mathcal{F}}(T) = T + \frac{c_1}{2}T^2 + \frac{c_2}{3}T^3 + \ldots \in \mathbb{Q}_p[[T]] \tag{3.10}$$

splňující

$$\log_{\mathcal{F}}(F(z_1, z_2)) = \log_{\mathcal{F}}(z_1) + \log_{\mathcal{F}}(z_2)$$

pro libovolné $z_1, z_2 \in p\mathbb{Z}_p$. Platí i obecnější varianta tohoto tvrzení, a to že $\log_{\mathcal{F}}$ je izomorfismem z $\hat{E}(p^n\mathbb{Z}_p)$ do $p^n\mathbb{Z}_p$ pro $n \in \mathbb{N}$ [3]. Podrobněji je $\log_{\mathcal{F}}$ diskutován v [21] (kapitola 4).

Označme

$$\psi_p = \log_{\mathcal{F}} \circ {v_p}^{-1}. \tag{3.11}$$

Pak ψ_p je izomorfismus z $E_n(\mathbb{Q}_p)$ do $p^n\mathbb{Z}_p$, jelikož

$$\log_{\mathcal{F}}({v_p}^{-1}(E_n(\mathbb{Q}_p))) = p^n\mathbb{Z}_p$$

a složení izomorfismů je také izomorfismus.

3.7 Druhý izomorfismus

Mějme $n \in \mathbb{N}$. Všimněme si, že $p^n\mathbb{Z}_p$ se sčítáním p-adických čísel je komutativní grupa (jedná se o podgrupu komutativní grupy $\mathbb{Q}_p$). Jakákoli její podgrupa je tedy normální. Konkrétně $p^{n+1}\mathbb{Z}_p$ je normální podgrupou $p^n\mathbb{Z}_p$. Pak dává dobrý smysl zavést zobrazení

$$\phi : p^n\mathbb{Z}_p \longrightarrow p^n\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p$$

předpisem

$$x \longmapsto x \bmod p^{n+1}.$$

ϕ je zřejmě na $p^n\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p$ a je homomorfismus, jelikož operace modulo zachovává operaci sčítání.

Označíme-li nyní

$$\omega = \phi \circ \psi_p : E_n(\mathbb{Q}_p) \longrightarrow p^n\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p,$$

je i ω homomorfismus na $p^n\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p$. Jedná se totiž o složení dvou surjektivních homomorfismů. V tuto chvíli můžeme použít První větu o izomorfismu pro zobrazení ω. Ta nám říká, že

$$E_n(\mathbb{Q}_p)/\ker(\omega) \cong p^n\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p.$$

Uvážíme-li, že

$$\ker(\omega) = \ker(\phi \circ \psi_p) = {\psi_p}^{-1}(\phi^{-1}(0)) = {\psi_p}^{-1}(p^{n+1}\mathbb{Z}_p) = E_{n+1}(\mathbb{Q}_p),$$

získáváme druhý důležitý izomorfismus

$$E_n(\mathbb{Q}_p)/E_{n+1}(\mathbb{Q}_p) \cong p^n\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p \cong \mathbb{F}_p^+,$$

kde $\mathbb{F}_p^+$ značí aditivní grupu $\mathbb{F}_p$.

3.8 Útok samotný

Mějme anomální eliptickou křivku $\bar{E}$ nad $\mathbb{F}_p$. Pro $\bar{E}$ tedy platí

$$\#\bar{E}(\mathbb{F}_p) = p. \tag{3.12}$$

Dále ať $\bar{P}, \bar{Q} \in \bar{E}(\mathbb{F}_p)$, kde $\bar{Q} = m\bar{P}$ pro nějaké $m \in \mathbb{N}$. Ukážeme, jak najít takové m a vyřešit tím tento ECDLP.

Nejprve spočteme zdvih E křivky $\bar{E}$ a zdvihy $P, Q \in E(\mathbb{Q}_p)$ bodů $\bar{P}$, $\bar{Q}$. Metoda zdvihu do $\mathbb{Q}_p$ je podrobně popsána v sekci 3.3. Dále vezmeme v úvahu redukci modulo p, které jsme se věnovali v sekci 3.2. Věta 3.25 nám říká, že redukce modulo p je homomorfismus, díky čemuž je

$$\operatorname{red}_p(Q - mP) = \operatorname{red}_p(Q) - m\operatorname{red}_p(P) = \bar{Q} - m\bar{P} = \mathcal{O}.$$

Potom dle definice 3.22 platí

$$Q - mP = R \in E_1(\mathbb{Q}_p). \tag{3.13}$$

Nyní využijeme dva izomorfismy, kterým jsou věnované sekce 3.4 a 3.7. Z prvního z nich,

$$E(\mathbb{Q}_p)/E_1(\mathbb{Q}_p) \cong \bar{E}(\mathbb{F}_p),$$

spolu s rovnicí (3.12) je vidět, že p-násobné sečtení sama se sebou zobrazí bod z $E(\mathbb{Q}_p)$ do $E_1(\mathbb{Q}_p)$ [3]. Proto $pP, pQ \in E_1(\mathbb{Q}_p)$. Alternativně bychom mohli totéž nahlédnout z rovnice (3.12) a definice 3.22 následovně:

$$\operatorname{red}_p(pP) = p\operatorname{red}_p(P) = p\bar{P} = \mathcal{O},$$
$$\operatorname{red}_p(pQ) = p\operatorname{red}_p(Q) = p\bar{Q} = \mathcal{O}.$$

Druhý izomorfismus,

$$E_n(\mathbb{Q}_p)/E_{n+1}(\mathbb{Q}_p) \cong \mathbb{F}_p^+,$$

využijeme analogicky s prvním. Tento nám říká, že pro $X \in E_n(\mathbb{Q}_p)$ je $pX \in E_{n+1}(\mathbb{Q}_p)$ [3]. Pak z rovnice (3.13) máme

$$p(Q - mP) = pQ - m(pP) = pR, \tag{3.14}$$

kde $pP, pQ \in E_1(\mathbb{Q}_p)$ a $pR \in E_2(\mathbb{Q}_p)$. Aplikujeme-li na obě strany rovnice (3.14) izomorfismus ψ_p zavedený v sekci 3.6, získáme

$$\psi_p(pQ) - m\psi_p(pP) = \psi_p(pR), \tag{3.15}$$

kde $\psi_p(pQ), \psi_p(pP) \in p\mathbb{Z}_p$ a $\psi_p(pR) \in p^2\mathbb{Z}_p$. Pročež

$$\psi_p(pQ) \equiv m\psi_p(pP) \pmod{p^2},$$
$$pb \equiv mpa \pmod{p^2}$$

pro nějaká $a, b \in \mathbb{Z}_p$. A odsud už můžeme určit hledané m vztahem

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

Takto získané m je určeno modulo p. To nám ovšem stačí, jelikož řád $\bar{E}$ je právě p.

Zbývá ukázat, jak určit hodnoty a, b, tedy jak pro $S \in E_1(\mathbb{Q}_p)$ spočítat $\psi_p(S) \bmod p^2$. Z rovnic (3.5) a definice 3.30 vidíme, že

$$v_p{}^{-1}(S) = -\frac{x(S)}{y(S)} \in p\mathbb{Z}_p,$$

kde $x(S)$ a $y(S)$ značí první, respektive druhou souřadnici bodu S. To nám dohromady s rovnicemi (3.10) a (3.11) dává

$$\psi_p(S) \equiv -\frac{x(S)}{y(S)} \pmod{p^2}.$$

Příklad 3.34. Mějme eliptickou křivku $\bar{E}$ danou rovnicí $y^2 = x^3+3x+5$ a body $\bar{P} = (6,6), \bar{Q} = (1,4) \in \bar{E}(\mathbb{F}_7)$. Ukážeme, jak vyřešit tento ECDLP, tedy jak najít $m \in \mathbb{N}$ takové, že $\bar{Q} = m\bar{P}$.

Zdvihem eliptické křivky $\bar{E}$ zvolíme eliptickou křivku E danou stejnou rovnicí. Spočteme zdvihy $P, Q \in E(\mathbb{Q}_7)$ bodů $\bar{P}$, $\bar{Q}$ (zdvih P jsme již spočetli v příkladu 3.19 a Q lze získat naprosto analogickým postupem). Pro tyto zdvihy platí

$$P = (6, 6 + 3 * 7 + 5 * 7^2 + \ldots),$$
$$Q = (1, 4 + 6 * 7 + 6 * 7^2 + \ldots).$$

Dále nás zajímají body pP a pQ. Ty lze získat za využití informací k zavedení sčítání bodů eliptické křivky ze sekce 1.1.1 a algoritmu 1.12. V tomto případě vyjde

$$pP = (4 * 7^{-2} + 6 * 7^{-1} + \ldots, 6 * 7^{-3} + 1 * 7^{-2} + \ldots),$$
$$pQ = (2 * 7^{-2} + 1 * 7^{-1} + \ldots, 1 * 7^{-3} + 3 * 7^{-2} + \ldots).$$

Na tyto body aplikujeme 7-adický logaritmus ψ_7:

$$\psi_7(pP) = -\frac{4 * 7^{-2} + 6 * 7^{-1} + \ldots}{6 * 7^{-3} + 1 * 7^{-2} + \ldots} \equiv 4 * 7 \pmod{7^2},$$
$$\psi_7(pQ) = -\frac{2 * 7^{-2} + 1 * 7^{-1} + \ldots}{1 * 7^{-3} + 3 * 7^{-2} + \ldots} \equiv 5 * 7 \pmod{7^2}.$$

Tím dostaneme finální vztah

$$\begin{aligned} 5 * 7 &\equiv m * 4 * 7 \pmod{7^2} \\ 5 &\equiv m * 4 \pmod{7} \\ m &\equiv 5 * 4^{-1} \pmod{7} \\ m &\equiv 3 \pmod{7}. \end{aligned}$$

Výsledek můžeme snadno ověřit výpočtem $3\bar{P} = 3(6,6) = (1,4) = \bar{Q}$.

Kapitola 4

Implementace a testování

V předchozích kapitolách jsme vystavěli teorii potřebnou pro chápání principu Smartova útoku a tento útok jsme popsali z matematického hlediska. V této kapitole se budeme zabývat jeho implementací. Zároveň ukážeme, jak generovat anomální eliptické křivky, a provedeme měření časové složitosti Smartova útoku na takto získaných křivkách.

Veškeré uvedené zdrojové kódy budou pro software SAGE. SAGE je volně dostupný open-source software založený na programovacím jazyce Python. Je schopný provádět některé netriviální algebraické operace. Hlavním důvodem pro jeho využití je podpora pro práci jak s eliptickými křivkami, tak s p-adickými čísly. Dokumentace, zdrojový kód i další informace jsou k nalezení v [28].

4.1 p-adická čísla v SAGE

Jak je vidět ze sekce 3.1, abychom mohli v počítači kompletně reprezentovat libovolné p-adické číslo, potřebovali bychom nekonečně mnoho paměti. SAGE proto pracuje s p-adickými čísly s omezenou přesností. Konkrétně SAGE rozeznává dva druhy přesnosti p-adického čísla – *absolutní* a *relativní*.

Je-li $x = c_k x^k + c_{k+1} x^{k+1} + \ldots \in \mathbb{Q}_p$ reprezentováno s absolutní přesností $n \in \mathbb{N}$, jedná se vlastně o reprezentaci modulo p^n,

$$x = c_k x^k + c_{k+1} x^{k+1} + \ldots + c_{n-1} x^{n-1}.$$

Relativní přesnost naproti tomu udává počet členů rozvoje x. S relativní přesností n je tedy

$$x = c_k x^k + c_{k+1} x^{k+1} + \ldots + c_{k+n-1} x^{k+n-1}.$$

Přesnost aritmetických operací je pak omezena přesností operandů. Více k práci s p-adickými čísly v SAGE je k nalezení v [29].

Kdykoli, kdy budeme v dalších sekcích pracovat s p-adickými čísly, budeme používat relativní přesnost.

4.2 Zdvih do $\mathbb{Q}_p$

Výpočet zdvihu bodu z $\bar{E}(\mathbb{F}_p)$ do $E(\mathbb{Q}_p)$ je realizován funkcí *lift*.

Algoritmus 4.1.

```
def lift(P, p, coeff, prec):
  x_P, y_P = P.xy()
  x_lift = ZZ(x_P)
  y_lift = ZZ(y_P)
  a, b = coeff
  half = inverse_mod(2, p)
  A = x_lift^3 + a * x_lift + b

  for i in range(1, prec):
    B = (y_lift^2 - A) / p^i
    t_i = ZZ(mod((-B) * half * inverse_mod(y_lift, p), p))
    y_lift = y_lift + t_i * p^i
  EQp = EllipticCurve(Qp(p, prec), coeff)
  return EQp([x_lift, y_lift])
```

Logika zdrojového kódu výše vychází ze sekce 3.3.2. Význam proměnných A, B a t_i přesně odpovídá tomu z výše uvedené sekce. Vstupní parametr

- P je bod, jehož zdvih hledáme,
- p je řád tělesa $\mathbb{F}_p$,
- *coeff* je dvojice (a, b) parametrů ze zjednodušené Weierstrassovy rovnice určující eliptickou křivku $\bar{E}$,
- *prec* udává stupeň rozvoje souřadnice y zdvihu – tato souřadnice bude spočtena modulo p^{prec}.

4.3 Smartův útok

Následuje kód samotného Smartova útoku.

Algoritmus 4.2.

```
def smarts_attack(P, Q, p, coeff):
  prec = 2
  canonical_lift = True
  while canonical_lift:
    coeff = [ t + randint(0, p) * p for t in coeff ]
    P_Qp = lift(P, p, coeff, prec)
    Q_Qp = lift(Q, p, coeff, prec)
    p_times_P = p * P_Qp
    p_times_Q = p * Q_Qp
```

```
    canonical_lift = p_times_P[2] == 0 or p_times_Q[2] == 0
x_P, y_P = p_times_P.xy()
x_Q, y_Q = p_times_Q.xy()
psi_P = -(x_P / y_P)
psi_Q = -(x_Q / y_Q)
m = psi_Q / psi_P
m = mod(m, p)
return m
```

Zdrojový kód výše vychází z [22] a pro jeho snazší pochopení doporučujeme věnovat pozornost sekci 3.8. Vstupní parametry P, Q jsou body, pro něž platí $Q = mP$, přičemž m je výstupem funkce. Zbylé vstupní parametry odpovídají parametrům shodného názvu popsaným pod algoritmem 4.1.

Poznámka 4.3.

a) V algoritmu 4.2 jsme pro výpočet zdvihů bodů P, Q zvolili přesnost 2. Jedná se totiž o nejnižší postačující přesnost pro provedení Smartova útoku [21].

b) Účelem *while*-cyklu v algoritmu 4.2 je zajistit, že nebyl zvolen nevhodný zdvih původní křivky. Taková situace nastává s pravděpodobností $\frac{1}{p}$, a to v případě, že zvolený zdvih je takzvaně *kanonický* [30]. Nevhodně zvolený zdvih detekujeme kontrolou bodů pP a pQ. Ty musí být vždy různé od $\mathcal{O}$ (tj. jejich třetí homogenní souřadnice musí být různá od 0), jinak by další výpočet vedl na dělení nulou. Takováto kontrola ovšem nemusí stačit, pokud bychom zdvihy bodů P, Q počítali s přesností vyšší, než jaká je uvedena v předchozím bodě. Konkrétní případ, kdy je zvolený zdvih kanonický, je popsán v příkladu 4.4.

c) Algoritmy 4.1 a 4.2 nepočítají s tím, že by některý ze vstupních bodů P, Q byl $\mathcal{O}$. Pokud by tomu tak totiž bylo, řešení vzniklého ECDLP by bylo triviální. Tato možnost tedy v kódu pro větší přehlednost ošetřena není.

Příklad 4.4. Uvažme eliptickou křivku $\bar{E}$ nad $\mathbb{F}_5$ danou rovnicí

$$y^2 = x^3 + 3x + 2 \tag{4.1}$$

a její body $\bar{P} = [1, 1]$, $\bar{Q} = [2, 1]$. I zde budeme s p-adickými čísly pracovat s relativní přesností 2. Zvolíme-li za zdvih křivky $\bar{E}$ eliptickou křivku E nad $\mathbb{Q}_5$ danou také rovnicí (4.1), získáme výše zmiňovaný kanonický zdvih. Pro zdvihy P, Q bodů $\bar{P}$, $\bar{Q}$ pak platí

$$\begin{aligned} P &= [1, 1 + 3 * 5], \\ Q &= [2, 1 + 4 * 5], \\ 5 * P &= \mathcal{O}, \\ 5 * Q &= \mathcal{O}. \end{aligned}$$

Smartův útok v takovém případě není možné dokončit. $\mathcal{O}$ totiž nemůžeme vyjádřit jako bod euklidovského prostoru a se souřadnicemi takového bodu bychom potřebovali následně pracovat.

Nyní zvolme jen mírně odlišný zdvih E původní křivky $\bar{E}$. E ať je dán rovnicí

$$y^2 = x^3 + 8x + 2.$$

Zde je důležité, že 8 je tvaru $3 + k * 5$ pro $k \in \mathbb{Z}$. Zdvihy P, Q původních bodů $\bar{P}$, $\bar{Q}$ pak splňují

$$\begin{aligned} P &= [1, 1 + 5], \\ Q &= [2, 1], \\ 5 * P &= [5^{-2}, 5^{-3}], \\ 5 * Q &= [4 * 5^{-2}, 2 * 5^{-3}] \end{aligned}$$

a Smartův útok je možné provést až do konce.

Použití funkce *smarts_attack* je vidět v následujícím příkladu.

Příklad 4.5.

```
p = 100003
coeff = [1, 1113]
Ep = EllipticCurve(GF(p), coeff)
P = Ep([6855, 33741])
Q = Ep([43749, 26725])
m = smarts_attack(P, Q, p, coeff)
print m
```

4.4 Generování anomálních eliptických křivek

Metoda generování anomálních eliptických křivek popsaná v [3] stojí na hledání prvočísel určitého tvaru a konstrukci samotné eliptické křivky skrze její j-invariant. Konkrétní možné tvary prvočísel p pro $m \in \mathbb{N}$ a příslušné hodnoty j-invariantu jsou zachyceny v tabulce níže. Jak byly tyto hodnoty získány, lze v [3] dohledat. Hledání anomálních křivek vyžaduje hluboké znalosti algebraické geometrie a podrobnější popis je nad rámec této práce.

p	j
$11m(m+1)+3$	-2^{15}
$19m(m+1)+5$	$-2^{15} * 3^3$
$43m(m+1)+11$	$-2^{18} * 3^3 * 5^3$
$67m(m+1)+17$	$-2^{15} * 3^3 * 5^3 * 11^3$
$163m(m+1)+41$	$-2^{18} * 3^3 * 5^3 * 23^3 * 29^3$

Máme-li prvočíslo p některého z výše uvedených tvarů a příslušný j-invariant, můžeme zkonstruovat eliptickou křivku E pomocí rovnice (1.4). Pak nastane jedna ze dvou možností

a) eliptická křivka E je anomální,

b) kvadratický twist eliptické křivky E je anomální [3].

Zvolíme-li tedy například prvočísla tvaru $p = 11m(m+1)+3$, získáme algoritmus 4.6.

Algoritmus 4.6.

```
m_max = 100
for m in range(m_max):
  p = 11 * m * (m + 1) + 3
  j = (-2^15) % p
  if p.is_prime():
    k = (j/(j-1728)) % p
    a = ((-3) * k) % p
    b = (2 * k) % p
    if (4*a^3 + 27*b^2) % p == 0:
      continue
    E = EllipticCurve(GF(p), [a, b])
    if E.order() != p:
      E = E.quadratic_twist()
    print E
```

Poznámka 4.7. S proměnnou *m_max* můžeme pracovat libovolně v rámci $\mathbb{N}$ podle toho, z jakého rozsahu mají být řády nalezených anomálních eliptických křivek.

4.5 Benchmarking

V rámci měření došlo k porovnání algoritmu 4.2 s algoritmy Baby-step giant-step a Pollard's Rho. U posledních dvou jmenovaných byla využita jejich implementace v SAGE. Byly tedy využity funkce *bsgs* a *discrete_log_rho*.

Data, na kterých jsme měřili, sestávala ze 100 anomálních eliptických křivek nad $\mathbb{F}_p$ pro p v rozsahu zhruba 10^5–10^9. Na každé křivce bylo vytvořeno 20 náhodných instancí ECDLP. Na každé z těchto instancí byl měřen čas, který jednotlivé algoritmy potřebovaly k jejímu řešení. Pro každý ze tří algoritmů jsme tak na každé eliptické křivce získali 20 časových údajů. Z těch jsme zaznamenali aritmetický průměr (pro daný algoritmus na dané křivce). U Smartova útoku byla kontrolována i správnost výsledku.

Měření proběhlo na stroji s procesorem Intel Core i5-6300HQ (4 jádra, 2.3 GHz) a 8 GB RAM.

4.5.1 Očekávané výsledky

Jak již bylo řečeno v sekci 2.1, jak Baby-step giant-step, tak Pollard's Rho má časovou složitost $O(\sqrt{n})$ grupových operací, kde n je řád grupy, na níž

ECDLP řešíme. V případě anomálních eliptických křivek jde tedy o složitost $O(\sqrt{p})$.

Podíváme-li se na algoritmus 4.2, vidíme, že jediná část vyžadující operace v grupě bodů eliptické křivky je výpočet bodů pP a pQ. Z poznámky 1.13 víme, že jeden tento výpočet lze provést v čase $O(\log(p))$. V rámci jednoho cyklu máme právě dva takové výpočty, složitost jedné iterace cyklu je tedy stále $O(\log(p))$. Za předpokladu, že funkce *randint* vrací opravdu náhodné číslo z daného rozsahu, je pravděpodobnost, že zvolený zdvih křivky je kanonický, $\frac{1}{p}$ (vizte poznámku 4.3b). Náhodná veličina X počtu iterací, v nichž je zvolen kanonický zdvih, má geometrické rozdělení a pro její střední hodnotu platí

$$\mathrm{E}X = \frac{1-(1-\frac{1}{p})}{1-\frac{1}{p}} = \frac{\frac{1}{p}}{\frac{p-1}{p}} = \frac{1}{p-1}.$$

Střední hodnota celkového počtu provedených iterací cyklu je tak

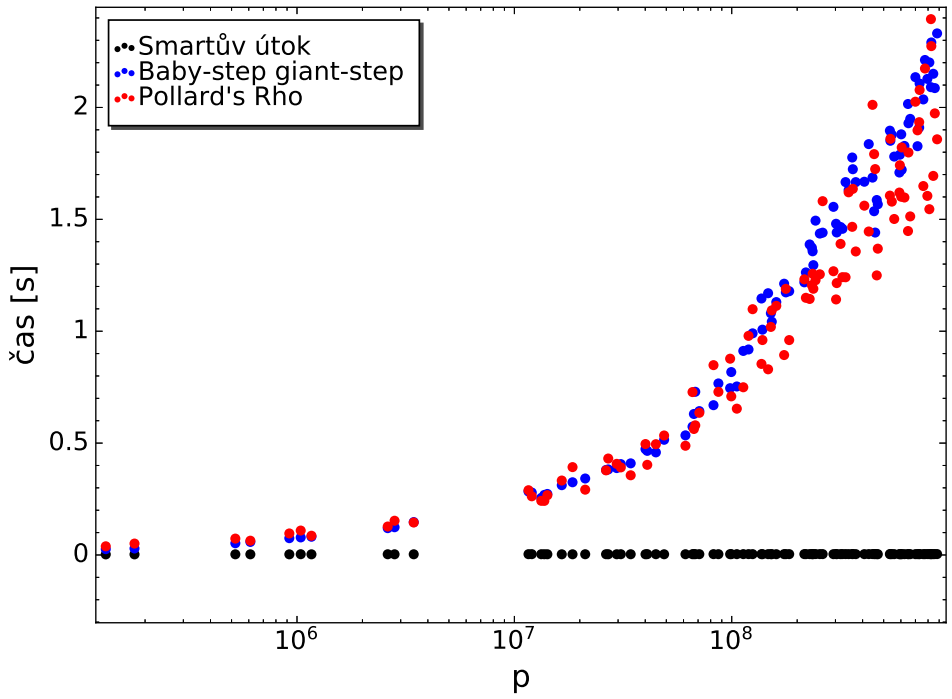
$$\frac{1}{p-1} + 1 = \frac{p}{p-1}.$$

Asymptoticky je proto i složitost celého algoritmu 4.2 právě $O(\log(p))$.

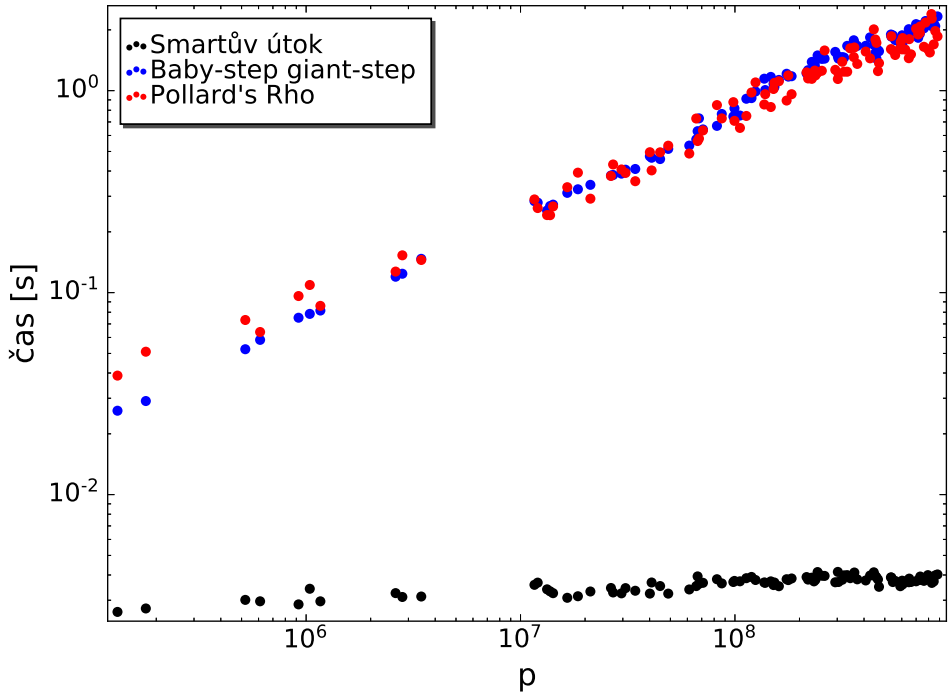
4.5.2 Reálné výsledky

Výsledky měření jsou zachyceny na obrázcích 4.1 a 4.2. Oba grafy popisují stejná data. Osa x je v obou případech škálována logaritmicky, takže vizuálně grafy popisují závislost času na délce p. Jediným rozdílem je, že graf na obrázku 4.2 má logaritmické škálování i na ose y, aby křivka odpovídající Smartovu útoku vedle zbylých dvou nezanikla.

Porovnáme-li očekávané výsledky s výsledky měření, můžeme říct, že všechny algoritmy se zachovaly tak, jak dle teorie měly.



Obrázek 4.1: Výsledky měření



Obrázek 4.2: Výsledky měření (logaritmické škálování času)

Závěr

V úvodu teoretické části této práce jsme postupně zavedli pojmy vedoucí k problému diskrétního logaritmu na eliptických křivkách. Popsali jsme algoritmy Baby-step giant-step a Pollard's Rho – algoritmy schopné řešit tento problém na libovolné eliptické křivce.

V jádru teoretické části práce jsme se věnovali jinému řešení tohoto problému fungujícímu na anomálních eliptických křivkách – Smartovu útoku. Vysvětlili jsme, co jsou p-adická čísla a jak jsou ve Smartově útoku využita. Zabývali jsme se tedy zdvihem eliptické křivky a jejích bodů do tělesa p-adických čísel, redukcí zpět do konečného tělesa $\mathbb{F}_p$, odvozením p-adického logaritmu a popisem vztahů některých podgrup zdvihu původní eliptické křivky. Všechny tyto poznatky jsme na závěr sestavili do jednoho logického celku objasňujícího, proč a jak Smartův útok funguje.

Na základě zpracované teorie jsme Smartův útok implementovali v softwaru SAGE a odvodili jsme časovou složitost vzniklého algoritmu. Základem implementace bylo jednoduché hotové řešení. Oproti tomu jsme ale udělali dvě zásadní změny. Nahradili jsme kód zdvihu bodů do $\mathbb{Q}_p$ tak, aby odpovídal obecnému popisu tohoto procesu z teoretické části práce. Druhá důležitá úprava řeší problém, který nastane, je-li zdvih původní křivky kanonický. Tato situace nebyla v původním kódu vůbec uvažována. My jsme ji ošetřili randomizací zdvihu křivky a kontrolním cyklem.

Abychom získali vhodná testovací data, popsali a implementovali jsme také algoritmus pro generování anomálních eliptických křivek. Implementace proběhla opět v softwaru SAGE. Na takto získaných křivkách jsme následně ověřili správnost implementace Smartova útoku a měřili reálný čas potřebný k jeho provedení. Stejný postup jsme aplikovali na dříve rozebrané algoritmy Baby-step giant-step a Pollard's Rho. Výsledky potvrdily jak správnost Smartova útoku, tak předpokládanou časovou složitost všech tří algoritmů.

Literatura

[1] Hankerson, D.; Menezes, A. J.; Vanstone, S.: *Guide to Elliptic Curve Cryptography*. 2003, ISBN 038795273X.

[2] Washington, L. C.: *Elliptic Curves: Number Theory and Cryptography, Second Edition*. 2008, ISBN 9781420071467.

[3] Leprevost, F.; Monnerat, J.; Varrette, S.; aj.: Generating anomalous elliptic curves. 2005, doi:10.1016/j.ipl.2004.11.008.

[4] University fo California, Riverside, Department of Mathematics: *Essential Concepts of Projective Geometry*. 2007. Dostupné z: `http://math.ucr.edu/~res/progeom/pg-all.pdf`

[5] McCurley, K. S.: The discrete logarithm problem. In *Proceedings of Symposia in Applied Mathematics*, 1990, s. 49–74.

[6] Diffie, W.; Hellman, M.: New directions in cryptography. *IEEE transactions on Information Theory*, 1976: s. 644–654.

[7] Lenstra, A. K.; Verheul, E. R.: Selecting cryptographic key sizes. *Journal of cryptology*, ročník 14, č. 4, 2001: s. 255–293, doi:10.1007/s00145-001-0009-4.

[8] Bos, J. W.; Halderman, J. A.; Heninger, N.; aj.: Elliptic curve cryptography in practice. In *International Conference on Financial Cryptography and Data Security*, 2014, s. 157–175.

[9] Blake-Wilson, S.; Bolyard, N.; Gupta, V.; aj.: Elliptic curve cryptography (ECC) cipher suites for transport layer security (TLS). Technická zpráva, RFC 4492, 2006.

[10] Stebila, D.; Green, J.: Elliptic curve algorithm integration in the secure shell transport layer. Technická zpráva, RFC 5656, 2009.

[11] Nakamoto, S.; aj.: A peer-to-peer electronic cash system. 2008. Dostupné z: https://bitcoin.org/bitcoin.pdf

[12] Galbraith, S. D.; Wang, P.; Zhang, F.: Computing elliptic curve discrete logarithms with improved baby-step giant-step algorithm. 2017, doi:10.3934/amc.2017038.

[13] Yasuda, M.; Izu, T.; Shimoyama, T.; aj.: On random walks of Pollard's rho method for the ECDLP on Koblitz curves. *Journal of Math-for-Industry*, ročník 3, č. 3, 2011: s. 107–112.

[14] Blumenfeld, A.: Pollard's Rho Algorithm for Elliptic Curves. 2015. Dostupné z: https://pdfs.semanticscholar.org/7ba8/ce07af736385e0e46c1922178b0132bb1ea9.pdf

[15] Pohlig, S.; Hellman, M.: An improved algorithm for computing logarithms over GF (p) and its cryptographic significance (Corresp.). *IEEE Transactions on information Theory*, ročník 24, č. 1, 1978: s. 106–110.

[16] Menezes, A. J.; Okamoto, T.; Vanstone, S. A.: Reducing elliptic curve logarithms to logarithms in a finite field. *iEEE Transactions on information Theory*, ročník 39, č. 5, 1993: s. 1639–1646.

[17] Galin, B.: Schoof-Elkies-Atkin Algorithm. 2007. Dostupné z: https://pdfs.semanticscholar.org/4df5/19f26a97c5a1c101d96a7e95a4d93dddc49c.pdf

[18] Schoof, R.: Counting points on elliptic curves over finite fields. *Journal de théorie des nombres de Bordeaux*, ročník 7, č. 1, 1995: s. 219–254. Dostupné z: http://archive.numdam.org/article/JTNB_1995__7_1_219_0.pdf

[19] Koblitz, N.: *p-adic Numbers, p-adic Analysis, and Zeta-Functions*. 1984, ISBN 0-387-96017-1.

[20] Heil, C.: *Metric Spaces*. 2018, ISBN 978-3-319-65322-8, s. 31–97.

[21] Silverman, J. H.: *Arithmetic of Elliptic Curves*. 2009, ISBN 978-0-387-09493-9.

[22] Novotney, P.: Weak Curves in Elliptic Curve Cryptography. 2010. Dostupné z: https://wstein.org/edu/2010/414/projects/novotney.pdf

[23] Baker, A. J.: An Introduction to p-adic Numbers and p-adic Analysis. 2011. Dostupné z: http://www.jon-arny.com/httpdocs/Elliptic/Baker%20padicnotes.pdf

[24] Carrell, J. B.: *Groups and Fields: The Two Fundamental Notions of Algebra*. 2017, ISBN 978-0-387-79428-0, s. 11–55.

[25] Kelley, J. L.; Pitcher, E.: Exact homomorphism sequences in homology theory. *Annals of Mathematics*, 1947: s. 682–709.

[26] Milne, J. S.: Algebraic Number Theory (v3.07). 2017. Dostupné z: `https://www.jmilne.org/math/CourseNotes/ANT.pdf`

[27] Wickless, W. J.: *A First Graduate Course in Abstract Algebra*. 2004, ISBN 9781482276688.

[28] Schilly, H.: SAGE webpage. Citováno 26. 5. 2020. Dostupné z: `https://www.sagemath.org/index.html`

[29] The Sage Development Team: Sage Reference Manual: p-Adics, Release 9.0. 2020. Dostupné z: `http://doc.sagemath.org/pdf/en/reference/padics/padics.pdf`

[30] Smart, N. P.: The Discrete Logarithm Problem on Elliptic Curves of Trace One. *Journal of Cryptology*, ročník 12, č. 3, 1999: str. 193–196, doi:10.1007/s001459900052. Dostupné z: `https://doi.org/10.1007/s001459900052`