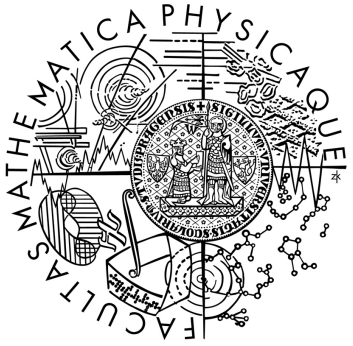
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

DIPLOMOVÁ PRÁCE



Petr Vácha

Počítání bodů na eliptických a hypereliptických křivkách

Katedra algebry

Vedoucí diplomové práce: RNDr. Jan Šťovíček, Ph.D.

Studijní program: Matematika

Studijní obor: Matematické metody informační bezpečnosti

Praha 2013

Děkuji vedoucímu své diplomové práce RNDr. Janu Šťovíčkovi, Ph.D. za cenné rady, připomínky a konzultace.

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

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

V Praze dne 30.7.2013 Podpis autora

Název práce: Počítání bodů na eliptických a hypereliptických křivkách

Autor: Petr Vácha

Katedra: Katedra algebry

Vedoucí diplomové práce: RNDr. Jan Šťovíček, Ph.D., Katedra algebry

Abstrakt: V předložené práci studujeme algoritmy pro určování počtu bodů na eliptických a hypereliptických křivkách. V prvních kapitolách jsou popsány nejjednodušší a nejméně efektivní algoritmy. Dále jsou popisovány složitější a efektivnější algoritmy. Tyto algoritmy(zejména Schoofův algoritmus) jsou důležité v kryptografii založené na diskrétním logaritmu v grupě bodů eliptické resp. hypereliptické křivky. Počet bodů křivky je totiž důležitý pro generování dat pro kryptosystém a pro vyloučení nežádoucích snadno napadnutelných případů.

Klíčová slova: eliptická křivka, hypereliptická křivka, počítání bodů, algoritmy eliptických křivek, Schoofův algoritmus

Title: Point Counting on Elliptic and Hyperelliptic Curves

Author: Petr Vácha

Department: Department of Algebra

Supervisor: RNDr. Jan Šťovíček, Ph.D., Department of Algebra

Abstract: In present work we study the algorithms for point counting on elliptic and hyperelliptic curves. At the beginning we describe a few simple and ineffective algorithms. Then we introduce more complex and effective ways to determine the point count. These algorithms(especially the Schoof's algorithm) are important for the cryptography based on discrete logarithm in the group of points of an elliptic or hyperelliptic curve. The point count is important to avoid the undesirable cases where the cryptosystem is easy to attack.

Keywords: elliptic curve, hyperelliptic curve, point counting, elliptic curves algorithms, Schoof's algorithm

Obsah

Úvod

V práci se budeme zabývat algoritmy pro určování počtu bodů eliptických a hypereliptických křivek nad konečnými tělesy. Tyto algoritmy mají význam zejména pro kryptografii založenou na eliptických křivkách. Využití eliptických křivek pro konstrukci asymetrických kryptosystémů navrhli nezávisle na sobě v roce 1985 Neal Koblitz a Victor S. Miller. Od té doby vznikla řada schémat a kryptosystémů založených na eliptických křivkách, jejichž bezpečnost spoléhá na obtížnost řešení problému diskrétního logaritmu v grupě bodů eliptické křivky. Jedná se zejména o Diffie-Hellmanův protokol pro výměnu klíče[11](Část 6.2), ElGamalovo šifrování s veřejným klíčem[11](Část 6.4) a schéma digitálního podpisu[11](Část 6.6). Motivací pro používání kryptografie založené na eliptických křivkách je fakt, že oproti kryptosystémům spoléhajícím na obtížnost faktorizace velkých čísel(např. RSA), nebo na obtížnost řešení diskrétního logaritmu v multiplikativní grupě konečného tělesa, stačí pro zajištění stejné úrovně bezpečnosti výrazně kratší klíče. Dle dokumentu [1](Tabulka 2) vydaného organizací NIST(National Institute of Standards and Technology) poskytuje například RSA s klíčem délky 1024 bitů stejnou bezpečnost jako kryptosystém založený na eliptických křivkách s klíčem délky 160-223 bitů. RSA s klíčem délky 2048 odpovídá svou bezpečností eliptickému kryptosystému s délkou klíče 224-255. U delších klíčů je rozdíl ještě vetší, například u RSA s klíčem dlouhým 15360 bitů stačí u eliptických křivek pro stejnou bezpečnost pouze třicetkrát kratší klíč. Kratší klíče znamenají menší paměťové nároky při výpočtech a proto jsou tyto kryptosystém dobře použitelné na místech s omezeným výpočetním výkonem a paměťovými zdroji, například na čipových kartách.

Již bylo zmíněno, že bezpečnost kryptografických schémat, o kterých se bavíme, závisí na obtížnosti řešení diskrétního logaritmu v grupě bodů eliptické křivky(ECDLP - Elliptic curve discrete logarithm problem). Zatím totiž není znám žádný efektivní(lepší než exponenciální) algoritmus pro obecné řešení tohoto problému. V některých případech může však být obtížnost řešení ECDLP oslabena.

Máme-li například křivku E nad tělesem $\mathbb{F}_p$ která má právě p bodů, lze podle [9] řešení diskrétního logaritmu v grupě jejích bodů převést na řešení diskrétního logaritmu v aditivní grupě tělesa $\mathbb{F}_p$ a sestavit tak dokonce lineární algoritmus pro řešení ECDLP nad touto křivkou.

Další případ snížení obtížnosti ECDLP nastane v situaci, kdy je počet bodů eliptické křivky součinem malých prvočísel. Pak lze totiž použít Pohlig-Hellmanovu redukci[4] a problém tak rozdělit na řešení více ECDLP v menších grupách, což je výhodnější.

Je tedy zřejmé, že pokud má křivka „nevhodný“ počet bodů, nemusí být řešení diskrétního logaritmu nad touto křivkou velký problém. A právě abychom

se vyvarovali používání takových křivek pro kryptografické účely, potřebujeme umět určovat počet jejich bodů. Generování křivky pro kryptografické účely pak může vypadat tak, že vygenerujeme náhodnou křivku, určíme počet jejích bodů a pokud se nám nelíbí(je například roven velikosti tělesa, nebo není dělitelný žádným velkým prvočíslem), tak vygenerujeme křivku novou.

Dále se algoritmy počítání bodů také dají využít při testování prvočíselnosti pomocí eliptických křivek[11](Část 7.2).

Cílem práce je tedy zpracovat různé metody určování počtu bodů eliptických a hyperelliptických křivek nad konečnými tělesy. Zejména pak Schoofův algoritmus, který je prvním polynomiálním algoritmem řešícím tento problém.

V první kapitole práce definujeme základní pojmy jako je eliptická a hyperelliptická křivka, dále na bodech eliptické křivky definujeme operaci sčítání tak, že body křivky s touto operací tvoří komutativní grupu.

Druhá kapitola popisuje způsob kterým budeme posuzovat složitost představovaných algoritmů a dále jsou v ní uvedeny složitosti některých základních operací, které budeme při sestavování algoritmů používat.

První algoritmus pro počítání bodů je představen v kapitole třetí. Jedná se o nejjednodušší, ale také o nejméně efektivní algoritmus. Algoritmus je exponenciální, a tedy efektivně použitelný pouze nad malými tělesy.

V další kapitole představíme algoritmus, který z počtu bodů křivky nad tělesem $\mathbb{F}_q$ dokáže určit počet jejích bodů nad nějakým rozšířením tělesa $\mathbb{F}_q$.

Pátá kapitola konečně využívá grupovou strukturu definovanou v první kapitole a zaměřuje se na využití řádu bodů. Řád bodu totiž vždy dělí řád grupy a tento fakt ve spojení Hasse-Weilovým odhadem pro počet bodů křivky nám dá algoritmus, který je stejně jako ten z první kapitoly exponenciální, ale exponenciální s menším základem. Je proto efektivně použitelný i pro trochu větší tělesa.

V poslední kapitole pak popisujeme Schoofův algoritmus. Nejprve definujeme množinu n-torzních bodů a dělící polynomy. Pak odvodíme některé vlastnosti dělících polynomů a formulujeme lemmata, která pak využijeme při popisu samotného algoritmu. Nakonec odvodíme, že se skutečně jedná o polynomiální algoritmus.

Značení

Zde uvádíme používané značení, které není v práci přímo zavedeno:

$\mathbb{F}_q$	Konečné těleso, které má q prvků.
$\mathrm{char}\,(K)$	Charakteristika tělesa K.
$\overline{K}$	Algebraický uzávěr tělesa K.
$K[x]$	Okruh polynomů nad tělesem K.
$\deg(f)$	Stupeň polynomu f.
$(G, +, 0)$	Grupa s nosnou množinou G, operací $+$ a nulovým prvkem 0.
$\log(x)$	Logaritmus čísla x se základem 2.
$\ln(x)$	Přirozený logaritmus čísla x.
$\lvert S\rvert$	Počet prvků množiny S.
$\lvert x\rvert$	Absolutní hodnota čísla x.
$\lceil x\rceil$	Horní celá část čísla x.
$\lfloor x\rfloor$	Dolní celá část čísla x.

$\mathbb{Z}$	Okruh celých čísel.
$\mathbb{C}$	Těleso komplexních čísel.
$\operatorname{lcm}(a, b)$	Nejmenší společný násobek čísel a a b.
$\operatorname{GCD}(a, b)$	Největší společný dělitel čísel nebo polynomů a a b.
$\operatorname{Ker}(\alpha)$	Jádro homomorfismu α.
$\det A$	Determinant matice A.

Kapitola 1

Eliptické a hypereliptické křivky

V této kapitole definujeme pojmy eliptické a hypereliptické křivky. Dále na jejich bodech definujeme operaci sčítání a tím dostaneme grupu, se kterou budeme dále pracovat.

1.1 Základní definice

Pro naše potřeby bude dostačující následující definice eliptické křivky.

Definice 1.1.1. *Eliptickou křivkou E nad tělesem K rozumíme množinu bodů $(x, y) \in \overline{K} \times \overline{K}$ splňujících rovnici*

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

společně s bodem $\mathcal{O}$, kde $a_1, \ldots, a_6 \in K$.

Rovnici 1.1 nazýváme *Weierstrassovou rovnicí* eliptické křivky a bod $\mathcal{O}$ bodem v nekonečnu. Je to bod, který nám pomůže definovat na bodech eliptické křivky strukturu grupy. Takto se zdá, že uměle přidáváme nějaký neexistující bod navíc, definice bodu v nekonečnu však vychází ze skutečnosti, že pokud uvažujeme v projektivním prostoru křivku s rovnicí

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{1.2}$$

vidíme, že jediným nevlastním bodem této křivky je bod $(0 : 1 : 0)$. Ostatní body jsou vlastní a pokud v rovnici za proměnnou Z dosadíme 1, dostaneme přesně rovnici 1.1 a vidíme tedy, že vlastní body řešící rovnici 1.2 odpovídají právě bodům řešícím rovnici 1.1. Hlubší teorie, kterou se zde zabývat nebudeme, pak říká, že body projektivní eliptické křivky tvoří grupu, přičemž za nulový bod lze volit libovolný bod této křivky. Nám jako nulový bod poslouží právě jediný nevlastní bod(který označíme $\mathcal{O}$), a protože ostatní body projektivní křivky jednoznačně odpovídají bodům křivky afinní, stačí nám uvažovat pouze afinní prostor, tedy rovnice typu 1.1.

Pro jednoduchost dále položíme

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

tedy Weierstrassova rovnice eliptické křivky odpovídá rovnici $w(x, y) = 0$

Mějme $L \supseteq K$ nadtěleso tělesa K. Množinu

$$E(L) = \{(x, y) \in L \times L | w(x, y) = 0\} \cup \{\mathcal{O}\}$$

nazveme množinou *L-racionálních* bodů křivky E. Pokud koeficienty rovnice leží v tělese K, říkáme, že křivka je definovaná nad tělesem K. Pokud $L = \overline{K}$ pak místo $E(\overline{K})$ píšeme pouze E.

Dále definujeme *diskriminant* křivky jako

$$\Delta(E) = -8b_4^3 - 27b_6^2 + 9b_2b_4b_6 - b_2^2b_8,$$

kde

$$\begin{aligned} b_2 &= 4a_2 + a_1^2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= 4a_6 + a_3^2 \\ b_8 &= 4a_2a_6 + a_2a_3^2 + a_6a_1^2 - a_4^2 - a_1a_3a_4 \end{aligned}$$

Nadále se budeme zabývat pouze křivkami které mají nenulový diskriminant, protože na těchto křivkách lze snadno definovat grupovou strukturu.

Takto definovaná eliptická křivka je jen speciálním případem křivky hypereliptické. Tu zadefinujeme nyní.

Definice 1.1.2. Hypereliptickou křivkou *E nad tělesem K budeme nazývat množinu bodů $(x, y) \in \overline{K} \times \overline{K}$ splňujících rovnici*

$$y^2 + yh(x) = f(x) \tag{1.3}$$

společně s bodem $\mathcal{O}$, kde $g \geq 1$ je přirozené číslo, $f, g \in K[x]$ jsou polynomy takové, že $\deg(f) = 2g + 1$ *a* $\deg(h) \leq g$. *Číslo g nazýváme* rodem *křivky E.*

Vidíme tedy, že eliptické křivky jsou právě hypereliptické křivky rodu 1. Stejně jako u eliptické křivky definujeme a značíme $E(L)$ množinu L-racionálních bodů pro nějaké rozšíření $L \supseteq K$. Rovnici 1.3 nazýváme také Weierstrassovou rovnicí. Rovnici 1.3 můžeme opět napsat ve tvaru $w(x, y) = 0$ pro $w \in K[x, y]$. Dále v celé práci budeme předpokládat, že derivace w podle obou proměnných jsou ve všech bodech křivky nenulové, tj. že neexistuje bod (x, y) ležící na křivce, pro který platí

$$2y + h(x) = 0 = f'(x) - yh'(x).$$

Křivky, které toto splňují, nazýváme *nesingulární*. Přímým výpočtem lze odvodit, že u eliptické křivky odpovídá podmínka nesingularity přesně podmínce nenulového diskriminantu.

Budeme-li dále hovořit o *křivce*, budeme mít na mysli nesingulární eliptickou nebo hypereliptickou křivku. Také se budeme zabývat pouze křivkami definovanými nad konečnými tělesy.

1.2 Grupová operace

Nyní definujeme na bodech nesingulární eliptické křivky operaci sčítání. Tuto operaci budeme značit $+$, operaci k ní opačnou pak budeme značit $-$. Sčítání bodů eliptické křivky lze definovat následujícím pravidlem:

> Součet všech bodů křivky ležících na jedné přímce je $\mathcal{O}$ a bod $\mathcal{O}$ je nulovým bodem vzhledem k této operaci. (1.4)

Přičemž ještě bereme v úvahu násobnost průniků přímky s křivkou, tj. pokud je v daném bodě přímka sečnou křivky, započítáme tento bod do součtu jednou, pokud je přímka v bodě tečnou křivky, započítáme ho do součtu dvakrát. Například pokud body $P_1, P_2, P_3 \in E(\mathbb{F}_q)$ leží na přímce a tato přímka je v těchto bodech sečna křivky E, pak je $P_1 + P_2 + P_3 = \mathcal{O}$. Pokud $Q_1, Q_2 \in E(\mathbb{F}_q)$ leží na přímce a tato přímka je v bodě Q_1 tečna ke křivce E a v bodě Q_2 sečna této křivky, pak platí $Q_1 + Q_1 + Q_2 = \mathcal{O}$.

Nyní za použití výše zmíněného pravidla odvodíme vzorce pro operace s body eliptické křivky. Mějme tedy eliptickou křivku E nad tělesem $\mathbb{F}_q$ definovanou Weierstrassovou rovnicí $w(x, y) = 0$ s koeficienty jako v 1.1.

Nejprve odvodíme vzorec pro opačný prvek, tj. pro počítání operace $-$. Mějme bod $P = (\alpha, \beta) \in E(\mathbb{F}_q)$. Uvažme přímku $l : x = \alpha$. Tato přímka prochází bodem P. Další průsečíky přímky l s křivkou E spočteme prostým dosazením rovnice přímky do rovnice křivky, tedy

$$y^2 + a_1\alpha y + a_3 y = \alpha^3 + a_2\alpha^2 + a_4\alpha + a_6.$$

Jedním řešením této rovnice je β, druhým řešením je pak druhá souřadnice dalšího průsečíku. Označme tento průsečík jako $Q = (\alpha, \beta')$. Neboť β a β' jsou řešením předchozí rovnice, můžeme tuto rovnici zapsat jako

$$(y - \beta)(y - \beta') = 0.$$

Porovnáním koeficientů u členu y v těchto dvou vyjádřeních stejné rovnice dostáváme

$$-\beta - \beta' = a_1\alpha + a_3,$$

tedy $\beta' = -\beta - a_1\alpha - a_3$. Body P a Q jsou všechny průsečíky křivky E s přímkou l, tedy dle pravidla 1.4 platí $P + Q = \mathcal{O}$, tedy $-P = Q$, tj.

$$-(\alpha, \beta) = (\alpha, -\beta - a_1\alpha - a_3) \tag{1.5}$$

Nyní mějme dva body $P_1 = (\alpha_1, \beta_2)$ a $P_2 = (\alpha_2, \beta_2)$. Chceme spočítat jejich součet. Pokud jsou různé a zároveň platí $\alpha_1 = \alpha_2$, je jejich součet $\mathcal{O}$ dle 1.5. Můžeme tedy dále předpokládat, že buď $P_1 = P_2$, nebo $\alpha_1 \neq \alpha_2$. Ať l je přímka procházející body P_1 a P_2. Pokud $P_1 = P_2$, ať l je tečna křivky E v tomto bodě. Můžou nastat dvě možnosti. Buď je rovnice přímky l ve tvaru $y = \lambda x + \mu$, nebo je přímka svislá a má rovnici $x = \alpha_1$. Podívejme se nejprve na první případ. Opět spočteme všechny průsečíky přímky l s křivkou E. Dosadíme tedy rovnici přímky do rovnice křivky. Dostáváme rovnici

$$(\lambda x + \mu)^2 + a_1 x(\lambda x + \mu) + a_3(\lambda x + \mu) = x^3 + a_2 x^2 + a_4 x + a_6$$
$$x^3 + (a_2 - \lambda^2 - a_1\lambda)x^2 + (a_4 - 2\lambda\mu - a_1\mu - a_3\lambda)x = \mu^2 + a_3\mu - a_6.$$

Máme polynomiální rovnici stupně 3 a víme, že α_1 a α_2 jsou její řešení. Označíme-li její třetí řešení jako α_3, můžeme rovnici přepsat do tvaru

$$(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)=0.$$

Porovnáním koeficientů u členu x^2 v těchto dvou vyjádřeních totožné rovnice dostáváme rovnost

$$-\alpha_1-\alpha_2-\alpha_3=a_2-\lambda^2-a_1\lambda,$$

tedy $\alpha_3=\lambda^2+a_1\lambda-a_2-\alpha_1-\alpha_2$. Získali jsme tedy první souřadnici třetího průsečíku křivky s přímkou l. Označme tento průsečík $P_3=(\alpha_3,\beta_3)$. Druhou souřadnici tohoto bodu dostaneme snadno dosazením do rovnice přímky l:

$$\beta_3=\lambda\alpha_3+\mu.$$

Body P_1,P_2,P_3 jsou tedy všechny body křivky E ležící na přímce l, proto dle pravidla 1.4 platí $P_1+P_2+P_3=\mathcal{O}$. Odečtením P_3 získáváme rovnost $P_1+P_2=-P_3$. Bod $-P_3$ už umíme spočítat pomocí vzorce 1.5. Dostáváme tedy

$$(\alpha_1,\beta_1)+(\alpha_2,\beta_2)=-(\alpha_3,\beta_3)\overset{1.5}{=}(\alpha_3,-\beta_3-a_1\alpha_3-a_3), \tag{1.6}$$

kde $\alpha_3=\lambda^2+a_1\lambda-a_2-\alpha_1-\alpha_2$ a $\beta_3=\lambda\alpha_3+\mu$. Zbývá ještě zmínit, jak spočteme směrnici λ přímky l. Pokud $\alpha_1\neq\alpha_2$, pak

$$\lambda=\frac{\beta_1-\beta_2}{\alpha_1-\alpha_2}.$$

Pokud je $P_1=P_2$ spočteme směrnici tečny pomocí derivací jako

$$\lambda=-\frac{\frac{\partial w}{\partial x}(\alpha_1,\beta_1)}{\frac{\partial w}{\partial y}(\alpha_1,\beta_1)}.$$

Zbývá vyřešit případ, kdy rovnice přímky l má tvar $x=\alpha_1$. Je $\alpha_1=\alpha_2$, tedy podle předpokladu je $P_1=P_2$ a l je proto tečnou v tomto bodě. Dosadíme-li vyjádření $x=\alpha_1$ do rovnice křivky, dostaneme polynomiální rovnici stupně 2. Protože však přímka l je tečnou, vyjde, že β_1 je dvojnásobným kořenem této rovnice. Žádný jiný bod křivky už tedy na přímce l neleží, proto je podle pravidla 1.4 $P_1+P_2=\mathcal{O}$. Toto je vlastně jeden z případů, který může nastat při odvozování vzorce pro opačný prvek 1.5. Tento případ navíc nastává právě když $\frac{\partial w}{\partial y}(\alpha_1,\beta_1)=0$. Definici operace rovnicí 1.6 tedy ještě musíme doplnit následovně: Pokud při počítání směrnice λ vyjde ve jmenovateli $\frac{\partial w}{\partial y}(\alpha_1,\beta_1)=0$, je $P_1+P_2=\mathcal{O}$.

Tím jsme dokončili definici sčítaní bodů eliptické křivky.

Lemma 1.2.1. *Množina $\mathbb{F}_q$-racionálních bodů eliptické křivky E společně s operací $+$ definovanou výše rovnicí 1.6 tvoří komutativní grupu s nulovým prvkem $\mathcal{O}$.*

Důkaz. Protože součet dvou $\mathbb{F}_q$-racionálních bodů se dle 1.6 počítá pouze z jejich souřadnic a koeficientů Weierstrassovi rovnice za použití základních operací v tělese, jsou i souřadnice výsledného bodu ve stejném tělese, tedy výsledkem je opět $\mathbb{F}_q$-racionální bod. Komutativita operace je zřejmá z vyjádření 1.6. O existenci inverzního prvku hovoří rovnost 1.5. Zbývá ukázat, že námi definovaná operace je asociativní. Tento důkaz lze najít například v [11](Část 2.4). □

Grupu $(E(\mathbb{F}_q), +, \mathcal{O})$ budeme značit opět pouze $E(\mathbb{F}_q)$ a nazývat *grupou bodů eliptické křivky*, popřípadě jen *grupou eliptické křivky.*

Pokud bychom se zabývali hlubší teorií, mohli bychom i u hypereliptické křivky nad tělesem $\mathbb{F}_q$ definovat strukturu grupy podobně. To ovšem v práci nebudeme potřebovat. Neformálně by se sčítáni dalo zavést následujícím pravidlem:

> Součet všech bodů hypereliptické křivky ležících na křivce s rovnicí $y = g(x)$, kde $g \in \mathbb{F}_q[x]$, je $\mathcal{O}$ a bod $\mathcal{O}$ je nulovým bodem vzhledem k operaci sčítání.

Dostali bychom pak grupu, jejíž každý prvek lze jednoznačně reprezentovat jako formální součet nejvýše g bodů křivky, kde g je její rod. V této práci však tuto grupu potřebovat nebudeme, proto se jí nebudeme věnovat podrobněji.

1.3 Krátký Weierstrassův tvar

V této části zavedeme pojmy polynomiálního zobrazení, izomorfních křivek a krátké Weierstrassovi rovnice křivky.

Připomeňme, že pro křivku E nad tělesem $\mathbb{F}_q$ značíme množinu $E(\overline{\mathbb{F}}_q)$ opět symbolem E. Definujme $E^+ = E \setminus \{\mathcal{O}\}$.

Definice 1.3.1. *Mějme křivky E a E' definované nad tělesem $\mathbb{F}_q$. Zobrazení*

$$\begin{aligned} \varphi : E^+ &\longrightarrow E'^+ \\ (a, b) &\longrightarrow \varphi((a, b)) \end{aligned}$$

nazveme polynomiální*, pokud existují polynomy $f_1, f_2 \in \mathbb{F}_q[x, y]$ takové, že platí*

$$\varphi((a, b)) = (f_1(a, b), f_2(a, b))$$

pro každý bod $(a, b) \in E^+$.

Definice 1.3.2. *Řekneme, že dvě křivky E a E' nad tělesem $\mathbb{F}_q$ jsou* izomorfní*, pokud existují polynomiální zobrazení $\varphi : E^+ \to E'^+$ a $\psi : E'^+ \to E^+$ taková, že pro každé $(a, b) \in E^+$ a pro každé $(a', b') \in E'^+$ platí*

$$\begin{aligned} \psi(\varphi((a, b))) &= (a, b) \\ \varphi(\psi((a', b'))) &= (a', b'). \end{aligned}$$

Důvodem, proč jsme izomorfismus křivek definovali právě takto je fakt, že pokud máme dvě izomorfní křivky, pak i grupy definované nad těmito křivkami v předchozí části jsou izomorfní[2]. Při zkoumání nějaké křivky nám tedy bude stačit zkoumat křivku s ní izomorfní.

Lemma 1.3.3. *Mějme dvě křivky E a E' nad tělesem $\mathbb{F}_q$ a polynomiální zobrazení $\varphi : E^+ \to E'^+$ dané polynomy $f_1(x, y) = x + a$ a $f_2(x, y) = y + bx + c$ pro nějaká $a, b, c \in \mathbb{F}_q$, tj.*

$$\varphi((x, y)) = (x + a, y + bx + c)$$

pro každý bod $(x, y) \in E^+$. Pokud φ je na, pak křivky E a E' jsou izomorfní.

Důkaz. Stačí ukázat existenci inverzního polynomiálního zobrazení k zobrazení φ. Tím ze zřejmě zobrazení ψ takové, že

$$\psi((x,y)) = (x-a, y-b(x-a)-c).$$

Podmínka, že φ je na, nám zajišťuje, že zobrazení ψ opravdu zobrazuje body E'^{+} na body E^{+}. □

Budeme-li tedy provádět transformace z předchozího lemmatu na rovnici křivky, budeme dostávat rovnice křivek izomorfních. Začneme tedy s obecnou Weierstrassovou rovnicí a tu budeme postupně upravovat do jednodušších tvarů. Mějme eliptickou křivku E nad tělesem $\mathbb{F}_q$ definovanou rovnicí

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.7}$$

Pokud je charakteristika tělesa $\mathbb{F}_q$ různá od 2, transformace $x \to x$, $y \to y - (a_1x)/2$ převede tuto rovnici na tvar

$$(y - \frac{a_1x}{2})^2 + a_1x(y - \frac{a_1x}{2}) + a_3(y - \frac{a_1x}{2}) = x^3 + a_2x^2 + a_4x + a_6$$
$$y^2 - a_1xy + \frac{a_1^2x^2}{4} + a_1xy - \frac{a_1^2x^2}{2} + a_3y - \frac{a_1a_3x}{2} = x^3 + a_2x^2 + a_4x + a_6.$$

Vidíme že člen s xy se odečetl, původní křivka je tedy izomorfní křivce

$$y^2 + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'$$

pro nějaké koeficienty a_i'. Další transformaci kterou provedeme, je $x \to x$, $y \to y - (a_3'/2)$. Tím dostáváme rovnici

$$(y - \frac{a_3'}{2})^2 + a_3'(y - \frac{a_3'}{2}) = x^3 + a_2'x^2 + a_4'x + a_6'$$
$$y^2 - a_3'y + \frac{{a_3'}^2}{4} + a_3'y - \frac{{a_3'}^2}{2} = x^3 + a_2'x^2 + a_4'x + a_6'.$$

Členy s y se nám odečtou a dostáváme tak izomorfní křivku s rovnicí

$$y^2 = x^3 + \bar{a}_2x^2 + \bar{a}_4x + \bar{a}_6$$

pro vhodné koeficienty $\bar{a}_i$. Pokud je navíc charakteristika tělesa různá od 3, můžeme provést transformaci $x \to x - (\bar{a}_2/3)$, $y \to y$. Tím dostaneme rovnici

$$y^2 = (x - \frac{\bar{a}_2}{3})^3 + \bar{a}_2(x - \frac{\bar{a}_2}{3})^2 + \bar{a}_4(x - \frac{\bar{a}_2}{3}) + \bar{a}_6.$$

Z této rovnice je opět vidět že se vynulují koeficienty u členu x^2, tedy dostaneme opět izomorfní křivku s rovnicí

$$y^2 = x^3 + \tilde{a}_4x + \tilde{a}_6.$$

Tímto výpočtem jsme dokázali následující lemma.

Lemma 1.3.4. *Pokud je* $\mathrm{char}\,(\mathbb{F}_q) \neq 2, 3$*, pak pro eliptickou křivku* E *definovanou nad tělesem* $\mathbb{F}_q$ *existuje jí izomorfní křivka* E' *definovaná nad tělesem* $\mathbb{F}_q$*, která má rovnici*

$$y^2 = x^3 + Ax + B. \tag{1.8}$$

Rovnici tvaru 1.8 nazýváme *krátkou Weierstrassovou rovnicí* eliptické křivky. Podobným způsobem lze zjednodušit i rovnice eliptických křivek v charakteristice 2 a 3, tyto rovnice však nebudeme potřebovat.

Stejně jako jsme upravovali rovnici eliptické křivky, můžeme totéž provést s rovnicí obecné křivky hypereliptické. Pokud pracujeme v liché charakteristice, můžeme rovnici 1.3

$$y^2 + yh(x) = f(x)$$

převést transformací $x \to x$, $y \to y - (h(x)/2)$ na rovnici

$$\begin{aligned}(y - \frac{h(x)}{2})^2 + (y - \frac{h(x)}{2})h(x) &= f(x)\\ y^2 - yh(x) + yh(x) - \frac{h(x)^2}{2} &= f(x).\end{aligned}$$

Členy obsahující y se odečtou a tím dostáváme rovnici

$$y^2 = \bar{f}(x)$$

pro vhodný polynom $\bar{f}$. Všimněme si, že stupeň polynomu $\bar{f}$ je stejný jako stupeň f. Můžeme tedy formulovat podobné lemma jako pro eliptickou křivku.

Lemma 1.3.5. *Ať* E *je hypereliptická křivka rodu* g *definovaná nad tělesem* $\mathbb{F}_q$*, kde* $\mathrm{char}\,(\mathbb{F}_q) \neq 2$*. Pak existuje křivka* E' *izomorfní s* E *taková, že její rovnice má tvar*

$$y^2 = f(x) \tag{1.9}$$

kde f *je polynom stupně* $2g + 1$*.*

Rovnici 1.9 také nazýváme *krátkou Weierstrassovou rovnicí.*
Několik poznámek závěrem:

- Podmínka nesingularity křivek daných rovnicemi 1.8 nebo 1.9 je ekvivalentní s podmínkou, že polynom na pravé straně rovnice nemá násobné kořeny.
- Vzorce pro výpočet grupových operací nad eliptickou křivkou s rovnicí 1.8 vypadají následovně:
  - Pro $P = (\alpha, \beta) \in E(\mathbb{F}_q)^+$ je $-P = (\alpha, -\beta)$.
  - Ať $P_1, P_2 \in E(\mathbb{F}_q)^+$ a $P_3 \in E(\mathbb{F}_q)$ jsou takové, že $P_1 + P_2 = P_3$. Pokud je $P_1 = (\alpha_1, \beta_1), P_2 = (\alpha_2, \beta_2)$ a $P_3 = (\alpha_3, \beta_3)$, pak platí

$$\begin{aligned}\alpha_3 &= \lambda^2 - \alpha_1 - \alpha_2\\ \beta_3 &= -\lambda(\alpha_3 - \alpha_1) - \beta_1,\end{aligned}$$

kde

$$\lambda = \begin{cases} \frac{\beta_1 - \beta_2}{\alpha_1 - \alpha_2} & \text{pokud } \alpha_1 \neq \alpha_2, \\ \frac{3\alpha_1^2 + A}{2\beta_1} & \text{pokud } P_1 = P_2 \text{ a } \beta_1 \neq 0. \end{cases}$$

V ostatních případech, tj. pokud $P_1 = P_2$ a $\beta_1 = 0$(případ bodu řádu 2), nebo pokud $\alpha_1 = \alpha_2$ a $\beta_1 \neq \beta_2$(případ opačných prvků v grupě), je $P_1 + P_2 = \mathcal{O}$.

Kapitola 2

Složitost výpočtů

V této kapitole uvedeme, jakým způsobem budeme posuzovat složitost uváděných algoritmů a také uvedeme výpočetní složitost některých základních operací jako například sčítání bodů v grupě eliptické křivky, nebo počítání s polynomy.

2.1 $\mathcal{O}$-notace

Nyní představíme pojem $\mathcal{O}$-notace a jejího použití pro asymptotické srovnávání složitosti algoritmů.

Definice 2.1.1. *Mějme dvě reálné funkce f a g. Řekneme, že $f \in \mathcal{O}(g)$ pokud existují $x_0 > 0$ a $k \in \mathbb{R}$ taková, že*

$$|f(x)| \leq |kg(x)|$$

pro každé $x > x_0$.

Složitost algoritmů budeme určovat v počtu základních bitových operací. Složitost většiny algoritmů závisí na velikosti jejich vstupu, proto se počet bitových operací typicky vyjadřuje jako hodnota funkce $f(n)$, kde n závisí na velikosti vstupu algoritmu. Říkáme tedy, že *algoritmus má složitost* $\mathcal{O}(f(n))$, pokud existuje konstanta $k \in \mathbb{R}$ taková, že pro všechny dostatečně velké vstupy je pro proběhnutí algoritmu potřeba nejvýše $kf(n)$ bitových operací. Předveďme si to na příkladu.

Příklad 2.1.2 (Násobení matic)**.** *Mějme dvě čtvercové matice $A, B \in \mathbb{Z}_2^{n^2}$. Ať $A = (a_{i,j})$ a $B = (b_{i,j})$. Označme $D = AB$, $D = (d_{i,j})$. Koeficient $d_{i,j}$ spočteme jako*

$$d_{i,j} = \sum_{k=1}^{n} a_{i,k} b_{k,j}.$$

K výpočtu koeficientu $d_{i,j}$ je tedy potřeba $2n-1$ bitových operací(n násobení a $n-1$ sčítání). Těchto koeficientů je n^2, je tedy potřeba celkem $n^2(2n-1) = 2n^3 - n^2$ bitových operací. Pro každé $n > 1$ platí

$$|2n^3 - n^2| \leq |2n^3| + |n^2| \leq |2n^3| + |n^3| = |3n^3|,$$

můžeme tedy říci, že složitost výpočtu matice D je $\mathcal{O}(n^3)$.

V příkladu byla složitost udávána ve vztahu k rozměrům násobených matic. My budeme posuzovat složitost algoritmů vzhledem k logaritmu velikosti tělesa, nad kterým budeme počítat. Pro tělesa $\mathbb{F}_p$, kde p je prvočíslo to odpovídá bitové délce prvočísla p.

2.2 Složitost základních operací

V této části uvedeme složitost některých základních operací, které budeme používat při sestavování algoritmů pro určení počtu bodů křivky.

Začneme operacemi v konečném tělese $\mathbb{F}_q$ a operacemi s polynomy nad tímto tělesem, přičemž předpokládáme, že stupně všech polynomů jsou nějak závislé na q. Jinak by totiž zápisy složitostí, ve kterých se stupně polynomů vyskytují, nedávaly velký smysl. Složitosti následujících operací jsou uvedeny například v [10].

- Sčítání a odčítání prvků tělesa $\mathbb{F}_q$ má složitost $\mathcal{O}(\log(q))$ [10](Část 5.2.1).
- Násobení prvků tělesa $\mathbb{F}_q$ má složitost $\mathcal{O}(\log(q)^2)$ [10](Část 5.2.1).
- Počítání inverzního prvku v $\mathbb{F}_q$ má složitost $\mathcal{O}(\log(q)^2)$ [10](Část 5.2.1).
- Součin dvou polynomů nad $\mathbb{F}_q$, které mají stupně d_1 a d_2 má složitost $\mathcal{O}(d_1 d_2 \log(q)^2)$ [10](Část 5.1.2).
- Podíl, nebo zbytek po dělení dvou polynomů nad $\mathbb{F}_q$ lze spočítat za použití $\mathcal{O}(d^2 \log(q)^2)$ bitových operací. Přičemž d je stupeň děleného polynomu [10](Část 5.1.3).
- Složitost výpočtu největšího společného dělitele dvou polynomů nad tělesem $\mathbb{F}_q$ je $\mathcal{O}(d_1 d_2 \log(q)^2)$, kde d_1 a d_2 jsou stupně příslušných polynomů [10](Část 5.1.4).

Dále se podíváme na složitost operace sčítání v grupě bodů eliptické křivky nad tělesem $\mathbb{F}_q$. Součet dvou bodů eliptické křivky se podle vzorce 1.6 počítá pomocí konstantního počtu sčítání, násobení a dělení prvků tělesa $\mathbb{F}_q$, nejsložitějšími z těchto operací jsou násobení a dělení, které mají složitost $\mathcal{O}(\log(q)^2)$, proto výpočet součtu dvou bodů křivky má také složitost $\mathcal{O}(\log(q)^2)$.

Násobení bodu eliptické křivky číslem n lze provést při použití binárního mocnění[10](Algoritmus 7) pomocí nejvýše $2\log(n)$ sčítání, tedy složitost výpočtu nP je $\mathcal{O}\left(\log(n)\log(q)^2\right)$. Zde opět předpokládáme, že číslo n nějak závisí na velikosti tělesa, tedy na q.

Kapitola 3

Explicitní vzorec

V této kapitole se seznámíme s explicitními vzorci, které udávají počet bodů eliptických a hypereliptických křivek. Jsou to asi nejvíce přímočaré algoritmy pro určení počtu bodů křivky. S časovou náročností jejich vyčíslení to však není nejlepší. Vyžadují totiž procházení všech prvků tělesa $\mathbb{F}_q$, nad kterým chceme zjistit počet bodů křivky. Tedy složitost jejich vyčíslení je exponenciální vzhledem k $\log(q)$. Konkrétně je tato složitost $\mathcal{O}(q^{1+\epsilon}) = \mathcal{O}((2^{1+\epsilon})^{\log(q)})$ pro libovolné $\epsilon > 0$, tedy exponenciální se základem $2^{1+\epsilon}$.

3.1 Charakteristika různá od 2

Mějme hypereliptickou křivku E nad tělesem $\mathbb{F}_q$, kde $q = p^k$ a p je prvočíslo různé od 2. V tomto případě můžeme dle kapitoly 1 převést rovnici křivky na krátký Weierstrassův tvar v podobě $y^2 = f(x)$, kde $f \in \mathbb{F}_q[x]$ je polynom bez násobných kořenů stupně $2g + 1$. Nejjednodušším algoritmem, jak zjistit počet bodů křivky je prostě vyzkoušet všechny možné body $(x, y) \in \mathbb{F}_q^2$ zda splňují rovnici křivky. Pro každé $x \in \mathbb{F}_q$ chceme tedy najít všechna $y \in \mathbb{F}_q$ taková, že $y^2 = f(x)$. Protože jsme v charakteristice různé od dvou, počet takových y je vždy 2 nebo 0.

Pro jednoduchost značení zavedeme nyní zobecněný Legendrův symbol.

Definice 3.1.1. *Pro prvek $a \in \mathbb{F}_q$ definujme zobecněný Legendrův symbol následovně*

$$\left(\frac{a}{\mathbb{F}_q}\right) = \begin{cases} 1 & \text{pokud existuje } 0 \neq x \in \mathbb{F}_q, \text{ že } x^2 = a \\ -1 & \text{pokud neexistuje } x \in \mathbb{F}_q, \text{ že } x^2 = a \\ 0 & \text{pokud } a = 0 \end{cases}$$

Nyní tedy můžeme snadno napsat vzorec pro počet bodů hypereliptické křivky.

Tvrzení 3.1.2. *Ať E je hypereliptická křivka definovaná nad $\mathbb{F}_q$ daná rovnicí $y^2 = f(x)$, pak*

$$|E(\mathbb{F}_q)| = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{f(x)}{\mathbb{F}_q}\right) \tag{3.1}$$

Důkaz. Pro dané $a \in \mathbb{F}_q$ je počet $b \in \mathbb{F}_q$ takových, že $(a, b) \in E(\mathbb{F}_q)$ právě $1 + \left(\frac{f(a)}{\mathbb{F}_q}\right)$. Započtením bodu v nekonečnu tedy dostáváme, že velikost $E(\mathbb{F}_q)$ je

$$|E(\mathbb{F}_q)| = 1 + \sum_{x \in \mathbb{F}_q} \left(1 + \left(\frac{f(x)}{\mathbb{F}_q}\right)\right)$$

Částečným sečtením sumy nyní dostaneme výsledek. □

Otázkou ještě zůstává, jak počítat zobecněné Legendrovi symboly, které se nám vyskytují ve vzorci a jestli má vůbec smysl je počítat. Následující lemma nám dá postup pro vyčíslení Legendrových symbolů.

Lemma 3.1.3. *Pro $a \in \mathbb{F}_q$ platí*

$$\left(\frac{a}{\mathbb{F}_q}\right) = a^{\frac{q-1}{2}}$$

Důkaz. Pokud je $\left(\frac{a}{\mathbb{F}_q}\right) = 1$, pak existuje $x \in \mathbb{F}_q$ takové, že $x^2 = a$. Je tedy

$$a^{\frac{q-1}{2}} = (x^2)^{\frac{q-1}{2}} = x^{q-1} = 1,$$

neboť $x^{q-1} = 1$ pro každé $x \in \mathbb{F}_q \setminus \{0\}$.

Ať je naopak $\left(\frac{a}{\mathbb{F}_q}\right) = -1$. Jako pro všechny prvky tělesa i pro a platí $a^{q-1} = 1$, tedy $a^{q-1} - 1 = 0$. To lze rozložit na

$$(a^{\frac{q-1}{2}} - 1)(a^{\frac{q-1}{2}} + 1) = 0.$$

Tedy jeden z činitelů musí být 0. Předpokládejme, že se nule rovná první z činitelů, tj. že $a^{(q-1)/2} - 1 = 0$. Tedy a je kořenem polynomu $g = x^{(q-1)/2} - 1$, $g \in \mathbb{F}_q[x]$. Ale počet prvků $b \in \mathbb{F}_q$ takových, že $\left(\frac{b}{\mathbb{F}_q}\right) = 1$ je $(q-1)/2$ a každý z nich je dle první části důkazu také kořenem polynomu g. Dostáváme tedy, že polynom g stupně $(q-1)/2$ má aspoň $(q-1)/2 + 1$ kořenů. To je ale pro polynom nad tělesem nemožné, proto byl náš předpoklad chybný a tedy se 0 musí rovnat druhý z činitelů, tj. $a^{(q-1)/2} + 1 = 0$, tedy dostáváme $a^{(q-1)/2} = -1$. □

V praxi bývá ale rychlejší si předpočítat seznam čtverců tělesa a pak jen kontrolovat zda pro dané $x \in \mathbb{F}_q$ je $f(x)$ v seznamu čtverců. To se například pro $\mathbb{F}_p$, kde p je prvočíslo, dá udělat docela efektivně za použití následujícího vztahu.

$$(i+1)^2 = i^2 + 2i + 1$$

Pomocí této rovnosti sestavíme rekurzivně posloupnost všech čtverců v $\mathbb{F}_p$. Definujme $a_1 = 1$ a $a_{i+1} = a_i + 2i + 1$. Pro takto definovanou posloupnost platí $a_i = i^2$, proto množina $\{a_1, \ldots, a_{(p-1)/2}\}$ je právě množinou všech čtverců v $\mathbb{F}_p$. Protože tento výpočet používá pouze sčítání, je výhodnější než prosté mocnění všech prvků tělesa.

Pro těleso $\mathbb{F}_q$, kde $q = p^k$, je to podobné. Ať je $\mathbb{F}_q$ reprezentováno jako $\mathbb{F}_q = \mathbb{F}_p[x]/(g(x))$, kde $g \in \mathbb{F}_p[x]$ je ireducibilní polynom stupně k. Využijeme vztahu

$$(\alpha + x^i)^2 = \alpha^2 + 2\alpha x^i + x^{2i}$$

pro $\alpha \in \mathbb{F}_p[x]/(g(x))$. Začneme-li s $\alpha = 0$, můžeme postupně vyčíslit čtverce všech prvků $\mathbb{F}_q$. Vždy totiž z již vypočteného čtverce použitím zmíněného vzorce spočteme čtverec prvku s o jedna větším koeficientem u x^i.

Podívejme se ještě na celkovou složitost výpočtu explicitního vzorce. Těleso $\mathbb{F}_q$ obsahuje $\mathcal{O}(q)$ čtverců. Podle uvedených vzorců lze každý čtverec spočítat pomocí

konstantního počtu sčítání a násobení prvků tělesa, složitější operací je násobení, které má dle části 2.2 složitost $\mathcal{O}(\log(q)^2)$. Předpočítání tabulky čtverců má tedy složitost $\mathcal{O}(\log(q)^2 q)$. K vyčíslení samotného vzorce pak potřebujeme $\mathcal{O}(q)$ sčítání, což má menší složitost než výpočet tabulky čtverců. Celková složitost je tedy $\mathcal{O}(\log(q)^2 q)$. Pro každé $\epsilon > 0$ a pro dostatečně velké q platí

$$\log(q)^2 q < q^{1+\epsilon},$$

proto lze celkovou složitost psát také jako $\mathcal{O}(q^{1+\epsilon}) = \mathcal{O}\left((2^{1+\epsilon})^{\log(q)}\right)$ pro libovolné $\epsilon > 0$. Stejná složitost vyjde u vzorce v charakteristice 2, který představíme nyní.

3.2 Charakteristika 2

Uvažujme nyní hypereliptickou křivku E definovanou nad tělesem $\mathbb{F}_{2^k}$, která je dána rovnicí

$$y^2 + yh(x) = f(x),$$

kde $\deg(f) = 2g + 1$ a $\deg(h) \leq g$. Budeme postupovat podobně jako v případě charakteristiky různé od 2. Budeme procházet všechna $a \in \mathbb{F}_{2^k}$ a zjišťovat kolik existuje prvků $b \in \mathbb{F}_{2^k}$ takových, že $(a, b) \in E(\mathbb{F}_{2^k})$. Rozlišíme dvě možnosti. Buď je a kořenem polynomu h tj. $h(a) = 0$, pak dostáváme rovnici $y^2 = f(a)$, a protože v konečném tělese charakteristiky 2 je druhá mocnina automorfismem, existuje právě jedno řešení, a tedy bod $(a, \sqrt{f(a)})$ je jediný bod křivky s první souřadnicí rovnou a.

Než se podíváme na druhý případ tj. $h(a) \neq 0$, ukážeme si, jak v charakteristice 2 rozhodnout o počtu řešení kvadratické rovnice. Mějme kvadratickou rovnici $ax^2 + bx + c = 0$. Pokud je $a = 0$ nebo $b = 0$, řešení je jednoduché. Předpokládejme tedy, že oba zmíněné koeficienty jsou nenulové. Lineární substitucí $z = (a/b)x$ převedeme rovnici na tvar $z^2 + z = d$, kde $d = -(ac)/b^2$. Dále se tedy budeme zabývat pouze rovnicí v tomto tvaru.

Definice 3.2.1. *Ať $\mathbb{F}_{q^k}$ je rozšířením tělesa $\mathbb{F}_q$. Pro $a \in \mathbb{F}_{q^k}$ definujeme* stopu prvku a v rozšíření $\mathbb{F}_q \subseteq \mathbb{F}_{q^k}$ *následovně*

$$\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(a) = a + a^q + a^{q^2} + \ldots + a^{q^{k-1}}.$$

Stopu v rozšíření kde $\mathbb{F}_q$ je prvotěleso tělesa $\mathbb{F}_{q^k}$, tj. $q = p$ pro nějaké prvočíslo p, budeme značit $\mathrm{Tr}(a)$ a nazývat stopou prvku a.

Lemma 3.2.2. *Nechť $a \in \mathbb{F}_{q^k} \supseteq \mathbb{F}_q$, pak $\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(a) \in \mathbb{F}_q$.*

Důkaz. Prvky tělesa $\mathbb{F}_q$ jsou právě takové prvky $x \in \mathbb{F}_{q^k}$, pro které platí $x^q = x$. Stačí tedy ukázat, že $(\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(a))^q = \mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(a)$. Proveďme tedy výpočet.

$$\begin{aligned}(\mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(a))^q &= \left(\sum_{i=0}^{k-1} a^{q^i}\right)^q = \sum_{i=0}^{k-1} a^{q^{i+1}} = \sum_{i=1}^{k} a^{q^i} = a^{q^k} - a + \sum_{i=0}^{k-1} a^{q^i} \\ &= \sum_{i=0}^{k-1} a^{q^i} = \mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}(a)\end{aligned}$$

V předposledním kroku využíváme faktu, že $a^{q^k} = a$. Tím je lemma dokázáno. □

Důsledek 3.2.3. *Důsledek tohoto lemmatu pro rozšíření $\mathbb{F}_2 \subseteq \mathbb{F}_{2^k}$ je, že stopa prvku z $\mathbb{F}_{2^k}$ je vždy 0, nebo 1.*

Lemma 3.2.4. *Mějme kvadratickou rovnici $z^2 + z = d$, kde $d \in \mathbb{F}_{2^k}$ pro nějaké k. Tato rovnice má řešení v tělese $\mathbb{F}_{2^k}$, právě když $\mathrm{Tr}\,(d) = 0$.*

Důkaz. Nejprve si pro libovolné $\alpha \in \overline{\mathbb{F}}_{2^k}$ spočteme stopu prvku $\alpha^2 + \alpha$.

$$\begin{aligned}\mathrm{Tr}\left(\alpha^2+\alpha\right) &= \sum_{i=0}^{k-1}(\alpha^2+\alpha)^{2^i} = \sum_{i=0}^{k-1}(\alpha^{2^{i+1}}+\alpha^{2^i}) \\ &= \sum_{i=0}^{k-1}\alpha^{2^{i+1}} + \sum_{i=0}^{k-1}\alpha^{2^i} = \sum_{i=1}^{k}\alpha^{2^i} + \sum_{i=0}^{k-1}\alpha^{2^i} \\ &= \alpha^{2^k} + \sum_{i=1}^{k-1}\alpha^{2^i} + \alpha + \sum_{i=1}^{k-1}\alpha^{2^i} = \alpha^{2^k} + \alpha\end{aligned}$$

Proto

$$\mathrm{Tr}\left(\alpha^2+\alpha\right) = \alpha^{2^k} + \alpha. \tag{3.2}$$

Nyní již k samotnému důkazu. Předpokládejme, že rovnice má řešení $\alpha \in \mathbb{F}_{2^k}$, tj. $\alpha^2 + \alpha = d$. Potom se stopa d spočítá následovně

$$\mathrm{Tr}\,(d) = \mathrm{Tr}\left(\alpha^2+\alpha\right) = \alpha^{2^k} + \alpha = 0.$$

Přičemž jsme využili rovnosti 3.2 a v poslední rovnosti toho, že pro každé $x \in \mathbb{F}_{2^k}$ platí $x^{2^k} = x$. První část tedy máme hotovou. Předpokládejme nyní naopak, že $\mathrm{Tr}\,(d) = 0$ a ukažme, že rovnice má řešení v $\mathbb{F}_{2^k}$. Vezměme si nějaké řešení rovnice v algebraickém uzávěru tělesa $\mathbb{F}_{2^k}$. Máme tedy $\alpha \in \overline{\mathbb{F}}_{2^k}$ takové, že $\alpha^2 + \alpha = d$. $\mathrm{Tr}\,(d) = 0$, počítejme tedy

$$0 = \mathrm{Tr}\,(d) = \mathrm{Tr}\left(\alpha^2+\alpha\right) \overset{3.2}{=} \alpha^{2^k} + \alpha$$

Proto platí $\alpha^{2^k} = \alpha$. Neboť ale $\mathbb{F}_{2^k}$ je množina právě takových prvků $x \in \overline{\mathbb{F}}_{2^k}$, pro které platí $x^{2^k} = x$, dostáváme, že $\alpha \in \mathbb{F}_{2^k}$. □

Nyní se konečně můžeme vrátit k rovnici naší hypereliptické křivky. Zbývá nám vyřešit případ, kdy $h(a) \neq 0$. Můžeme proto provést substituci $z = y/h(a)$, tím dostaneme rovnici

$$z^2 + z = \frac{f(a)}{h(a)^2}.$$

Podle předchozího lemmatu a důsledku má tato rovnice řešení v $\mathbb{F}_{2^k}$, pokud stopa prvku $f(a)/h(a)^2$ je rovna 0. Pokud řešení nemá, stopa $f(a)/h(a)^2$ je 1. Navíc z tvaru rovnice je vidět, že pokud má řešení, pak má právě dvě různá řešení. Tedy pokud $h(a) \neq 0$ a $\mathrm{Tr}\,(f(a)/h(a)^2) = 0$, existují dva body ležící na křivce, které mají první souřadnici a. Pokud $h(a) \neq 0$ a $\mathrm{Tr}\,(f(a)/h(a)^2) = 1$, pak takový bod neexistuje žádný.

Započítáme-li ještě bod v nekonečnu, máme dokázáno následujícího tvrzení.

Tvrzení 3.2.5. *Ať E je hypereliptická křivka definovaná nad $\mathbb{F}_{2^k}$ daná rovnicí $y^2 + yh(x) = f(x)$. Definujme $V_h = \{x \in \mathbb{F}_{2^k} | h(x) = 0\}$, pak*

$$|E(\mathbb{F}_{2^k})| = 1 + |V_h| + 2 \sum_{x \in \mathbb{F}_{2^k} \setminus V_h} \left(1 - \mathrm{Tr}\left(\frac{f(x)}{h(x)^2}\right)\right)$$

Nakonec ještě ukážeme, že počítat stopu prvku není tak náročné, jak se zdá. Je tam sice výpočet mocnin, ale ve skutečnosti to při vhodné reprezentaci tělesa lze provést jako součet předpočítaných hodnot. Ať $\mathbb{F}_{2^k} = \mathbb{F}_2[x]/(g(x))$ kde g je ireducibilní polynom stupně k nad $\mathbb{F}_2$. Prvek $a \in \mathbb{F}_{2^k}$ je tedy reprezentován jako polynom $a = \sum_{i=0}^{k-1} a_i x^i$, kde $a_i \in \mathbb{F}_2$ pro každé i. Jeho stopa pak je

$$\begin{aligned}\mathrm{Tr}\,(a) &= \sum_{j=0}^{k-1} \left(\sum_{i=0}^{k-1} a_i x^i\right)^{2^j} = \sum_{j=0}^{k-1}\sum_{i=0}^{k-1} a_i^{2^j} x^{i2^j} = \sum_{j=0}^{k-1}\sum_{i=0}^{k-1} a_i x^{i2^j} \\ &= \sum_{i=0}^{k-1} \left(a_i \sum_{j=0}^{k-1} x^{i2^j}\right) = \sum_{i=0}^{k-1} a_i \mathrm{Tr}\left(x^i\right)\end{aligned}$$

Hodnoty $\mathrm{Tr}\,(x^i)$ se použijí při výpočtu pro libovolné a, proto si je pro každé $i = 0, 1, \ldots, k-1$ spočteme předem. Při výpočtu stopy pak už jen projdeme koeficienty $a_0, a_1, \ldots, a_{k-1}$ a posčítáme všechny hodnoty $\mathrm{Tr}\,(x^i)$, pro které je a_i nenulové, tj. $a_i = 1$.

Kapitola 4

Využití podtěles

Mějme eliptickou křivku E danou Weierstrassovou rovnicí $w(x, y) = 0$ definovanou nad tělesem $\mathbb{F}_q$. V této kapitole ukážeme, jak využít znalost počtu $\mathbb{F}_q$-racionálních bodů křivky pro určení počtu $\mathbb{F}_{q^k}$-racionálních bodů. Jinak řečeno jak se znalostí $|E(\mathbb{F}_q)|$ spočítat $|E(\mathbb{F}_{q^k})|$. Pro obecnou hypereliptickou křivku E rodu g ukážeme postup, jak ze znalosti $|E(\mathbb{F}_{q^j})|$ pro každé $j \leq g$ spočítat $|E(\mathbb{F}_{q^k})|$ pro libovolné $k > g$. V první části ukážeme výpočet pro eliptické křivky, ve druhé potom jeho zobecnění na křivky hypereliptické.

4.1 Eliptické křivky

Lemma 4.1.1. *Zobrazení*

$$\begin{aligned} \phi_q : E(\overline{\mathbb{F}}_q) &\longrightarrow E(\overline{\mathbb{F}}_q) \\ (x, y) &\longmapsto (x^q, y^q) \\ \mathcal{O} &\longmapsto \mathcal{O} \end{aligned}$$

je endomorfismem grupy $E(\overline{\mathbb{F}}_q)$.

Důkaz. Neboť mocnění na q je endomorfismem tělesa $\overline{\mathbb{F}}_q$ a souřadnice součtu dvou bodů lze vyjádřit jako racionální funkce, je operace sčítání kompatibilní s tímto zobrazením, tedy se jedná o endomorfismus. □

Definice 4.1.2. *Zobrazení z předchozího lemmatu nazýváme* Frobeniovým endomorfismem *křivky E.*

Výpočet pro eliptické křivky se bude opírat o následující tvrzení.

Tvrzení 4.1.3. *Ať E je eliptická křivka nad tělesem $\mathbb{F}_q$ a ať $t = q + 1 - |E(\mathbb{F}_q)|$. Pak pro každý bod $P \in E(\overline{\mathbb{F}}_q)$ platí*

$$\phi_q^2(P) - t\phi_q(P) + qP = \mathcal{O}.$$

Navíc t je jednoznačně určeno, tj. t je jediné celé číslo takové, že rovnost platí pro každé $P \in E(\overline{\mathbb{F}}_q)$.

Jinými slovy toto tvrzení říká, že endomorfismus $\phi_q^2 - t\phi_q + q$ je nulový endomorfismus na eliptické křivce E.

Důkaz. Kompletní důkaz lze najít např. v [8](Kapitola 5, Tvrzení 2.3.1). Části důkazu pro těleso charakteristiky různé od 2 a 3 pak uvedeme v části 6.2. □

Uvažme polynom $\chi(x) = x^2 - tx + q$, $\chi \in \mathbb{Z}[x]$. V komplexních číslech má tento polynom dva kořeny, označme je tedy α a β. Protože χ je monický, je $\chi(x) = (x - \alpha)(x - \beta)$. Následující lemma nám řekne něco o tom, jak vypadají součty $\alpha^n + \beta^n$ pro $n \in \mathbb{Z}$.

Lemma 4.1.4. *Ať χ, α a β jsou jako výše. Označme $s_n = \alpha^n + \beta^n$, pak*

$$\begin{aligned} s_0 &= 2 \\ s_1 &= t \\ s_{n+1} &= ts_n - qs_{n-1} \end{aligned}$$

pro každé $n \in \mathbb{N}$.

Důkaz. α je kořenem χ, tj. $\alpha^2 - \alpha t + q = 0$. Pokud tuto rovnost vynásobíme α^{n-1}, dostaneme $\alpha^{n+1} = \alpha^n t - \alpha^{n-1} q$. To samé můžeme udělat pro β, tedy $\beta^{n+1} = \beta^n t - \beta^{n-1} q$. Sečtením těchto dvou rovností získáváme požadované tvrzení. □

Důsledek 4.1.5. *Přestože α a β jsou obecně komplexní čísla, z předchozího lemmatu plyne, že součty s_n jsou vždy čísla celá, proto následující tvrzení dává smysl.*

Tvrzení 4.1.6. *Mějme eliptickou křivku E definovanou nad tělesem $\mathbb{F}_q$. Ať $|E(\mathbb{F}_q)| = q - t + 1$ a $\chi(x) = x^2 - tx + q = (x - \alpha)(x - \beta)$. Pak pro každé $k \in \mathbb{N}$ platí*

$$|E(\mathbb{F}_{q^k})| = q^k - (\alpha^k + \beta^k) + 1.$$

Důkaz. Uvažme polynom

$$f(x) = (x^k - \alpha^k)(x^k - \beta^k) = x^{2k} - (\alpha^k + \beta^k)x + (\alpha\beta)^k = x^{2k} - (\alpha^k + \beta^k)x + q^k.$$

Z předchozího důsledku víme, že $f \in \mathbb{Z}[x]$. α a β jsou kořeny tohoto polynomu, proto polynom χ dělí f v $\mathbb{C}[x]$. Označme jejich podíl v $\mathbb{C}[x]$ jako g. Ukážeme, že $g \in \mathbb{Z}[x]$. Protože polynom χ je monický, můžeme jím v okruhu $\mathbb{Z}[x]$ vydělit se zbytkem polynom f, proto existují celočíselné polynomy r a s takové, že $f = r\chi + s$, kde $\deg(s) < \deg(\chi)$. g jsme definovali tak, že $f = \chi g$, máme tedy

$$\begin{aligned} \chi g &= r\chi + s \\ \chi(g - r) &= s. \end{aligned}$$

Stupeň s je ale ostře menší než stupeň χ, proto musí být obě strany rovnosti nulové, a tedy $g = r$. Dostáváme tedy, že polynom g má celočíselné koeficienty. To potřebujeme, aby dávalo smysl následující dosazení Frobeniova automorfismu do polynomu.

$$\begin{aligned} \phi_{q^k}^2 - (\alpha^k + \beta^k)\phi_{q^k} + q^k &= \phi_q^{2k} - (\alpha^k + \beta^k)\phi_q^k + q^k = f(\phi_q) \\ &= g(\phi_q)\chi(\phi_q) = g(\phi_q)(\phi_q^2 - t\phi_q + q) = 0. \end{aligned}$$

Rovnost chápeme jako rovnost endomorfismů křivky E, přičemž v posledním kroku jsme využily tvrzení 4.1.3. Máme tedy

$$\phi_{q^k}^2 - (\alpha^k + \beta^k)\phi_{q^k} + q^k = 0.$$

Všiměme si, že rovnost odpovídá rovnosti z tvrzení 4.1.3, pokud místo tělesa $\mathbb{F}_q$ uvažujeme těleso $\mathbb{F}_{q^k}$. Tedy aplikací dodatku o jednoznačnosti z tvrzení 4.1.3 na tuto rovnost dostáváme požadovaný výsledek, tj. $|E(\mathbb{F}_{q^k})| = q^k - (\alpha^k + \beta^k) + 1$. □

4.2 Hypereliptické křivky

I pro hypereliptické křivky se dá použít obdobný postup, k ukázání jeho správnosti je však třeba obecnější aparát. Proto nyní zavedeme pojem *zeta-funkce* a uvedeme její důležité vlastnosti.

Definice 4.2.1. *Buď E křivka definovaná nad tělesem $\mathbb{F}_q$. Označme $N_k = |E(\mathbb{F}_{q^k})|$. Funkci*

$$Z_E(T) = exp\left(\sum_{k=1}^{\infty} \frac{N_k}{k} T^k\right)$$

nazveme zeta-funkcí *křivky E.*

Funkci $exp(x)$ zde chápeme jako mocninou řadu $\sum_{n=0}^{\infty} x^n/n!$. Zeta-funkce tedy nese informaci o počtech $\mathbb{F}_{q^k}$-racionálních bodů křivky E. S takovouto definicí zeta-funkce by se nám nepracovalo dobře, následující věta uvedená v [2](Tvrzení 8.3) však ukáže některé její zajímavé vlastnosti a alternativní vyjádření.

Věta 4.2.2 (Weilova hypotéza)**.** *Mějme křivku E rodu g. Ať Z_E je zeta-funkce křivky E nad tělesem $\mathbb{F}_q$, pak*

1. *funkce Z_E je ve skutečnosti racionální funkce s celočíselnými koeficienty,*
2. *funkce Z_E splňuje následující funkční rovnost*

$$Z_E(T) = q^{g-1} T^{2g-2} Z_E\left(\frac{1}{qT}\right), \tag{4.1}$$

3. *existuje polynom $L(T) \in \mathbb{Z}[T]$ stupně nejvýše $2g$ takový, že*

$$Z_E(T) = \frac{L(T)}{(1-T)(1-qT)}. \tag{4.2}$$

Navíc $L(T)$ lze vyjádřit jako

$$L(T) = \prod_{i=1}^{2g} (1 - \alpha_i T) \tag{4.3}$$

pro nějaká komplexní čísla $\alpha_1, \alpha_2, \ldots, \alpha_{2g}$ taková, že pro každé i platí $|\alpha_i| = \sqrt{q}$

Polynom L z předchozí věty nazýváme *L-polynomem* křivky E nad tělesem $\mathbb{F}_q$. Vyjádření 4.3 nyní můžeme dosadit do rovnice 4.2 a spočítat logaritmus obou stran.

$$\ln(Z_E(T)) = \ln\left(\frac{\prod_{i=1}^{2g}(1-\alpha_i T)}{(1-T)(1-qT)}\right)$$

$$\sum_{k=1}^{\infty} \frac{N_k}{k} T^k = \sum_{i=1}^{2g} \ln(1-\alpha_i T) - \ln(1-T) - \ln(1-qT).$$

Pravou stranu nyní upravíme za využití rozvoje logaritmu $-\ln(1-x) = \sum_{k=1}^{\infty} x^k/k$.

$$\sum_{k=1}^{\infty} \frac{N_k}{k} T^k = -\sum_{i=1}^{2g} \sum_{k=1}^{\infty} \frac{(\alpha_i T)^k}{k} + \sum_{k=1}^{\infty} \frac{T^k}{k} + \sum_{k=1}^{\infty} \frac{(qT)^k}{k}.$$

Prostým porovnáním koeficientů u členů T^k/k pro každé k dostáváme následující rovnost.

$$N_k = q^k + 1 - \sum_{i=1}^{2g} \alpha_i^k \tag{4.4}$$

A právě tuto rovnost využijeme pro určení počtu bodů křivky. Zůstává však otázkou, jak zjistit hodnoty $\alpha_1, \alpha_2, \ldots, \alpha_{2g}$, popřípadě jak zjistit rovnou jejich součet. Ať $a_0, a_1, \ldots, a_{2g} \in \mathbb{Z}$ jsou koeficienty polynomu L, tj. $L(T) = \sum_{i=0}^{2g} a_i T^i$. Pokud bychom tyto koeficienty znali, měli bychom dvě možnosti. Buď faktorizovat polynom L nad komplexními čísly, pak jeho kořeny jsou právě převrácené hodnoty prvků α_i. Druhá možnost je využít rekurzivního vzorce přímo pro výpočet součtu $-\sum_{i=1}^{2g} \alpha_i^k$, který vychází z následujícího lemmatu.

Lemma 4.2.3 (Newtonova identita)**.** *Ať $x_1, x_2, \ldots, x_n$ jsou algebraicky nezávislé prvky nad tělesem K. Pro $k \in \mathbb{Z}$ a $l = 1, 2, \ldots, n$ definujme*

$$S_k = \sum_{i=1}^{n} x_i^k$$
$$P_l = (-1)^l \sum_{i_1 < \ldots < i_l} x_{i_1} x_{i_2} \ldots x_{i_l}.$$

Pak platí

$$S_d + P_1 S_{d-1} + P_2 S_{d-2} + \ldots + P_n S_{d-n} = 0 \text{ pokud } d \geq n,$$
$$S_d + P_1 S_{d-1} + P_2 S_{d-2} + \ldots + P_{d-1} S_1 + d P_d = 0 \text{ pokud } 1 \leq d < n.$$

Důkaz. Definujeme-li polynom $f(x)$ jako

$$f(x) = (x - x_1)(x - x_2) \ldots (x - x_n),$$

můžeme si všimnout, že jeho koeficienty jsou právě prvky P_l, konkrétně

$$f(x) = x^n + P_1 x^{n-1} + \ldots + P_{n-1} x + P_n.$$

Pro každé i je $f(x_i) = 0$, dostáváme tedy rovnost

$$x_i^n + P_1 x_i^{n-1} + \ldots + P_{n-1} x_i + P_n = f(x_i) = 0 \text{ pro každé } i = 1, 2, \ldots, n \tag{4.5}$$

Pokud tyto rovnice pro každé i sečteme dohromady, dostaneme

$$S_n + P_1 S_{n-1} + \ldots + P_{n-1} S_1 + P_n S_0 = 0.$$

To je přesně požadované tvrzení pro případ $d = n$. Případ, kdy $d > n$ ukážeme také jednoduše. Stačí i-tou rovnici z 4.5 vynásobit prvkem x_i^{d-n} a opět všechny rovnice posčítat. Tím dostaneme

$$S_d + P_1 S_{d-1} + \ldots + P_{d-1} S_1 + P_n S_{d-n} = 0,$$

tedy právě požadované tvrzení. Zbývá tedy už jen vyřešit případ, kdy $d < n$. Postupujeme stejně jako v předchozím případu, i-tou rovnici z 4.5 vynásobíme prvken x_i^{d-n} po sečtení všech rovnic dostáváme rovnost

$$S_d + P_1 S_{d-1} + \ldots + P_{d-1} S_1 + P_d S_0 + P_{d+1} S_{-1} + P_{d+2} S_{-2} + \ldots + P_n S_{d-n} = 0.$$

Protože $S_0 = n$, můžeme člen $P_d S_0$ napsat jako nP_d a rozdělit na součet $dP_d + (n-d)P_d$, tedy

$$(S_d + P_1 S_{d-1} + \ldots + P_{d-1} S_1 + dP_d) + ((n-d)P_d + P_{d+1} S_{-1} + \ldots + P_n S_{d-n}) = 0.$$

V první závorce máme přesně výraz o kterém chceme dokázat, že se rovná nule. Označme si první závorku jako A a druhou jako B. Pokud bychom všechny členy roznásobili, dostali bychom součet monomů tvaru $x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ kde $k_i \in \mathbb{Z}$. Je zřejmé, že člen A se skládá z monomů, ve kterých jsou všechna k_i nezáporná. My ukážeme, že člen B má naopak v každém monomu aspoň jeden záporný exponent. Pak je totiž zřejmé, že se monomy z A a B nemohou vzájemně odečíst(zde se využívá algebraické nezávislosti prvků $x_1, x_2, \ldots, x_n$) a je tedy nutné, aby $A = B = 0$. Je

$$B = (n-d)P_d + P_{d+1} S_{-1} + P_{d+2} S_{-2} + \ldots + P_n S_{d-n}.$$

Členy $P_{d+j} S_{-j}$ pro $j \geq 2$ mají na první pohled v každém monomu aspoň jeden záporný exponent, zbývá tedy totéž ukázat o zbytku členu B, tj. o výrazu $(n-d)P_d + P_{d+1} S_{-1}$. Výraz rozepíšeme jako

$$\begin{aligned}
&(n-d)(-1)^d \sum_{i_1<\ldots<i_d} x_{i_1} x_{i_2} \ldots x_{i_d} + \left((-1)^{d+1} \sum_{i_1<\ldots<i_{d+1}} x_{i_1} x_{i_2} \ldots x_{i_{d+1}} \right) \left(\sum_{j=1}^{n} \frac{1}{x_j} \right) \\
&= (n-d)(-1)^d \sum_{i_1<\ldots<i_d} x_{i_1} x_{i_2} \ldots x_{i_d} + \left((-1)^{d+1} \sum_{i_1<\ldots<i_{d+1}} \sum_{j=1}^{n} \frac{x_{i_1} x_{i_2} \ldots x_{i_{d+1}}}{x_j} \right).
\end{aligned}$$

Monomy v poslední sumě, které mají všechny indexy i_k různé od indexu j mají záporný exponent u x_j, tedy splňují naši podmínku. Monomy, u kterých pro nějaké k platí $i_k = j$ naši podmínku sice nesplňují ale my ukážeme, že se odečtou s monomy v první sumě, tedy úplně zmizí. Monom $x_{i_1} x_{i_2} \ldots x_{i_d}$ vznikne ze členu druhé sumy který má tvar $x_{i_1} x_{i_2} \ldots x_j \ldots x_{i_d} / x_j$ kde $j \neq i_k$ pro každé k. Takových možností pro j je $n-d$, proto vznikne právě $n-d$ monomů $x_{i_1} x_{i_2} \ldots x_{i_d}$ to je stejný počet jako v první sumě, díky opačným znaménkům tedy všechny tyto monomy zmizí. Tím je lemma dokázáno. □

To, že jsme tento vztah dokázali pro algebraicky nezávislé prvky, nyní znamená, že ho můžeme použít pro libovolné prvky nad libovolným tělesem. Je to vlastně vztah polynomů v proměnných $x_1, x_2, \ldots, x_n$, tedy musí platit i pokud do těchto polynomů dosadíme libovolné prvky tělesa.

Vraťme se k počítání bodů. Rovnice 4.4 říká $N_k = q^k + 1 - \sum_{i=1}^{2g} \alpha_i^k$. Označme

$$S_k = -\sum_{i=1}^{2g} \alpha_i^k.$$

Dále máme $L(T) = \sum_{i=0}^{2g} a_i T^i = \prod_{i=1}^{2g}(1 - \alpha_i T)$. Po roznásobení dostaneme

$$a_k = (-1)^k \sum_{i_1 < \ldots < i_k} \alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_k}$$

pro $k \neq 0$ a $a_0 = 1$. Lemma 4.2.3 nám nyní dává rekurentní vztahy mezi koeficienty L-polynomu křivky a mezi součty S_k, které jednoznačně určují počty $\mathbb{F}_{q^k}$-racionálních bodů. Platí tedy

$$\begin{aligned} S_k + a_1 S_{k-1} + a_2 S_{k-2} + \ldots + a_{2g} S_{k-2g} &= 0 \text{ pokud } k \geq 2g, \\ S_k + a_1 S_{k-1} + a_2 S_{k-2} + \ldots + a_{k-1} S_1 &= k a_k \text{ pokud } 1 \leq k < 2g. \end{aligned} \tag{4.6}$$

Tyto rovnosti se daní využít dvěma způsoby. Bud můžeme ze znalostí koeficientů a_i počítat součty S_k, nebo naopak pokud známe $S_1, ..., S_k$, jsme schopni spočítat koeficient a_k. Ještě než však uvedeme konečnou podobu výpočtu $|E(\mathbb{F}_{q^k})|$, ukážeme, že L-polynom je jednoznačně určen polovinou svých koeficientů.

Lemma 4.2.4. *Ať $a_0, a_1, \ldots, a_{2g}$ jsou koeficienty L-polynomu křivky E nad tělesem $\mathbb{F}_q$, pak $a_{2g-i} = q^{g-i} a_i$*

Důkaz. Rovnost dokážeme přímočarým výpočtem za použití druhé a třetí části Weilovy hypotézy 4.2.2.

$$\begin{aligned} \sum_{i=0}^{2g} a_i T^i = L(T) &= (1-T)(1-qT)Z_E(T) \\ &= (1-T)(1-qT)q^{g-1}T^{2g-2}Z_E\left(\frac{1}{qT}\right) \\ &= (1-T)(1-qT)q^{g-1}T^{2g-2}\frac{L\left(\frac{1}{qT}\right)}{\left(1-\frac{1}{qT}\right)\left(1-q\frac{1}{qT}\right)} \\ &= (1-T)(1-qT)q^{g-1}T^{2g-2}\frac{L\left(\frac{1}{qT}\right)}{\left(\frac{qT-1}{qT}\right)\left(\frac{T-1}{T}\right)} \\ &= q^g T^{2g} L\left(\frac{1}{qT}\right) = q^g T^{2g} \sum_{i=0}^{2g} a_i \left(\frac{1}{qT}\right)^i = \sum_{i=0}^{2g} q^{g-i} a_i T^{2g-i} \end{aligned}$$

Porovnáním koeficientů dostáváme požadovanou rovnost. □

Nyní již máme vše potřebné pro popis výpočtu velikosti $E(\mathbb{F}_{q^k})$. Předpokládejme, že známe $|E(\mathbb{F}_{q^j})|$ pro všechna $j \leq g$(mohli jsme si tyto velikosti například spočítat pomocí explicitního vzorce). Tedy z rovnosti 4.4 známe S_j pro každé $j \leq g$. Pomocí rekurentních vztahů 4.6 spočítáme koeficienty a_j pro $j \leq g$. Za použití vztahu $a_{2g-j} = q^{g-j} a_j$ z předchozího lemmatu spočteme koeficienty a_j pro $j = g+1, g+2, \ldots, 2g$. Máme tedy všechny koeficienty a_j a můžeme opět použít rekurzivní vztahy 4.6 pro výpočet hodnot S_k pro všechna $k > g$. Počet bodů křivky je potom $|E(\mathbb{F}_{q^k})| = q^k + 1 + S_k$.

Kapitola 5

Využití řádu prvků

V této kapitole konečně využijeme i toho, že na bodech eliptické křivky máme definovanou operaci sčítání a že body s touto operací tvoří grupu. Grupu tvořenu $\mathbb{F}_q$-racionálními body budeme stejně jako množinu $\mathbb{F}_q$-racionálních bodů značit $E(\mathbb{F}_q)$. *Řádem* bodu $P \in E(\mathbb{F}_q)$ nazýváme nejmenší přirozené číslo n takové, že platí $nP = \mathcal{O}$. Budeme ho značit $\mathrm{ord}\,(P)$. V každé grupě platí, že řád každého jejího prvku dělí řád(velikost) celé grupy. Pokud tedy vybereme náhodný bod eliptické křivky a spočteme jeho řád, dostáváme netriviální informaci o velikosti grupy, tj. o počtu $\mathbb{F}_q$-racionálních bodů. Pokud vezmeme další náhodný bod a opět spočítáme jeho řád, pak nejmenší společný násobek těchto dvou řádů opět dělí velikost grupy. Takto můžeme postupovat dále a postupně zvětšovat číslo o kterém víme, že dělí řád grupy. Pokud však grupa obsahuje pouze prvky malého řádu, nemusí takový postup nutně vést k odhalení řádu grupy, my ale v této kapitole ukážeme, že u eliptických křivek tento postup funguje. V první části ukážeme jak lze počítat řády prvků a potom uvedeme, proč nastíněný postup funguje pro eliptické křivky a formulujeme algoritmus pro určení počtu bodů křivky nad $\mathbb{F}_p$ s asymptotickou složitostí $\mathcal{O}(p^{3/4+\epsilon})$ pro libovolné $\epsilon > 0$. Je

$$\mathcal{O}\left(p^{\frac{3}{4}+\epsilon}\right) = \mathcal{O}\left(2^{(\frac{3}{4}+\epsilon)\log(p)}\right) = \mathcal{O}\left(\left(2^{\frac{3}{4}+\epsilon}\right)^{\log(p)}\right).$$

Složitost algoritmu bude tedy stejně jako u explicitního vzorce exponenciální, ale už ne se základem $2^{1+\epsilon}$, ale jen $2^{3/4+\epsilon} \doteq 1.68 + \epsilon'$ pro libovolné $\epsilon' > 0$. Tedy tento algoritmus bude efektivnější než vyčíslování explicitního vzorce.

5.1 Baby Steps-Giant Steps

V této části ukážeme, jak počítat řád bodu v grupě eliptické křivky. Řád bodu P, to je vlastně diskrétní logaritmus bodu $\mathcal{O}$ o základu P. Šlo by proto použít libovolný algoritmus pro počítání diskrétního logaritmu v grupě eliptické křivky. Na problému diskrétního logaritmu však stojí bezpečnost kryptosystémů založených na eliptických křivkách, je tedy zřejmé, že žádný algoritmus pro počítání logaritmu nebude moc efektivní. Počítání obecného logaritmu však není totéž, jako počítáni logaritmu pouze u prvku $\mathcal{O}$. Nyní předvedeme algoritmus, který pro daný bod P v grupě bodů eliptické křivky spočte buď řád prvku P, nebo určí rovnou řád grupy $E(\mathbb{F}_q)$. To vše za předpokladu, že máme nějaký odhad na

velikost $E(\mathbb{F}_q)$. Jedná se o lehce modifikovaný algoritmus pro počítání diskrétního logaritmu v obecná grupě, kterému se říká Baby Steps-Giant Steps.

Mějme tedy grupu $E(\mathbb{F}_q) = (E(\mathbb{F}_q), +, \mathcal{O})$ a předpokládejme, že $b \leq |E(\mathbb{F}_q)| \leq c$ pro nějaká přirozená čísla b a c. Ať P je bod jehož řád chceme zjistit. Zvolme m takové, že $m > \sqrt{c-b}$. Může to být například $m = \lceil \sqrt{c-b} \rceil + 1$. Samotný výpočet bude probíhat následovně:

1. Spočteme a uložíme si prvky $-jP$ pro každé $j = 0, 1, \ldots, m$.
2. Spočteme $Q = bP$.
3. Spočteme a uložíme prvky $Q + imP$ pro každé $i = 0, 1, \ldots, m$.
4. Najdeme kolize mezi seznamy bodů spočtenými v prvním a třetím kroku, tj. najdeme všechny dvojice (i, j) takové, že platí $-jP = Q + imP$.
5. Pokud je takováto dvojice právě jedna, pak $|E(\mathbb{F}_q)| = b+im+j$ a algoritmus končí.
6. Pokud je takových dvojic více, seřadíme je všechny podle uspořádání $\preceq$, kde $(i, j) \preceq (i', j')$ právě když $i < i'$ nebo $i = i' \wedge j \leq j'$.
7. Vezmeme dvě sousední dvojice ze vzniklého uspořádaného seznamu. Označme je (i, j) a (i', j') a předpokládejme, že $(i, j) \preceq (i', j')$. Pak řád prvku P je $i'm + j' - im - j$.

Následuje několik poznámek k jednotlivým bodům a vysvětlení proč algoritmus skutečně počítá to, co tvrdíme.

- Body v prvním seznamu není třeba počítat každý nezávisle. Bod $-jP$ spočteme snadno z předchozího prostým odečtením bodu P, tedy $-jP = -(j-1)P - P$. Tomuto kroku říkáme baby step.
- Stejně tak v druhém seznamu je $Q - imP = Q + (i-1)mP + mP$, tedy na začátku si stačí spočítat mP a tento bod postupně přičítat. Těmto krokům se říká giant steps.
- Skutečně v bodu 4 vždy najdeme nějakou kolizi? V klasickém Baby Steps-Giant Steps algoritmu není zaručeno, že mezi dvěma spočtenými seznamy existuje kolize. V našem případě ale kolize nastane vždy. Je to zajištěno volbou m. Při volbě $m > \sqrt{c-b}$ totiž platí, že každé číslo x takové, že $0 \leq x \leq c - b < m^2$ lze právě jedním způsobem zapsat ve tvaru $x = im + j$ kde $i, j \in \{0, 1, 2, \ldots m-1\}$. Proto také každé číslo y, že $b \leq y \leq c$ lze právě jedním způsobem zapsat ve tvaru $y = b+im+j$. Z předpokladu víme, že $b \leq |E(\mathbb{F}_q)| \leq c$, tedy existuje $i, j \in \{0, 1, 2, \ldots m-1\}$, že $|E(\mathbb{F}_q)| = b + im + j$. A protože $|E(\mathbb{F}_q)|R = \mathcal{O}$ pro každý bod $R \in E(\mathbb{F}_q)$, existuje aspoň jedna kolize mezi oběma seznamy, konkrétně

  $$\mathcal{O} = |E(\mathbb{F}_q)|P = (b + im + j)P = Q + imP + jP,$$

  tedy

  $$-jP = Q + imP.$$

  To znamená, že j-tý prvek prvního seznamu se shoduje s i-tým prvkem seznamu druhého.

- Pokud existuje právě jedna kolize, musí to být přesně ta, kterou jsme popsali v předchozím bodu. Tedy pokud je kolize mezi body $-jP = Q + imP$, musí platit $b + im + j = |E(\mathbb{F}_q)|$. Tento případ nastane pro bod P, právě když interval od b do c obsahuje právě jeden násobek jeho řádu. Ekvivalentně tento případ nastává, právě když řád prvku P je větší než $c - b$.

- V kroku 4 ve skutečnosti není potřeba najít všechny kolize. Pokud totiž hledáme kolize postupně pro každé $i = 0, 1, \ldots, m$. Můžeme při nálezu druhé kolize výpočet dalších giant-steps ukončit a tyto dvě nalezené kolize použít rovnou pro krok 7.

- Proč je výsledek kroku 7 právě řád bodu P? Ať máme dvě kolize $-jP = Q + imP$ a $-j'P = Q + i'mP$ zvolené v bodu 7. Označme $n = b + im + j$ a $n' = b + i'm + j'$. Pak platí $nP = \mathcal{O}$ a $n'P = \mathcal{O}$, proto jsou n i n' násobky řádu bodu P. Vzhledem k tomu, že dvojice (i, j) a (i', j') jsme volili jako sousední v uspořádaném seznamu z kroku 6, neexistuje žádné n'', pro které platí $n < n'' < n'$ a zároveň $n''P = \mathcal{O}$. Proto se čísla n a n' liší právě o řád bodu P, tedy řád bodu P je $n' - n = b + i'm + j' - b - im - j = i'm + j' - im - j$.

Ukázali jsme tedy, že tento algoritmus funguje. Ještě se podívejme na jeho složitost. Nejnáročnějšími operacemi jsou výpočty seznamů bodů. Ve výpočtu je potřeba $2m$ sečtení bodů a jedno násobení bodu číslem. Hledání kolizí lze udělat efektivně za použití binárního vyhledávacího stromu následovně: Nejprve zvolíme nějaké uspořádání bodů křivky. Pro křivku nad tělesem $\mathbb{F}_p$ to může být například uspořádání podle velikosti první a následně druhé souřadnice pokud budeme na prvky $\mathbb{F}_p$ v souřadnicích hledět jako na celá čísla. Při výpočtu prvního seznamu bodů je neukládáme do pole vedle sebe, ale přímo je zatřiďujeme do binárního stromu tak, že první bod dáme do kořenu, a že každý uzel má v levém podstromu pouze menší body(ve zvoleném uspořádání) a v pravém podstromu pouze body větší. Když potom počítáme body druhého seznamu, hned testujeme, zda spočtený bod není ve stromě vytvořeném z bodů prvního seznamu. Vyhledávání v takto uspořádaném stromě pak trvá pouze $\mathcal{O}(\log(m))$ kroků. Ostatní kroky algoritmu jsou již výpočetně nenáročné.

5.2 Hasse-Weilův odhad

Ve výše popsaném algoritmu jsme předpokládali, že známe nějaký odhad na velikost grupy bodů eliptické křivky. Potřebný odhad nám dává následující věta.

Věta 5.2.1 (Hasse-Weilova)**.** *Ať E je eliptická křivka nad tělesem $\mathbb{F}_q$, pak pro počet jejích bodů platí*

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

Důkaz. L-polynom eliptické křivky je polynom stupně 2, můžeme ho tedy napsat jako $L(T) = (1 - \alpha_1 T)(1 - \alpha_2 T)$. Rovnost 4.4 pro $k = 1$ říká

$$|E(\mathbb{F}_q)| = q + 1 - (\alpha_1 + \alpha_2).$$

Zároveň podle Weilovy hypotézy 4.2.2 je $|\alpha_1| = |\alpha_2| = \sqrt{q}$. S využitím trojúhelníkové nerovnosti tedy dostáváme

$$||E(\mathbb{F}_q)| - (q+1)| = |-\alpha_1 - \alpha_2| \leq |\alpha_1| + |\alpha_2| = 2\sqrt{q},$$

tedy právě požadované tvrzení. □

Pro obecnou eliptickou křivku je tento odhad nejlepší možný. Minimálně v případech kdy $q = p$ nebo $q = p^m$ pro prvočíslo p a sudé přirozené číslo m totiž podle [2](Tvrzení 13.30) platí, že nad $\mathbb{F}_q$ existuje křivka, která má právě $q + 1 - 2\lfloor\sqrt{q}\rfloor$ $\mathbb{F}_q$-racionálních bodů. A stejně tak existuje křivka, jejíž počet bodů nabývá horní meze, tj. počet jejích bodů je $q + 1 + 2\lfloor\sqrt{q}\rfloor$.

Nyní můžeme spojit Hasse-Weilův odhad a algoritmus zmíněný v minulé části. Při zachování značení z popisu algoritmu máme

$$\begin{aligned} b &= q + 1 - 2\sqrt{q} \\ c &= q + 1 + 2\sqrt{q} \\ m &= \lceil\sqrt{c-b}\rceil + 1 = \lceil\sqrt{4\sqrt{q}}\rceil + 1 = \lceil 2\sqrt[4]{q}\rceil + 1 \end{aligned}$$

Tedy algoritmus potřebuje přibližně $4\sqrt[4]{q}$ sčítání bodů a jedno násobení bodu číslem $q+1-2\sqrt{q}$. Násobení bodu číslem $q+1-2\sqrt{q}$ lze provést za použití $\mathcal{O}(\log(q))$ sčítání. Celkem je tedy potřeba $\mathcal{O}(4\sqrt[4]{q} + \log(q))$ sčítání. Sčítání bodů má podle části 2.2 složitost $\mathcal{O}\left(\log(q)^2\right)$, celková složitost algoritmu Baby Steps-Giant Steps při použití Hasse-Weilova odhadu je tedy $\mathcal{O}\left(\log(q)^2(4\sqrt[4]{q} + \log(q))\right) = \mathcal{O}\left(\log(q)^2\sqrt[4]{q}\right)$. Pro libovolné $\epsilon > 0$ a dostatečně velké q platí

$$\log(q)^2\sqrt[4]{q} = 2^{\log(\log(q)^2)+\frac{1}{4}\log(q)} \leq 2^{(\frac{1}{4}+\epsilon)\log(q)} = q^{\frac{1}{4}+\epsilon}.$$

Složitost algoritmu Baby Steps-Giant Steps lze tedy psát jako $\mathcal{O}\left(q^{1/4+\epsilon}\right)$ pro libovolné $\epsilon > 0$.

5.3 Algoritmus

Jak jsme již v úvodu kapitoly nastínily, algoritmus Baby Steps-Giant Steps je možné pro určování počtu bodů křivky používat následovně:

1. Položíme $n = 1$
2. Náhodně zvolíme bod $P \in E(\mathbb{F}_q)$.
3. Provedeme algoritmus Baby Steps-Giant Steps s bodem P a s volbou $m = \lceil 2\sqrt[4]{q}\rceil + 1$.
4. Pokud nám algoritmus vrátil velikost grupy, jsme hotovi a končíme.
5. Pokud nám algoritmus vrátil pouze řád prvku P, spočteme nejmenší společný násobek n a ord (P) a tímto násobkem nahradíme n, tj. $n \leftarrow \text{lcm}\,(n, \text{ord}\,(P))$. Tedy n vždy dělí velikost $E(\mathbb{F}_q)$.

6. Pokud je $n > 4\sqrt{q}$, pak existuje právě jeden násobek čísla n v intervalu $[q+1-2\sqrt{q}, q+1+2\sqrt{q}]$ a tento násobek je hledaným počtem bodů křivky, tedy algoritmus končí.

7. Pokud je $n \leq 4\sqrt{q}$, pokračujeme bodem 2.

Je zřejmé, že pokud algoritmus skončí, tak nám dá počet bodů křivky. Ovšem není, zcela zřejmé, jestli algoritmus opravdu skončí. Podívejme se na následující příklad.

Příklad 5.3.1. *Mějme křivku E definovanou nad tělesem $\mathbb{F}_{19}$, která je dána rovnicí*

$$y^2 = x^3 + 3x + 15.$$

Hasse-Weilův odhad říká, že počet bodů této křivky máme hledat v uzavřeném intervalu $[12, 28]$. Křivka $E(\mathbb{F}_{19})$ má však pouze body řádů 2,4 a 8 a je izomorfní grupě $\mathbb{Z}_2 \times \mathbb{Z}_8$. Neexistuje tedy žádný bod jehož násobek je v Hasse-Weilově intervalu právě jednou, tedy v bodě 4 náš algoritmus neskončí. Navíc z řádů prvků plyne, že průběžná hodnota n v našem algoritmu se může dostat nejvýše na hodnotu 8 a to je menší než $4\sqrt{19}$, tedy v tomto bodě algoritmus také neskončí.

Je tedy vidět, že tento algoritmus nebude fungovat pro všechny eliptické křivky. V následující části však ukážeme, že se pomocí něj dá určit počet $\mathbb{F}_q$-racionálních bodů všech křivek definovaných nad tělesem $\mathbb{F}_q$, pro $q = p$, kde p je dostatečně velké prvočíslo.

5.4 Kvadratický twist

V této části definujeme kvadratický twist eliptické křivky a ukážeme, jak lze jeho vlastnosti využít ve výše uvedeném algoritmu. V celé části budeme pracovat pouze v tělesech $\mathbb{F}_p$, kde p je liché prvočíslo.

Definice 5.4.1. *Mějme eliptickou křivku E definovanou nad tělesem $\mathbb{F}_p$, která je dána krátkou Weierstrassovou rovnicí*

$$E : y^2 = x^3 + Ax + B.$$

Ať $0 \neq d \in \mathbb{F}_p$ je nečtverec v tělese $\mathbb{F}_p$, tj. $\left(\frac{d}{\mathbb{F}_p}\right) = -1$. Kvadratickým twistem *eliptické křivky E nazýváme eliptickou křivku $\tilde{E}$ definovanou rovnicí*

$$\tilde{E} : y^2 = x^3 + d^2Ax + d^3B.$$

Nyní ukážeme jaký je vztah počtu bodů eliptické křivky a počtu bodů jejího kvadratického twistu.

Lemma 5.4.2. *Nechť E je eliptická křivka nad tělesem $\mathbb{F}_p$ a $\tilde{E}$ nechť je její kvadratický twist. Pak platí*

$$|E(\mathbb{F}_p)| + |\tilde{E}(\mathbb{F}_p)| = 2p + 2.$$

Důkaz. Ať křivka E má krátkou Weierstrassovu rovnici

$$y^2 = x^3 + Ax + B$$

a její kvadratický twist $\tilde{E}$ ať je křivka s rovnicí

$$y^2 = x^3 + d^2Ax + d^3B$$

pro nějaký nečtverec $d \in \mathbb{F}_p$. Označme $f(x) = x^3 + Ax + B$. Změnou souřadnic $x = dx'$ a $y = d^2y'$ dostaneme z křivky $\tilde{E}$ izomorfní křivku s rovnicí

$$dy'^2 = x'^3 + Ax' + B.$$

Její počet bodů je tedy stejný jako u křivky $\tilde{E}$. Rovnici nové křivky můžeme přepsat jako

$$y'^2 = \frac{f(x')}{d}.$$

Počet jejích bodů spočteme pomocí tvrzení 3.1.2 následovně

$$|\tilde{E}(\mathbb{F}_p)| = p + 1 + \sum_{x' \in \mathbb{F}_p} \left(\frac{f(x')/d}{\mathbb{F}_p} \right).$$

Lze snadno ukázat, že pro každé $a, b \in \mathbb{F}_q$ platí $\left(\frac{ab}{\mathbb{F}_q}\right) = \left(\frac{a}{\mathbb{F}_q}\right)\left(\frac{b}{\mathbb{F}_q}\right)$. Dále pokud je d nečtverec, je také $1/d$ nečtverec. Dostáváme tedy

$$\begin{aligned} |\tilde{E}(\mathbb{F}_p)| &= p + 1 + \sum_{x' \in \mathbb{F}_p} \left(\frac{f(x')/d}{\mathbb{F}_p} \right) = p + 1 + \sum_{x' \in \mathbb{F}_p} \left(\frac{\frac{1}{d}}{\mathbb{F}_p} \right)\left(\frac{f(x')}{\mathbb{F}_p} \right) \\ &= p + 1 + \sum_{x' \in \mathbb{F}_p} (-1) \left(\frac{f(x')}{\mathbb{F}_p} \right) = p + 1 - \sum_{x' \in \mathbb{F}_p} \left(\frac{f(x')}{\mathbb{F}_p} \right). \end{aligned}$$

Počet bodů původní křivky E je dle explicitního vzorce 3.1.2

$$|E(\mathbb{F}_p)| = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{f(x)}{\mathbb{F}_p} \right).$$

Sečtením s předchozí rovností nyní dostaneme právě požadované tvrzení. □

Následující tvrzení nám poskytne návod, jak používat algoritmus uvedený v části 5.3, abychom se dočkali výsledku i u křivek podobných té, která je uvedená v příkladu 5.3.1. Důkaz tvrzení lze najít například v [7](Tvrzení 3.1).

Tvrzení 5.4.3. *Mějme eliptickou křivku E definovanou nad tělesem $\mathbb{F}_p$, kde p je prvočíslo takové, že $p > 457$. Ať $\tilde{E}$ je kvadratický twist křivky E, pak aspoň jedna z křivek E a $\tilde{E}$ obsahuje $\mathbb{F}_p$-racionální bod řádu aspoň $4\sqrt{p}$.*

Znamená to tedy že buď u eliptické křivky, nebo u jejího kvadratického twistu existuje $\mathbb{F}_p$-racionální bod takový, že násobek jeho řádu se vyskytuje ve Weierstrassově intervalu právě jednou. Pokud tedy budeme provádět algoritmus 5.3 zároveň pro křivku E i pro její kvadratický twist, po nějaké době musíme na jedné

z těchto křivek narazit na výše zmíněný bod velkého řádu a algoritmus 5.3 skončí v bodě 4. Pokud se tak stane u křivky E, máme počet jejích $\mathbb{F}_p$-racionálních bodů. Pokud se tak naopak stane u křivky $\tilde{E}$, známe velikost $\tilde{E}(\mathbb{F}_p)$ a počet $\mathbb{F}_p$-racionálních bodů křivky E spočteme podle lemmatu 5.4.2 jako $|E(\mathbb{F}_p)| = 2p + 2 - |\tilde{E}(\mathbb{F}_p)|$.

Tím jsme tedy kompletně popsali algoritmus, který počítá velikost $E(\mathbb{F}_p)$ pro dostatečně velké prvočíslo p. Zbývá se ještě podívat na jeho celkovou složitost.

5.5 Složitost

V části 5.2 jsme již uvedli, že na jedno provedení algoritmu Baby Steps-Giant Steps je potřeba přibližně $4\sqrt[4]{p}$ sčítání v grupě eliptické křivky. Pokud budeme provádět algoritmus zároveň pro křivku i její kvadratický twist, je potřeba dvakrát tolik operací. Zbývá ještě objasnit, kolikrát se vlastně algoritmus Baby Steps-Giant Steps bude opakovat než dostaneme výsledek. K tomu nám pomůže následující lemma.

Lemma 5.5.1. *Ať G je grupa. Pokud $g \in G$ je prvek řádu n, pak v grupě G existuje aspoň $n/(2\log n)$ prvků řádu n.*

Důkaz. Prvek g generuje v grupě G cyklickou podgrupu H velikosti n. Každý jiný generátor této grupy má také řád n. Proto budeme odhadovat počet generátorů grupy H. Počet generátorů cyklické grupy udává Eulerova funkce φ. Pokud $n = \prod_{i=1}^{m} {p_i}^{k_i}$ pak počet generátorů cyklické grupy řádu n je

$$\varphi(n) = \prod_{i=1}^{m} (p_i - 1) p_i^{k_i - 1}$$

Neboť $2 \leq p_i$ pro každé i, je $2^m \leq n = 2^{\log(n)}$, tedy $m \leq \log(n)$. Dále pokud prvočísla p_i jsou seřazena tak, že rostou s rostoucím indexem, pak $p_i \geq i + 1$. Tyto dvě nerovnosti využijeme v následujícím odhadu. Odhadujme $\varphi(n)$ zdola

$$\begin{aligned}
\varphi(n) = \prod_{i=1}^{m} (p_i - 1) p_i^{k_i - 1} &= \frac{n \prod_{i=1}^{m} (p_i - 1) p_i^{k_i - 1}}{\prod_{i=1}^{m} {p_i}^{k_i}} = \frac{n \prod_{i=1}^{m} (p_i - 1)}{\prod_{i=1}^{m} p_i} \\
&= n \prod_{i=1}^{m} \frac{(p_i - 1)}{p_i} = n \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right) \geq n \prod_{i=1}^{m} \left(1 - \frac{1}{i+1}\right) \\
&= \frac{n}{m+1} \geq \frac{n}{2m} \geq \frac{n}{2\log(n)}.
\end{aligned}$$

Tedy jsme dostali spodní odhad na počet generátorů grupy H, tedy odhad na počet prvků řádu n. Lemma je tím dokázáno. □

Nyní toto lemma aplikujeme na náš algoritmus. Víme, že eliptická křivka, nebo její kvadratický twist obsahuje bod řádu aspoň $4\sqrt{p}$. Předchozí lemma nám říká, že v takovém případě obsahuje příslušná křivka aspoň

$$\frac{4\sqrt{p}}{2\log(4\sqrt{p})} = \frac{4\sqrt{p}}{2(\log(4) + \frac{1}{2}\log(p))} = \frac{4\sqrt{p}}{4 + \log(p)}$$

bodů tohoto řádu. Zajímá nás kolik pokusů průměrně potřebujeme, abychom při náhodné volbě bodu vybrali právě jeden z těchto bodů. Pravděpodobnost výběru jednoho z těchto bodů je podíl jejich počtu a velikosti grupy. Průměrný počet pokusů než natrefíme na ten správný bod je pak převrácená hodnota této pravděpodobnosti. Potřebujeme tedy aspoň

$$\frac{\max\{|E(\mathbb{F}_p)|, |\tilde{E}(\mathbb{F}_p)|\}}{\frac{4\sqrt{p}}{4+\log(p)}}$$

pokusů. Pokud provedeme pokusů více, pravděpodobnost úspěch jen zvyšujeme, budeme tedy dělat horní odhad tohoto výrazu

$$\begin{aligned}\frac{\max\{|E(\mathbb{F}_p)|, |\tilde{E}(\mathbb{F}_p)|\}}{\frac{4\sqrt{p}}{4+\log(p)}} &\leq \frac{p+1+2\sqrt{p}}{\frac{4\sqrt{p}}{4+\log(p)}} \leq \frac{p+1+2\sqrt{p}}{\frac{4\sqrt{p}}{2\log(p)}} \leq \frac{2p}{\frac{4\sqrt{p}}{2\log(p)}} \\ &= \frac{4p\log(p)}{4\sqrt{p}} = \log(p)\sqrt{p}\end{aligned}$$

Průměrný počet pokusů, tj. náhodného výběru bodu a počítání algoritmu Baby Steps-Giant Steps, tedy nebude větší než $2\log(p)\sqrt{p}$. Provádíme tedy $2\log(p)\sqrt{p}$ opakování algoritmu, který má dle části 5.2 složitost $\mathcal{O}\left(\log(p)^2\sqrt[4]{p}\right)$. Celková složitost tedy vychází

$$\mathcal{O}\left(2\log(p)\sqrt{p}\log(p)^2\sqrt[4]{p}\right) = \mathcal{O}\left(\log(p)^3 p^{\frac{3}{4}}\right).$$

Pro libovolné $\epsilon > 0$ a dostatečně velké p platí

$$\log(p)^3 p^{\frac{3}{4}} = 2^{\log(\log(p)^3)+\frac{3}{4}\log(p)} \leq 2^{(\frac{3}{4}+\epsilon)\log(p)} = q^{\frac{3}{4}+\epsilon}.$$

Tedy celková složitost je $\mathcal{O}(p^{\frac{3}{4}+\epsilon})$ bitových operací pro libovolné $\epsilon > 0$.

Kapitola 6

Schoofův algoritmus

V této kapitole představíme algoritmus, který publikoval René Schoof [6] v roce 1985 jako první polynomiální algoritmus pro počítání bodů eliptické křivky nad tělesem $\mathbb{F}_{p^m}$, kde p je prvočíslo větší než 3. Nejprve si řekneme něco o dělících polynomech, pak popíšeme samotný algoritmus a na závěr se budeme zabývat jeho složitostí.

6.1 Dělící polynomy

Definice 6.1.1. *Mějme eliptickou křivku E definovanou nad tělesem $\mathbb{F}_q$. Pro $n \in \mathbb{N}$ definujme*

$$E[n] = \{P \in E(\overline{\mathbb{F}}_q) | nP = \mathcal{O}\}.$$

Tuto množinu nazýváme množinou n-torzních bodů *křivky E.*

Je zřejmé, že množina $E[n]$ je uzavřená na operaci sčítání bodů a že $\mathcal{O} \in E[n]$. Pro každé n je tedy $E[n]$ podgrupou grupy $E(\overline{\mathbb{F}}_q)$.

Nyní se podíváme jak vypadá grupa $E[n]$ pro $n = 2, 3$. Jak bylo uvedeno v úvodu kapitoly, zabýváme se pouze křivkami v charakteristice větší než 3, tedy křivkami s krátkou Weierstrassovou rovnicí

$$E : y^2 = x^3 + Ax + B. \tag{6.1}$$

2-torzní grupa této křivky je $E[2] = \{P \in E(\overline{\mathbb{F}}_q) | 2P = \mathcal{O}\}$, tedy je tvořena body $P \in E(\overline{\mathbb{F}}_q)$, pro které platí $P = -P$. Pokud $P \neq \mathcal{O}$ a pokud označíme $P = (\alpha, \beta)$, pak podle vzorců odvozených v první kapitole máme $-P = (\alpha, -\beta)$. Bod $(\alpha, \beta) \in E(\overline{\mathbb{F}}_q)$ je tedy v $E[2]$, právě když $(\alpha, \beta) = (\alpha, -\beta)$, tedy právě když $\beta = 0$. Dosazením do rovnice křivky dostaneme, že $0 = \alpha^3 + A\alpha + B$. Tato rovnice má v algebraickém uzávěru právě tři různá řešení(různá proto, že uvažujeme pouze nesingulární křivky, tedy polynom na pravé straně nemá násobné kořeny), proto $E[2]$ obsahuje právě 3 nenulové body. A protože všechny tyto body jsou řádu 2, musí platit, že $E[2] \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

Pro $n = 3$ máme $E[3] = \{P \in E(\overline{\mathbb{F}}_q) | 3P = \mathcal{O}\}$. $E[3]$ tedy obsahuje body, pro které platí $-P = 2P$. Pokud nenulový bod $P \in E[3]$ zapíšeme jako $P = (\alpha, \beta)$, pak podmínku $-P = 2P$ můžeme pomocí vzorců z první kapitoly zapsat následovně:

$$(\alpha, -\beta) = (\lambda^2 - 2\alpha, -\lambda((\lambda^2 - 2\alpha) - \alpha) - \beta), \tag{6.2}$$

kde $\lambda = \frac{3\alpha^2+A}{2\beta}$. Porovnáním prvních souřadnic dostáváme podmínku

$$\lambda^2 = 3\alpha$$
$$\frac{(3\alpha + A)^2}{4\beta^2} = 3\alpha.$$

β^2 můžeme za použití rovnice křivky nahradit výrazem $\alpha^3 + A\alpha + B$ a dostaneme

$$\frac{(3\alpha^2 + A)^2}{4\alpha^3 + 4A\alpha + 4B} = 3\alpha$$
$$9\alpha^4 + 6A\alpha^2 + A^2 = 12\alpha^4 + 12A\alpha^2 + 12B\alpha$$
$$3\alpha^4 + 6A\alpha^2 + 12B\alpha - A^2 = 0.$$

Porovnáním druhých souřadnic v rovnosti 6.2 dostaneme totožnou rovnost, platí tedy, že bod $(\alpha, \beta) \in E(\overline{\mathbb{F}}_q)$ leží v $E[3]$ právě když platí $3\alpha^4+6A\alpha^2+12B\alpha-A^2 = 0$. Ukáže se, že obdobnou rovnici můžeme sestavit pro libovolné n a vždy to bude polynomiální rovnice v proměnných α a β. Platí pak tedy, že pro každé $n \in \mathbb{N}$ existuje polynom $\psi_n \in \mathbb{F}_q[x, y]$ takový, že pro každý bod $(\alpha, \beta) \in E(\overline{\mathbb{F}}_q)$ platí: $(\alpha, \beta) \in E[n]$ právě když $\psi_n(\alpha, \beta) = 0$.

Definice 6.1.2. *Polynomy ψ_n zmíněné výše nazýváme* dělícími polynomy *křivky E.*

Existenci dělících polynomů jsme zatím ukázali jen pro $n = 2, 3$. Pro $n = 2$ nám vyšel polynom y a pro $n = 3$ jsme odvodili polynom $3x^4+6Ax^2+12Bx-A^2$. Nyní naznačíme, proč by dělící polynomy měly existovat pro libovolné přirozené číslo n. Mějme tedy $n \in \mathbb{N}$. Grupa $E[n]$ obsahuje všechny body řádu, který dělí n. Nejprve se podíváme na body řádu právě n. Takové body splňují rovnici

$$(n-1)P = -P. \tag{6.3}$$

Protože bod P je řádu n, platí $kP \neq \pm P$ pro každé k takové, že $1 < k < n-1$. Proto se výpočet bodu na levé straně rovnice 6.3 dá realizovat jako opakované použití vzorce pro sčítaní bodů, kde sčítané body jsou různé. Důležité je, že pro každý bod $P = (\alpha, \beta)$ řádu n se použije stejný vzorec. Souřadnice levé strany rovnice se tedy dají vyjádřit jako racionální funkce v proměnných α a β, tj. existují racionální funkce ρ_{n-1} a σ_{n-1} takové, že pro každý bod $P = (\alpha, \beta)$ řádu n platí

$$(n-1)P = (\rho_{n-1}(\alpha, \beta), \sigma_{n-1}(\alpha, \beta)).$$

Obdobné funkce existují i pro každé $k < n-1$. Označme tedy ρ_k a σ_k funkce takové, že

$$kP = (\rho_k(\alpha, \beta), \sigma_k(\alpha, \beta)) \tag{6.4}$$

pro každý bod P řádu n. Rovnici 6.3 tedy můžeme přepsat do souřadnic následovně:

$$(\rho_{n-1}(\alpha, \beta), \sigma_{n-1}(\alpha, \beta)) = (\alpha, -\beta).$$

Porovnáním jednotlivých souřadnic v této rovnici nyní dostaneme rovnosti

$$\rho_{n-1}(\alpha,\beta) = \alpha$$
$$\sigma_{n-1}(\alpha,\beta) = -\beta.$$

Pokud první rovnost vynásobíme jmenovatelem $\rho_{n-1}(\alpha,\beta)$, dostaneme rovnost tvaru $g_n(\alpha,\beta) = 0$ pro vhodný polynom $g_n \in \mathbb{F}_q[x,y]$. Snadným výpočtem lze ověřit, že porovnáním druhých souřadnic dostaneme totožnou rovnost. Pokud totiž rovnici 6.3 rozepíšeme jako

$$(n-2)P + P = -P,$$

dostaneme za použití značení 6.4 rovnost

$$(\rho_{n-2}(\alpha,\beta), \sigma_{n-2}(\alpha,\beta)) + (\alpha,\beta) = (\alpha,-\beta).$$

Použitím vzorce pro sčítaní bodů dostáváme

$$(\lambda^2 - \rho_{n-2}(\alpha,\beta) - \alpha, -\lambda(\lambda^2 - \rho_{n-2}(\alpha,\beta) - 2\alpha) - \beta) = (\alpha,-\beta),$$

kde λ je směrnice příslušné sečny. Z této rovnosti je již vidět, že porovnáním prvních i druhých souřadnic dostaneme stejnou rovnost. Odvodili jsme tedy následující: Bod $P = (\alpha,\beta)$ je řádu n, pak platí $g_n(\alpha,\beta) = 0$. Dále bychom totéž potřebovali pro body řádu dělícího n a také bychom potřebovali i opačnou implikaci, tedy že polynom g_n je nenulový ve všech ostatních bodech. To už ale není tak jednoduché ověřit. Pro přesné odvození dělících polynomů lze nahlédnout do [3]. Lze tedy uvěřit, že nějaká posloupnost dělících polynomů existuje(postupnou aplikací vzorce pro sčítání bodů, bychom ji dokázali sestrojit). My však dále budeme používat posloupnost dělících polynomů zavedenou v [11](Část 3.2) popřípadě [3], o které hovoří následující lemma, jehož důkaz lze najít v uvedených zdrojích.

Lemma 6.1.3. *Mějme křivku E danou Weierstrassovou rovnicí $y^2 = x^3+Ax+B$ definovanou nad tělesem $\mathbb{F}_q$. Definujme polynomy*

$$\begin{aligned}
\psi_1 &= 1\\
\psi_2 &= 2y\\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2\\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 4A^2x^2 - 4ABx - A^3 - 8B^2)\\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \text{ pro } m \geq 2\\
\psi_{2m} &= (\psi_m)(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)/2y \text{ pro } m \geq 3.
\end{aligned}$$

Tyto polynomy jsou dělícími polynomy křivky E.

Dle [11](Tvrzení 3.6) platí pro polynomy definované v předchozím lemmatu následující:

Lemma 6.1.4. *Ať $P = (x,y)$ je bod eliptické křivky E definované rovnicí 6.1 a ať $n \in \mathbb{N}$. Pokud $P \notin E[n]$, pak*

$$nP = \left(x - \frac{\psi_{n+1}\psi_{n-1}}{\psi_n^2}, \frac{\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2}{4y\psi_n^3}\right), \tag{6.5}$$

kde pro přehlednost namísto $\psi_k(x,y)$ píšeme pouze ψ_k.

Lemma 6.1.5. *Pro polynomy definované v lemmatu 6.1.3 platí:* $\psi_n \in \mathbb{F}_q[x, y^2]$ *pro* n *liché a* $\psi_n \in 2y\mathbb{F}_q[x, y^2]$ *pro* n *sudé.*

Důkaz. Důkaz je snadný pomocí indukce. Pro $n \leq 4$ lemma zřejmě platí. Ať $n = 2m + 1$ a $n > 4$. Dle indukčního předpokladu lemma platí pro všechny polynomy použité v definici ψ_{2m+1}. Pokud je m sudé, pak dle indukčního předpokladu $\psi_{m+2}, \psi_m \in 2y\mathbb{F}_q[x, y^2]$ a $\psi_{m-1}, \psi_{m+1} \in \mathbb{F}_q[x, y^2]$. Součin dvou prvků z $2y\mathbb{F}_q[x, y^2]$ vždy leží v $\mathbb{F}_q[x, y^2]$ a $\mathbb{F}_q[x, y^2]$ je uzavřené na sčítání i násobení, proto i $\psi_n \in \mathbb{F}_q[x, y^2]$. Pokud je naopak m liché, pak dle indukčního předpokladu $\psi_{m-1}, \psi_{m+1} \in 2y\mathbb{F}_q[x, y^2]$ a $\psi_{m+2}, \psi_m \in \mathbb{F}_q[x, y^2]$, totožný argument jako v předchozím případě nám opět říká, že $\psi_n \in \mathbb{F}_q[x, y^2]$.

Zbývá vyřešit případ, kdy $4 < n = 2m$. Pokud je m sudé, je $\psi_m, \psi_{m-2}, \psi_{m+2} \in 2y\mathbb{F}_q[x, y^2]$. Součin $(\psi_m)(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)$ tedy leží v $4y^2\mathbb{F}_q[x, y^2]$, proto $\psi_n \in 2y\mathbb{F}_q[x, y^2]$. Pokud je naopak m liché, platí $\psi_m \in \mathbb{F}_q[x, y^2]$ a $\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2 \in 4y^2\mathbb{F}_q[x, y^2]$, proto $\psi_n \in 2y\mathbb{F}_q[x, y^2]$. Tím je lemma dokázáno. □

Polynom ψ_n tedy vždy leží buď v $\mathbb{F}_q[x, y^2]$, nebo v $2y\mathbb{F}_q[x, y^2]$. Protože se nacházíme na křivce s rovnicí $y^2 = x^3 + Ax + B$, můžeme všechny výskyty y^2 nahradit polynomem x^3+Ax+B. Dostaneme tím posloupnost polynomů ψ'_n které leží buď v $\mathbb{F}_q[x]$, nebo v $2y\mathbb{F}_q[x]$, a které jsou taktéž dělícími polynomy křivky E. Pomocí polynomů ψ'_n nyní definujeme poslední posloupnost polynomů, kterou budeme využívat ve Schoofově algoritmu.

Definice 6.1.6. *Pro* $n \in \mathbb{N}$ *definujeme:*

$$f_n = \frac{\psi'_n}{y} \text{ pro } n \text{ sudé,}$$
$$f_n = \psi'_n \text{ pro } n \text{ liché.}$$

Tyto polynomy nazýváme redukované dělící polynomy *křivky* E.

Poznámka 6.1.7. *Protože polynomy* ψ'_n *leží vždy buď v* $\mathbb{F}_q[x]$, *nebo v* $2y\mathbb{F}_q[x]$ *v závislosti na sudosti* n, *jsou polynomy* f_n *pouze v proměnné* x, *tj.* $f_n \in \mathbb{F}_q[x]$ *pro každé* n.

Lemma 6.1.8. *Ať* $P \in E(\overline{\mathbb{F}}_q)$ *je nenulový bod řádu různého od dvou a ať* $n \in \mathbb{N}$. *Označíme-li* $P = (\alpha, \beta)$, *pak platí:* $P \in E[n]$, *právě když* $f_n(\alpha) = 0$.

Důkaz. Předpokládejme, nejprve, že n je liché. Pak je podle definice $f_n(x) = \psi'_n(x, y)$. Protože ψ'_n je dělící polynom křivky E, je $(\alpha, \beta) \in E[n]$, právě když $f_n(\alpha) = \psi'_n(\alpha, \beta) = 0$, tedy lemma platí.

Pokud je naopak n sudé, je $yf_n(x) = \psi'_n(x, y)$. Pokud je $P \in E[n]$, musí být $\psi'_n(\alpha, \beta) = 0$, neboť ψ'_n je dělící polynom. Platí tedy $0 = \psi'_n(\alpha, \beta) = \beta f_n(\alpha)$. Pokud by bylo $\beta = 0$, byl by bod P řádu 2, to ale dle předpokladu není, proto je nulový druhý činitel, tedy $f_n(\alpha) = 0$.

Chybí tedy už jen opačná implikace. Ať je tedy $f_n(\alpha) = 0$, pak $\psi'_n(\alpha, \beta) = \beta f_n(\alpha) = 0$. A neboť ψ'_n je dělící polynom, je $P \in E[n]$. □

Nyní pro polynomy f_n odvodíme rekurentní vztahy podobné těm, kterými jsme v lemmatu 6.1.3 definovali posloupnost $\{\psi_n\}_{n\in\mathbb{N}}$.

Lemma 6.1.9. *Redukované dělící polynomy splňují následující rekurentní vztahy:*

$$\begin{aligned}
f_1 &= 1 \\
f_2 &= 2 \\
f_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2 \\
f_4 &= 4(x^6 + 5Ax^4 + 20Bx^3 - 4A^2x^2 - 4ABx - A^3 - 8B^2) \\
f_{2m+1} &= f_{m+2}f_m^3 - \tilde{f}^2 f_{m-1}f_{m+1}^3 \text{ pro liché } m \geq 2 \\
f_{2m+1} &= \tilde{f}^2 f_{m+2}f_m^3 - f_{m-1}f_{m+1}^3 \text{ pro sudé } m \geq 2 \\
f_{2m} &= (f_m)(f_{m+2}f_{m-1}^2 - f_{m-2}f_{m+1}^2)/2 \text{ pro } m \geq 3,
\end{aligned}$$

kde $\tilde{f} = x^3 + Ax + B$.

Důkaz. Pokud uvážíme polynomy ψ_n' jako polynomy v okruhu $\mathbb{F}_q[x,y]/(y^3 - x^3 + Ax + B)$, platí pro ně totožné rekurentní vztahy, jako pro polynomy ψ_n. Dosazením do těchto vztahů podle definice 6.1.6 a nahrazením všech výskytů y^2 polynomem $\tilde{f}$ dostaneme požadované vztahy pro polynomy f_n. □

Následující dvě lemmata ukazují způsob, kterým budeme v algoritmu využívat redukované dělící polynomy.

Lemma 6.1.10. *Mějme liché* $n \in \mathbb{N}$ *a polynom* $g \in \mathbb{F}_q[x]$. *Pak* $g \equiv 0 \pmod{f_n}$, *právě když pro každý nenulový bod* $(\alpha, \beta) \in E[n]$ *platí* $g(\alpha) = 0$.

Důkaz. Ať $g \equiv 0 \pmod{f_n}$, to znamená, že f_n dělí g, tedy existuje polynom h takový, že $g = hf_n$. Zvolme libovolný bod $(\alpha, \beta) \in E[n]$. Protože f_n je redukovaný dělící polynom a bod (α, β) není řádu dva, je $f_n(\alpha) = 0$. Tedy $g(\alpha) = h(\alpha)f_n(\alpha) = 0$ a první implikace je dokázána.

Ať naopak pro každý bod $(\alpha, \beta) \in E[n]$ platí $g(\alpha) = 0$. Protože polynom f_n má za kořeny právě všechna α taková, že $(\alpha, \beta) \in E[n]$, musí platit $f_n | g$, tedy $g \equiv 0 \pmod{f_n}$. □

Lemma 6.1.11. *Mějme liché* $n \in \mathbb{N}$ *a polynom* $g \in \mathbb{F}_q[x]$. *Pak* $\mathrm{GCD}\,(g, f_n) \neq 1$, *právě když existuje nenulový bod* $(\alpha, \beta) \in E[n]$ *takový, že* $g(\alpha) = 0$.

Důkaz. Ať $\mathrm{GCD}\,(g, f_n) = h \neq 1$, pak můžeme psát $f_n = hf_n'$ a $g = hg'$ pro vhodné polynomy g', f_n'. Protože kořeny polynomu f_n jsou právě všechny prvky α takové, že $(\alpha, \beta) \in E[n]$ pro nějaké β, musí existovat α takové, že $h(\alpha) = 0$. Pro takto zvolené α platí $g(\alpha) = h(\alpha)g'(\alpha) = 0$ a tím je dokázána první implikace.

Ať nyní existuje bod $(\alpha, \beta) \in E[n]$, pro který platí $g(\alpha) = 0$. Taktéž platí, že $f_n(\alpha) = 0$, proto jsou polynomy f_n a g oba dělitelné minimálním polynomem prvku α nad tělesem $\mathbb{F}_q$, a tedy $\mathrm{GCD}\,(g, f_n) \neq 1$. □

Pro odhad složitosti algoritmu budeme ještě potřebovat znát stupně redukovaných dělících polynomů.

Lemma 6.1.12. *Ať p je charakteristika tělesa $\mathbb{F}_q$, nad kterým je definována křivka E. Pokud p nedělí n, pak*

$$\deg(f_n) = \frac{n^2-1}{2} \text{ pokud je } n \text{ liché,}$$
$$\deg(f_n) = \frac{n^2-4}{2} \text{ pokud je } n \text{ sudé.}$$

Důkaz. Z rekurentních vztahů odvozených v lemmatu 6.1.9 vidíme, že polynomy f_n lze uvažovat jako polynomy okruhu $\mathbb{Z}[x, A, B]$. Nahlížejme na ně nyní tedy tímto způsobem. Indukcí dokážeme, že takto nahlížené polynomy f_n mají vedoucí koeficienty $\operatorname{lc}(f_n) = n$ a stupně jaké tvrdíme v lemmatu. Přičemž vedoucím koeficientem polynomu f_n rozumíme v tomto případě vedoucí koeficient tohoto polynomu uvažovaného jako polynom v proměnné x nad okruhem $\mathbb{Z}[A, B]$. Pro $n \leq 4$ lemma zřejmě platí. Ať je $n > 4$. Podívejme se na případ, kdy n je liché a $n = 2m + 1$ pro nějaké liché $m \geq 2$. Podle 6.1.9 je

$$f_{2m+1} = f_{m+2}f_m^3 - \tilde{f}^2 f_{m-1}f_{m+1}^3.$$

Podle indukčního předpokladu je

$$\deg(f_{m+2}f_m^3) = \frac{(m+2)^2-1}{2} + 3\frac{m^2-1}{2} = 2m^2 + 2m = \frac{n^2-1}{2}$$
$$\deg(\tilde{f}^2 f_{m-1}f_{m+1}^3) = 4 + \frac{(m-1)^2-4}{2} + 3\frac{(m+1)^2-4}{2} = 2m^2 + 2m = \frac{n^2-1}{2}.$$

Protože oba členy mají stejný stupeň, je $\operatorname{lc}(f_n) = \operatorname{lc}(f_{m+2}f_m^3) - \operatorname{lc}\left(\tilde{f}^2 f_{m-1}f_{m+1}^3\right)$. Podle indukčního předpokladu je ale

$$\operatorname{lc}\left(f_{m+2}f_m^3\right) = \operatorname{lc}(f_{m+2})\operatorname{lc}(f_m)^3 = (m+2)m^3 = m^4 + 2m^3$$
$$\operatorname{lc}\left(\tilde{f}^2 f_{m-1}f_{m+1}^3\right) = \operatorname{lc}\left(\tilde{f}\right)^2 \operatorname{lc}(f_{m-1})\operatorname{lc}(f_{m+1})^3 = (m-1)(m+1)^3$$
$$= m^4 + 2m^3 - 2m - 1,$$

tedy $\operatorname{lc}(f_n) = (m^4+2m^3)-(m^4+2m^3-2m-1) = 2m+1 = n$. Tedy dostáváme, že člen nejvyššího stupně v polynomu f_n uvažovaném v $\mathbb{Z}[x, A, B]$ má tvar $nx^{(n^2-1)/2}$, a právě to jsme chtěli dokázat. A protože p nedělí n, zůstává tento člen nenulový, i pokud uvažujeme polynom f_n jako polynom v $\mathbb{F}_q[x]$. Případ kdy $n = 2m + 1$ a m je sudé se vyřeší obdobně. Stejně tak případ, kdy $n = 2m$. □

Poslední věc týkající se dělících polynomů, kterou budeme potřebovat, je vyjádření souřadnic n-násobku bodu eliptické křivky jako racionálních funkcí v proměnné x respektive v proměnných x, y.

Lemma 6.1.13. *Pro každé $n \in \mathbb{N}$ existují polynomy $R_n, r_n, S_n, s_n \in \mathbb{F}_q[x]$ takové, že pro každý nenulový bod $P = (x, y) \in E(\overline{\mathbb{F}}_q) \setminus E[n]$ platí*

$$nP = \left(\frac{R_n(x)}{r_n(x)}, y\frac{S_n(x)}{s_n(x)}\right). \tag{6.6}$$

Důkaz. Vyjdeme z rovnice 6.5 a z faktu, že se pohybujeme na eliptické křivce, tedy že $y^2 = x^3+Ax+B$ pro každý bod (x, y) ležící na křivce. Označme $\tilde{f} = x^3+Ax+B$. Pokud je n liché, je

$$\begin{aligned} nP &= \left(x - \frac{\psi_{n+1}\psi_{n-1}}{\psi_n^2}, \frac{\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2}{4y\psi_n^3} \right) \\ &= \left(x - y^2\frac{f_{n+1}f_{n-1}}{f_n^2}, \frac{y^2 f_{n+2}f_{n-1}^2 - y^2 f_{n-2}f_{n+1}^2}{4yf_n^3} \right) \\ &= \left(x - \frac{\tilde{f}f_{n+1}f_{n-1}}{f_n^2}, y\frac{f_{n+2}f_{n-1}^2 - f_{n-2}f_{n+1}^2}{4f_n^3} \right), \end{aligned}$$

tedy stačí položit

$$\begin{aligned} R_n &= xf_n(x)^2 - \tilde{f}(x)f_{n+1}(x)f_{n-1}(x) \\ r_n &= f_n(x)^2 \\ S_n &= f_{n+2}(x)f_{n-1}(x)^2 - f_{n-2}(x)f_{n+1}(x)^2 \\ s_n &= 4f_n^3(x). \end{aligned}$$

Pokud je naopak n sudé, je

$$\begin{aligned} nP &= \left(x - \frac{\psi_{n+1}\psi_{n-1}}{\psi_n^2}, \frac{\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2}{4y\psi_n^3} \right) \\ &= \left(x - \frac{f_{n+1}f_{n-1}}{y^2 f_n^2}, \frac{yf_{n+2}f_{n-1}^2 - yf_{n-2}f_{n+1}^2}{4y^4 f_n^3} \right) \\ &= \left(x - \frac{f_{n+1}f_{n-1}}{\tilde{f}f_n^2}, y\frac{f_{n+2}f_{n-1}^2 - f_{n-2}f_{n+1}^2}{4\tilde{f}^2 f_n^3} \right), \end{aligned}$$

tedy položíme

$$\begin{aligned} R_n &= x\tilde{f}(x)f_n(x)^2 - f_{n+1}(x)f_{n-1}(x) \\ r_n &= \tilde{f}(x)f_n(x)^2 \\ S_n &= f_{n+2}(x)f_{n-1}(x)^2 - f_{n-2}(x)f_{n+1}(x)^2 \\ s_n &= 4\tilde{f}(x)^2 f_n^3(x). \end{aligned}$$

Přičemž pro přehlednost jsme opět psali pouze ψ_n, f_n a $\tilde{f}$ místo $\psi_n(x, y)$, $f_n(x)$ a $\tilde{f}(x)$. □

Značení z posledního lemmatu budeme používat i v následujících částech.

6.2 Charakteristická rovnice Frobeniova endomorfismu

Po dělících polynomech se podíváme na další důležité tvrzení, které je klíčové pro Schoofův algoritmus. Jedná se konkrétně o tvrzení 4.1.3 týkající se charakteristické rovnice Frobeniova endomorfismu, které jsme již zmínili a použili v části 4.1. V této části uvedeme části důkazu tohoto tvrzení pro křivku nad tělesem charakteristiky různé od 2 a 3.

Frobeniův endomorfismus křivky E jsme definovali následovně

$$\begin{aligned} \phi_q : E(\overline{\mathbb{F}}_q) &\longrightarrow E(\overline{\mathbb{F}}_q) \\ (x, y) &\longmapsto (x^q, y^q) \\ \mathcal{O} &\longmapsto \mathcal{O} \end{aligned}$$

a tvrzení, které se zde odvodíme říká, že pro každý bod $P \in E(\overline{\mathbb{F}}_q)$ platí rovnost

$$\phi_q^2(P) - t\phi_q(P) + qP = \mathcal{O}.$$

Právě tuto rovnost nazýváme charakteristickou rovnicí Frobeniova endomorfismu.

Pomocí Frobeniova endomorfismu lze identifikovat všechny F_q-racionální body křivky jako $E(\mathbb{F}_q) = \{P \in E | \phi_q(P) = P\}$. Je to proto, že prvky tělesa $\mathbb{F}_q$ se v algebraickém uzávěru $\overline{\mathbb{F}}_q$ poznají právě tak, že splňují $x^q = x$. Označíme-li identický endomorfismus křivky E jako Id, můžeme množinu $\mathbb{F}_q$-racionálních bodů zapsat jako $E(\mathbb{F}_q) = \mathrm{Ker}\,(\phi_q - \mathrm{Id})$. Toto vyjádření se nám bude hodit při odvozování charakteristické rovnice Frobeniova endomorfismu. Při odvozování budeme studovat restrikci Frobeniova endomorfismu na grupy $E[n]$, kde charakteristika $\mathbb{F}_q$ nedělí n.

Proto nyní ukážeme, jak ve skutečnosti vypadá grupa n-torzních bodů eliptické křivky pro n, které není dělitelné charakteristikou tělesa $\mathbb{F}_q$, nad kterým danou křivku uvažujeme.

Lemma 6.2.1. *Ať E je eliptická křivka definovaná nad tělesem $\mathbb{F}_q$ charakteristiky p. Dále mějme $n \in \mathbb{N}$, které není dělitelné číslem p. Pak platí $|E[n]| = n^2$*

Důkaz. V důkazu využijeme lemma 6.1.12 které říká, že stupně redukovaných dělících polynomů f_n jsou $(n^2-1)/2$ pro n liché a $(n^2-4)/2$ pro n sudé. Lze ukázat, že tyto polynomy nemají násobné kořeny [11](Část 4.5), proto mají právě $(n^2-1)/2$, respektive $(n^2-4)/2$ různých kořenů. Pro n liché existují pro každý z $(n^2-1)/2$ kořenů α právě dva prvky $\beta \in \mathbb{F}_q$ takové, že $(\alpha, \beta) \in E[n]$. To je celkem $n^2 - 1$ bodů. Započítáme-li ještě bod $\mathcal{O}$, dostáváme, že $|E[n]| = n^2$. Pro n sudé postupujeme obdobně: Z kořenů polynomu f_n dostaneme $n^2 - 4$ bodů ležících v $E[n]$. Protože je ale n sudé, musíme ještě započítat body řádu dva. V kapitole o dělících polynomech jsme odvodili, že takové body jsou právě tři. započítáme-li navíc bod v nekonečnu, dostáváme opět, že $|E[n]| = n^2$. Velikost $E[n]$ je tedy n^2 pro každé n nedělitelné charakteristikou p. □

Lemma 6.2.2. *Mějme eliptickou křivku E definovanou nad tělesem $\mathbb{F}_q$ charakteristiky p. Dále mějme $n \in \mathbb{N}$, které není dělitelné číslem p. Pak platí*

$$E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$$

Důkaz. Nejprve provedeme důkaz pro $n = l$, kde l je prvočíslo, pak indukcí pro $n = l^m$ a nakonec pro obecné složené číslo $n \in \mathbb{N}$. Ať je tedy $n = l$, kde l je prvočíslo. Pak všechny nenulové body $E[l]$ jsou řádu l a dle předchozího lemmatu je $|E[l]| = l^2$. Jediná(až na izomorfismus) komutativní grupa velikosti l^2, jejíž každý nenulový bod má řád l, je právě $\mathbb{Z}_l \oplus \mathbb{Z}_l$. Tedy máme lemma dokázáno pro prvočísla.

Každá konečná komutativní grupa, tedy i $E[n]$ je izomorfní grupě

$$\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$$

pro nějaká $k, n_1, n_2, \ldots, n_k$ taková, že $n_i | n_{i+1}$ pro každé $i = 1, 2, \ldots, k-1$. Pokud nějaké prvočíslo l dělí n_1, pak $l | n_i$ pro každé i a grupa tak obsahuje alespoň l^k prvků řádu l. Těch je však v $E[n]$ právě l^2, proto musí být $k = 2$. Máme tedy že $E[n] \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ pro nějaká n_1, n_2 taková, že $n_1 | n_2$. Nyní použijeme indukci k dokázání lemmatu pro $n = l^m$, kde l je prvočíslo. Předpokládejme, že pro l^{m-1} lemma platí. Protože $E[l^{m-1}] \leq E[l^m]$, je $\mathbb{Z}_{l^{m-1}} \oplus \mathbb{Z}_{l^{m-1}} \leq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$. Protože velikost $E[l^m]$ je dle předchozího lemmatu l^{2m}, jsou pouze dvě možnosti, jak může grupa $E[l^m]$, respektive $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ vypadat. Je to buď $\mathbb{Z}_{l^m} \oplus \mathbb{Z}_{l^m}$, nebo $\mathbb{Z}_{l^{m-1}} \oplus \mathbb{Z}_{l^{m+1}}$. Druhý případ však snadno vyloučíme. Druhá grupa totiž obsahuje prvek řádu l^{m+1}. Takový prvek ale v grupě $E[l^m]$ není, proto nemohou být tyto grupy izomorfní. Nastává tedy první případ, což je přesně znění lemmatu pro $n = l^m$.

Nyní provedeme důkaz pro libovolné složené n. Ať $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ je prvočíselný rozklad čísla n. Pro každé i je $E[p_i^{e_i}] \leq E[n]$, tedy $\mathbb{Z}_{p_i^{e_i}} \oplus \mathbb{Z}_{p_i^{e_i}} \leq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$, tedy $p_i^{e_i} | n_1$ a také $p_i^{e_i} | n_2$ pro každé i. Platí tedy $n | n_1$ a $n | n_2$, a protože $n^2 = n_1 n_2$, musí platit $n_1 = n_2 = n$ a lemma je tím dokázáno. □

Víme tedy už, jaká je struktura grupy n-torzních bodů pro n nedělitelné charakteristikou $\mathbb{F}_q$. Nyní se budeme zabývat restrikcí Frobeniova endomorfismu na tuto grupu. Tuto restrikci označíme $\phi_{q,n}$, tedy

$$\begin{aligned} \phi_{q,n} : E[n] &\longrightarrow E[n] \\ (x, y) &\longmapsto (x^q, y^q) \\ \mathcal{O} &\longmapsto \mathcal{O}. \end{aligned}$$

Protože ϕ_q je endomorfismus, řád bodu $\phi_q(P)$ vždy dělí řád bodu P, proto restrikce $\phi_{q,n}$ zobrazuje body $E[n]$ opět na body $E[n]$. Dle předchozího lemmatu víme, že $E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$, můžeme na ni tedy nahlížet jako na modul nad okruhem $\mathbb{Z}_n$ s dvouprvkovou bází. Každý endomorfismus $E[n]$ lze tedy ztotožnit s maticí typu 2×2 nad okruhem $\mathbb{Z}_n$. Matici odpovídající $\phi_{q,n}$ budeme opět značit $\phi_{q,n}$. Ať je

$$\phi_{q,n} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Matice odpovídající endomorfismu $\phi_{q,n} - \mathrm{Id}$ je tedy potom

$$\phi_{q,n} - E = \begin{pmatrix} a-1 & b \\ c & d-1 \end{pmatrix},$$

kde E značí jednotkovou matici. Z [11](Tvrzení 2.21 a 3.15) plyne, že platí následující dva vztahy:

$$|\mathrm{Ker}\,(\phi_q - Id)\,| \equiv \det(\phi_{q,n} - E) \pmod{n} \tag{6.7}$$

a také

$$ad - bc = \det(\phi_{q,n}) \equiv q \pmod{n}. \tag{6.8}$$

V tvrzení 4.1.3, jehož speciální případ se nyní snažíme odvodit, jsme definovali $t = q + 1 - |E(\mathbb{F}_q)|$, tj. $|E(\mathbb{F}_q)| = q + 1 - t$. Za využití uvedených vztahů nyní můžeme počítat:

$$\begin{aligned} q + 1 - t = |E(\mathbb{F}_q)| &= |\mathrm{Ker}\,(\phi_q - Id)\,| \overset{6.7}{\equiv} \det(\phi_{q,n} - E) \\ &= (a-1)(d-1) - bc = ad - bc - a - d + 1 \overset{6.8}{\equiv} q - (a+d) + 1 \pmod{n}. \end{aligned}$$

Tím jsme dostali vztah

$$t \equiv a + d \pmod{n}. \tag{6.9}$$

Pro endomorfismus $\phi_{a,n}$, respektive pro jeho matici $\phi_{a,n}$ nyní upravujme výraz $\phi_{q,n}^2 - t\phi_{q,n} + qE$:

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^2 - t\begin{pmatrix} a & b \\ c & d \end{pmatrix} + q\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} a^2 + bc & ab + bd \\ ac + cd & bc + d^2 \end{pmatrix} - \begin{pmatrix} ta - q & tb \\ tc & td - q \end{pmatrix} \\ &= \begin{pmatrix} a^2 + bc - ta + q & ab + bd - tb \\ ac + cd - tc & bc + d^2 - td + q \end{pmatrix} \end{aligned}$$

Protože koeficienty matic jsou z okruhu $\mathbb{Z}_n$, můžeme v nich nahrazovat prvky podle odvozeného vztahu 6.9 a podle vztahu 6.8. Pokračujme tedy ve výpočtu

$$= \begin{pmatrix} a^2 + ad - q - (a+d)a + q & ab + bd - (a+d)b \\ ac + cd - (a+d)c & d^2 - (a+d)d + ad \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Ukázali jsme tedy, že endomorfismus $\phi_{q,n}^2 - t\phi_{q,n} + q\mathrm{Id}$ je identicky nulovým endomorfismem grupy $E[n]$. Protože se však $\phi_{q,n}$ na grupě $E[n]$ shoduje s ϕ_q(je to jeho restrikce), platí totéž i pro endomorfismus ϕ_q. Dostáváme tedy, že pro každý bod $P \in E[n]$ platí $\phi_q(P)^2 - t\phi(P) + qP = \mathcal{O}$. Pro využití ve Schoofově algoritmu je toto tvrzení dostatečné, odpovídá totiž rovnici 6.11 která je klíčová pro celý algoritmus. Chceme-li vztah ukázat pro libovolné $P \in E$ a tím dokázat tvrzení 4.1.3, stačí dle [11](Část 2.9) ukázat, že jádro endomorfismu $\phi_q^2 - t\phi + q$ není konečné. To ovšem platí, neboť existuje nekonečné množství čísel n nedělitelných charakteristikou $\mathbb{F}_q$ a pro každé takové n je uvedený endomorfismus nulový na celé grupě $E[n]$, proto nemá konečné jádro a je tedy identicky nulový na celé grupě E.

6.3 Algoritmus

Nyní již máme vše potřebné pro popis algoritmu. Mějme eliptickou křivku E danou Weierstrassovou rovnicí

$$E : y^2 = x^3 + ax + b \tag{6.10}$$

definovanou nad tělesem $\mathbb{F}_q$, kde $q = p^m$ pro liché prvočíslo p. Schoofův algoritmus využívá Hasse-Weilovu větu 5.2.1. Ta říká, že pro počet bodů takto zadané křivky platí následující nerovnost:

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

Označme $t = q + 1 - |E(\mathbb{F}_q)|$. Vyčíslit t je tedy totožný problém jako určit velikost $E(\mathbb{F}_q)$. Hasseho věta říká že $|t| \leq 2\sqrt{q}$, tj. $-2\sqrt{q} \leq t \leq 2\sqrt{q}$. Hledáme tedy t v intervalu o velikosti $4\sqrt{q}$, proto pokud dokážeme spočítat t mod N pro nějaké $N > 4\sqrt{q}$, dokážeme jednoznačně určit i t. Číslo N zvolíme tak, aby to byl součin co nejmenších prvočísel různých od 2 a p. Tedy

$$N = \prod_{l \in S} l$$

kde $S = \{3, 5, 7, 11, ..., L\} \backslash \{p\}$ je nejmenší množina prvočísel taková, že $N > 4\sqrt{q}$. Pokud bychom nyní uměli vyčíslit t mod l pro každé $l \in S$, dokázali bychom za použití čínské věty o zbytcích spočítat i t mod N. Dále se tedy budeme zabývat tím, jak rychle počítat t mod l pro celkem malé prvočíslo l.

K tomu použijeme Frobeniův endomorfismus, jeho charakteristickou rovnici a redukované dělící polynomy. Frobeniův endomorfismus definovaný v 4.1.2 značíme ϕ_q a je dán předpisem

$$\begin{aligned} \phi_q : E(\overline{\mathbb{F}}_q) &\longrightarrow E(\overline{\mathbb{F}}_q) \\ (x, y) &\longmapsto (x^q, y^q) \\ \mathcal{O} &\longmapsto \mathcal{O}. \end{aligned}$$

Jeho charakteristická rovnice je dle tvrzení 4.1.3

$$\phi^2 - t\phi + q = 0$$

kde nula na pravé straně znamená triviální zobrazení, tedy takové, které každý bod $E(\overline{\mathbb{F}}_q)$ zobrazuje na bod v nekonečnu. Jinými slovy tedy pro každý bod $P \in E(\overline{\mathbb{F}}_q)$ platí

$$\phi_q^2(P) - t\phi_q(P) + qP = \mathcal{O},$$

to jest

$$\phi_q^2(P) + qP = t\phi_q(P)$$

Uvažujme nyní bod $P \in E[l]$. Ať $q_l, t_l \in \{0, 1, 2, \ldots, l-1\}$ jsou taková, že platí

$$\begin{aligned} q_l &\equiv q \pmod{l} \\ t_l &\equiv t \pmod{l}. \end{aligned}$$

Protože bod P je řádu l, platí $qP = q_l P$, a protože ϕ_q je endomorfismus, je i bod $\phi_q(P)$ řádu l, tedy také $t\phi_q(P) = t_l\phi_q(P)$. Dostáváme tedy, že pro každý bod $P \in E[l]$ platí rovnost

$$\phi_q^2(P) + q_l P = t_l \phi_q(P). \tag{6.11}$$

Číslo t_l je touto rovností určeno jednoznačně. Pokud bychom totiž měli nějaké t_l' takové, že pro všechny $P \in E[l]$ platí

$$\phi_q^2(P) + q_l P = t_l' \phi_q(P),$$

odečtením od rovnice 6.11 bychom dostali, že $(t_l - t_l')\phi_q(P) = \mathcal{O}$ pro alespoň jeden nenulový bod $P \in E[l]$. Protože endomorfismus ϕ_q je prostý a bod $\phi_q(P)$ je řádu l, znamenalo by to, že $t_l \equiv t_l' \pmod{l}$.

Hodnotu t_l tedy můžeme získat tak, že budeme procházet všechny možné hodnoty $\tau \in \{0, 1, \ldots, l-1\}$ a zkoušet pro kterou hodnotu platí

$$\forall P \in E[l] \text{ je } \phi_q^2(P) + q_l P = \tau \phi_q(P).$$

Protože vzorce pro sčítaní bodů odvozené v první kapitole závisí na tom, zda jsou sčítané body různé, nebo stejné, rozdělíme náš postup na dva případy.

- Případ 1: Existuje nenulový bod $P \in E[l]$, pro který platí $\phi_q^2(P) = \pm q_l P$
  - Případ 1a: $\phi_q^2(P) = -q_l P$
  - Případ 1b: $\phi_q^2(P) = q_l P$
- Případ 2: Pro každý nenulový bod $P \in E[l]$ platí $\phi_q^2(P) \neq \pm q_l P$

Nyní si ukážeme, jak spočítat hodnotu t_l v jednotlivých případech. Potom ukážeme, jak poznat, ve kterém případě se pro dané l nacházíme.

Případ 1a: Dle předpokladu existuje bod $P \in E[l]$ takový, že platí

$$\phi_q^2(P) = -q_l P.$$

Rovnice 6.11 tedy vypadá následovně:

$$\mathcal{O} = t_l \phi_q(P).$$

Protože ϕ_q je prostý endomorfismus a P nenulový bod, je nutně $t_l = 0$.

Případ 1b: Dle předpokladu existuje bod $P \in E[n]$, pro který platí

$$\phi_q^2(P) = q_l P. \tag{6.12}$$

Rovnici 6.11 tedy můžeme přepsat jako

$$2q_l P = t_l \phi_q(P). \tag{6.13}$$

Aplikací Frobeniova endomorfismu na obě strany této rovnice dostaneme nyní rovnost

$$2q_l \phi_q(P) = t_l \phi_q^2(P). \tag{6.14}$$

Nyní upravujme výraz $t_l^2 q_l P$:

$$t_l^2 q_l P \overset{6.12}{=} t_l^2 \phi_q^2(P) \overset{6.14}{=} 2t_l q_l \phi_q(P) \overset{6.13}{=} 4q_l^2 P.$$

Protože P je nenulový bod řádu l, platí dle poslední rovnosti $t_l^2 q_l \equiv 4q_l^2 \pmod{l}$. Protože $q_l \neq 0$ můžeme jím vydělit a dostaneme

$$t_l^2 \equiv 4q_l \pmod{l}. \tag{6.15}$$

Z této ekvivalence vyplývá, že q_l je čtverec modulo l. Mějme tedy w takové, že $w^2 \equiv q_l \pmod{l}$. Dosazením do 6.15 dostaneme ekvivalenci $t_l^2 \equiv 4w^2 \pmod{l}$, tedy $t_l \equiv \pm 2w \pmod{l}$. Dosazením to rovnosti 6.13 obdržíme vztah

$$\begin{aligned} 2w^2 P &= \pm 2w \phi_q(P) \\ 2w^2 P \mp 2w \phi_q(P) &= \mathcal{O} \\ 2w(wP \mp \phi_q(P)) &= \mathcal{O}, \end{aligned}$$

a protože bod, který vyjde v závorce, má řád l a číslo w je nenulové modulo l(neboť je odmocninou nenulového čísla), musí platit $wP \mp \phi_q(P) = \mathcal{O}$, tedy

$$\phi_q(P) = \pm wP. \tag{6.16}$$

Tedy jsou dvě možnosti. Pokud je $\phi_q(P) = wP$, dosazením za $\phi_q(P)$ do rovnosti 6.13 dostaneme

$$\begin{aligned} 2q_l P &= t_l wP, \text{ to jest} \\ 2w^2 P &= t_l wP, \end{aligned}$$

tedy nutně platí $t_l \equiv 2w \pmod{l}$. Pokud je naopak $\phi_q(P) = -wP$, vyjde stejným postupem, že $t_l \equiv -2w \pmod{l}$. Zbývá tedy rozlišit jaká z těchto dvou možností nastává. Ať $P = (x, y)$. Přepíšeme-li rovnost 6.16 do souřadnic, tak za použití značení z lemmatu 6.1.13 dostáváme

$$\begin{aligned} (x^q, y^q) &= \pm \left(\frac{R_w(x)}{r_w(x)}, y\frac{S_w(x)}{s_w(x)} \right), \text{ tedy} \\ (x^q, y^q) &= \left(\frac{R_w(x)}{r_w(x)}, \pm y\frac{S_w(x)}{s_w(x)} \right). \end{aligned}$$

První možnost(tj. $\phi_q(P) = wP$) tedy nastává, právě když

$$y^q = y\frac{S_w(x)}{s_w(x)},$$

což je ekvivalentní podmínce

$$y^q s_w(x) - yS_w(x) = 0.$$

Označíme-li $\tilde{f} = x^3 + Ax + B \in \mathbb{F}_q[x]$, můžeme podmínku s využitím rovnice křivky přepsat jako

$$y(\tilde{f}(x)^{\frac{q-1}{2}} s_w(x) - S_w(x)) = 0,$$

a protože žádný bod $E[l]$ není řádu 2, je $y \neq 0$ a můžeme jím tedy rovnici vydělit. Dostáváme tedy podmínku

$$\tilde{f}(x)^{\frac{q-1}{2}} s_w(x) - S_w(x) = 0. \tag{6.17}$$

Celkem tedy máme: Bod $P = (x, y)$ splňuje $\phi_q(P) = wP$, právě když platí 6.17. Pravá strana této podmínky je polynom v jedné proměnné, můžeme tedy využít lemma 6.1.11. To říká, že pokud je GCD $\left(\tilde{f}(x)^{\frac{q-1}{2}} s_w(x) - S_w(x), f_l(x)\right) = 1$, pak neexistuje žádný bod $Q = (\alpha, \beta) \in E[l]$, pro který platí rovnost

$$\tilde{f}(\alpha)^{\frac{q-1}{2}} s_w(\alpha) - S_w(\alpha) = 0,$$

a tedy pro žádný bod $Q \in E[l]$ neplatí $\phi_q(Q) = wQ$. Protože $P \in E[l]$, neplatí to ani pro něj, tedy musí nastat druhá možnost kde $\phi_q(P) = -wP$. Pokud naopak vyjde GCD $\left(\tilde{f}(x)^{\frac{q-1}{2}} s_w(x) - S_w(x), f_l(x)\right) \neq 1$, lemma 6.1.11 říká, že existuje bod $P' \in E[l]$, pro který platí $\phi_q(P') = wP'$. Můžeme tedy stejný výpočet, jaký

jsme udělali pro bod P za rovností 6.16, provést i pro bod P' a získat tak hodnotu t_l(neboť pro takové P' také platí $\phi_q(P')^2 = q_l P'$ a mohli jsme tedy celý výpočet případu 1b provádět pro tento bod). Tímto jsme kompletně vyřešili případ 1b.

Případ 2: Toto je případ, kdy pro každý nenulový bod $P \in E[l]$ platí $\phi_q^2(P) \neq \pm q_l P$, víme tedy, že $t_l \neq 0$. V tomto případu, jak již bylo naznačeno výše, budeme procházet všechny možné hodnoty $\tau \in \{1, 2, \ldots, l-1\}$ a zkoušet, zda pro dané τ platí

$$\forall P \in E[l] \text{ je } \phi_q^2(P) + q_l P = \tau \phi_q(P). \tag{6.18}$$

Pro takové τ je pak $\tau \equiv t_l \pmod{l}$, což jednoznačně určuje hodnotu t_l. Mějme libovolný bod $P = (x, y) \in E[l]$ a nějaké $\tau \in \{1, 2, \ldots, l-1\}$. Chceme zjistit za jakých podmínek platí rovnost

$$\phi_q^2(P) + q_l P = \tau \phi_q(P). \tag{6.19}$$

Po přepsání do souřadnic tato rovnost vypadá následovně

$$\left(x^{q^2}, y^{q^2}\right) + \left(\frac{R_{q_l}(x)}{r_{q_l}(x)}, y\frac{S_{q_l}(x)}{s_{q_l}(x)}\right) = \left(\frac{R_\tau(x^q)}{r_\tau(x^q)}, y^q\frac{S_\tau(x^q)}{s_\tau(x^q)}\right).$$

Protože body na levé straně jsou dle předpokladu různé, víme, jaký vzorec pro jejich součet použít a dostáváme

$$\left(\lambda^2 - x^{q^2} - \frac{R_l(x)}{r_l(x)}, -\lambda\left(\lambda^2 - 2x^{q^2} - \frac{R_l(x)}{r_l(x)}\right) - y^{q^2}\right) = \left(\frac{R_\tau(x^q)}{r_\tau(x^q)}, y^q\frac{S_\tau(x^q)}{s_\tau(x^q)}\right),$$

kde

$$\lambda = \frac{x^{q^2} - \frac{R_l(x)}{r_l(x)}}{y^{q^2} - y\frac{S_l(x)}{s_l(x)}}.$$

Hledíme-li jen na první souřadnice, máme rovnost

$$\lambda^2 - x^{q^2} - \frac{R_l(x)}{r_l(x)} = \frac{R_\tau(x^q)}{r_\tau(x^q)}.$$

Nahrazením prvků y^2 podle rovnice křivky a vynásobením jmenovateli všech členů lze tuto rovnici převést na tvar

$$H_\tau(x) = 0,$$

kde H_τ je vhodný polynom. Podobně rovnost druhých souřadnic můžeme pro vhodný polynom G_τ zapsat ve tvaru

$$yG_\tau(x) = 0,$$

a protože $E[l]$ neobsahuje body řádu 2, je $y \neq 0$ a rovnici lze tedy ekvivalentně psát jen jako

$$G_\tau(x) = 0.$$

Máme tedy, že rovnost 6.19 platí pro bod $P = (x, y) \in E[l]$ právě když $H_\tau(x) = 0$ a zároveň $G_\tau(x) = 0$. Nyní využijeme lemma 6.1.10 z předchozí části. To nám v tomto případě říká, že rovnost 6.19 platí pro každý bod $E[l]$ právě když

$$H_\tau \equiv 0 \pmod{f_l} \text{ a zároveň } G_\tau \equiv 0 \pmod{f_l}. \tag{6.20}$$

Pokud tedy pro nějaké τ platí podmínka 6.20, pak pro něj platí i 6.18, a tedy $\tau \equiv t_n \pmod{l}$. Postup lze ještě vylepšit tak, že nebudeme muset procházet všechna možná τ, ale pouze jejich polovinu. Pokud totiž pro nějaké τ platí $H_\tau \equiv 0 \pmod{f_l}$ znamená to rovnost prvních souřadnic v rovnici 6.19. Pokud se však dva body křivky E shodují v prvních souřadnicích, tak to podle vzorců pro sčítání znamená, že jsou tyto body totožné. nebo opačné. Pokud tedy neplatí $G_\tau \equiv 0 \pmod{f_l}$ pak to znamená, že rovnost 6.19 platí, ale s opačným znaménkem, tedy

$$\forall P \in E[l] \text{ je } \phi_q^2(P) + q_l P = -\tau\phi_q(P).$$

Proto v tomto případě platí $-\tau \equiv t_n \pmod{l}$.

Tím jsme si ukázali, jak spočítat hodnotu t_n v jednotlivých případech. Nyní ukážeme, jak pro konkrétní l zjistit, jaký z případů pro něj nastává. Mějme tedy libovolné $l \in S$. Případy 1 a 2 rozlišíme následovně: Zajímá nás, zda existuje $P = (x, y) \in E[l]$ takový, že platí

$$\phi_q^2(P) = \pm q_l P, \text{ neboli}$$
$$\left(x^{q^2}, y^{q^2}\right) = \left(\frac{R_{q_l}(x)}{r_{q_l}(x)}, \pm y\frac{S_{q_l}(x)}{s_{q_l}(x)}\right).$$

To nastává právě tehdy, když se oba body shodují v první souřadnici, tedy právě když platí

$$x^{q^2} r_{q_l}(x) - R_{q_l}(x) = 0. \tag{6.21}$$

Lemma 6.1.11 říká, že bod $P = (x, y) \in E[l]$ splňující 6.21 existuje, právě když

$$\mathrm{GCD}\left(x^{q^2} r_{q_l}(x) - R_{q_l}(x), f_l(x)\right) \neq 1. \tag{6.22}$$

Pokud tedy podmínka 6.22 platí, nacházíme se v případu 1, pokud podmínka neplatí, jsme nutně v případu 2.

Zbývá tedy už jen rozlišit případy 1a a 1b v rámci případu 1. Nastal-li případ 1, existuje bod $P \in E[l]$, že

$$\phi_q^2(P) = \pm q_l P.$$

Pro rozlišení případů 1a a 1b chceme ověřit existenci bodu splňujícího výše uvedenou rovnici pro konkrétní znaménko. To lze udělat za pomoci lemmatu 6.1.11 podobně, jako jsme rozlišovali případy 1 a 2. Dostaneme, že existuje bod $P \in E[l]$ pro který platí

$$\phi_q^2(P) = q_l P,$$

právě když platí

$$\mathrm{GCD}\left(\tilde{f}^{\frac{q^2-1}{2}}(x) s_{q_l}(x) - S_{q_l}(x), f_l(x)\right) \neq 1. \tag{6.23}$$

Takto tedy můžeme, rozlišit případy 1a a 1b. V některých případech ale můžeme použít efektivnější postup. Z uvedeného výpočtu v případu 1b můžeme získat několik nutných podmínek, za kterých tento případ může nastat. Pomocí těchto podmínek lze tedy tento případ vyloučit. První nutná podmínka, kterou jsme odvodili během výpočtu, je, že q_l je čtverec modulo l. Další nutnou podmínkou je, že pro w takové, že $w^2 \equiv q_l \pmod{l}$, existuje $P \in E[l]$, že $\phi_q(P) = \pm wP$. Postup v případu 1 bude tedy následující: Nejprve otestujeme, zda q_l je čtverec modulo l. Pokud není, víme, že nemůžeme být v případu 1b, musí proto nastávat případ 1a. Pokud q_l je čtverec, spočteme jeho odmocninu modulo l a označíme ji w. Dále otestujeme, zda existuje $P = (x, y) \in E[l]$ takové, že

$$\begin{aligned} \phi_q(P) &= \pm wP, \text{ tj.} \\ (x^q, y^q) &= \left(\frac{R_w(x)}{r_w(x)}, \pm y \frac{S_w(x)}{s_w(x)} \right). \end{aligned}$$

To platí, právě když se rovnají první souřadnice. S využitím lemmatu 6.1.11 dostaneme, že takový bod existuje, právě když

$$\mathrm{GCD}\left(x^q r_w(x) - R_w(x), f_l\right) \neq 1.$$

Pokud nám tedy vyjde $\mathrm{GCD}\left(x^q r_w(x) - R_w(x), f_l\right) = 1$, nemůžeme se nacházet v případu 1b a jsme tedy v případu 1a.

Nyní již máme vše pro přesnější symbolický zápis celého algoritmu:

Schoofův algoritmus - symbolický zápis

1. Zvolíme množinu prvočísel $S = \{3, 5, 7, ...L\} \backslash \{p\}$ tak, že platí $N = \prod_{l \in S} l > 4\sqrt{q}$. L volíme co nejmenší.

2. Zvolíme $l \in S$ takové, které jsme ještě nezpracovali. Pokud jsme již zpracovali všechna $l \in S$, pokračujeme bodem 3.

   (a) Spočteme q_l tak, že $q_l \equiv q \pmod{l}$.

   (b) Pokud $\mathrm{GCD}\left(x^{q^2} r_{q_l}(x) - R_{q_l}(x), f_l(x)\right) = 1$, pokračujeme bodem 2c

      i. Spočteme $\left(\frac{q_l}{l}\right)$.
      ii. Pokud $\left(\frac{q_l}{l}\right) = -1$, volíme $t_l = 0$ a pokračujeme bodem 2.
      iii. Spočteme w takové, že $w^2 \equiv q_l \pmod{l}$.
      iv. Pokud $\mathrm{GCD}\left(x^q r_w(x) - R_w(x), f_l\right) = 1$, volíme $t_l = 0$ a pokračujeme bodem 2
      v. Pokud $\mathrm{GCD}\left(\tilde{f}(x)^{\frac{q-1}{2}} s_w(x) - S_w(x), f_l(x)\right) = 1$, volíme t_l tak, aby $t_l \equiv -2w \pmod{l}$ a pokračujeme bodem 2.
      vi. Volíme t_l tak, aby $t_l \equiv 2w \pmod{l}$ a pokračujeme bodem 2.

   (c) Volíme $\tau \in \{1, 2, \ldots (l-1)/2\}$ takové, které jsme pro aktuální l ještě nezpracovali.

      i. Pokud $H_\tau \not\equiv 0 \pmod{f_l}$, pokračujeme bodem 2c.
      ii. Pokud $G_\tau \equiv 0 \pmod{f_l}$, volíme t_l tak, aby $t_l \equiv \tau \pmod{l}$ a pokračujeme bodem 2.

iii. Volíme t_l tak, aby $t_l \equiv -\tau \pmod{l}$ a pokračujeme bodem 2.

3. Pro každé $l \in S$ jsme spočetli hodnotu t_l, pro kterou platí $t_l \equiv t \pmod{l}$. Pomocí všech těchto hodnot spočteme za použití čínské věty o zbytcích hodnotu t_N, pro kterou platí $t_N \equiv t \pmod{N}$. Podmínky $t \equiv t_N \pmod{N}$ a $|t| < 2\sqrt{q}$ již nyní určují hodnotu t jednoznačně.

4. Počet bodů křivky je $|E(\mathbb{F}_q)| = q - 1 - t$.

Poznámka 6.3.1. *Případu 1 odpovídají v zápisu algoritmu body 2(b)i - 2(b)vi. Případu 2 pak odpovídá bod 2c a jeho části 2(c)i - 2(c)iii.*

6.4 Složitost

Poslední, co zbývá, je odhad složitosti uvedeného algoritmu. Nejprve odhadneme velikost prvočísla L a ostatních prvočísel $l \in S$, potom budeme postupně procházet všechny body symbolického zápisu algoritmu z konce předchozí části a u každého z nich odhadneme jeho složitost. Nakonec dáme vše dohromady a uvedeme výslednou složitost celého algoritmu.

Velikost prvočísel

Podle [5](Důsledek tvrzení 4) platí následující lemma.

Lemma 6.4.1. *Pro $n \geq 41$ platí*

$$e^{n\left(1-\frac{1}{\ln(n)}\right)} < \prod_{\substack{l \text{ prvočíslo} \\ l \leq n}} l.$$

Toho využijeme k odhadu velikosti čísla L.

Lemma 6.4.2. *Zvolme $M = 4\ln(q)$ a L volme jako největší prvočíslo, které je menší než M. Ať $S = \{3, 5, \ldots, L\} \setminus \{p\}$. Pak pro dostatečně velké q platí*

$$4\sqrt{q} < \prod_{l \in S} l.$$

Důkaz. Budeme zdola odhadovat hodnotu $M/2$ (pro dostatečně velké M):

$$\frac{M}{2} = 2\ln(q) \geq \ln(8) + \ln(q) + \frac{1}{2}\ln(q) \geq \ln(8) + \ln(p) + \frac{1}{2}\ln(q) = \ln(8p\sqrt{q}).$$

Aplikací exponenciální funkce na obě strany dostáváme nerovnost

$$8p\sqrt{q} \leq e^{\frac{M}{2}}, \text{ neboli}$$
$$4\sqrt{q} \leq \frac{e^{\frac{M}{2}}}{2p}.$$

Pro dostatečně velké q tedy platí

$$4\sqrt{q} \leq \frac{e^{\frac{M}{2}}}{2p} \leq \frac{e^{M\left(1-\frac{1}{\ln(M)}\right)}}{2p} \overset{6.4.1}{<} \frac{1}{2p} \prod_{\substack{l \text{ prvočíslo} \\ l \leq n}} l \leq \prod_{l \in S} l$$

□

Z lemmatu je tedy vidět, že pro splnění podmínky $\prod_{l \in S} l > 4\sqrt{q}$ v prvním bodu algoritmu stačí volit L menší než $4\ln(q)$. Tedy i velikost množiny S je menší než $4\ln(q)$. Můžeme proto dále psát, že velikost množiny S je $\mathcal{O}(\log q)$. Stejně tak o velikosti všech prvočísel z S můžeme psát, že jejich velikost je $\mathcal{O}(\log q)$.

Složitost jednotlivých bodů

V prvním bodě se počítá seznam prvočísel od 3 až do L. To lze například za použití Eratostenova síta zvládnout za použití $\mathcal{O}(\log q^2)$ operací.

Pro druhý bod potřebujeme spočítat všechny redukované dělící polynomy $f_1, f_2, \ldots, f_L$. Lemma 6.1.12 říká, že stupeň polynomu f_l je $\mathcal{O}(l^2)$, tedy můžeme psát, že stupeň každého f_l je $\mathcal{O}(\log(q)^2)$. Složitost výpočtu každého z polynomů odhadneme složitostí výpočtu toho posledního, tj. f_L. Ten se počítá dle rekurentních vzorců 6.1.9 pomocí konstantního počtu násobení a sčítání polynomů stupně $\mathcal{O}(\log(q)^2)$. Sčítání je vzhledem k násobení zanedbatelné. Násobení polynomů má dle části 2.2 složitost $\mathcal{O}(d_1 d_2 \log(q)^2)$ kde d_1 a d_2 jsou stupně násobených polynomů. V tomto případě jsou tyto stupně oba $\mathcal{O}(\log(q)^2)$, tedy celková složitost výpočtu polynomu f_L je $\mathcal{O}(\log(q)^6)$. A protože počet všech potřebných redukovaných dělících polynomů je L, tj. $\mathcal{O}(\log(q))$, je celková složitost výpočtu těchto polynomů $\mathcal{O}(\log(q)^7)$.

Výpočetně nejnáročnější operace bodu dva jsou počítání největších společných dělitelů v bodech 2b, 2(b)iv a 2(b)v a potom redukce polynomů H_τ a G_τ modulo f_l v bodech 2(c)i a 2(c)ii. Pro složitost výpočtu největšího společného dělitele dvou polynomů jsou podstatné jejich stupně. Výpočet může probíhat následovně: Nejprve zredukujeme členy x^{q^2}, x^q a $\tilde{f}^{\frac{q-1}{2}}$ vyskytující se v prvním argumentu modulo polynom f_l, tím dostaneme v obou argumentech polynomy stupně $\mathcal{O}(\log(q)^2)$ a složitost výpočtu takového NSD je potom dle části 2.2 rovna $\mathcal{O}((\log(q)^2)^2 \log(q)^2) = \mathcal{O}(\log(q)^6)$. Členy x^{q^2}, x^q a $\tilde{f}^{\frac{q-1}{2}}$ lze modulo f_l spočítat pomocí binárního mocnění za použití $\mathcal{O}(\log(q))$ násobení polynomů stupně $\mathcal{O}(\log(q)^2)$. Takové násobení má složitost $\mathcal{O}(\log(q)^6)$, tedy celková složitost redukce těchto členů modulo f_l je $\mathcal{O}(\log(q)^7)$. To je více než složitost následného výpočtu NSD, proto celková složitost kroků 2b, 2(b)iv a 2(b)v je $\mathcal{O}(\log(q)^7)$.

Výpočet polynomů H_τ a G_τ modulo f_l v krocích 2(c)i a 2(c)ii probíhá podobně, nejprve za použití $\mathcal{O}(\log(q)^7)$ operací zredukujeme členy x^{q^2}, x^q a $\tilde{f}^{\frac{q-1}{2}}$ vyskytující se ve vyjádření těchto polynomů a pak spočteme zbytek po vydělení f_l. Výpočet zbytku po dělení má v tomto případě složitost $\mathcal{O}(log(q)^6)$. Celková složitost bodů 2(c)i a 2(c)ii je tedy $\mathcal{O}(\log(q)^7)$.

Body 2(c)i a 2(c)ii však provádíme pro každé $\tau \in \{1, 2, \ldots, (l - 1/2)\}$. To je tedy $\mathcal{O}(\log(q))$ opakování těchto kroků, tedy $\mathcal{O}(\log(q)^8)$ operací pro výpočet všech iterací kroku 2c. Máme tedy složitost výpočtu t_l pro jedno konkrétní l. Protože prvočísel l je v množině S $\mathcal{O}(\log(q))$, je složitost všech iterací kroku 2 $\mathcal{O}(\log(q)^9)$.

Krok 3 spočívá v jedné aplikaci čínské věty o zbytcích. To lze provést například pomocí Garnerova algoritmu(např. [10](Algoritmus 12)) za použití pouhých $\mathcal{O}(\log(q)^2 \log(\log(q))^2)$ operací.

Poslední krok je pak už jen sčítání prvků tělesa, má tedy vzhledem ke zbytku algoritmu zanedbatelnou složitost. Nejnáročnější částí algoritmu je tedy krok 2, proto je celková složitost Schoofova algoritmu $\mathcal{O}\left(\log(q)^9\right)$.

Závěr

Cílem práce bylo nastudovat, a zpracovat vybrané algoritmy pro určování počtu bodů eliptických a hypereliptických křivek nad konečnými tělesy. Po vysvětlení základní teorie a uvedení několika exponenciálních algoritmů jsme se zaměřili na základní verzi Schoofova algoritmu, protože jde o první polynomiální algoritmus řešící tento problém. Nejdříve jsme zpracovali potřebnou teorii a poté podrobně popsali průběh algoritmu. Nakonec jsme ukázali, že se skutečně jedné o polynomiální algoritmus.

Existují další algoritmy, které Schoofův algoritmus dále zefektivňují. Jedná se zejména o algoritmus SEO(Schoof–Elkies–Atkin)[2](Část 17.2.2), který mimo jiné využívá namísto námi definovaných polynomů f_n polynomy nižšího stupně a tím se stává o něco efektivnějším. Dále jsme se také nezabývali žádným polynomiálním algoritmem pro křivky nad tělesem charakteristiky 2. Ty jsou také důležité, neboť tělesa charakteristiky 2 jsou v kryptografii oblíbená díky své efektivní implementaci. Jedná se například o algoritmus AGM(Arithmetic–Geometric–Mean)[2](Část 17.3.2.b). Tyto algoritmy se tak stávají námětem pro další studium.

Seznam použité literatury

[1] BARKER Elaine, William BARKER, William BURR, William POLK a Miles SMID. *Recommendation for Key Management – Part 1: General (Revision 3)*. NIST Special Publication 800-57, National Institute of Standards and Technology, Jul 2012.

[2] COHEN, Henri, Gerhard FREY a Roberto AVANZI. *Handbook of elliptic and hyperelliptic curve cryptography*. Boca Raton: Chapman, 2006, xxxiv, 808 p. ISBN 15-848-8518-1.

[3] LANG, Serge. *Elliptic curves diophantine analysis*. Berlin: Springer, 1978, 11, 261 s. Grundlehren der mathematischen Wisenschaften. ISBN 35-400-8489-4.

[4] POHLIG, S. a M. HELLMAN. *An improved algorithm for computing logarithms over GF(p)and its cryptographic significance*. IEEE Transactions on Information Theory. 1978, vol. 24, issue 1, s. 106-110.

[5] ROSSER, J. Barkley a Lowell SCHOENFELD. *Approximate formulas for some functions of prime numbers*. Illinois Journal of Mathematics, Vol. 6, No. 1962, p. 64-94, 1962

[6] SCHOOF, René. *Elliptic curves over finite fields and the computation of square roots mod p*. Mathematics of Computation, Vol. 44, No. 170, 1985, p. 483-494.

[7] SCHOOF, René. *Counting points on elliptic curves over finite fields*. Journal de Théorie des Nombres de Bordeaux, Vol. 7, No. 1, 1995, p. 219-254.

[8] SILVERMAN, Joseph H. *The arithmetic of elliptic curves*. 2nd ed. Dordrecht: Springer, 2009, xx, 513 s. Graduate texts in mathematics. ISBN 978-0-387-09493-9.

[9] SMART, Nigel P. *The Discrete Logarithm Problem on Elliptic Curves of Trace One*. Journal of Cryptology, Vol. 12, Issue 3, June 1999, p. 193-196.

[10] STANOVSKÝ, David a Libor BARTO. *Počítačová algebra*. 1. vyd. Praha: Matfyzpress, 2011, 180 s. ISBN 978-80-7378-167-5.

[11] WASHINGTON, Lawrence C. *Elliptic curves: number theory and cryptography*. 2nd ed. Boca Raton, FL: Chapman, 2008, xviii, 513 p. ISBN 14-200-7146-7.