STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST

Obor č. 1: Matematika a statistika

Isogenie v kryptografii

Zdeněk Pezlar
Jihomoravský kraj

Brno 2021

STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST

Obor č. 1: Matematika a statistika

Isogenie v kryptografii

Isogeny Based Cryptography

Autor: Zdeněk Pezlar
Škola: Gymnázium Brno, třída Kapitána Jaroše, p. o.
Kraj: Jihomoravský
Konzultanti: Mgr. Vojtěch Suchánek
Mgr. Marek Sýs Phd.

Prohlášení

Prohlašuji, že jsem svou práci SOČ vypracoval samostatně a použil jsem pouze prameny a literaturu uvedené v seznamu bibliografických záznamů. Prohlašuji, že tištěná verze a elektronická verze soutěžní práce SOČ jsou shodné. Nemám závažný důvod proti zpřístupňování této práce v souladu se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) v platném znění.

V Brně dne: ..... Podpis: .....

jihomoravský kraj

Poděkování

Tom pozdravuje.

Abstrakt

V naší práci podáme lehký úvod do studia isogenií eliptických křivek bez předchozího studia algebraické geometrie. V práci rovněž diskutujeme několik vybraných protokolů a poskytujeme úvod do studia algebraické teorie čísel. Pomocí jejího studia pak podrobněji studujeme okruhy endomorfismů supersingulárních křivek. Práce je obohacena o implementace některých zmíněných protokolů, přičemž poskytujeme první implementaci velmi slibného protokolu SITH.

Klíčová slova

isogenie; eliptická křivka; okruh endomorfismů; grupa tříd ideálů; kvantový počítač; Diffie-Hellman; SIDH; CSIDH; SITH

Abstract

We provide a gentle introduction to the study of elliptic curve isogenies without any assumed knowledge in algebraic geometry. We then discuss several chosen protocols and give a brief introduction to algebraic number theory. After that, we apply the gained knowledge on the study of endomorphism rings of supersingular curves. The thesis is accompanied by a couple of implemented protocols, providing the first ever implementation of the very promising protocol SITH.

Key words

isogeny; elliptic curve; endomorphism ring; ideal class group; quantum computer; Diffie-Hellman; SIDH; CSIDH; SITH

Obsah

Úvod

Mějme pro začátek dvě kladná reálná čísla a, b. Jejich *aritmetický* a *geometrický průměr* splňují elementární nerovnost:

$$\frac{a+b}{2} \geqslant \sqrt{ab}.$$

Uvažme posloupnost dvojic kladných čísel takovou, že každá dvojice je tvořená právě těmito dvěma průměry, tedy $a_0 = a, b_0 = b$ a:

$$(a_{n+1}, b_{n+1}) = \left(\frac{a_n + b_n}{2}, \sqrt{a_n b_n} \right).$$

Platí tedy $a_n \geqslant b_n$ pro kladné n. Pro n jdoucí k nekonečnu a_n i b_n konvergují ke společné limitě, tzv. *aritmetickému geometrickému průměru* čísel a, b. Tento průměr studoval již Carl Friedrich Gauss [?] a ukázal, že tato na první pohled nevinná posloupnost je spojena s eliptickými integrály. Později se dokonce ukázalo, že tuto posloupnost můžeme využít k rychlému počítání čísla π i evaluování funkcí jako e^x či $\arcsin(x)$.

Co se ale na posloupnost podívat v jiném světle, konkrétně nad konečnými tělesy? V jistých tělesech můžeme definovat jednoznačně „konzistentní“ odmocninu z čísla a tak adaptovat naši posloupnost. Tentokrát posloupnost již ne vždy nekonverguje, zato však tvoří možná zajímavější struktury. Pokud sestavíme orientované grafy popisující naši posloupnost pro všechny dvojice (a, b) nad naším tělesem, získáme grafy, které vypadají následovně:
-IMG-
Tento graf nazveme *medúzou*. Už to, že grafy tvoří takovéto struktury je pozoruhodné, medúzy ale zde zdaleka nekončí. Ukážeme, že svým způsobem popisují *třídy isomorfismů eliptických křivek* nad naším tělesem, ?.

Kapitola 1

AG nad reálnými čísly

1.1 ?

Nejprve se zaměřme na posloupnost v nejpřirozenějším světle, totiž nad reálnými čísly.

Definice 1.1.1. Ať a, b jsou dvě kladná reálná čísla. Pak definujme *AG posloupnost* tak, že $(a_0, b_0) = (a, b)$ a:

$$(a_{n+1}, b_{n+1}) = \left(\frac{a_n + b_n}{2}, \sqrt{a_n b_n} \right).$$

Toto značení ponechme po zbytek sekce. Například si zvolme $a =?, b =?$. Pak .....

Příklad 1.1.2. nejakej vypocetni priklad.

Vidíme, že v tomto případě prvky *AG* posloupnosti zdárně konvergují ke společné hodnotě. Toto nastane vždy.

Věta 1.1.3. *Ať (a_i, b_i) je AG posloupnost. Pak limity a_n a b_n, pro n jdoucí do nekonečna, existují a jsou si navzájem rovné.*

Důkaz. Nejprve si všimněme, že aritmetický i geometrický průměr dvou čísel leží vždy mezi nimi. Z elementární nerovnosti též $a_n \geqslant b_n$ a proto:

$$b_{n+1} = \sqrt{a_n b_n} \geqslant b_n.$$

Posloupnost b_i je tedy neklesající a zároveň shora ohraničena prvek $a_0 = a$, limita a_n, $n \to \infty$ proto existuje. Obdobně platí:

$$a_{n+1} = \frac{a_n + b_n}{2} \leqslant a_n$$

a $a_n \geqslant b$, takže posloupnost a_i má limitu též. Jelikož platí:

$$a_n - b_n = 2\left(a_n - \frac{a_n + b_n}{2} \right) = 2(a_n - a_{n+1}),$$

tak limity posloupností a_i a b_i v nekonečnu se musí rovnat. □

Definice 1.1.4. Tuto společnou limitu nazvěme *aritmeticko-geometrickým průměrem*, zkráceně *AG-průměrem*, čísel a, b. Toto číslo značme $\mathrm{AG}(a, b)$.

Protože b_i je neklesající posloupnost, tak můžeme pozorovat skutečnost:

$$a_{n+1} - b_{n+1} \leqslant a_{n+1} - b_n = \frac{1}{2}(a_n - b_n) \leqslant \cdots \leqslant \frac{1}{2^{n+1}}(a - b).$$

Rela

Věta 1.1.5. *Pro AG posloupnost platí:*

(i) $\mathrm{AG}(a, a) = a$,

(ii) $\mathrm{AG}(ka, kb) = k\,\mathrm{AG}(a, b)$,

(iii) $\mathrm{AG}(a, b) = \mathrm{AG}(a_1, b_1) = \mathrm{AG}(a_2, b_2) = \ldots$,

Prozatím může vypadat, že tato posloupnost leží na uzavřeném ostrůvku vzdálená od jiných oblastní matematiky. Toto zdání však nemůže být dál od pravdy.

Na příkladu ?? totiž vidíme, že aritmetickou-geometrický průměr čísel 1 a 3 (???) konverguje k číslu, které nevykazuje žádné známky racionality. Na povrch proto vychází otázka, jak přesně tento průměr spočítat. K nalezení její odpověďi budeme muset nakouknout do sféry „eliptických integrálů“.

1.2 Eliptické integrály

Definice 1.2.1. Definujme „eliptický integrál prvního druhu“ jako následující určitý integrál:

$$K(t) := \int_0^{\pi/2} \frac{d\theta}{\sqrt{1 - t^2 \sin\theta^2}}.$$

Eliptický integrál druhého druhu získáme tak, že integrand převrátíme, tj.:

$$K'(t) := \int_0^{\pi/2} \sqrt{1 - t^2 \sin\theta^2} d\theta.$$

Tyto integrály mají mnoho využití, například v počítání délky oblouku na elipse, ve světě fyziky zase například pomáhají najít periodu kmitu kyvadla [?].

Taktéž jsou intimně spojené s AG posloupností, umožní nám totiž přesně vyjádřit hodnotu $AG(a, b)$.

Věta 1.2.2. *(Gauss) Pro $x < 1$ platí:*

$$\frac{\pi}{2} \cdot \frac{1}{\mathrm{AG}(1, x)} = K(.)$$

Kecy o důkazu. Jelikož AG posloupnost konverguje kvadraticky, tato spojitost nám může pomoci počítat právě eliptické integrály velmi rychle.

1.3 Rychlé výpočty elementárních funkcí

Kapitola 2

AG nad konečnými tělesy

2.1 Základní poznatky

Když jsme nyní zodpovědně prozkoumali AG posloupnost nad reálnými čísly, pojďme se na tuto posloupnost podívat nad konečným tělesem. Vzhledem k tomu, na kolika místech můžeme nad reálnými čísly narazit na AG posloupnost, nepřekvapí nás, že i v konečném případě tato posloupnost skýtá obrovské množství zajímavých ??.

Hned ze začátku narážíme na první problém. Ne vždy totiž není součin $a, b \in \mathbb{F}_q$ čtvercem v $\mathbb{F}_q$ a i pokud je, jak rozlišíme tu správnou odmocninu? Kvůli tomuto problému se prozatím zaměříme na tělesa $\mathbb{F}_q$ s $q = p^k \equiv -1 \pmod 4$, pak v $\mathbb{F}_q$ neexistuje odmocnina z -1. V každé nenulové dvojici $(x, -x)$ se proto nachází právě jeden čtverec a tak si vždy můžeme zvolit korektní odmocninu, aby byla posloupnost korektně definovaná i dále.

Poznámka. Ve skutečnosti jsme na tento problém narazili i nad reálnými čísly, tehdy ale jsou všechna kladná čísla čtverci, tedy je správná volba odmocniny intuitivnější.

Definice 2.1.1. Definujme „zobecněný Legendreho symbol“ ϕ_q nad $\mathbb{F}_q$ tak, že $\phi_q(0) = 0$ a pro x nenulové je $\phi_q(x)$ rovno 1, pokud x je v $\mathbb{F}_q$ čtvercem, a -1 jinak.

Definice 2.1.2. Ať $a, b \in \mathbb{F}_q^\times$ splňují $\phi_q(ab) = 1$. Pak definujeme $AG_{\mathbb{F}_q}(a, b)$ jako posloupnost (a_i, b_i) s $(a_0, b_0) = (a, b)$ a :

$$(a_{n+1}, b_{n+1}) = \left(\frac{a_n + b_n}{2}, \sqrt{a_n b_n} \right),$$

přičemž b_{n+1} volíme tak, že $\phi_q(a_{n+1} b_{n+1}) = 1$.

Všimněme si, že naše posloupnost je dobře definovaná. Aritmetický průměr by nám dělal problém, jen pokud by součet $a_{n+1} + b_{n+1}$ byl nulový. To by znamenalo:

$$a_n + b_n = -2\sqrt{ab}, \qquad \text{takže po umocnění} \qquad (a_n - b_n)^2 = 0.$$

Díky tomu, že odmocniny z čísla jsou navzájem opačná čísla a $\phi_q(-1) = -1$, víme, že pro $a_n b_n \neq 0$ je právě jedno z čísel $\sqrt{a_n b_n}$ a $-\sqrt{a_n b_n}$ čtvercem, mi si b_{n+1} zvolíme tak, aby součin $a_{n+1} b_{n+1}$ byl čtvercem. Můžeme tak pokračovat psát posloupnost i nadále.

Navíc, podmínka $a_i, b_i \in \mathbb{F}_q^\times$ je zachovaná i nadále. Pokud by totiž bylo jedno z čísel a_{n+1}, b_{n+1} nulové, jistě to musí být a_{n+1} a tak muselo být $a_n = -b_n$, to je ale ve sporu s volbou $\phi_q(a_n b_n) = 1$.

Posloupnost budeme vizualizovat jako orientovaný graf, kde hrana vede právě mezi po sobě jdoucími členy posloupnosti.

Definice 2.1.3. Definujme *graf* $AG_{\mathbb{F}_q}$ jako orientovaný graf, jehož vrcholy jsou uspořádané dvojice (a, b) prvků nad $\mathbb{F}_q^\times$, jejichž součin je čtverec. Všechny orientované hrany vedou mezi vrcholem (a, b) a (a_1, b_1).

PRIKLAD, ze meduz. Obrázky!

Na předchozích příkladech vidíme, že krom samostatných vrcholů (a, a) je graf $AG_{\mathbb{F}_q}$ tvořený z několika souvislých komponent, které mají všechny velmi specifický tvar, tj. cyklus, kde z každého jeho vrcholu vychází hrana délky jedna. Tento tvar je typický a libovolná komponenta jej tvoří.

Definice 2.1.4. Souvislý graf G nazveme *medúzou*, pokud je tvořen jediným cyklem a ke každému vrcholu grafu je připojen právě jeden list.

Nejprve si charakterizujme, které vrcholy mají v $AG_{\mathbb{F}_q}$ předchůdce, poté již bude popis celého grafu nasnadě.

Lemma 2.1.5. *Vrchol $(a, b) \in AG_{\mathbb{F}_q}$ má předchůdce, právě pokud platí $\phi_q(a^2 - b^2) = 1$.*

Důkaz. Nejprve předpokládejme (a, b) má předchůdce (c, d), platí tedy:

$$a = \frac{c+d}{2}, \quad b = \sqrt{cd}.$$

Potom:

$$a^2 - b^2 = \left(\frac{c+d}{2}\right)^2 - cd = \left(\frac{c-d}{2}\right)^2$$

je čtverec. Naopak ať $a^2 - b^2$ je čtverec a x je nějaká jeho odmocnina. Pak uvažme vrchol $(a - x, a + x)$, jeho následník je:

$$\left(\frac{a - x + a + x}{2}, \sqrt{a^2 - x^2}\right) = (a, b)\,,$$

kde b je ta „správná“ odmocnina. □

Věta 2.1.6. *Graf $AG_{\mathbb{F}_q}$ je tvořen z několika samostatných vrcholů a medúz.*

Důkaz. Jistě pokud $a \neq b$, tak (a, b) není samostatný vrchol. Graf je určen zobrazením $(u, v) \longrightarrow (u_1, v_1) \longrightarrow \ldots$ na konečné množině, takže každá taková posloupnost jednou vstoupí v cyklus, který bude mít délku větší než 1.

Dejme tomu, že (c, d) je členem nějaké cyklu, předchozí člen v cyklu je (C, D), platí $C + D = 2c$ a $CD = d^2$, tedy (C, D) jsou kořeny polynomu $x^2 - 2c + d^2$. Takový polynom

má nad $\mathbb{F}_q$ právě dva kořeny, C a D. Všichni předkové vrcholu (c, d) v $AG_{\mathbb{F}_q}$ jsou proto (C, D) a (D, C). Díky $q \equiv -1 \pmod 4$ je $\phi_q(-1) = -1$, proto díky předchozímu lemmatu má právě jeden z těchto dvou vrcholů předchůdce, ten je jistě taky součástí cyklu. Každý vrchol, který není členem cyklus, proto nemá předchůdce a $AG_{\mathbb{F}_q}$ je proto medúzou. □

Pojďme si nyní charakterizovat, jaké různé medúzy můžeme v celém grafu najít. Naše posloupnost je v jistém smyslu homogenní, přesněji podle analogu bodu ii) věty 1.1.5 můžeme přenásobit všechny vrcholy nějakým $k \in \mathbb{F}_q$ a získat *isomorfní* medúzu. Příklady takových medúz jsou na TOM PŘÍKLADU NA ZAČÁTKU. Jaký je však počet takových isomorfních medúz? Na to zodpovídá následující propozice:

Věta 2.1.7. *Ať $(a, b) \in AG_{\mathbb{F}_q}$ leží v cyklu a i je první index, že $(a_i, b_i) = (ka, kb)$. Pak počet medúz isomorfních s tou, ve které leží (a, b), je:*

$$\frac{p-1}{\mathrm{ord}_p(k)}.$$

Důkaz.

Pro taxonomické účely se nám hodí tyto isomorfní medúzy uskupit dohromady, zaveďme proto pojem *hejno*.

Definice 2.1.8. Ať $H \subseteq AG_{\mathbb{F}_q}$ je medúza a $H_1, \ldots, H_k$ jsou všechny medúzy s ní isomorfní. Pak $H \cup H_1, \cup \cdots \cup H_k$ nazvěme *hejnem medúz*.

2.2 AG pro tělesa bez odmocniny z jedné

V první kapitole jsme si ukázali, že pokud místo aritmetického a geometrického průměru zvolíme jinou dvojici průměrů, získáme posloupnosti úzce propojené s AG posloupností. Co tedy se podívat na jejich obdoby v konečných tělesech?

2.3 HG posloupnost

Nejprve zapojme do práce geometrický a harmonický průměr, kde samozřejmě definujeme harmonický průměr dvou nenulových čísel s nenulovým součtem jako:

$$\frac{2}{\frac{1}{a} + \frac{1}{b}} = \frac{2ab}{a+b},$$

kde $\frac{1}{a}$ je multiplikativní inverze čísla a. Pilný čtenář si ověří, že s multiplikativními inverzemi můžeme pracovat obdobně jako v reálných číslech. Definujme pak HG-posloupnost nad konečným tělesem.

Definice 2.3.1. Ať $a, b \in \mathbb{F}_q^\times$ splňují $\phi_q(ab) = 1$. Pak definujeme $HG_{\mathbb{F}_q}(a, b)$ jako posloupnost (a_i, b_i) s $(a_0, b_0) = (a, b)$ a :

$$(a_{n+1}, b_{n+1}) = \left(\frac{2}{\frac{1}{a_n} + \frac{1}{b_n}}, \sqrt{a_n b_n} \right),$$

přičemž b_{n+1} volíme tak, že $\phi_q(a_{n+1} b_{n+1}) = 1$.

PRIKLADY, GRAF.

Při porovnání předchozího příkladu se můžeme dovtípit, že tato posloupnost je pouze přestrojená AG posloupnost. V tomto přesvědčení nás může utvrdit i kritérium, kdy vrchol má předchůdce.

Lemma 2.3.2. *Vrchol $(a, b) \in HG_{\mathbb{F}_q}$ má předchůdce, právě pokud platí $\phi_q(b^2 - a^2) = 1$.*

Důkaz. Nejprve předpokládejme (a, b) má předchůdce (c, d), platí tedy:

$$a = \frac{2cd}{c + d}, \quad b = \sqrt{cd}.$$

Potom:

$$b^2 - a^2 = cd - \left(\frac{2cd}{c + d} \right)^2 = cd \left(\frac{c - d}{c + d} \right)^2$$

je čtverec, protože pracujeme pouze s dvojicemi, jejichž součin je čtvercem. Naopak ať $b^2 - a^2$ je čtverec a x je nějaká jeho odmocnina. Pak uvažme vrchol $\left(\frac{b^2 + bx}{a}, \frac{b^2 - bx}{a} \right)$, jeho následník je:

$$\left(\frac{2b^2(b + x)(b - x)}{a^2 \left(\frac{b^2 + bx}{a} + \frac{b^2 - bx}{a} \right)}, \sqrt{\frac{b^2(b^2 - x^2)}{a^2}} \right) = \left(\frac{2b^2 \cdot a^2}{2a \cdot b^2}, b \right) = (a, b),$$

kde b vybíráme jako tu „správnou“ odmocninu z b^2. □

Důsledek 2.3.3. *Graf $GH_{\mathbb{F}_q}$ je tvořen z několika samostatných vrcholů a medúz.*

Důkaz. Naprosto analogické k důkazu věty 2.1.6. □

Rozdíl mezi oběma grafy je ten, že vrchol (a, b) pro a, b je součástí cyklu v *právě jednom* z grafů $AG_{\mathbb{F}_q}$ a $HG_{\mathbb{F}_q}$.

Věta 2.3.4. *grafy jsou isomorfní.*

Kapitola 3

Propojení s eliptickými křivkami

Je pozoruhodné, že tak jednoduchá věc, jako AG či HG posloupnost, generuje nad konečnými tělesy tak pravidelné grafy jako medúzy. Toto není vůbec náhoda, podobné grafy ?

3.1 Rychlý úvod do eliptických křivek

V této sekci rychle a svižně probereme základy teorie eliptických křivek nad konečnými tělesy. Pro podrobnější text nemohu nedoporučit svou SOČ [], další excelentní cizojazyčné zdroje jsou [],[],[].

Kapitola 4

AH posloupnost

4.1 Základní poznatky

Zatím jsme pracovali s dvěma dvojicemi průměrů z trojice - aritmetický, geometrický a harmonický. Co se proto podívat i na tu poslední? Tentokrát již musíme ze začátku aplikovat jiné předpoklady, i přesto se můžeme ptát, jak souvisí tato posloupnost s předchozími dvěma, obzvláště ve spojení s eliptickými křivkami.

Definice 4.1.1. Ať q je mocnina prvočísla splňující $\phi_q(2) = -1$ a $a, b \in \mathbb{F}_q^\times$ mají nenulový součet. Pak definujeme $AH_{\mathbb{F}_q}(a, b)$ jako posloupnost (a_i, b_i) s $(a_0, b_0) = (a, b)$ a :

$$(a_{n+1}, b_{n+1}) = \left(\frac{a_n + b_n}{2}, \frac{2}{\frac{1}{a_n} + \frac{1}{b_n}} \right),$$

Musíme ověřit, že posloupnost nám vždy umožní spočítat další člen, tj., že harmonický průměr vždy bude definován. Ať je naopak pro nějaká (a_0, b_0) a n nezáporné $\frac{1}{a_{n+1}} + \frac{1}{b_{n+1}} = 0$, pak i $a_{n+1} + b_{n+1} = 0$. Muselo pak být:

$$\begin{aligned}
\frac{a_n + b_n}{2} + \frac{2a_n b_n}{a_n + b_n} &= 0, \\
(a_n + b_n)^2 + 4a_n b_n &= 0, \\
\left(\frac{a_n}{b_n} + 1 \right)^2 + 4\frac{a_n}{b_n} &= 0, \\
\left(\frac{a_n}{b_n} \right)^2 + 6\frac{a_n}{b_n} + 1 &= 0.
\end{aligned}$$

Poznamenejme, že $b_n \neq 0$. Tato kvadratická rovnice má kořen nad $\mathbb{F}_q$, právě pokud 2 je v $\mathbb{F}_q$ čtvercem. Pro tělesa, kde $\phi_q(2) = -1$, proto můžeme AH posloupnost uvažovat v „plném rozsahu“, my se zaměříme na tělesa $\mathbb{F}_q$ s $q \equiv \pm 3 \pmod 8$.

PRIKLAD

Na příkladu vidíme, že při vizualizaci AH posloupnosti získáme krom medúz i vulkány hloubky 2.

Lemma 4.1.2. *Vrchol $(a, b) \in AH_{\mathbb{F}_q}$ má předchůdce, právě pokud platí $\phi_q(a^2 - ab) = 1$.*

Důkaz. Nejprve předpokládejme (a, b) má předchůdce (c, d), platí tedy:

$$a = \frac{c+d}{2}, \quad b = \frac{2cd}{c+d}.$$

Potom:

$$a(a-b) = \frac{c+d}{2}\left(\frac{c+d}{2} - \frac{2cd}{c+d}\right) = \left(\frac{c-d}{2}\right)^2$$

je čtverec. Naopak ať $a(a-b)$ je čtverec a x je nějaká jeho odmocnina. Pak uvažme vrchol $(a-x, a+x)$, jeho následník je:

$$\left(\frac{a-x+a+x}{2}, \frac{2(a-x)(a+x)}{a-x+a+x}\right) = (a, b)\,.$$

□

Toto tvrzení je velmi zajímavé tím, jak nám rozdělí práci pro případy, kdy q dává zbytek 3 a 5 po dělení osmi. Pokud se totiž podíváme na čísla, která udávají, kdy vrcholy (a, b) a (b, a) mají předchůdce - $a(a-b)$ a $b(b-a)$ - tak jejich součin je:

$$-ab(a-b)^2.$$

V případě $q \equiv 3 \pmod 8$ není -1 v $\mathbb{F}_q$ čtvercem a proto a, b s $\phi_q(ab) = 1$ má právě jeden z vrcholů (a, b), (b, a) předchůdce. Pokud ab není čtverec, tak buď oba vrcholy mají předchůdce, nebo ani jeden. Samozřejmě pro $q \equiv 5$ je tato situace prohozena. Toto rozdělení nám též pomůže odhalit, proč některé grafy jsou medúzy a jiné jsou vulkány větší hloubky.

Věta 4.1.3. *Graf $AH_{\mathbb{F}_q}$ je tvořen z několika samostatných vrcholů, medúz a vulkánů hloubky* 2*.*

Důkaz. Uvažujme bez újmy na obecnosti $q \equiv 3 \pmod 8$, tedy $\phi_q(-1) = -1$, případ $q \equiv 5 \pmod 8$ je analogicky, pouze se prohodí role vrcholů (a, b) s $\phi_q(ab) = 1$ a $\phi_q(ab) = -1$. Ukážeme, že vrcholy (a, b), pro které není součin ab čtvercem, tvoří medúzy, a pokud $\phi_q(ab) = 1$, tak tvoří vulkány hloubky 2.

K tomu užijeme právě fakt, který jsme naznačili výše, že pokud ab je čtverec, tak právě jeden z vrcholů (a, b) a (b, a) má předchůdce. Jako v případě AG posloupnosti tedy vyberme libovolný vrchol (a, b), $a \neq b$, a hledejme další členy posloupnosti $(a_1, b_1), (a_2, b_2), \ldots$, dokud nedojdeme do cyklu. Ať (c, d) je členem cyklu a jeho předchůdci jsou vrcholy (C, D), (D, C). Víme, že jeden z těchto dvou nemá předchůdce a ten druhý proto musí být členem cyklu. Graf je tedy medúzou.

Nyní přijde ta zajímavější část, tedy že pokud ab čtvercem není, tak náš graf je tvořen vulkány.

??? connection s AG??? Nemůže tomu ale tak být, protože na příkladech v ?? jsme si ukázali, že medúza může obsahovat mnohem více, než kp prvků. Tentokrát je ale každá medúza ohraničena jednoduchým invariantem - součinem čísel ve dvojici.

Lemma 4.1.4. *Uvažme graf $AH_{\mathbb{F}_q}$ a nějakou jeho souvislou komponentu V. Pro libovolnou dvojici $(a, b) \in V$ je ab fixní.*

Důkaz. Stačí nám ukázat, že pro vrchol (a, b) a jeho následníka platí $a_1 b_1 = ab$, jelikož (a_1, b_1) má právě dva předchůdce, (a, b) a (b, a). A opravdu:

$$a_1 \cdot b_1 = \frac{a+b}{2} \cdot \frac{2ab}{a+b} = ab.$$

□

Důsledek 4.1.5. *Každá souvislá komponenta v grafu $AH_{\mathbb{F}_q}$ obsahuje nejvýše $q-1$ vrcholů.*

Důkaz. Pro dané $k \in \mathbb{F}_q$ je nad $\mathbb{F}_q$ jistě $q-1$ dvojic se součinem k, konkrétně $\left(a, \frac{k}{a}\right)$ pro $a \in \mathbb{F}_q^\times$. Podle předchozího lemmatu mají všechny prvky jedné souvislé komponenty stejný součin prvků, je jich proto nejvýše $q-1$. □

Poznamenejme, že z těchto $q-1$ prvků ne nutně všechny vyhovují, podívejme se na těleso $\mathbb{F}_{11}$. Pro součin roven čtyřem se jistě nezaobíráme dvojicí $(2, 2)$, též ale pro součin 10 nepočítáme dvojici $(1, 10)$, jejíž součet je nulový.

Zde získáme další rozdíl s AG posloupností. Každá souvislá komponenta nemá více, než q vrcholů, zatímco na příkladu ? vidíme, že některé komponenty grafu AG mohou mít mnohokrát více.

Kapitola 5

Tři? náhledy na AH posloupnost

V procesu studia AH posloupnosti jsem se pokusil propojit tuto posloupnost s teorií obklopující eliptické křivky, podobně jako autoři původního článku ? udělali s AG posloupností. Našel jsem hned dvě různá propojení, jedno osvětlující strukturu grafů a druhé, které nám trochu usnadní úvahy o velikostech těchto grafu.

5.1 Dynamické systémy

AH posloupnost se od dvou, které jsme studovali před chvílí, liší tím, že nemusíme nijak svévolně vybírat tu „správnou“ odmocninu. Tato posloupnost je tím mnohem jednodušeji studovatelná, protože je udaná zobrazeními, která jsou pouze lomenými funkcemi.

V AH posloupnosti zobrazíme prvek $(x, 1)$ na $\left(\frac{x+1}{2}, \frac{2x}{x+1}\right)$. Jaké poznatky můžeme vytěžit, kdybychom i tento prvek znovu normalizovali na $\left(\frac{(x+1)^2}{4x}, 1\right)$? Poté se zabýváme iterací zobrazení:

$$x \longmapsto \frac{(x+1)^2}{4x}$$

a jejím chováním na $\mathbb{F}_q$. Toto je přesně úkolem oblasti matematiky studující *dynamické systémy* lomených funkcí nad konečnými tělesy.

Dynamické systémy byly přes poslední dekády hojně zkoumány, i přesto se o nich ví poměrně málo. Přehledový článek z roku 2013 [?] dává do kontextu, kolik jejich struktury je nám zatím neznámo, dokonce i pouhé očekávané chování dynamického systému.

Obecný kecy.

Pohled dynamických systémů nám pomůže najít největší cyklus, na který můžeme narazit.

–říct, že cyklus v AH je ekvivalentně s cyklem Dynamic system–

Rovnice:

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

s parametrem a má nad $\mathbb{F}_q$ řešení, právě pokud diskriminant výsledné kvadratické rovnice $x^2 + (2-4a)x + 1 = 0$, tedy $4(1-a)^2 - 4 = 4a(a-1)$, je nad $\mathbb{F}_q$ čtvercem.

???

Věta 5.1.1. *Počet $a \in \mathbb{F}_q \setminus \{?\}$ takových, že $\phi_q(a^2 - a) = 1$ je $\frac{q-(-1)^{(q+1)/4}}{4}$.*

Důkaz. Určíme součet:

$$\sum_a \phi_q(a(a-1)) = \sum_a \phi_q(a)\phi_q(a-1).$$

Protože pro libovolné $a \neq 1$ platí $\phi_q(a-1)^2 = 1$, tak díky multiplikativitě ϕ_q máme $\phi_q(a-1) = \phi_q(a-1)^{-1}$. Tím získáme:

$$\begin{aligned}\sum_a \phi_q(a)\phi_q(a-1) &= \sum_a \phi_q(a)\phi_q(a-1)^{-1} \\ &= \sum_a \phi_q\left(\frac{a}{a-1}\right).\end{aligned}$$

Nyní přejdeme na proměnnou $x = \frac{a}{a-1}$, které splňuje $a = \frac{x}{x-1}$. Pro každé $x \notin \{\}$ existuje $a \notin \{\}$, takže blabla ok.

Jelikož Legendreho symbol nabývá pouze hodnot $0, 1$ a -1, přičemž v našem součtu figuruje ? sčítanců, z nich dva nulové. To znamená, že právě ? z nich je rovno jedné, což jsme chtěli. □

Poznámka. Tento součet a ostatně i trik, kde podělíme výraz $\phi_q(a-1)^2$, je inspirován teorií obklopující tzv. *Jacobiho sumy* multiplikativních charakterů nad $\mathbb{F}_q$. Konkrétně součet $\sum \phi_q(a(a-1))$ je roven $\phi_q(-1)\sum \phi_q(a)\phi_q(1-a)$, což je Jacobiho suma $\phi_q(-1)J(\phi_q, \phi_q)$. Tyto sumy jsou intimně spojené s počtem řešení rovnic typu $a_1x_1^{b_1} + \cdots + a_nx_n^{b_n} = k$ nad konečnými tělesy. Pro excelentní, byť mírně pokročilý, úvod do jejich studia doporučuji [IR].

Důsledek 5.1.2. *Každý cyklus, který udává dynamika $\frac{(x+1)^2}{4x}$, má délku nejvýše $\frac{q-1}{4}$.*

Důkaz. □

Jak moc je tento odhad těsný? Pokud si spočítáme poměr p a největšího cyklu, který nalezneme nad $\mathbb{F}_p$, tak získáme následující data: -obrázek-

Vidíme tedy, že poměrně mnoho prvočísel dosahuje této maximální délky cyklu, další trendy se poté drží u podílů $1/5, 1/6$ a poté většina prvočísel spadá pod podíl $1/12$. (vysvětlení?)

5.2 Isogenie?

Mé další pokusy o studování AH posloupnosti vedly opět směrem eliptických křivek, v tom, co následuje, jsem se pokusil napodobit postup autorů původního článku [] a aplikovat jej i pro tuto posloupnost.

5.3 Montgomeryho křivky

Vulkány isogenií ale zcela nekončí spojení této posloupnosti s eliptickými křivkami. Pro tuto sekci proto sledujme trochu pozorněji časovou osu studia dynamických systémů, mnohé z nich vedly směrem isogenií přímo na křivkách, tzv. *endomorfismů*.

Vraťme se hned čtyři dekády nazpět, kdy Miller a Koblitz stáli u zrodu kryptografie pomocí eliptických křivek. Pro strukturovanější úvod do studia šifrování pomocí eliptických křivek a konkrétněji isogenií opět skromně doporučuji konzultovat mou práci []. Při studiu šifrování ryze nad eliptickými křivkami, tedy se zabýváme pouze skalárními isogeniemi $[n]P$, hledáme křivky, které obzvláště elegantní vzorce pro násobení, zpravidla hledáme jednoduché vzorce pro $[2]P$ a $[3]P$. Právě Neal Koblitz zjistil, že pro eliptickou křivku (ne ve Weiestrassově tvaru):

$$E : y^2 + xy = x^3 + 1$$

nad konečným tělesem charakteristiky 2 mají body velmi pěkné dvojnásobky:

?

Mohou nám však pomoci studovat i dynamiku funkce $x + \frac{1}{x}$ nad tělesy $\mathbb{F}_{2^n}$. V [?] je totiž ukázáno, že pro bod $P = (x, y) \in E$ a $\pi : (x, y) \longmapsto (x^2, y^2)$ Frobeniův automorfismus platí:

$$P + \pi(P) = \left(x + \frac{1}{x}, \quad x^2 + y + 1 + \frac{1}{x^2} + \frac{y}{x^2} \right).$$

Pokud se tedy zaobíráme čistě x-ovou souřadnicí, endomorfismus $1 + \pi$ zobrazí x na prvek $x + \frac{1}{x}$.

Kapitola 6

Eliptické křivky

It is possible to write endlessly on elliptic curves (This is not a threat.)

Serge Lang

V naší první kapitole se budeme procházet světem isogenií eliptických křivek a učit se s nimi pracovat. Kořeny této teorie sahají hluboko do algebraické geometrie, pro porozumění této kapitoly její znalost ale nevyžadujeme, čtenář si bohatě vystačí se znalostmi abstraktní algebry, viz například [63]. Budeme postupovat volně dle [75], nicméně další vhodný úvodní materiál se nachází na [20]. Ne vždy budeme uvádět důkazy tvrzení, neboť jsou mnohdy příliš pokročilé či technické, v takových případech se odkážeme na relevantní literaturu.

6.1 Základy

Po celou dobu budeme pracovat nad projektivním prostorem nad uzávěrem tělesa K, což je zjednodušeně řečeno množina bodů v $\overline{K}^n$, kde dva body považujeme za ekvivalentní, pokud leží v přímce s počátkem, můžeme proto místo jednotlivých bodů pracovat s přímkami procházejícími skrz počátek.

Definice 6.1.1. Buďte K těleso a n přirozené číslo. *Projektivní prostor* $\mathbb{P}^n(\overline{K})$ definujeme jako množinu tříd nenulových vektorů $(a_0, \ldots, a_n) \in \overline{K}^{n+1}$ s relací ekvivalence $(a_0, \ldots, a_n) \sim (b_0, \ldots, b_n)$, pokud existuje $\lambda \in \overline{K}$, že $(a_0, \ldots, a_n) = \lambda(b_0, \ldots, b_n)$. Tyto třídy ekvivalence budeme značit $(a_0 : \cdots : a_n)$ a nazývat *body*.

Představme si v $\mathbb{R}^3$ množinu M všech přímek procházejících počátkem a množinu N všech rovin procházejících počátkem. Každé dvě různé přímky z M určují jedinou rovinu z N a naopak každé dvě různé roviny se protínají v jedné přímce z M. Nyní uvažme rovinu například $z = 1$, každá přímka z M, která s ní není rovnoběžná, ji protíná v jednom bodě a každá rovina z N, která s ní není rovnoběžná, ji protíná v jedné přímce. Abychom každé přímce přiřadili právě jeden bod, můžeme v každém směru přiřadit rovnoběžným přímkám bod v nekonečnu v příslušném směru. Body dané průsečíky přímek z M s rovinou $z = 1$, i v případě průsečíku v nekonečnu, tvoří tzv. *projektivní rovinu* $\mathbb{P}^2(\mathbb{R})$,

Poznámka. Je zajímavé uvážit souvislosti projektivních prostorů a barycentrických souřadnic, kde je každý bod vyjádřen jako vážený průměr vrcholů referenčního simplexu. Tyto souřadnice jsou též homogenní a každé dvě přímky se protínají, byť některé v nekonečnu, takové body mají součet vah roven 0. Můžeme o barycentrických souřadnicích tedy přemýšlet jako o projektivním prostoru s jiným základem.

Připomeňme si pak definici eliptické křivky. Čtenář je možná obeznámen s *Weierstrassovým tvarem* eliptické křivky $y^2 = x^3 + ax + b$ pro $x, y \in K$, ten však nekreslí celou situaci. Často se eliptické křivky definují jako nesingulární projektivní křivky genu 1 v $\overline{K}^3$, tj. jako množinu bodů $(X : Y : Z)$ splňujících:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

s koeficienty $a_i \in K$. Pro naše účely si definici zúžíme a práci podstatně zjednodušíme. Konkrétně se budeme pohybovat nad tělesy, jejichž charakteristika není 2 ani 3. Tato tělesa často nabízí praktické výhody, my je však vynecháme. Nejprve totiž můžeme substitucí $Y \mapsto Y - \frac{a_1X + a_3Z}{2}$ zapsat naši křivku jako:

$$Y^2Z - \left(\frac{a_1X + a_3Z}{2}\right)^2 Z = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$
$$Y^2Z = X^3 + \frac{b_2}{4}X^2Z + \frac{b_4}{2}XZ^2 + \frac{b_6}{4}Z^3,$$

kde $b_2 = a_1^2 + 4a_2, b_4 = a_1a_3 + 2a_4$ a $b_6 = a_3^2 + 4a_6$. Substituce $X \mapsto X - \frac{b_2}{12}Z$ dále zjednodušuje tvar křivky:

$$Y^2Z = \left(X - \frac{b_2}{12}Z\right)^3 + \frac{b_2}{4}\left(X - \frac{b_2}{12}Z\right)^2 Z + \frac{b_4}{2}\left(X - \frac{b_2}{12}Z\right)Z^2 + \frac{b_6}{4}Z^3,$$
$$Y^2Z = X^3 + \left(\frac{24b_4 - b_2^2}{48}\right)XZ^2 + \left(\frac{b_2^2 + 216b_6 - 36b_2b_4}{864}\right)Z^3.$$

Naši křivku proto můžeme zapsat ve tvaru:

$$Y^2Z = X^3 + aXZ^2 + bZ^3,$$

kde $a, b \in K$. Libovolná taková rovnice udává eliptickou křivku za podmínky, že takzvaný *diskriminant* této křivky, $4a^3 + 27b^2$, je nenulový. Tato skutečnost je ekvivalentní s faktem, že eliptická křivka je nesingulární, přičemž lineární transformace proměnných zachovají (ne)singularitu křivky. Geometricky lze tuto podmínku interpretovat tak, že křivka sama sebe neprotíná, tedy nemá „hrot“.

Definice 6.1.2. Mějme K těleso charakteristiky různé od 2 a 3. Pro $a, b \in K$ taková, že $4a^2 + 27b^3 \neq 0$, definujeme v $\mathbb{P}^2(\overline{K})$ *eliptickou křivku* jako množinu bodů $(X : Y : Z) \in \overline{K}^3$ splňující:

$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

Značení 6.1.3. Pokud všechny koeficienty eliptické křivky E náleží do tělesa K, značíme ji E/K.

Průsečíky naší křivky s přímkou $Z = 0$ nutně mají i X-ovou souřadnici nulovou, všechny jsou proto reprezentovány třídou $(0 : 1 : 0)$. V opačném případě můžeme přejít na proměnné $x := X/Z, y := Y/Z$, tedy bod $(x : y : 1)$, čímž získáme křivku ve známém *afinním*, v literatuře často uváděném i jako Weierstrassově, tvaru:

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

Množina bodů na naší křivce tedy sestává z bodů $(x, y) \in K^2$ na naší afinní křivce spolu s bodem v nekonečnu $\mathcal{O} = (0 : 1 : 0)$, jenž je exklusivní její projektivní variantě.

Značení 6.1.4. Množinu všech bodů E se souřadnicemi nad K (společně s $\mathcal{O}$) budeme značit $E(K)$ a pokud K je konečné těleso, počet prvků $E(K)$ budeme značit $\#E(K)$.

Počet bodů na E nad konečným tělesem $\mathbb{F}_q$ je shora ohraničen číslem $2q+1$, protože pro každé $x \in \mathbb{F}_q$ existují v $\mathbb{F}_q$ nejvýše 2 odmocniny z x^3+ax+b, a poslední bod do počtu je $\mathcal{O}$. V $\mathbb{F}_q$ leží právě $\frac{q+1}{2}$ čtverců, tudíž za předpokladu, že $x^3 + ax + b$ pokrývá $\mathbb{F}_q$ rovnoměrně, bychom na E očekávali okolo q bodů, společně s bodem v nekonečnu $q + 1$. Roku 1933 tento odhad Helmut Hasse dokázal, tedy skutečně se $\#E(\mathbb{F}_q)$ nepříliš liší od $q + 1$.

Věta 6.1.5. *(Hasse) Nechť $E/\mathbb{F}_q$ je eliptická křivka. Pak:*

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

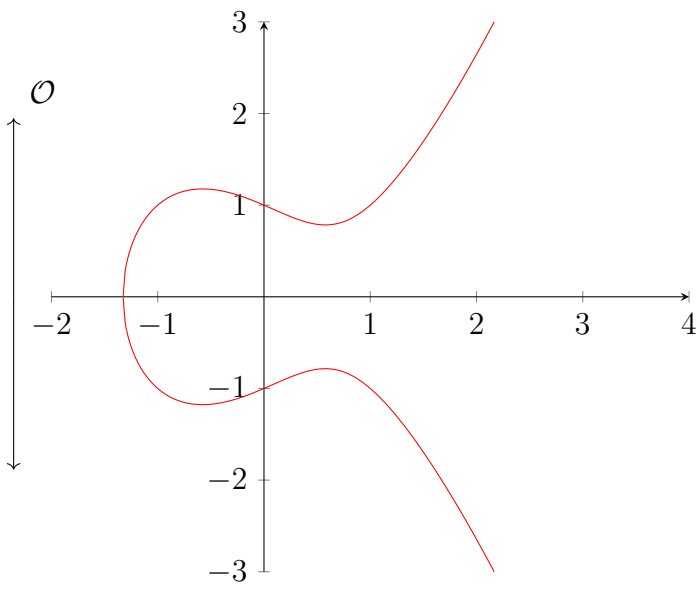
Důkaz je k nalezení v [69, Thm. V.1.1]. Již zde, ještě na začátku naší poutě, musíme a priori brát jako platný jeden z nejdůležitějších výsledků ohledně eliptických křivek, ne však bez důvodu. Většina učebních textu jej dokáže v průběhu studia algebraické geometrie, v našem případě bychom potřebovali udělat poměrně velkou odbočku. Na naší cestě se přesto setkáme s místy, kde uvidíme taký či onaký způsob pohledu na problém poskytující řešení.

Všimněme si, že rozlišujeme body na eliptické křivce definované nad daným tělesem. Jako body na samotné křivce E/K nebudeme, jak by se na první pohled mohlo zdát, brát pouze body definované nad K, nýbrž nad celým uzávěrem, abychom zachytili celou její strukturu.

Značení 6.1.6. Pod bodem $P \in E$ rozumíme $P = (x, y) \in E(\overline{K})$.

Podívejme se nyní na eliptickou křivku E geometricky, tedy v rovině vyznačme všechny body, které na ní leží. Je zjevné, že E je symetrická podle osy x, definujme proto k $P \in E$ opačný bod $-P \in E$ jako obraz P podle osy x. Pokud bychom na bodech naší křivky definovali součet, přirozeně bychom chtěli, aby součet P a $-P$ byl $\mathcal{O}$.

Řekneme-li, že tečna k E ji protíná ve dvou identických bodech, pak každá přímka protíná E v právě třech bodech včetně multiplicity. Průsečíky lineární rovnice s kubickou křivkou budou i s případným bodem v nekonečnu tři. Speciálně tečna v bodě s $y = 0$ tento bod



Obrázek 6.1: Eliptická křivka $y^2 = x^3 - x + 1$ nad $\mathbb{R}$.

protíná dvakrát a ten třetí je bod v nekonečnu E. Přichází tedy na mysl definice součtu na E taková, že součet každých tří bodů v přímce je $\mathcal{O}$. Pokud přímka procházející $P, Q \in E$ protíná E potřetí v R, definujeme tedy $P + Q = -R$. Pro součet bodů $P, Q \in E$ můžeme poté odvodit několik klíčových vlastností:

(i) $P + Q = Q + P$,

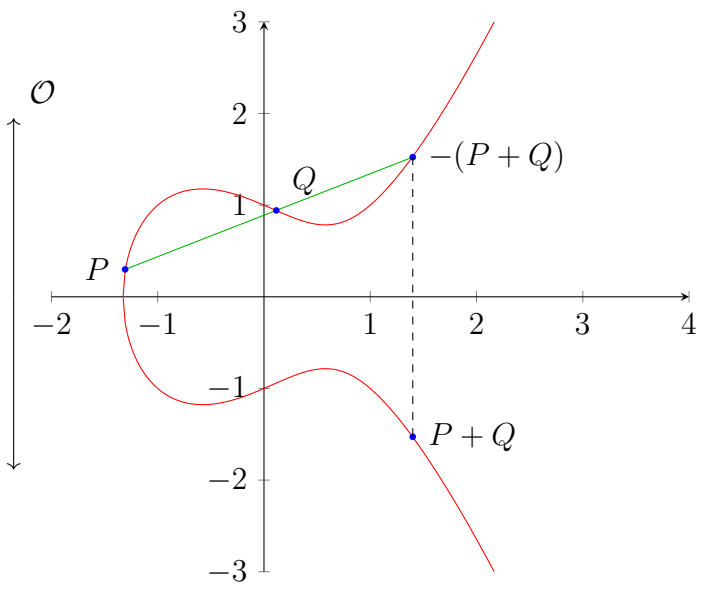
(ii) $(P + Q) + R = P + (Q + R)$,

(iii) $P + \mathcal{O} = P$,

(iv) $P + (-P) = \mathcal{O}$.

Rovnosti (i),(iii) a (iv) jsou dle naší definice sčítání intuitivně jasné, potíže však nastanou s bodem (ii), který je notoricky obtížné dokázat. Jeho klasický důkaz užívá pokročilejších metod algebraické geometrie, konkrétně Riemann-Rochovu větu, či větu Cayley-Bacharacha, která u dvou kubických křivek protínajících se v 9 bodech zaručuje, že každá jiná kubická křivka procházející osmi z nich obsahuje i ten poslední. Tato poslední věta má aplikace i mimo eliptické křivky, klasické výsledky projektivní geometrie jako Pappova či Pascalova věta z ní totiž snadno plynou. Poměrně elementární, byť výpočetně zdlouhavý důkaz Cayley-Bacharovy věty i jejích zmíněných důsledků se dá najít v [79, Sec. 2.3].

Při takto definovaném součtu můžeme s body na E pracovat jako s abelovskou grupou se sčítáním $+$ a neutrálním prvkem $\mathcal{O}$. Samozřejmě součet dvou bodů dokážeme za pomocí analytické geometrie přímo spočíst. Přímka procházející dvěma různými body $P = (x_1, y_1)$



Obrázek 6.2: Sčítání na eliptické křivce.

a $Q = (x_2, y_2)$ v rovině je daná rovnicí $y = \frac{y_2 - y_1}{x_2 - x_1}(x - x_1) + y_1$. Známe-li dva průsečíky této přímky s E, tedy P a Q, dosazením do rovnice E jsme schopni spočíst jejich třetí průsečík, bod $-(P + Q)$.

Jediné, co nám chybí ke spokojenosti, je najít dvojnásobek bodu P, omezme se na případ P neležící na ose x. Tečna k E v bodě P je přímka PQ, když se Q limitně blíží k P. Sklon této přímky je tedy dán implicitní derivací $y^2 = x^3 + ax + b$ v bodě $P = (x_1, y_1)$, tedy $2y_1y' = 3x_1^2 + a$. Tečna k E v P je pak určena vztahem $2y_1(y - y_1) = (3x_1^2 + a)(x - x_1)$. Z této rovnosti vyjádříme y a dosadíme do rovnice přímky E, kde je x_1 dvojnásobný kořen. Můžeme proto vyfaktorizovat člen $(x - x_1)^2$ a jako třetí lineární člen získat řešení pro $-(P + P)$.

Předchozí úvahy shrnuje následující tvrzení:

Věta 6.1.7. *Buďte $P = (x_1, y_1), Q = (x_2, y_2)$ afinní body na křivce $E : y^2 = x^3 + ax + b$, přičemž $P \neq -Q$. Pak $P + Q = (x_3, y_3)$ je daný:*

$$x_3 = \lambda^2 - x_1 - x_2,$$
$$y_3 = -\lambda x_3 - y_1 + \lambda x_1,$$

kde:

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{pokud } x_1 \neq x_2, \\ \frac{3x_1^2 + a}{2y_1}, & \text{pokud } x_1 = x_2. \end{cases}$$

Úplný výpočet neuvádíme. Je možné dokázat asociativitu sčítání i tím, že pro body $P = (x_1, y_1), Q = (x_2, y_2)$ a $R = (x_3, y_3)$ spočteme bod $(P + Q) + R$ a ukážeme, že

je symetrický ve dvojicích (x_1, x_3) a (y_1, y_3), případně že je přímo roven $P + (Q + R)$. Tyto výpočty nejsou prakticky proveditelné bez výpočetních přístrojů, nicméně za pomocí například programu Wolfram Mathematica se můžeme přesvědčit, že asociativita platí.

Pro zkrácení zápisu píšeme skalární násobky bodů, jinak řečeno $P + \cdots + P$, následovně:

Definice 6.1.8. Mějme bod $P \in E$. Pak pro n přirozené definujeme jeho n-násobek:

$$[n]_E P = \underbrace{P + \cdots + P}_{n},$$

přičemž definujeme $[0]_E P = \mathcal{O}$ a pro $n < 0 : [n]_E P = [-n]_E(-P)$.

Díky asociativitě sčítání je bod $[n]_E P$ dobře definovaný. Pokud bude z kontextu jasná eliptická křivka, nad kterou pracujeme, budeme značit násobení skalárem pouze $[n]P$. Pojďme se pokusit n-násobek bodu spočíst co nejrychleji, zjevně se stačí omezit na případ $n > 0$.

Naivní postup výpočtu $[n]P$ jímá $n - 1$ sčítání, to jistě dokážeme vylepšit. Analogickým postupem jako při rychlém umocňování využijeme zápis n v binární soustavě. Inicializujeme $Q = \mathcal{O}$ a v k-tém kroku si budeme pamatovat bod $[2^k]P$, který ke Q přičteme jen pokud k-tý bit v binárním zápisu n je 1, přičemž postupujeme od nejméně významného bitu. Spočteme si pak $[2][2^k]P = [2^{k+1}]P$ a celý proces opakujeme znovu.

Příklad 6.1.9. Spočtěme padesátinásobek nějakého bodu P. Binární zápis 50 je 110010. Počítejme pak:

$$\begin{array}{lccccccccccc}
 & \mathcal{O} & \longrightarrow & P & \longrightarrow & [2]P & \longrightarrow & [4]P & \longrightarrow & [8]P & \longrightarrow & [16]P & \longrightarrow & [32]P \\
Q: & \mathcal{O} & \longrightarrow & \mathcal{O} & \longrightarrow & [2]P & \longrightarrow & [2]P & \longrightarrow & [2]P & \longrightarrow & [18]P & \longrightarrow & [50]P \\
 & & & & & +[2]P & & & & & & +[16]P & & +[32]P
\end{array}$$

Užijeme tedy pouze 10 operací sčítání.

Dohromady při výpočtu užijeme nejvýše $\lfloor \log_2(n) \rfloor - 1 \leqslant \log_2(n) - 1$ operací sčítání i dvojnásobení. Dvojnásobek prvků spočteme alespoň tak rychle jako součet dvou bodů, tedy tímto postupem spočteme $[n]P$ v nejvýše $2(\log_2(n) - 1)$ sčítáních.

Příklad 6.1.10. Určeme dvojnásobek bodu $P = (x, y)$ na $E : y^2 = x^3 + ax + b$. V duchu značení věty 6.1.7 máme pro $[2]P = (x_1, y_1)$:

$$x_1 = \lambda^2 - 2x = \frac{(3x^2 + a)^2 - 8y^2 x}{4y^2} = \frac{(3x^2 + a)^2 - 8(x^3 + ax + b)x}{4(x^3 + ax + b)} = \frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3 + ax + b)},$$

$$y_1 = -\lambda x_1 - y + \lambda x = \frac{(3x^2 + a)[-(3x^2 + a)^2 + 12y^2 x] - 8y^4}{8y^4} y$$

$$= \frac{(3x^2+a)[-(3x^2+a)^2+12(x^3+ax+b)x]-8(x^3+ax+b)^2}{8(x^3+ax+b)^2}y$$
$$= \frac{x^6+5ax^4+20bx^3-5a^2x^2-4abx-a^3-8b^2}{8(x^3+ax+b)^2}y.$$

Všimněme si, že pro $P=(x,y)$ na eliptické křivce s $y=0$ je $[2]P=\mathcal{O}$. Pro bod $Q=(6,27):=(x_0,y_0)$ na křivce:

$$y^2=x^3+54x+189$$

nad $\mathbb{Q}$ zase ověříme, že platí:

$$x_0^6+5ax_0^4+20bx_0^3-5a^2x_0^2-4abx_0-a^3-8b^2=0,$$

tedy $[4]Q=\mathcal{O}$. Obecně by nás mohlo zajímat, které body zobrazí násobení n do nekonečna.

Definice 6.1.11. Buď n celé číslo. O množině všech $P\in E$, že $[n]P=\mathcal{O}$, řekneme, že tvoří *n-torzi* na E, a tuto množinu budeme značit $E[n]$.

Definice 6.1.12. Buď P bod na E. Pokud n je nejmenší kladné číslo, že $[n]P=\mathcal{O}$, nazveme n *řádem* P. Pokud takové n neexistuje, tak řekneme, že P má nekonečný řád.

Torze na eliptické křivce E tvoří podgrupu $E(\overline{K})$, neboť pokud $[n]P=\mathcal{O}=[n]Q$, tak $[n](P+Q)=[n]P+[n]Q=\mathcal{O}$. Torzní grupy nám pomáhají hlouběji studovat eliptické křivky v mnohých směrech. Zprvu si můžeme všimnout, že $E(\overline{\mathbb{F}_q})$ je sjednocením všech torzních grup, tedy že každý bod má konečný řád.

Věta 6.1.13. *Každý bod P na eliptické křivce E nad konečným tělesem má konečný řád.*

Důkaz. Mějme bod $P\in E(\overline{\mathbb{F}_q})$. Bod P leží v konečném rozšíření $E(\mathbb{F}_q)$, neboli pro nějaké přirozené k platí $P\in E\left(\mathbb{F}_{q^k}\right)$. V konečné grupě má každý prvek konečný řád, přičemž neutrální prvek grupy $E\left(\mathbb{F}_{q^k}\right)$ je $\mathcal{O}$, tedy P má na E konečný řád. □

Zatímco $E(\mathbb{F}_q)$ je konečná grupa, množina bodů na racionální křivce $E(\mathbb{Q})$ obecně není a existují na ní i body nekonečného řádu. Příkladem mřížového bodu nekonečného řádu na křivce je bod $(17,70)$ na křivce:

$$E: y^2=x^3-13,$$

tedy jeho násobením můžeme získat nekonečně mnoho racionálních bodů na E. Body nekonečného řádu jsou obecně těžko spočitatelné, nicméně body s řádem konečným dokážeme všechny najít za pomocí věty Lutz-Nagella [79, Thm. 8.7], dle které všechny takové racionální body (x,y) jsou mřížové a buď 2-torzní, či y^2 dělí diskriminant naší křivky.

6.2 Zobrazení mezi eliptickými křivkami

Když studujeme algebraické struktury, často nás zajímají zobrazení mezi nimi. Násobení bodů na E skalárem určuje homomorfismus grup $E(\overline{K}) \longrightarrow E(\overline{K})$, definuje proto endomorfismus na $E(\overline{K})$ daný lomenou funkcí nad K. Nyní se trochu obecněji podíváme na zobrazení mezi jednotlivými eliptickými křivkami, opět homomorfismy grup $E_1(\overline{K}) \longrightarrow E_2(\overline{K})$.

Nejprve studujme zobrazení invertibilní, tedy lineární změny souřadnic x, y. Pokud zobrazení $(x, y) \mapsto (ax + by + c, dx + ey + f)$ převádí eliptické křivky ve Weierstrassově tvaru, snadno porovnáním koeficientů, například xy a x^2y, dojdeme k nulovosti členů b, c, d i f. Následně, aby členy při y^2 i x^3 byly po krácení oba rovny jedné, musí být $a = u^2, b = u^3$ pro nějaké nenulové číslo $u \in \overline{K}$. Taková zobrazení, $(x, y) \mapsto (u^2x, u^3y)$, převádí křivky:

$$E_1 : y^2 = x^3 + u^4ax + u^6b \quad \longrightarrow \quad E_2 : y^2 = x^3 + ax + b$$

pro nenulové $u \in \overline{K}$. Jako lineární zobrazení mezi $E_1(\overline{K})$ a $E_2(\overline{K})$ jistě naše zobrazení zachovává přímky a tedy i součet bodů na našich křivkách, definuje proto homomorfismus z $E_1(\overline{K})$ do $E_2(\overline{K})$. Díky jeho invertibilitě definuje mezi těmito grupami dokonce isomorfismus.

Definice 6.2.1. Buďte $E_1/K : y^2 = x^3 + ax + b, E_2/K : y^2 = x^3 + cx + d$ eliptické křivky. Pak řekneme, že E_1 a E_2 jsou isomorfní, pokud existují $u \in \overline{K}$ splňující $a = u^4c$ a $b = u^6d$.

Isomorfismy nemusí nutně být definované K, ale nad jeho rozšířením. Aby byl nad $\overline{K}$ definovaný, musí být díky předpisu $(x, y) \mapsto (u^2x, u^3y)$ psán nad rozšířením K stupně dělícího 12.

Definice 6.2.2. Buďte E, E' křivky isomorfní nad rozšířením K, ale ne nad K. Pak řekneme, že E' je *twistem* E nad K.

Zobrazení z $E : y^2 = x^3 + ax + b$ dané $(x, y) \mapsto \left(\frac{x}{d}, \frac{y}{\sqrt{d^3}}\right)$ pro $\sqrt{d} \notin K, d \in K$, nám dává isomorfismus do:

$$E_d : y^2 = x^3 + d^2ax + d^3b,$$

avšak ne nad K, ale nad jeho kvadratickým rozšířením $K(\sqrt{d})$. Křivku E_d nazveme *kvadratickým twistem* E.

Pro křivky s $a = 0$, resp. $b = 0$, můžeme analogicky najít *kubický* a *sextický*, resp. *kvartický* twist:

$$\begin{aligned} y^2 = x^3 + b \quad &\longrightarrow \quad y^2 = x^3 + d^2b, \\ y^2 = x^3 + b \quad &\longrightarrow \quad y^2 = x^3 + db, \\ y^2 = x^3 + ax \quad &\longrightarrow \quad y^2 = x^3 + dax, \end{aligned}$$

dané po řadě $(x, y) \mapsto \left(\frac{x}{\sqrt[3]{d^2}}, \frac{y}{d}\right)$ a $(x, y) \mapsto \left(\frac{x}{\sqrt[3]{d}}, \frac{y}{\sqrt{d}}\right)$, resp. $(x, y) \mapsto \left(\frac{x}{\sqrt{d}}, \frac{y}{\sqrt[4]{d^3}}\right)$. Vidíme, že poslední dvě zmíněné křivky jsou navíc kvadratickými twisty po řadě kubického a kvadratického twistu E.

Chtěli bychom říci, kdy mezi dvěma eliptickými křivkami existuje isomorfismus, tedy najít nějaký invariant, který isomorfní křivky sdílí. Takovou funkci splňuje právě j-invariant, jehož definice se táhne hluboko do komplexní analýzy.

Definice 6.2.3. Pro eliptickou křivku $E : y^2 = x^3 + ax + b$ definujeme její *j-invariant* jako:

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

Poznamenejme, že ten je vždy nad K definovaný, neboť eliptické křivky mají nenulový diskriminant.

Věta 6.2.4. *Dvě křivky definované nad K jsou isomorfní nad $\overline{K}$, právě pokud mají stejný j-invariant.*

Důkaz. Nejprve předpokládejme, že křivky $E_1 : y^2 = x^3 + a_1x + b_1$ a $E_2 : y^2 = x^3 + a_2x + b_2$ jsou nad $\overline{K}$ isomorfní. Máme pak $a_2 = u^2a_1$ a $b_2 = u^3b_1$ pro nějaké $b \in \overline{K}$. Spočtěme j-invariant obou křivek:

$$j(E_2) = 1728\frac{4u^6a_1^3}{4u^6a_1^3 + 27u^6b_1^2} = 1728\frac{4a_1^3}{4a_1^3 + 27b_1^2} = j(E_1),$$

j-invarianty isomorfních křivek se proto rovnají.

Nyní předpokládejme, že $j(E_1) = j(E_2)$. Počítejme:

$$\begin{aligned} 1728\frac{4a_1^3}{4a_1^3 + 27b_1^2} &= 1728\frac{4a_2^3}{4a_2^3 + 27b_2^2}, \\ a_1^3(4a_2^3 + 27b_2^2) &= a_2^3(4a_1^3 + 27b_1^2), \\ a_1^3b_2^2 &= a_2^3b_1^2. \end{aligned}$$

Pokud by například a_1 bylo nulové, je z nesingularity E_1 nutně b_1 nenulové, tudíž $a_2 = 0$. Proto ani b_2 není rovno nule, tedy pro $u \in \overline{K}$ s $u^3 = \frac{b_1}{b_2}$ máme $(0, b_1) = (0, u^3b_2)$. Analogicky pokud b_i jsou nulová, máme $(a_1, 0) = (u^2a_2, 0)$ pro u s $u^2 = \frac{a_1}{a_2} \in \overline{K}$.

Konečně v případě, že $a_1a_2b_1b_2 \neq 0$, máme $\frac{a_1^3}{a_2^3} = \frac{b_1^2}{b_2^2}$, což je druhou i třetí mocninou, tedy i šestou mocninou nějakého $u \in \overline{K}$. Toto číslo je tak šestou mocninou i všech šestých odmocnin u^6 v $\overline{K}$, pro tato u je tak $\frac{a_1}{a_2}$ rovno u^2 násobeno třetí odmocninou z 1 (ne nutně primitivní) a $\frac{b_1}{b_2}$ rovno u^3 násobeno odmocninou z 1. Pro nějaké z těchto šesti u se obě odmocniny rovnají 1, čili $a_1 = u^2a_2$ a $b_1 = u^3b_2$. □

Poznámka. Čtenáře by mohla zarazit konstanta $1728 = 12^3$, kterou j-invariant násobíme. Koncept j-invariantu se definuje nejen pro eliptické křivky, ale i pro tzv. *mřížky* (lattice), viz [75, Def. 16.2]. j-invariant těchto struktur je spojen s tzv. *Laurentovou expanzí*, která je po násobení 1728 vždy celočíselná, viz [17, Ch. 11]. Poznamenejme též, že Weierstrassův tvar není jediný možný vyjadřující eliptickou křivku, existují rodiny křivek vyjádřitelné v tzv. *Legendreově* či *Edwardsově* tvaru, každá z nich mající svou vlastní formu j-invariantu.

Příklad 6.2.5. Vezměme si následujících pět křivek nad $\mathbb{F}_{101}$:

$$\begin{aligned} E_1 &: y^2 = x^3 + x + 1, \\ E_2 &: y^2 = x^3 + 5x + 23, \\ E_3 &: y^2 = x^3 + x - 1, \\ E_4 &: y^2 = x^3 + 2x, \\ E_5 &: y^2 = x^3 + 2, \end{aligned}$$

a spočtěme si jejich j-invarianty (což jsou čísla v $\mathbb{F}_{101}$):

$$\begin{aligned} j(E_1) &= 1728\frac{4}{31}, \\ j(E_2) &= 1728\frac{4 \cdot 5^3}{4 \cdot 5^3 + 27 \cdot 23^2} = 1728\frac{4 \cdot 24}{4 \cdot 24 + 27 \cdot 24} = 1728\frac{4}{31}, \\ j(E_3) &= 1728\frac{4}{31}, \\ j(E_4) &= 1728, \\ j(E_5) &= 0. \end{aligned}$$

Vidíme, že j-invarianty E_1 a E_2 se shodují, přičemž v $\mathbb{F}_{101}$ se oba rovnají $1728 \cdot 4 \cdot 88$, nutně mezi nimi nad $\overline{\mathbb{F}}_{101}$ existuje isomorfismus. Snadno ověříme, že zobrazení:

$$(x, y) \longmapsto (3^2x, 3^3y) = (9x, 27y)$$

převádí:

$$\begin{aligned} y^2 = x^3 + x + 1 \qquad \longrightarrow \qquad 27^2y^2 &= 9^3x^3 + 9x + 1, \\ 22y^2 &= 22x^3 + 9x + 1, \\ 22y^2 &= 22x^3 + 110x + 506, \\ y^2 &= x^3 + 5x + 23. \end{aligned}$$

Inverzní isomorfismus $E_2 \longrightarrow E_1$ je pak daný $(x, y) \mapsto (34^2x, 34^3y) = (45x, 15y)$, neboť multiplikativní inverze 3 v $\mathbb{F}_{101}$ je 34.

Křivka E_3 má stejný j-invariant jako E_1 a E_2, nad $\mathbb{F}_{101}$ mezi nimi a E_3 přesto isomorfismus neexistuje. E_3 je kvadratickým twistem E_1 nad $\mathbb{F}_{101^2} = \mathbb{F}_{101}[i]$, jakožto zobrazení $(x, y) \mapsto \left(\frac{x}{i^2}, \frac{y}{i^3}\right) = (-x, iy)$ převádí:

$$\begin{aligned} y^2 = x^3 + x + 1 \quad \longrightarrow \quad -y^2 &= -x^3 - x + 1, \\ y^2 &= x^3 + x - 1. \end{aligned}$$

Obdobně můžeme najít isomorfismus definovaný nad $\mathbb{F}_{101^2}$ mezi E_1 a E_3.

Dvě speciální hodnoty j-invariantu jsou 0 a 1728, kterých nabývají křivky, které mají po řadě lineární, resp. konstantní člen roven 0. Právě křivky s j-invariantem 0 mají kubický (a sextický) twist, ty s j-invariantem 1728 zase kvartický.

Na propojení twistů křivek a počtu bodů na křivce poukazuje následující věta:

Věta 6.2.6. *Uvažme křivku $E/\mathbb{F}_q : y^2 = x^3 + ax + b$ a $\tilde{E}/\mathbb{F}_q : y^2 = x^3 + g^2ax + g^3b$ její kvadratický twist. Pak $\#E(\mathbb{F}_q) + \#\tilde{E}(\mathbb{F}_q) = 2(q+1)$.*

Důkaz. Jistě je $g \in \mathbb{F}_q^\times$ kvadratický nezbytek. Ukážeme, že každé $x_1 \in \mathbb{F}_q$ přispívá právě dvěma body na obou křivkách. Pokud platí $x_1^3 + ax_1 + b = 0$, číslo x_1 dává po jednom bodu na obou křivkách, $(x_1, 0)$, resp. $(gx_1, 0)$. Pro zbylé body tvrdíme, že je právě jedno z tvrzení pravdivé:

- Existují dva body na $E(\mathbb{F}_q)$ s x-ovou souřadnicí x_1,
- Existují dva body na $\tilde{E}(\mathbb{F}_q)$ s x-ovou souřadnicí gx_1.

Druhá odrážka je ekvivalentní s faktem, že:

$$(gx_1)^3 + g^2a(gx_1) + g^3b = g \cdot g^2(x_1^3 + ax_1 + b)$$

je nenulový čtverec. Připomeňme, že součin dvou kvadratických nezbytků je kvadratický zbytek a součin kvadratického zbytku a nezbytku je nezbytek. Protože g není čtverec v $\mathbb{F}_q$, je právě jedno z čísel $x_1^3 + ax_1 + b, g(x_1^3 + ax_1 + b)$ (nenulovým) čtvercem, tedy v $\mathbb{F}_q$ má dvě odmocniny. Afinních bodů na obou křivkách je tak dohromady $2q$. Poslední dva jsou příslušné body v nekonečnu. □

Počet různých j-invariantů v K určuje počet tříd isomorfismů křivek nad $\overline{K}$, případně kterých hodnot j-invariant nikdy nenabude. Jak si nyní ukážeme, tento počet je nejvyšší možný.

Věta 6.2.7. *Pro každé $s \in K$ existuje eliptická křivka E nad K s $j(E) = s$.*

Důkaz. Pro $s \in \{0, 1728\}$ poslouží jako příklady po řadě křivky $y^2 = x^3 + 1, y^2 = x^3 + x$. Pro zbylá $s \in K$ uvažme křivku:

$$E : y^2 = x^3 + 3s(1728 - s)x + 2s(1728 - s)^2.$$

Za předpokladu $\operatorname{char} K \notin \{2, 3\}$ je E vskutku eliptická, můžeme tedy definovat j-invariant. Ten je roven:

$$\begin{aligned} j(E) &= 1728\frac{4[3s(1728-s)]^3}{4[3s(1728-s)]^3 + 27[2s(1728-s)^2]^2} \\ &= 1728s\frac{4 \cdot 27s^2(1728-s)^3}{4 \cdot 27s^2(1728-s)^3(s+1728-s)} = \frac{1728}{1728}s = s. \end{aligned}$$

Křivka E proto má j-invariant roven s. □

Věta 6.2.8. *Pro každé $s \in \overline{K}$ existuje eliptická křivka E nad $K(s)$, že $j(E) = s$.*

Důkaz. Opět si rozmyslíme, že křivka $y^2 = x^3 + 3s(1728-s)x + 2s(1728-s)^2$ je definovaná nad $K(s)$, tedy může posloužit jako řešení. □

Jak násobení bodů E skalárem, tak isomorfismy křivek, jsou homomorfismy bodů křivek nad tělesem K, resp. jeho rozšířením. Spadají tak pod rodinu zobrazení eliptických křivek zvaných *isogenie*, o kterých se budeme dále bavit.

6.3 Isogenie

Podívejme se trochu obecněji na zobrazení mezi křivkami. Hlavní vlastnost, kterou bychom chtěli na takových zobrazeních vynutit, by bylo zachování grupové struktury bodů na křivce. Ukáže se, že taková zobrazení mají několik velmi dobrých vlastností.

Definice 6.3.1. Ať E_1, E_2 jsou eliptické křivky nad tělesem K. Surjektivní homomorfismus grup $\phi : E_1(\overline{K}) \longrightarrow E_2(\overline{K})$ tvaru $\phi : (x : y : z) \longmapsto (u(x,y,z) : v(x,y,z) : w(x,y,z))$ pro polynomy $u, v, w \in K[x]$ nazveme *isogenií*.

Dá se ukázat, viz [37, II.6.8.] a [69, III.4.8.], že nekonstantní zobrazení mezi eliptickými křivkami dané polynomy nad K je surjektivní homomorfismus mezi grupami $E_1(\overline{K}) \longrightarrow E_2(\overline{K})$, definice výše je tedy příliš silná. Zachycuje nicméně všechny důležité vlastnosti, které v isogeniích hledáme.

Isogenie ale můžeme obecně zapsat mnohem kompaktněji:

Věta 6.3.2. *Buďte E_1, E_2 eliptické křivky nad K a $\phi : E_1 \longrightarrow E_2$ isogenie. Pak ji můžeme zapsat ve tvaru:*

$$\phi(x, y) = (u(x), v(x)y)$$

pro u, v lomené funkce nad K.

Důkaz. Víme, že isogenii můžeme vyjádřit jako $\phi : (x, y) \mapsto (u(x, y), v(x, y))$ pro u, v lomené funkce nad K. Z rovnice eliptické křivky $E_1 : y^2 = x^3 + ax + b$ můžeme y v sudé mocnině nahradit polynomem v x, čímž zajistíme, že u i v dokážeme vyjádřit jako funkce r, s, jejichž stupeň v y je nejvýše 1. Speciálně mějme $u(x, y) = \frac{f_1(x)+f_2(x)y}{f_3(x)+f_4(x)y}$ pro $f_i \in K[x]$. Pokud tento zlomek rozšíříme o $f_3(x) - f_4(x)y$, vyruší se nám všechny liché mocniny y ve jmenovateli a sudé dokážeme nahradit polynomem v x. Můžeme proto předpokládat $u(x, y) = \frac{f_1(x)+f_2(x)y}{f_3(x)}$.

Protože ϕ je homomorfismem mezi grupami $E_1(\overline{K}) \longrightarrow E_2(\overline{K})$, platí rovnost $\phi(x, y) = -\phi(x, -y)$, tedy f_2 je identicky nulový polynom a u je lomená funkce v x. Pokud obdobně vyjádříme $v(x, y) = \frac{g_1(x)+g_2(x)y}{g_3(x)}$, získáme $g_1 \equiv 0$ a $v(x, y) = \frac{g_2(x)}{g_3(x)}y$ pro $g_2, g_3 \in K[x]$. □

Definice 6.3.3. Buď $\phi : E_1 \longrightarrow E_2$ isogenie. Pod *standardním tvarem* ϕ rozumíme vyjádření $\phi(x, y) = \left(\frac{u(x)}{v(x)}, \frac{r(x)}{s(x)}y\right)$, kde $u, v \in K[x]$ a $r, s \in K[x]$ jsou dvojice nesoudělných polynomů.

Díky této charakterizaci můžeme začít s isogeniemi pořádně pracovat. Nyní již nebude překvapením se zabývat otázkou, které body se zobrazí do nekonečna. Zprvu vidíme, že do nekonečna se zobrazí body s x-ovou souřadnicí kořenem v, s. Tyto polynomy mají navíc stejnou množinu kořenů, právě protože bod $\mathcal{O}$ je isogenií zachován.

Nás zajímají pouze eliptické křivky nad konečnými tělesy a každý polynom nad konečným tělesem má pouze konečně mnoho kořenů, množina bodů zobrazených do nekonečna isogenií

je konečná. Tyto body opět tvoří podgrupu $E_1(\overline{K})$, protože isogenie jsou homomorfismy grup bodů na křivkách.

Definice 6.3.4. Pod *jádrem* isogenie ϕ rozumíme jádro ϕ ve smyslu homomorfismu grup $E_1(\overline{K}) \longrightarrow E_2(\overline{K})$. Značíme $\ker\phi$ a počet jeho prvků $\#\ker\phi$.

Propůjčme si i další terminologii zabývající se lomenými funkcemi, abychom isogenie mohli přesněji popisovat.

Definice 6.3.5. Pod *stupněm* isogenie ϕ budeme rozumět $\max(\deg u, \deg v)$, kde u, v jsou definované v definici 6.3.3, a značit $\deg\phi$. Definujeme $\deg[0] = 0$.

Značení 6.3.6. Skládání, resp. sčítání isogenií definujeme následovně: pro libovolné isogenie $\phi : E \longrightarrow E_1$ a $\psi : E_1 \longrightarrow E_2$ definujeme $(\psi \circ \phi)P := \psi(\phi(P))$ pro každý bod $P \in E$ a pro isogenie $\phi, \psi : E \longrightarrow E_1$ zase $(\phi + \psi)P := \phi(P) + \psi(P)$ pro každý $P \in E$. Značme též isogenii opačnou jako $-\phi := [-1] \circ \phi$.

Všimněme si, že složení dvou isogenií je zjevně opět isogenií. Všechny vlastnosti stupňů racionálních funkcí jsou u stupňů isogenií zachovány, zejména jejich multiplikativita.

S isogeniemi jsme se již na naší (prozatím) krátké cestě hned několikrát setkali, jak násobení (nenulovým) skalárem, tak isomorfismy zmíněné v předchozí kapitole, jsou isogeniemi, druhý případ dokonce dává jediné invertibilní. Násobení $[n]$ má jádro $E[n]$ a za chvíli si ukážeme, že má coby isogenie stupeň n^2. Zobrazení $[0]$ není surjektivní a proto není isogenií. Isomorfismy jsou isogenie lineární a mají pouze triviální jádro. Zobrazení:

$$\phi : y^2 = x^3 + x \quad \longrightarrow \quad y^2 = x^3 + 11x + 62$$

mezi křivkami nad $\mathbb{F}_{101}$ dané $(x, y) \mapsto \left(\frac{x^2+10x-2}{x+10}, \frac{x^2+20x+1}{x^2+20x-1}y\right)$ je též isogenií, tentokrát stupně dva. Jádrem ϕ je množina $\{\mathcal{O}, (-10, 0)\}$, protože $x^2 + 20x - 1 = (x + 10)^2$ v $\mathbb{F}_{101}$.

Jedním z nejdůležitějších zobrazení na $\overline{\mathbb{F}}_p$ je tzv. *Frobeniův morfismus*, pojmenovaný po Ferdinandu Frobeniovi, jemuž diktuje předpis $\pi : x \mapsto x^p$. Pevné body Frobeniova morfismu jsou přesně prvky $\mathbb{F}_p$, tudíž pro lomenou funkci f nad $\mathbb{F}_p$ a $x_i \in \overline{\mathbb{F}}_p$ platí $f(x_1^p, \ldots, x_n^p) = f(x_1, \ldots, x_n)^p$. Speciálně platí vztahy $0^p = 0, 1^p = 1, a^p + b^p = (a + b)^p$ a $a^p \cdot b^p = (ab)^p$ pro libovolné $a, b \in \overline{\mathbb{F}}_p$. Navíc toto zobrazení je nad $\overline{\mathbb{F}}_p$ prosté, pokud $a^p = b^p$:

$$0 = a^p - b^p = (a - b)^p,$$

tedy $a = b$. Frobeniův morfismus je proto nad $\overline{\mathbb{F}}_p$ automorfismem.

Mocninu Frobeniova automorfismu definujeme jako $\pi^n : x \mapsto x^{p^n}$, neboli složení n iterací π. Rozkladové těleso polynomu $x^{p^n} - x$ je $\mathbb{F}_{p^n}$, což znamená, že π^n se chová jako identita právě na konečných tělesech $\mathbb{F}_q$, kde $q = p^k$ s $k \leqslant n$.

Zobrazení s podobným předpisem převádějící eliptické křivky též nese jméno po Frobeniovi.

Definice 6.3.7. Buď $E/\mathbb{F}_q : y^2 = x^3 + ax + b$ eliptická křivka. Zobrazení $\pi_E : E \longrightarrow E$ dané $(x, y) \longmapsto (x^q, y^q)$ se nazývá *Frobeniovým endomorfismem.*

Díky vlastnostem π definuje π_E homomorfismus mezi grupami křivek, tedy je vskutku isogenií. Frobeniův endomorfismus fixuje právě $E(\mathbb{F}_q)$ a má pouze triviální jádro. Dále komutuje s libovolnou isogenií nad $\mathbb{F}_q$, tj.:

$$\pi_{E'} \circ \phi = \phi \circ \pi_E,$$

kde $\phi : E \longrightarrow E'$ je isogenie. Mocninu Frobeniova endomorfismu analogicky definujeme jako ${\pi^n}_E := \underbrace{\pi_E \circ \pi_E \circ \cdots \circ \pi_E}_{n}$ a má vlastnosti analogické k π. Pokud bude jasné, kdy mluvíme o isogenii a ne o zobrazení na $\mathbb{F}_q$, zneužitím notace budeme π_E značit pro jednoduchost též π.

Můžeme též definovat p-Frobeniův morfismus $\pi_p : (x, y) \mapsto (x^p, y^p)$ na E nad $\mathbb{F}_q$ pro $q \neq p$, který je opět homomorfismem grup bodů eliptických křivek, ale již ne nutně definuje endomorfismus.

Když již máme solidní představu pojmu isogenie, pojďme se nyní pobavit o několika jejich základních vlastnostech. Jedním z nejdůležitějších výsledků ohledně isogenií mluví o jejich duálu.

Věta 6.3.8. *Buď $\phi : E \longrightarrow E_1$ isogenie stupně n. Pak existuje jediná isogenie $\hat{\phi} : E_1 \longrightarrow E$ splňující $\phi \circ \hat{\phi} = [n]_E$. Tuto isogenie nazýváme k ϕ duální. Definujeme též $\hat{[0]} = [0]$.*

Důkaz existence duální isogenie je poměrně zdlouhavý a vyžaduje rozebírání mnoha případů, zde jej proto vynecháme. Čtenář jej však může najít v [69, Thm. III.6.1.], trochu elementárnější přístup se nachází v [75, Thm. 7.8.].

Duální isogenie konečně opodstatňuje fakt, který na první pohled není vůbec jasný, že „být isogenní“ je relace ekvivalence. Několik základních vlastností duální isogenie stanovuje následující věta:

Věta 6.3.9. *Buďte $E/K, E'/K$ eliptické křivky a $\phi : E \longrightarrow E'$ isogenie stupně n. Pak její duální isogenie pro každou jinou isogenii $\psi : E' \longrightarrow E_1, \chi : E \longrightarrow E'$ splňuje:*

(i) $\phi \circ \hat{\phi} = [n]_E$,

(ii) $\hat{\phi} \circ \phi = [n]_{E'}$,

(iii) $\widehat{\phi \circ \psi} = \hat{\psi} \circ \hat{\phi}$,

(iv) $\widehat{\phi + \chi} = \hat{\phi} + \hat{\chi}$,

(v) $\hat{\hat{\phi}} = \phi$.

Důkaz. Dokážeme vlastnosti *(ii)*, *(iii)* a *(v)*. Platí:

$$(\hat{\phi} \circ \phi) \circ \hat{\phi} = \hat{\phi} \circ (\phi \circ \hat{\phi}) = \hat{\phi} \circ [n]_E = [n]_{E'} \circ \hat{\phi},$$

kde poslední rovnost platí, protože isogenie jsou jsou homomorfismy grup. Protože isogenie jsou surjektivní, musí platit $\hat{\phi} \circ \phi = [n]_{E'}$. Dále, protože isogenie jsou homomorfismy grup bodů na křivkách, platí:

$$(\hat{\psi} \circ \hat{\phi}) \circ (\phi \circ \psi) = \hat{\psi} \circ (\hat{\phi} \circ \phi) \circ \psi = \hat{\psi} \circ [\deg \phi] \circ \psi = \hat{\psi} \circ \psi \circ [\deg \phi] = [\deg \psi] \circ [\deg \phi]$$
$$= [\deg \psi \circ \phi] = [\deg \phi \circ \psi] = \widehat{(\phi \circ \psi)} \circ (\phi \circ \psi),$$

tedy protože isogenie $\phi \circ \psi$ je surjektivní, platí $\hat{\psi} \circ \hat{\phi} = \phi \hat{\circ} \psi$. Konečně, bod (v) plyne z (i) a (ii), platí totiž $\hat{\hat{\phi}} \circ \hat{\phi} = [n]_E = \phi \circ \hat{\phi}$, tedy $\hat{\hat{\phi}} = \phi$. Čtvrtá vlastnost je ukázána v [69, Thm. III.6.1, Exc. 3.31] pro $\operatorname{char} K = 0$ a důkaz je naznačen pro tělesa konečná. □

Lemma 6.3.10. *Platí:*

$$\widehat{[n]} = [n] \qquad a \qquad \deg[n] = n^2.$$

Důkaz. Zjevně $\widehat{[0]} = [0]$ a $\widehat{[1]} = [1]$. Za pomocí věty 6.3.9, (iv), máme pro každé celé n:

$$\widehat{[n+1]} = \widehat{[n]} + \widehat{[1]} = [n] + [1] = [n+1],$$

standardní oboustranný indukční argument pak dokončí první část. Z definice sčítání máme $[m] \circ [n] = [mn]$, tudíž $[n] \circ \widehat{[n]} = [n^2]$. Dle věty 6.3.9$(ii)$, je $[n]$ isogenií stupně n^2. □

Poznámka. V literatuře se vlastnosti duální isogenie dokazují tak, že se elementárnějšími úvahami, například o tzv. *division polynomials*, ukáže $\deg[n] = n^2$, kde pak jednoduše plynou odrážky (ii), (iii) a (v). Čtvrtý bod je obzvláště těžké dokázat a jeho nejvíce přímočarý důkaz užívá *Weilových párování*, kterým se v naší práci nevěnujeme.

Je důležité si uvědomit, co nám předchozí charakterizace vlastně říkají o duální isogenii. Duální isogenie k ϕ je z našeho lemmatu též isogenií stupně n, která má velmi pěkné vlastnosti. Navíc pro libovolnou isogenii ϕ z E stupně n je $\ker \phi \subseteq E[n]$, neboť libovolný prvek v jádře ϕ se skrz $\hat{\phi}$ zobrazí do nekonečna E.

Když víme, že „být isogenní“ je relace ekvivalence, dalším krokem je jistě hledat způsob, jak klasifikovat třídy isogenních křivek. V minulé sekci jsme si ukázali, že na kvadratickém twistu křivky leží pouze určitý počet bodů. I případ isogenií definovaných nad tělesem $\mathbb{F}_q$ úzce souvisí s počtem bodů ležících na křivce. Samo kritérium zní až překvapivě jednoduše:

Věta 6.3.11. *(Sato-Tate) Buďte E, E' eliptické křivky nad $\mathbb{F}_q$. Pak tyto křivky jsou nad $\mathbb{F}_q$ isogenní, právě pokud platí $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$.*

Důkaz. Isogenie jsou surjektivní, přičemž isogenie nad $\mathbb{F}_q$ zobrazuje $E(\mathbb{F}_q)$ samu na sebe. Pokud jsou E a E' isogenní, platí pak $\#E(\mathbb{F}_q) \geqslant \#E'(\mathbb{F}_q)$ a $\#E'(\mathbb{F}_q) \geqslant \#E(\mathbb{F}_q)$, což dává jednu polovinu věty. Druhá část již tak jednoduše nepřichází a její důkaz dokonce není ani zdaleka přístupný z pohledu algebraické geometrie. Poprvé byla druhá implikace (resp. tvrzení jí ekvivalentní) zveřejněno v jedné z nejvlivnějších publikací Johna Tate, [77]. □

Body, které se nachází v jádru isogenie, tvoří podgrupu $E(\overline{K})$, přičemž její velikost je shora omezena stupněm isogenie. Limitní případ v tomto smyslu má zajímavé vlastnosti.

6.4 Separabilní isogenie

Definice 6.4.1. Mějme E, E' křivky nad K a $\phi : E \longrightarrow E'$ isogenii stupně n. Pokud je $\#\ker\phi = n$, pak o ϕ řekneme, že je *separabilní*. V opačném případě řekneme, že ϕ je *neseparabilní*. V případě, že je $\deg\phi$ roven mocnině $\operatorname{char} K$, mluvíme o ϕ jako o *čistě neseparabilní*.

Pozoruhodné na tomto pojmenování je fakt, že separabilita a čistá neseparabilita se ne nutně vylučují. Každý isomorfismus je isogenií stupně 1 s jádrem velikosti 1, tedy separabilní, přičemž $p^0 = 1$, takže isomorfismy jsou čistě neseparabilní. Naopak Frobeniův endomorfismus je isogenie neseparabilní i čistě neseparabilní. Charakterizujme dále separabilní isogenie.

Věta 6.4.2. *Ať E, E' jsou eliptické křivky nad K a $\phi : E \longrightarrow E'$ je isogenie daná standardní formou $(x, y) \mapsto \left(\frac{u(x)}{v(x)}, \frac{r(x)}{s(x)}y\right)$. Pak $\left(\frac{u}{v}\right)' \neq 0$ nastane právě pokud ϕ je separabilní.*

Důkaz. Položme $p = \operatorname{char} K$. Rovnost $0 = \left(\frac{u}{v}\right)' = \frac{u'v - v'u}{v^2}$ v K nastane, právě pokud $u'v = v'u$. Protože je ϕ isogenie, jsou u, v nenulové polynomy nad K. Předpokládejme, že u', a tedy i v' nejsou nulové. Z nesoudělnosti polynomů u, v nutně každý kořen u je kořenem u' s nejméně stejnou násobností. Nicméně pro $u' \neq 0$ je $\deg u > \deg u'$, což je spor. Rovnost $u'v = v'u$ proto můžeme relaxovat na $u' = v' = 0$, tedy každý nenulový jednočlen u, v má exponent dělitelný p a tak $u = f(x^p)$ a $v = g(x^p)$ pro nějaké polynomy $f, g \in K[x]$. Pak ale $\frac{u(x)}{v(x)} = \frac{f(x^p)}{g(x^p)} = \left(\frac{f(x)}{g(x)}\right)^p$ a v jistě nemá jádro velikosti $\deg u/v$, ať už $p > 0$ či ne.

Uvažme nyní (a, b) bod v obrazu $E(\overline{K})$ ve ϕ takový, že $ab \neq 0$ a a není podílem vedoucích koeficientů u a v. Takový bod jistě existuje, protože obraz $\phi(E(\overline{K}))$ je nekonečná množina. Uvažme nyní množinu M všech předobrazů (a, b) ve ϕ, neboli bodů $(x, y) \in E$ s $\phi(x, y) = (a, b)$. Protože ϕ je homomorfismus grup, počet prvků M je přesně roven velikosti jádra ϕ.

Pro každé $(x, y) \in \mathsf{M}$ dále platí:

$$\frac{u(x)}{v(x)} = a, \qquad \frac{r(x)}{s(x)}y = b.$$

Díky předpokladu $b \neq 0$ je každé vyhovující y jednoznačně určeno daným x jako $b\frac{s(x)}{r(x)}$, což znamená, že velikost M je rovna počtu x splňujících první naši rovnost, tedy počtu různých kořenů polynomu $h := u - av$, který má díky podmínkám na a stupeň $\deg\phi$. Dejme tomu, že x_0 je vícenásobný kořen h, pak platí:

$$u(x_0) = av(x_0),$$
$$u'(x_0) = av'(x_0).$$

Násobení protějších stran těchto rovností dává $u'(x_0)v(x_0) = u(x_0)v'(x_0)$, x_0 je tedy kořenem (nenulového) polynomu $u'v - uv'$, který má v $\overline{K}$ pouze konečně mnoho kořenů. Protože $\phi(E(\overline{K}))$ je nekonečná a M konečná množina, můžeme si zvolit (a, b) bod takový,

že h žádný násobný kořen nemá. Pak $\#\ker\phi = |\mathsf{M}| = \deg h = \deg\phi$. □

Speciálně nad tělesem s nulovou charakteristikou jsou všechny isogenie neseparabilní. Zaměřme se na konečný případ, kde musí pro ϕ ve standardním tvaru platit $(u/v)' = 0$, tedy jak jsme si ukázali v důkazu předchozí věty, u/v je složením racionální funkce nad $\mathbb{F}_q$ a p-Frobeniova morfismu na $\mathbb{F}_q$. Vypadá to tedy, že i y-ová souřadnice se bude chovat podobně, bohužel dokázat tento fakt je poměrně ošklivější, než ho konstatovat.

Důsledek 6.4.3. *Buď ϕ isogenie nad $\mathbb{F}_q$. Pak existuje separabilní isogenie ψ a $n \in \mathbb{N}_0$, že:*

$$\phi = \psi \circ \pi_p^n.$$

Důkaz. Stačí ukázat, že pro každou neseparabilní isogenii ϕ existuje separabilní isogenie ψ s $\phi = \psi \circ \pi$. Pro x-ovou souřadnici tento výsledek známe, zbytek důkazu se dá najít na [75, Lemma 6.3.]. Tento důkaz není nijak zvlášť instruktivní, zde ho proto vynecháváme. Iterací tohoto faktu a skutečností, že Frobenius komutuje s libovolnou isogenií nad $\mathbb{F}_q$, pak získáme výsledek. □

Separabilní isogenie, jako takové, zatím nevypadají příliš zajímavě. Mají ale jednu vlastnost úzce spojenou s jejich jádrem, která je pro naši práci natolik stěžejní, že bez jejího zmínění by text byl poloviční.

Věta 6.4.4. *Buďte E eliptická křivka a $\phi : E \longrightarrow E'$ libovolná separabilní isogenie s jádrem $G \subseteq E(\overline{K})$. Pak všechny křivky E' jsou spolu isomorfní.*

Důkaz tvrzení je uveden v [79, Prop. 12.12], nicméně autor jej zde podává s notnou dávkou Galoisovy teorie, jejíž znalost od čtenáře nepředpokládáme.

Značení 6.4.5. Buď $G \subseteq E(\overline{\mathbb{F}}_q)$ konečná grupa. Značme E/G až na isomorfismus unikátní křivku, která pro každou separabilní isogenii $\phi : E \longrightarrow E'$ s jádrem G splňuje $E' \cong E/G$.

Poznámka. Ač E/G je pouze značení pro křivku a nesmí být naivně bráno ve smyslu faktorizace, není zcela nepodložené. Ve zkratce zde načrtněme důvod. Každá konečná podgrupa $G \subseteq E(\overline{K})$ definuje surjektivní homomorfismus grup $\phi : E \longrightarrow E/G$ s jádrem G, kde E/G je isomorfní faktorgrupě $E(\overline{K})/G$. Není naprosto vůbec zjevné, že E/G je eliptickou křivkou, ani že ϕ je isogenií, detaily faktorizace E/G též vyžadují náramnou péči. Čtenář obeznámen s teorií tělesových vnoření a obecně Galoisovou teorií nalezne podrobnější náznak důkazu na [75, Thm. 6.10.].

Jednoznačnost (až na isomorfismus) cílové křivky separabilní isogenie má kolosální dopady na naše pochopení isogenií. Říká nám totiž, že separabilní isogenie můžeme uvažovat ne mezi přímo eliptickými křivkami, ale mezi jejich j-invarianty, což je jedna z klíčových vlastností vedoucí na praktické protokoly užívající isogenií.

Separabilní isogenie z $E \longrightarrow E'$ je daná lomenými funkcemi nad K a známe-li její jádro, dokážeme ji explicitně spočíst, přičemž libovolná konečná podgrupa $E(\overline{K})$ je jádrem

separabilní isogenie. Vzorce udávající (až na isomorfismus) přesný tvar separabilní isogenie z $E \longrightarrow E'$ s daným jádrem se nazývají *Véluovy* po Jeanu Véluovy, který je první publikoval roku 1971 ve [78]. Jejich zápis je obecně velice nezáživný a pro nás nepodstatný, stačí nám mít v povědomí, že separabilní isogenie s daným jádrem můžeme explicitně vyjádřit. Jejich přesnou formu a důkaz správnosti jsou k uvedeny v [18, Ch. 8.2]. V Sage 9.0 jsou Véluovy vzorce implementovány pro isogenii z E s jádrem G s časovou složitostí $O(\#G)$ příkazem:

`EllipticCurveIsogeny(E,ker G)`.

Příklad 6.4.6. Spočtěme separabilní isogenii ϕ s doménou eliptickou křivkou $E/\mathbb{F}_{101} : y^2 = x^3 + 8x + 23$ a jádrem cyklickou grupou generovanou bodem $P = (68, 9) \in E$. Bod P má řád 4 a grupa $\langle P\rangle = \{P, [2]P, [3]P, \mathcal{O}\} = \{(68, 9), (29, 0), (68, 92), \mathcal{O}\}$ je tedy jádrem ϕ. Příkaz `phi = EllipticCurveIsogeny(E,P)` v Sage 9.0 vygeneruje isogenii ϕ a tu určíme s pomocí Véluových formulí příkazem `phi.rational_maps()`:

$$\phi : (x, y) \longmapsto \left(\frac{x^4 + 37x^3 - 26x^2 - 15x - 21}{x^3 + 37x^2 - 17x + 32}, \frac{x^5 + 41x^4 - 9x^3 + 5x^2 + 3x - 7}{x^5 + 41x^4 - 18x^3 + 6x^2 + 35x - 21} y \right).$$

Příkaz `phi.codomain()` dává cílovou křivku ϕ spočtenou pomocí Vélouvých formulí a je to $E'/\mathbb{F}_{101} : y^2 = x^3 + 53x + 41$, samozřejmě všechny křivky s ní isomorfní jsou doménou eliptické křivky s jádrem $\langle P\rangle$. Kořeny polynomu $x^5 + 41x^4 - 18x^3 + 6x^2 + 35x - 21$ nad $\mathbb{F}_{101}$ jsou pouze 29 a 68, přičemž 29 dvojnásobný a 68 trojnásobný, což odpovídá faktu, že grupa $\langle P\rangle$ se zobrazí do nekonečna. V době psaní této práce je Sage schopen spočíst pouze isogenie s cyklickým jádrem a pomocí Véluových formulí.

Jistě složením neseparabilní isogenie s libovolnou jinou získáme opět neseparabilní isogenii. Podobné vlastnosti má ale i součet isogenii.

Věta 6.4.7. *Buďte $\phi, \psi : E \longrightarrow E_1$ isogenie, přičemž ϕ je neseparabilní. Pak $\phi + \psi$ je neseparabilní, právě pokud ψ je neseparabilní.*

Důkaz. Označme $\pi_p : (x, y) \to (x^p, y^p)$ p-Frobeniův endomorfismus na E, ten komutuje s libovolnou isogenií, a navíc isogenie π je nějakou jeho mocninou. Podle věty 6.4.4 existují separabilní isogenie $\eta, \vartheta : E \longrightarrow E_1$ splňující $\phi = \eta \circ \pi_p^a$ a $\psi = \vartheta \circ \pi_p^b$, kde $a > 0$. Pokud ψ je neseparabilní, je exponent b kladný, tedy součet $\phi + \psi$ je roven:

$$\phi + \psi = \eta \circ \pi_p^a + \vartheta \circ \pi_p^b = (\eta \circ \pi_p^{a-1} + \vartheta \circ \pi_p^{b-1}) \circ \pi_p,$$

neseparabilní isogenii. Naopak je-li isogenie $\phi+\psi$ neseparabilní, je $\psi = (\phi+\psi)-\phi$ součtem neseparabilních isogenií $\phi + \psi$ a $-\phi$, o kterém jsme právě ukázali, že je neseparabilní. □

Poznámka. Tato věta má hned několik důležitých aplikací, jednu z nich si ukážeme hned o dvě sekce dále. Je ale též jednou z klíčových ingrediencí důkazu Hasseho věty 6.1.5. Konkrétně z ní plyne, že $[1] - \pi$ je separabilní isogenie, tedy $\deg[1] - \pi = \#\ker[1] - \pi = \#E(\mathbb{F}_q)$, k tomuto fakt se ještě vrátíme. Stačí si pak všimnout, že příslušné členy v Hasseho větě jsou po řadě $\deg[1]-\pi, \deg[1], \deg -\pi$ a užít jednu speciální formu Cauchy-Schwarzovy nerovnosti, na detaily čtenáře odkazujeme na [69, Thm. V.1.1.].

Konečně, pojďme se pokusit spočítat separabilní isogenie efektivněji. Je-li velikost jádra této isogenie prvočíselné (a tedy jádro cyklické), nespočteme ji jistě v čase lepším než lineárním vzhledem k velikosti jádra. Pokud ale pracujeme jádrem *hladké* velikosti, tedy dělitelné pouze prvočísly do dané hranice, můžeme postupovat mnohem rychleji.

Věta 6.4.8. *Každou isogenii ϕ složeného stupně můžeme rozložit na kompozici isogenií prvočíselných stupňů.*

Důkaz. Dejme tomu, že ϕ převádí křivky $E \longrightarrow E_1$. Protože π má prvočíselný stupeň charakteristiky našeho tělesa, stačí nám díky větě 6.4.3 uvažovat ϕ isogenii separabilní. Postupujme nyní silnou indukcí vzhledem k počtu dělitelů $\deg \phi$. Pokud $G = \ker \phi$ je triviální či má prvočíselný řád, jsme hotovi. V opačném případě dejme tomu, že všechny isogenie s jádrem nižšího počtu dělitelů než $\#\ker \phi$ jsou rozložitelné. Víme, že G obsahuje podgrupu H prvočíselného řádu (tzv. *Sylowova podgrupa*), která určuje separabilní isogenii $\psi : E \longrightarrow E_2 \cong E/H$. Pak obraz G v ψ je konečná podgrupa $E_1(\overline{K})$, která je isomorfní G/H, a definuje isogenii $\chi : E_2 \longrightarrow E_3 \cong E_2/\psi(G)$. Jádro $\chi \circ \psi$ je právě G, tedy podle věty 6.4.4 existuje isomorfismus $\iota : E_3 \longrightarrow E_2$ splňující $\phi = \iota \circ \chi \circ \psi$. Podle předpokladu $\iota \circ \chi$ je buďto isomorfismus nebo je rozložitelná na kompozici separabilních isogenií prvočíselných stupňů. □

Tato věta zní hezky z čiře teoretického pohledu studia křivek, je ale hlavní ingrediencí v rychlejším počítání (separabilních) isogenií. Označíme $\langle G \rangle$ podgrupu $E(\overline{K})$ generovanou množinou $G = \{P, Q, R, \dots\}$ a pojďme se pokusit efektivně spočíst isogenii $\phi : E \longrightarrow E/\langle G \rangle$. Postačí nám spočíst separabilní isogenii $\psi : E \longrightarrow E/\langle P \rangle$, kde P má prvočíselný řád, pro podgrupy generované $Q, R, \dots$ spočteme analogicky separabilní isogenie převádějící $E/\langle P \rangle := E' \longrightarrow E'/\langle Q \rangle := E'' \longrightarrow E''/\langle R \rangle \dots$. Věta 6.4.4 nám zaručí, že složení všech takových isogenií bude mít jádro $\langle G \rangle$.

Ale isogenii $E \longrightarrow E/\langle P \rangle$ spočteme jednoduše:

$$E \xrightarrow{\phi_1} E/\langle \ell^{a-1} P \rangle \xrightarrow{\phi_2} E/\langle \ell^{a-2} \phi_1(P) \rangle \xrightarrow{\phi_3} \cdots \xrightarrow{\phi_a} E/\langle \phi_{a-1} \circ \phi_{a-2} \circ \cdots \circ \phi_1(P) \rangle,$$

kde řád P je ℓ^a. Snadno nahlédneme, že jádro $\phi_i \circ \cdots \circ \phi_1$ je $\langle \ell^{a-i} P \rangle$ a tedy separabilní isogenie daná složením všech ϕ_i má jádro přesně $\langle P \rangle$.

Véluovy formule nám umožní každou ϕ_i spočíst v $O(\ell)$ operacích a tedy celý proces je hotov pouze v $O(\ell a)$ operacích. Celou isogenii $E \longrightarrow E/\langle G \rangle$ takto spočteme v logaritmickém čase vzhledem k velikosti jádra.

6.5 Torzní body

Vraťme se k operaci násobení bodů. Za pomocí vlastností isogenií vyvinutých v předchozích částech budeme konečně schopni přijít na kloub struktuře torzních grup a na základě toho i samotné grupě $E(\mathbb{F}_q)$. Začněme tedy směrem k tomuto cíli dělat první krůčky.

Charakterizovat $E[2]$ je jednoduché. Spolu s bodem v nekonečnu jsou násobením dvěma anihilované právě tři další body, jejich x-ové souřadnice jsou jednotlivými (různými!)

kořeny $x^3 + ax + b$. Protože torze tvoří grupu a na naší 2-torzi má každý afinní bod řád 2, musí nutně být $E[2] \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

3-torze jsme též schopni diskutovat. Body na ní splňují $[2]P = -P$, speciálně se x-ové souřadnice obou stran rovnají. To znamená, že:

$$\left(\frac{3x^2 + a}{2y}\right)^2 - 2x = x,$$

neboli díky rovnosti $y^2 = x^3 + ax + b$:

$$(3x^2 + a)^2 = 12x(x^3 + ax + b),$$

což je kvartická rovnice, která se snadno ověří jako s nenulovým diskriminantem. Každému ze čtyř různých vyhovujících x přísluší právě dvě hodnoty y (krom $\mathcal{O}$ se 2 a 3-torze neprotínají) a body (x, y) mají všechny řád 3. Spolu s $\mathcal{O}$ náleží 3-torzi právě 9 bodů. Snadno pak dojdeme k závěru $E[3] \cong \mathbb{Z}_3 \times \mathbb{Z}_3$.

V obou případech argumenty implicitně závisí na faktu, že q není mocnina 2 ani 3, jinak naše eliptická křivka nemá tvar, který jí připisujeme. Tento případ je podrobněji rozebírán v [79, Ch. 3.1].

Mohli bychom se tedy dovtípit, že n-torze pro n nesoudělné s q je isomorfní $\mathbb{Z}_n \times \mathbb{Z}_n$. Tato skutečnost je díky existenci duální isogenie velmi úzce spjata se separabilitou n-násobící isogenie.

Lemma 6.5.1. *Buď E/K eliptická křivka s $p = \operatorname{char} K$ a n celé číslo. Pak $[n]$ je neseparabilní, právě pokud $p \mid n$.*

Důkaz. Dejme tomu, že $[n]$ je neseparabilní, pak díky důsledku 6.4.3 je $[n] = \pi \circ \phi$ pro nějakou isogenii ϕ a tedy $p \mid \deg \pi \cdot \deg \phi = \deg \pi \circ \phi = \deg[n] = n^2$, neboli $p \mid n$. Mějme naopak $p \mid n$, můžeme pak psát $[n] = [p][n/p]$. Víme, že $[p]$ je neseparabilní, protože $\pi \circ \widehat{\pi} = [\deg \pi] = [p]$. Definice separability pomocí velikosti jádra jistě implikuje, že složení neseparabilní isogenie, zde $[p]$, s libovolnou jinou vyprodukuje isogenii neseparabilní, tedy $[n]$ je neseparabilní sama. □

Nejprve se zaměříme na prvočísla a jejich mocniny.

Věta 6.5.2. *Buď E/K eliptická křivka s $p = \operatorname{char} K$ a $\ell \neq p$ prvočíslo. Pak:*

$$E[\ell^e] \cong \mathbb{Z}_{\ell^e} \times \mathbb{Z}_{\ell^e}$$

pro každé $e \geqslant 1$.

Důkaz. Postupujme silnou indukcí podle e. Isogenie $[\ell]$ je pro prvočísla $\ell \neq p$ separabilní, tedy $\#E[\ell] = \#\ker[\ell] = \ell^2$. Každý afinní prvek $E[\ell]$ má řád ℓ, tedy platí $E[\ell] \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$. Nyní již uvažme abelovskou grupu $E[\ell^e]$ pro nějaké $e > 1$ a předpokládejme, že věta platí pro všechna kladná $a < e$. Opět víme, že $\#E[\ell^e] = \#\ker[\ell^e] = \ell^{2e}$ a každý afinní prvek $E[\ell^e]$ nemá řád vyšší než ℓ^e. Navíc pro každé $a < e$ existuje na $E[\ell^e]$ právě ℓ^{2a} prvků řádu ℓ^a, tedy $E[\ell^e]$ má shodnou strukturu jako $\mathbb{Z}_{\ell^e} \times \mathbb{Z}_{\ell^e}$. □

Důsledek 6.5.3. *Buď E/K eliptická křivka s $p = \operatorname{char} K$ a $p \nmid m$ přirozené číslo. Pak $E[m] \cong \mathbb{Z}_m \times \mathbb{Z}_m$.*

Důkaz. Pokud m, n jsou nesoudělná čísla, jistě platí $E[m] \times E[n] \cong E[mn]$. Čínská zbytková věta pro taková m, n tvrdí $(\mathbb{Z}_m \times \mathbb{Z}_m) \times (\mathbb{Z}_n \times \mathbb{Z}_n) \cong \mathbb{Z}_{mn} \times \mathbb{Z}_{mn}$, tedy pokud $m = p_1^{a_1} \cdots p_k^{a_k}$ rozložíme na součin prvočíselných mocnin, s pomocí předchozí věty platí:

$$E[m] \cong E[p_1^{a_1}] \times \cdots \times E[p_k^{a_k}] \cong \left(\mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_1^{a_1}}\right) \times \cdots \times \left(\mathbb{Z}_{p_k^{a_k}} \times \mathbb{Z}_{p_k^{a_k}}\right) \cong \mathbb{Z}_m \times \mathbb{Z}_m,$$

což jsme chtěli dokázat. □

Zásadní rozdíl nastává při násobení mocninou charakteristiky našeho tělesa, isogenie $[p]$ je totiž (čistě) neseparabilní. Případ $\operatorname{char} K = 0$ je triviální, podíváme se proto opět pouze na konečný případ.

Věta 6.5.4. *Buď $E/\mathbb{F}_q$ s $q = p^k$ eliptická křivka. Pak platí:*

$$E[p^e] \cong \begin{cases} \{\mathcal{O}\}, & \text{pro každé nezáporné } e, \\ \mathbb{Z}_{p^e}, & \text{pro každé nezáporné } e. \end{cases}$$

Důkaz. Isogenie $[p]$ je neseparabilní a její jádro má tedy řád ostře nižší než $\deg[p] = p^2$. Každý prvek $E[p]$ má ale řád dělící p, platí tedy buď $E[p] \cong \{\mathcal{O}\}$, či $\mathbb{Z}_p$. První případ jistě znamená $E[p^e] \cong \{\mathcal{O}\}$ pro každé $e \geqslant 0$, nyní tedy předpokládejme $E[p] \cong \mathbb{Z}_p$.

Dále postupujme silnou indukcí podle $e \geqslant 1$, $e = 0, 1$ je dáno. Dále ať dané tvrzení platí pro všechna nezáporná čísla nepřevyšující e. Isogenie $[p]$ je surjektivní, tedy pro každé $f \leqslant e$ a P bod řádu p^f existuje bod Q splňující $[p]Q = P$, jehož řád je p^{f+1}. Speciálně existuje bod $P_0 \in E[p^{e+1}]$ řádu p^{e+1}. Takový bod ale existuje díky $E[p^e] \cong \mathbb{Z}_{p^e}$ pouze jeden a $E[p^e] \cong \mathbb{Z}_{p^e}$. □

Předchozí věta ukazuje, že existují dvě rodiny křivek s drasticky odlišnými p-torzemi. Abychom si je mohli vložit do správných přihrádek, zavedeme nové názvosloví:

Definice 6.5.5. Pokud máme $E[p] \cong \{\mathcal{O}\}$, nazveme E *supersingulární*. Jinak E budeme říkat *obyčejná*.

Znalost struktury ℓ-torzí pro ℓ prvočíslo nám pomůže spočítat, kolik separabilních isogenií prvočíselného stupně vychází z dané křivky. K tomu si nejprve pochopitelně musíme spočítat podgrupy na E řádu ℓ. Ty musí být generované bodem řádu ℓ, tedy celá podgrupa leží v $E[\ell]$. Přirozeně tedy chceme spočítat podgrupy ℓ-torze řádu ℓ. Případ $\ell = p$ dává buď žádnou či jednu podgrupu, v závislosti na supersingularitě křivky, dále tento případ neuvažujme.

Lemma 6.5.6. *Buď $E/\mathbb{F}_q$ křivka s $q = p^k$ a $\ell \neq p$ prvočíslo. Pak $E[\ell^e]$ obsahuje právě $\ell^{e-1}(\ell + 1)$ podgrup řádu ℓ^e.*

Důkaz. Díky větě 6.5.2 platí $E[\ell^e] \cong \mathbb{Z}_{\ell^e} \times \mathbb{Z}_{\ell^e}$, mějme P, Q její generátory. Každá podgrupa $E[\ell^e]$ řádu ℓ^e je cyklická generovaná prvkem $R = [a]P + [b]Q$. Ten musí mít řád ℓ^e, tedy právě jeden z a, b není dělitelný ℓ^e. Počet takových a je pak roven $\ell^{e-1}(\ell - 1)$ a počet b je ℓ^e, dohromady dávají $\ell^{2e-1}(\ell - 1)$ možných bodů. Započítali jsme ale případy, kdy oba mají řád ℓ^e dvakrát, takových případů je $(\ell^{e-1}(\ell - 1))^2$. Konečně, zde počítáme každou podgrupu $\ell^{e-1}(\ell - 1)$-krát, jednou pro každý její bod řádu ℓ^e, tedy hledaný počet je roven:

$$\frac{2\ell^{2e-1}(\ell - 1) - (\ell^{e-1}(\ell - 1))^2}{\ell^{e-1}(\ell - 1)} = \ell^{e-1}(\ell + 1).$$

□

Důsledek 6.5.7. *Buď $E/\mathbb{F}_q$ křivka s $q = p^k$ a $\ell \neq p$ prvočíslo. Pak existuje přesně $\ell + 1$ až na isomorfismus různých separabilních isogenií stupně ℓ vycházejících z E definovaných nad $\overline{\mathbb{F}}_q$.*

Důkaz. Podle věty 6.4.4 je počet separabilních isogenií vycházejících z E stupně ℓ dán počtem podgrup E řádu ℓ. Všechny takové grupy musí být obsaženy v $E[\ell]$ a předchozí lemma pak tvrdí, že hledaný počet je právě $\ell + 1$. □

Jak jsme zmínili před chvíli, pro nesoudělná m, n platí $E[m] \times E[n] \cong E[mn]$, tedy pomocí před chvílí zmíněného páru vět jsme schopni kompletně charakterizovat libovolnou torzní podgrupu E. Speciálně toho můžeme říci mnoho o samotné grupě bodů nad konečným tělesem $E(\mathbb{F}_q)$:

Věta 6.5.8. *Buď $E/\mathbb{F}_q$ eliptická křivka s $q = p^k$. Pak:*

$$E(\mathbb{F}_q) \cong \mathbb{Z}_m \times \mathbb{Z}_n$$

pro $p \nmid m \mid n$ přirozená čísla.

Důkaz. Pokud p nedělí řád $E(\mathbb{F}_q)$, který označme m, pak $E(\mathbb{F}_q) \subseteq E[m] \cong \mathbb{Z}_m \times \mathbb{Z}_m$ je podgrupa řádu nejvýše 2, lze ji proto zapsat jako direktní součin $\mathbb{Z}_m \times \mathbb{Z}_n$ s $m \mid n$ a $p \nmid mn$, kde umožňujeme případ $m = 1$. Jinak existuje podgrupa $G \subseteq E(\mathbb{F}_q)$ řádu nejvyšší mocniny p, kde $E(\mathbb{F}_q) \cong G \times H$ a $H \cong \mathbb{Z}_m \times \mathbb{Z}_m$ nemá řád dělitelný p. Grupu $E(\mathbb{F}_q)$ tedy můžeme zapsat jako direktní součin nejvýše dvou cyklických grup a pouze jedna z nich má řád dělitelný p. □

Působení isogenie na libovolnou m-torzi či samotnou grupu $E(\mathbb{F}_q)$ je jednoznačně určeno jejím chováním na (nejvýše dvou) generátorech těchto grup. Isogenie jsou totiž homomorfismy grup bodů na křivkách, pro příslušné generátory G_1, G_2 a bod $P = [m]G_1 + [n]G_2$ platí:

$$\phi([m]G_1 + [n]G_2) = [m]\phi(G_1) + [n]\phi(G_2).$$

Isogenie na dané křivce, tedy $\phi : E \longrightarrow E$, působí na $E(\mathbb{F}_q)$ i na její torzní podgrupy jako 2×2 celočíselné matice, v případě m-torzní grupy dokonce jako matice modulo m. Jak se chovají takové isogenie na torzích budeme podrobněji studovat ve čtvrté kapitole.

Před chvíli jsme ale eliptické křivky rozlišily na dvě třídy podle jejich p-torze. Ty „neobyčejné“ z nich, supersingulární, jsou více než zajímavé.

6.6 Supersingulární křivky

Slovo supersingulární napovídá, že na křivky takto pojmenované nenarazíme příliš často, že jsou mezi všemi eliptickými křivkami vzácné. Tato malá větev křivek se od obyčejných fundamentálně liší, přičemž jejich četné rozdíly jsou spolu mnohdy těsně provázané. Ve skutečnosti se některé vlastnosti, o kterých se zmíníme, berou jako ekvivalentní definice supersingularity, každá vhodná v jistém úhlu pohledu. Jejich vlastnosti ve všech směrech, které jsme prozatím studovali, dopodrobna prozkoumáme, počínaje definicí pomocí torze.

Počítání celé p-torze je pro velká prvočísla výpočetně náročné, chtěli bychom najít vhodnější kritéria supersingularity. Ukáže se, že supersingulární eliptické křivky nesou pouze specifické počty bodů.

Věta 6.6.1. *Nechť E je křivka nad $\mathbb{F}_q$, kde $q = p^r$ je mocnina prvočísla $p > 3$. Pak:*

$$\#E(\mathbb{F}_q) \equiv 1 \pmod{p}$$

nastane právě pokud E je supersingulární.

Důkaz. Věta 6.3.9 říká:

$$[\deg([1] - \pi)] = ([1] - \pi) \circ (\widehat{[1] - \pi}) = ([1] - \pi) \circ (\widehat{[1]} - \widehat{\pi}) = ([1] - \pi) \circ ([1] - \widehat{\pi}),$$

neboli, protože isogenie jsou homomorfismy grup, isogenie:

$$\pi + \widehat{\pi} = [1] - [\deg([1] - \pi)] + \pi \circ \widehat{\pi} = [1] - [\deg([1] - \pi)] + [p]$$

působí jako skalární násobení na E. Isogenie $[1] - \pi = [1] - \pi_p^r$ má jádro $E(\mathbb{F}_q)$, protože tato množina je pod Frobeniovým endomorfismem invariantní. Navíc $-\pi$ je neseparabilní a $[1]$ zase separabilní, tedy věta 6.4.7 tvrdí, že $[1] - \pi$ je isogenií separabilní se stupněm rovným velikosti jádra, $\#E(\mathbb{F}_q)$. Pak tedy platí:

$$\pi + \widehat{\pi} = [1] - [\deg([1] - \pi)] + [p] = [1 - \deg([1] - \pi) + p] = [p + 1 - \#E(\mathbb{F}_q)].$$

Pokud E je supersingulární, je $\ker \pi \circ \widehat{\pi} = \ker[p] \cong \{\mathcal{O}\}$, neboli $\widehat{\pi}$ má triviální jádro a je neseparabilní. Podle věty 6.4.7 je $\pi + \widehat{\pi}$ neseparabilní, $[p+1-\#E(\mathbb{F}_q)]$ je proto neseparabilní též. Konečně, díky lemmatu 6.5.1 p dělí $p + 1 - \#E(\mathbb{F}_q)$.

Naopak pokud platí $E(\mathbb{F}_q) \equiv 1 \pmod{p}$, isogenie:

$$\pi + \widehat{\pi} = [p + 1 - \#E(\mathbb{F}_q)]$$

je neseparabilní. Víme, že π je neseparabilní isogenie a $\pi + \widehat{\pi}$ taky, opět utilizujeme větu 6.4.7, dle které i $\widehat{\pi}$ není separabilní. Protože stupeň $\widehat{\pi}$ je prvočíselný, $\widehat{\pi}$ má nutně triviální jádro, kompozice $[p] = \widehat{\pi} \circ \pi$ jej proto má též a E je supersingulární. □

Poznámka. Fakt, že $\phi + \widehat{\phi}$ je rovno skalární isogenii $[m]_E$ pro nějaké m zřejmě není unikátní pro Frobeniův endomorfismus. Stejný postup můžeme replikovat pro každou jinou isogenii $E \longrightarrow E$. My si však tento fakt „připomeneme“ na vhodnějším místě ve čtvrté kapitole.

Poznámka. Pozorování, že $\pi + \widehat{\pi} = [p + 1 - \#E(\mathbb{F}_q)]$ a že isogenie $\phi : E \longrightarrow E$ působí na torzní grupy jako 2×2 matice, navádí na důkaz Hasseho věty s pomocí znalostí, které nyní máme, spolu s trochu hlubším studiem působení isogenií $\phi : E \longrightarrow E$ na torzní podgrupy. Naznačme jej tu rychle, plný důkaz se nachází na [75, Thm. 8.1, Thm. 7.17]. Pokud M je 2×2 matice udávající akci π na nějakou fixní torzi $E[n]$, pro libovolná celá r, s lze fakt $\deg([r] \circ \pi - [s]) \geqslant 0$ pro dostatečně velké n převést na nezápornost determinantu matice $rM - Is$, což lze upravit na nezápornost kvadratického polynomu. Konečně se ukáže, že nekladnost jeho diskriminantu je jen jiná forma Hasseho věty.

Důsledek 6.6.2. *Ať E je křivka nad $\mathbb{F}_p$ s $p > 3$. Pak:*

$$\#E(\mathbb{F}_p) = p + 1$$

nastane, právě pokud E je supersingulární.

Důkaz. Pokud $\#E(\mathbb{F}_p) = p + 1$, tak dle předchozí věty je E supersingulární. Pro E supersingulární je $\#E(\mathbb{F}_p) \equiv 1 \pmod{p}$, tedy jestli $\#E(\mathbb{F}_p) \neq p + 1$, je číslo $p + 1 - \#E(\mathbb{F}_p)$ v absolutní hodnotě alespoň p. Dle Hasseho věty 6.1.5, kterou a priori bereme za platnou, toto číslo v absolutní hodnotě nepřesahuje $2\sqrt{p}$, neboli:

$$2\sqrt{p} \geqslant |p + 1 - \#E(\mathbb{F}_p)| \geqslant p,$$

což je spor s $p > 3$. □

Při zkoumání počtu bodů na supersingulárních křivek jsme narazili na číslo $t = q + 1 - \#E(\mathbb{F}_q)$, které je úzce spojené s Frobeniovým endomorfismem. Tento pár spolu rozhodně nevidíme naposledy, kapitola zaměřena na okruhy endomorfismů jejich pouto prohloubí.

Samotné počítání bodů na eliptické křivce je pro nás zatím obtížný úkon, pro $\mathbb{F}_p$ s malým p můžeme jednoduše projít všechny možné hodnoty x, jak můžeme vidět na následujícím příkladu:

Příklad 6.6.3. Ukažme, že křivka:

$$E : y^2 = x^3 + 10x + 7$$

nad $\mathbb{F}_{13}$ je supersingulární.

Řešení. Mějme $(x, y) \in E(\mathbb{F}_{13})$. Pokud je číslo $x^3 + 10x + 7$ v $\mathbb{F}_{13}$ nenulový čtverec, existují dvě vyhovující y, jedno, pokud je rovno nule, a jinak žádné. Můžeme si proto vypsat hodnoty pravé strany ve všech možných hodnotách a za pomocí Eulerova kritéria snadno určit, zda je výraz čtvercem, viz následující tabulka:

x	$x^3+10x+7$	$\left(\frac{x^3+10x+7}{13}\right)$	počet řešení
0	7	-1	0
1	5	-1	0
2	9	1	2
3	12	1	2
4	7	-1	0
5	0	0	1
6	10	1	2
7	4	1	2
8	1	1	2
9	7	-1	0
10	2	-1	0
11	5	-1	0
12	9	1	2

Spolu s bodem v nekonečnu je $\#E(\mathbb{F}_{13}) = 13+1 = 14$ a jsme hotovi z důsledku 6.6.2. □

U speciálních případů křivek můžeme rafinovaně využít poznatky z elementární teorie čísel:

Příklad 6.6.4. Ukažme, že křivka:

$$E/\mathbb{F}_p : y^2 = x^3 + kx$$

pro $p \equiv -1 \pmod 4$ je supersingulární.

Řešení. Pro $p \equiv -1 \pmod 4$ je $\left(\frac{-1}{p}\right) = -1$, takže pokud pro a, b platí $p \mid a^2 + b^2$, jsou obě dělitelná p. V opačném případě totiž z $a^2 \equiv -b^2 \pmod p$ vyvodíme:

$$\left(\frac{a}{b}\right)^2 \equiv -1 \pmod p,$$

spor. Nenulových čtverců v $\mathbb{F}_p$ je právě $\frac{p-1}{2}$, tudíž každý prvek $\mathbb{F}_p$ je buď čtverec nebo mínus čtverec. Pro $x = 0$ máme pouze $y = 0$ a pro každé $x \in \mathbb{F}_p^\times$ je právě jedno z čísel $x^3 + kx, (-x)^3 - kx$ nenulovým čtvercem, protože je $x^2 \neq -1$. Pro každou dvojici $(x, -x)$ tak máme právě dvě řešení, dohromady $p-1$. Spolu s $(0,0)$ a bodem v nekonečnu je $\#E(\mathbb{F}_p) = p+1$, díky větě 6.6.2 je E supersingulární. □

Příklad 6.6.5. Ukažme, že křivka:

$$E/\mathbb{F}_p : y^2 = x^3 + k$$

pro $p \equiv -1 \pmod 3$ je supersingulární.

Důkaz. Ukážeme, že třetí mocnina je na $\mathbb{F}_p$ bijekcí. Pokud totiž pro $x \not\equiv y$ platí $x^3 \equiv y^3 \pmod{p}$, tak:

$$p \mid (x-y)(x^2+xy+y^2) \Rightarrow p \mid x^2+xy+y^2$$

Ukážeme, že pak už $p \mid x, y$, v opačném případě p nedělí ani jedno. Poslední rovnost pak vynásobíme čtyřmi a máme:

$$p \mid (x+2y)^2+3x^2 \Rightarrow \left(\frac{x+2y}{x}\right)^2 \equiv -3 \pmod{p}.$$

Pro $p \equiv -1 \pmod 3$ je ale -3 kvadratický nezbytek, opět získáváme spor. Pro každé $y \in \mathbb{F}_p$ tedy existuje unikátní třetí odmocnina z y^2-k dávající bod $(x,y) \in E$. Dohromady máme na E přesně p afinních bodů a ten poslední samozřejmě leží v nekonečnu. □

Protože supersingularita nezávisí na konkrétním rozšíření, křivky výše jsou supersingulární nad libovolným konečným tělesem s charakteristikou po řadě $p \equiv -1 \pmod 4$, resp. $p \equiv -1 \pmod 3$.

Náš první postup počítání počtu bodů na křivce běží nejlépe v $O(p)$ čase, což je pro prvočísla $\log_2(p) > 500$, tedy praktické kryptografické velikosti, jednoduše příliš pomalé. Jedním z nejdřívějších velkých pokroků v oblasti počítání bodů byl *Schoofův algoritmus*, zveřejněn roku 1985 v [66], který $\#E(\mathbb{F}_q)$ jako první dokáže spočíst deterministicky v čase polynomiálním v $\log(q)$. Poskytuje tedy exponenciální zrychlení oproti našemu předchozímu postupu.

Pojďme se podívat na samotnou strukturu bodů na supersingulární E nad konečným tělesem. Ústřední při našem studiu isogenií je fakt, že supersingularita je pod působením isogenie zachována.

Věta 6.6.6. *Buď $E/\mathbb{F}_q$ eliptická křivka s $q = p^k$ a $\phi : E \longrightarrow E'$ libovolná isogenie vycházející z E. Pak E je supersingulární, právě pokud je E' supersingulární.*

Důkaz. Mějme $\phi : E \longrightarrow E'$ isogenii. Protože isogenie jsou homomorfismy grup bodů na křivkách nad $\mathbb{F}_q$, speciálně zachovají p-násobení:

$$\phi \circ [p]_E = [p]_{E'}$$

a analogická rovnost platí pro duální isogenii. Pokud na p-torzi jedné z křivek existuje netriviální bod, tak nějaký leží v p-torzi i druhé křivky, tedy pokud jedna z křivek je obyčejná, obě jsou. Naopak pokud p torze na E triviální, díky $[p]_{E'} = \phi \circ [p]_E$ je i $E'[p] \cong \{\mathcal{O}\}$ a samozřejmě i naopak. □

Speciálně toto tvrzení platí pro isomorfismy, každý j-invariant je proto exklusivní buď obyčejným, či supersingulárním křivkách, můžeme tedy j-invarianty rozřadit na obyčejné nebo supersingulární podle typu křivek jej sdílejících.

Pokud uvážíme graf všech j-invariantů nad $\overline{\mathbb{F}}_p$ (kterým přiřadíme jejich příslušnou třídu isomorfismů), kde dva vrcholy jsou propojené, právě pokud křivky jim náležící jsou isogenní

pod isogenií prvočíselného stupně ℓ, získáme neorientovaný(!) $\ell+1$-regulární (díky větě 6.5.7) graf rozdělený na obyčejné a supersingulární komponenty. Supersingulární křivky dokonce tvoří jednu jedinou souvislou komponentu, viz [45, Cor. 78]. Ve čtvrté kapitole budeme tyto grafy studovat trochu podrobněji studovat a ukážeme, že pokud se zaměříme na isogenie definované pouze nad $\mathbb{F}_q$, grafy supersingulárních j-invariantů se zásadně liší od grafů těch obyčejných. Z každého vrcholu totiž vždy vede buď $0, 1, 2$ či $\ell+1$ hran, přičemž supersingulární komponenty jsou pořád $\ell+1$ regulární, zatímco komponenty obyčejné tvoří tzv. *vulkány*, kde regulární graf stupně nejvýše 2 slouží jako „kráter“ a každý jiný vrchol je buď listem, či má $\ell+1$ sousedů.

Na grafu isogenií nad $\mathbb{F}_{19}$ se nachází pouze 2 supersingulární vrcholy, což potvrzuje fakt, že tyto křivky se nachází v menšině. Tento trend se drží i pro vyšší rozšíření, nad celým uzávěrem $\mathbb{F}_p$ se nachází relativně málo supersingulárních j-invariantů.

Věta 6.6.7. *Označme S množinu všech supersingulárních j-invariantů nad $\overline{\mathbb{F}}_p$. Pak platí:*

$$\#S = \left\lfloor \frac{p}{12} \right\rfloor + \begin{cases} 0, & \text{pokud} \quad p \equiv 1 \pmod{12}, \\ 1, & \text{pokud} \quad p \equiv 5, 7 \pmod{12}, \\ 2, & \text{pokud} \quad p \equiv 11 \pmod{12}. \end{cases}$$

Důkaz se nachází na [79, Cor. 4.40].

Předchozí věta nám říká, že když se budeme přesouvat do vyšších rozšíření tělesa $\mathbb{F}_p$, nenarazíme na další a další supersingulární j-invarianty. Dokonce se zastavíme už na $\mathbb{F}_{p^2}$:

Věta 6.6.8. *Buď E supersingulární eliptická křivka nad $\mathbb{F}_q$. Pak $j(E) \in \mathbb{F}_{p^2}$.*

Důkaz. Isogenie $[p]$ na supersingulární křivce E je neseparabilní s triviálním jádrem a stupněm p^2. Podle věty 6.4.3 je pak rovna složení dvou kopii Frobeniova endomorfismu s isomorfismem, $[p] = \iota \circ \pi^2$. Isogenie π^2 zobrazuje:

$$\pi^2 \quad : \quad E : y^2 = x^3 + ax + b \quad \longrightarrow \quad E' : y^2 = x^3 + a^{p^2}x + b^{p^2},$$

tyto dvě křivky jsou proto isomorfní pod ι. Díky vlastnostem charakteristiky:

$$j(E) = j(E') = 1728\frac{4a^{3p^2}}{4a^{3p^2} + 27b^{2p^2}} = \left(1728\frac{4a^3}{4a^3 + 27b^2}\right)^{p^2} = j(E)^{p^2},$$

j-invariant naší křivky je tedy fixovaný automorfismem $x^{p^2} = x$ na $\overline{\mathbb{F}}_q$ a leží tak v $\mathbb{F}_{p^2}$. □

Důsledek 6.6.9. *Buď $E/\mathbb{F}_q$ supersingulární křivka. Pak existuje supersingulární $E'/\mathbb{F}_{p^2}$, která je s E isomorfní.*

Důkaz. Protože $j := j(E)$ leží v $\mathbb{F}_{p^2}$, příklad vyhovující křivky nad $\mathbb{F}_{p^2}$ pro $j \neq 0, 1728$ dává křivka $E' : y^2 = x^3 + 3j(1728-j)x + 2j(1728-j)^2$ s $j(E') = j$, viz věta 6.2.7, a případy $j = 0, 1728$ jsou zřejmé. □

Při uvažování grafů supersingulárních j-invariantů se zajímáme vesměs pouze na třídy isomorfismů, postačí nám tedy uvažovat všechny křivky pouze nad $\mathbb{F}_{p^2}$.

Značení 6.6.10. Buďte p, ℓ prvočísla. Graf supersingulárních j-invariantů nad $\overline{\mathbb{F}}_p$ spojené isogeniemi stupně ℓ značme $G_\ell(\overline{\mathbb{F}}_p)$.

Závěr

zu ende

Použitá značení

$a \mid b$	a dělí b
$\frac{1}{a}$	multiplikativní inverze a, tj. a^{-1}
$\nu_p(n)$	p-adická valuace n
$\left(\frac{a}{p}\right)$	Legendreův symbol a vzhledem k p
$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	množina přirozených, celých, racionálních, reálných, komplexních čísel
$\mathbb{Z}_d$	okruh zbytků modulo d
$\mathbb{F}_q$	konečné těleso s q prvky
$\overline{K}$	algebraický uzávěr tělesa K
$K^\times$	multiplikativní podrupa tělesa K
$\mathbb{P}^n(K)$	projektivní prostor nad K o dimenzi $n+1$
$E(K)$	množina bodů křivky E nad K
$\#E(K)$	počet bodů na křivce E nad konečným tělesem K
$\mathcal{O}, O$	bod v nekonečnu křivky E
$[n]_E, [n]$	násobení n na křivce E
π, π_E	Frobeniův endomorfismus
$\widehat{\phi}$	isogenie duální k ϕ
$\deg \phi$	stupeň isogenie ϕ
$\ker \phi$	jádro isogenie ϕ
$\#\ker \phi$	velikost jádra isogenie ϕ
$\langle G \rangle$	podgrupa generovaná množinou G
E/G	obraz E v separabilní isogenii s jádrem G
$E/\mathfrak{a}$	obraz E v isogenii generované ideálem $\mathfrak{a}$
$E[n]$	n-torze křivky E
$\mathrm{End}(E)$	okruh endomorfismů E
$\mathrm{Ell}_\mathcal{O}$	množina eliptických křivek nad $\mathbb{F}_p$ s okruhem endomorfismů $\mathrm{End}(E) \cong \mathcal{O}$

$M \otimes_R N$	tenzorový součin R-modulů M a N
$\mathrm{End}^0(E)$	algebra endomorfismů E
$\mathrm{Tr}\,\phi, \mathrm{Tr}\,\alpha$	stopa endomorfismu ϕ, stopa $\alpha \in \mathrm{End}^0(E)$
$\mathrm{N}\,\alpha$	norma $\alpha \in \mathrm{End}^0(E)$
$\widehat{\alpha}$	Rosatiho involuce $\alpha \in \mathrm{End}^0(E)$
$j(E)$	j-invariant křivky E
$G_\ell(\overline{\mathbb{F}}_p)$	graf supersingulárních j-invariantů nad $\overline{\mathbb{F}}_p$ spojených isogeniemi stupně ℓ
$R[x]$	okruh polynomů s koeficienty nad okruhem R
$K(a_1, \ldots, a_n)$	nejmenší nadtěleso K obsahující prvky $a_1, \ldots, a_n$
$[K : L]$	stupeň rozšíření tělesa K nad L
$\alpha(x)$	lineární transformace $x \mapsto \alpha x$ působící na $\mathbb{Q}(\theta)$
M_α	matice odpovídající $\alpha(x)$
$\mathrm{Tr}\,M$	stopa matice M
$\det M$	determinant matice M
$Tr_K(\alpha)$	stopa prvku α v K
$N_K(\alpha)$	norma prvku α v K
$\mathcal{O}_K$	okruh celých algebraických čísel tělesa K
$Cl(\mathcal{O})$	grupa tříd ideálů pořádku $\mathcal{O}$
$h_\mathcal{O}$	řád grupy $Cl(\mathcal{O})$
(a)	hlavní ideál generovaný prvkem a
$\frac{\mathfrak{a}}{m}$	lomený ideál $\frac{\mathfrak{a}}{m}$
$N_\mathcal{O}(\mathfrak{a})$	norma ideálu $\mathfrak{a} \subseteq \mathcal{O}$, tj. $\lvert\mathcal{O}/\mathfrak{a}\rvert$
$\mathfrak{a} + \mathfrak{b}$	součet ideálů $\mathfrak{a}$ a $\mathfrak{b}$
$\mathfrak{ab}, \mathfrak{a} \cdot \mathfrak{b}$	součin ideálů $\mathfrak{a}$ a $\mathfrak{b}$
$\mathfrak{a}\vert\mathfrak{b}$	ideál $\mathfrak{a}$ dělí ideál $\mathfrak{b}$
G/H	faktorgrupa G podle H
$\deg f$	stupeň polynomu, lomené funkce f
f'	derivace f
$f\vert_M$	zúžení f na množinu M
$\phi\vert_\ell$	zúžení isogenie ϕ na ℓ-torzi
$f \in O(g)$	f roste asymptoticky nejvýše stejně rychle jako g

Literatura

[1] Azarderakhsh, Reza, Matthew Campagna, Craig Costello, Luca De Feo, Basil Hess, Amir Jalali, Brian Koziel, Brian LaMacchia, Patrick Longa, Michael Naehrig, Joost Renes, Vladimir Soukharev a David Urbanik: *SIKE: Supersingular Isogeny Key Encapsulation*. 2017.

[2] Beullens, Ward, Thorsten Kleinjung a Frederik Vercauteren: *CSI-FiSh: Efficient Isogeny based Signatures through Class Group Computations*. 2019. Dostupné z: https://eprint.iacr.org/2019/498.

[3] Bottinelli, Paul, Victoria de Quehen, Christopher Leonardi, Anton Mosunov, Filip Pawlega a Milap Sheth: *The Dark SIDH of Isogenies*. ISARA Corporation, Waterloo, Canada. 2019. Dostupné z: https://eprint.iacr.org/2019/1333.

[4] Bisson, Gaetan a Andrew V. Sutherland: *Computing the Endomorphism Ring of an Ordinary Elliptic Curve Over a Finite Field*. 2009. Dostupné z: https://arxiv.org/abs/0902.4670.

[5] Castirik, Wouter, Tanja Lange, Chloe Martindale, Lorenz Panny a Joost Renes: *CSIDH: An Efficient Post-Quantum Commutative Group Action*. 2018.

[6] Čermák, Filip a Matěj Doležálek: *Teorie nejen čísel*. Seriál korespondenčního matematického semináře.

[7] Cervantes-Vázquez, Daniel, Eduaro Ochoa-Jiménez a Francisco Rodríguez-Henríquez: *eSIDH: the revenge of the SIDH*. 2020.

[8] Chen, Evan: *An Infinitely Large Napkin*. Dostupné z: https://venhance.github.io/napkin/Napkin.pdf.

[9] Childs, Andrew, David Jao a Vladimir Soukharev: *Constructing elliptic curve isogenies in quantum subexponential time*. Journal of Mathematical Cryptology,8(1), 2014. Dostupné z: https://arxiv.org/abs/1012.4019

[10] Chuang, Isaac L. a Michael A. Nielsen: *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.

[11] Conrad, Keith: *Trace and Norm*. University of Connecticut, Connecticut. Dostupné z: https://kconrad.math.uconn.edu/blurbs/galoistheory/tracenorm.pdf.

[12] Conrad, Keith: *Ideal Factorization*. University of Connecticut, Connecticut. Dostupné z: https://kconrad.math.uconn.edu/blurbs/gradnumthy/idealfactor.pdf.

[13] Conrad, Keith: *The Conductor Ideal*. University of Connecticut, Connecticut. Dostupné z: https://kconrad.math.uconn.edu/blurbs/gradnumthy/idealfactor.pdf.

[14] Costello, Craig: *B-SIDH: supersingular isogeny Diffie-Hellman using twisted torsion*. Microsoft Research, USA, 2019. Dostupné z: https://eprint.iacr.org/2019/1145.

[15] Costello, Craig: *Supersingular isogeny key exchange for beginners*. Microsoft Research, USA, 2019. Dostupné z: https://eprint.iacr.org/2019/1321.

[16] Couveignes, Jean-Marc: *Hard Homogenous Spaces*. 2006. Dostupné z: https://eprint.iacr.org/2006/291.pdf.

[17] Cox, David: *Primes of the form $x^2 + ny^2$: Fermat, Class Field Theory and Complex Multiplication*. New York, 1989.

[18] De Feo, Luca: *Fast Algorithms for Towers of Finite Fields and Isogenies*. EcolePolytechnique X, 2010.

[19] De Feo, Luca, David Jao a Jérôme Plût: *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*. Math. Cryptol. 8(3): 209-247, 2014. Dostupné z: https://eprint.iacr.org/2011/506.pdf.

[20] De Feo, Luca: *Mathematics of Isogeny Based Cryptography*. Université de Versailles & Inria Saclay, 2017. Dostupné z: https://arxiv.org/abs/1711.04062.

[21] De Feo, Luca: *Isogeny based Cryptography: what's under the hood?* École des Mines de Saint-Étienne, Gardanne, 2018. Dostupné z: http://defeo.lu/docet/talk/2018/11/15/gardanne/.

[22] De Feo, Luca, Jean Kieffer a Benjamin Smith: *Towards practical key exchange from ordinary isogeny graphs*. 2018. Dstupné z: https://eprint.iacr.org/2018/485.

[23] De Feo, Luca a Steven Galbraith: *SeaSign: Compact isogeny signatures from class group actions*. EUROCRYPT 2019. Dostupné z: https://eprint.iacr.org/2018/824.

[24] De Feo, Luca, David Kohel, Antonin Leroux, Christopher Petit a Benjamin Wesolowski: *SQISign: compact post-quantum signatures from quaternions and isogenies*. 2020. Dostupné z: https://eprint.iacr.org/2020/1240.

[25] Deng, Yu-Hao, Xing Ding, Lin Gan, Peng Hu, Yi Hu, Ming-Cheng Chen, Xiao Jiang, Hao Li, Li Li, Yuxuan Li, Nai-Le Liu, Chao-Yang Lu, Yi-Han Luo, Jian-Wei Pan, Li-Chao Peng, Jian Qin, Hui Wang, Zhen Wang, Zhen Wang, Guangwen Yang, Lixing You, Han-Sen Zhong:*Quantum computational advantage using photons.* Science Magazine. 2020. Dostupné z: https://science.sciencemag.org/content/370/6523/1460.full

[26] Delfs, Christina a Steven D. Galbraith: *Computing isogenies between supersingular elliptic curves over* $\mathbb{F}_p$. Des. Codes Cryptography, 78(2), 2016. Dostupné z: https://arxiv.org/abs/1310.7789.

[27] Deuring, Max: *Die typen der multiplikatorenringe elliptischer funktionenkörper*. Abhandlungen aus dem mathematischen Seminar der Universität Hamburg 14, 1941.

[28] Diffie, Whitfield a Martin Hellman: *New Directions in Cryptography*. IEEE Transactions on Information Theory 22, 1976.

[29] Eisenträger, Sean H., Kristin Lauter, Travis Morrison a Christopher Petit: *Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions*. Advances in Cryptology – EUROCRYPT 2018, Lecture Notes in Computer Science, pages 329–368. Springer International Publishing, 2018.

[30] Feynman, Richard P.: *Simulating physics with computers*. Int J Theor Phys 21, 467–488, 1982. Dostupné z: https://doi.org/10.1007/BF02650179.

[31] Galbraith, Steven D.: *Constructing Isogenies Between Elliptic Curves Over Finite Fields*. LMS J. Comput. Math., 199, 118-138, 1999. Dostupné z: https://www.math.auckland.ac.nz/~sgal018/iso.pdf.

[32] Galbraith, Steven D., Florian Hess a Nigel P. Smart: *Extending the GHS Weil descent attack*. EUROCRYPT 2002, Springer LNCS 2332 29-44, 2002.

[33] Galbraith, Steven D. a Anton Stolbunov: *Improved Algorithm for the Isogeny Problem for Ordinary Elliptic Curves*. Applicable Algebra in Engineering, Communication and Computing, Vol. 24, No. 2, 2013. Dostupné z: https://arxiv.org/abs/1105.6331.

[34] Galbraith, Steven D., Christopher Petit, Barak Shani a Yan Bo Ti: *On the security of supersingular isogeny cryptosystems*. International Conference on the Theory and Application of Cryptology and Information Security. Springer, 2016.

[35] Griffiths, Robert B.: *Hilbert Space Quantum Mechanics*. 2014.

[36] Grover, Lov K.: *A fast quantum mechanical algorithm for database search.*28th Annual ACM Symposium on the Theory of Computing, 1996. Dostupné z: https://arxiv.org/abs/quant-ph/9605043.

[37] Hartshorne, Robin: *Algebraic Geometry*. Berkley: Springer-Verlag, 1977.

[38] Ireland, Kenneth a Michael Rosen: *A Classical Introduction to Modern Number Theory*. New York, Berlin a Heidelberg: Springer-Verlag, 1982.

[39] Jao, David a David Urbanik: *Extra Secrets from Automorphisms and SIDH-based NIKE*, 2018.

[40] Johnson, Don, Alfred Menenzes a Scott Vanstone: *The Elliptic Curve Digital Signature Algorithm (ECDSA)*. Certicom a Department of Combinatorics & Optimization, University of Waterloo, Ontario, Canada. 2001.

[41] Johnson, Lee W., Ronald Dean Riess a Jimmy Thomas Arnold: *Introduction to Linear Algebra*. Fifth edition. Virginia Polytechnic Institute and State University: Addison-Wesley, 2002.

[42] Karamlou, Amir H, Willieam A. Simon, Amara Katabarwa, Travis L. Scholten, Borja Peropandre a Yudong Cao: *Analyzing the Performance of Variational Quantum Factoring on a Superconducting Quantum Processor*. Zapata Computing, Boston; Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge a IBM Quantum, IBM T. J. Watson Research Center, New York, 2020. Dostupné z: https://www.zapatacomputing.com/publications/analyzing-the-performance-of-variational-quantum-factoring-on-a-superconducting-quantum-processor/.

[43] Karásková, Zdislava: *Supersingulární isogenie a jejich využití v kryptografii*. Diplomová práce. Brno: Masarykova univerzita, 2019. Dostupné z: https://is.muni.cz/th/mt87i/.

[44] Koblitz, Neal: *Elliptic curve cryptosystems*. Mathematics of Computation. 48 (177): 203–209, 1987.

[45] Kohel, David R.: *Endomorphism rings of elliptic curves over finite fields*. University of California, Berkley, 1996.

[46] Lagarias, Jeffrey C. a Andrew M. Odlyzko: *Effective Versions of the Chebotarev Density Theorem*. Algebraic Number Fields,L-Functions and Galois Properties (A. Fröhlich, ed.), pp. 409–464. New York, London: Academic Press, 1977.

[47] Leonardi, Christopher: *A Note on the Ending Elliptic Curve in SIDH*. 2020. Dostupné z: https://eprint.iacr.org/2020/262.

[48] Marcus, Daniel A.: *Number fields*. New York: Springer-Verlag, 1977.

[49] Matushak, Andy a Michael A. Nielsen: *Quantum computing for the very curious*. San Francisco, 2019. Dostupné z: https://quantum.country/qcvc.

[50] Menezes, Afred, Tatsuki Okamoto a Scott Vanstone: *Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field*. IEEE Transactions on Information Theory 39, 1993.

[51] Miller, Victor: *Use of elliptic curves in cryptography*. Advances in Cryptology—CRYPTO '85, Lecture Notes in Computer Science, vol 218. Springer, pp 417–426, 1986.

[52] Mordell, Luis J.: *On the rational solutions of the indeterminate equations of the third and fourth degrees*. Cambridge, 1922.

[53] Neukirch, Jürgen: *Algebraic Number Theory*. New York: Springer-Verlag, 1999.

[54] NIST. Post-Quantum Cryptography. Dostupné z: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/.

[55] Perutka, Tomáš: *Vyjadřování prvočísel kvadratickými formami*. Středoškolská odborná činnost. Brno: Masarykova univerzita, 2017. Dostupné z: https://socv2.nidv.cz/archiv39/getWork/hash/ff6e75d5-f922-11e6-848a-005056bd6e49.

[56] Perutka, Tomáš: *Užití dekompoziční grupy k důkazu zákona kvadratické reciprocity*. Středoškolská odborná činnost. Brno: Masarykova univerzita, 2018. Dostupné z: https://socv2.nidv.cz/archiv40/getWork/hash/1984482c-1298-11e8-90e4-005056bd6e49.

[57] Pezlar, Zdeněk: *Zajímavá využití algebraické teorie čísel*. Středoškolská odborná činnost. Brno: Masarykova univerzita, 2020. Dostupné z: https://socv2.nidv.cz/archiv42/getWork/hash/921aa7aa-568d-11ea-9fea-005056bd6e49.

[58] Pizer, Arnold K.: *Ramanujan graphs and Hecke operators*. Bulletin of the American Math Society, 23, 1990.

[59] Proos, John a Christof Zalka: *Shor's discrete logarithm quantum algorithm for elliptic curves*. Department of Combinatorics & Optimization, University of Waterloo, Ontario, Canada, 2008. Dostupné z: https://arxiv.org/abs/quant-ph/0301141.

[60] Pupík, Petr: *Užití grupy tříd ideálů při řešení některých diofantických rovnic*. Diplomová práce. Brno: Masarykova univerzita, 2009. Dostupné z: https://is.muni.cz/th/v8xsj/.

[61] Raclavský, Marek: *Racionální body na eliptických křivkách*. Bakalářská práce. Praha: Univerzita Karlova, 2014. Dostupné z: https://is.cuni.cz/webapps/zzp/detail/143352/.

[62] Rivest, Ronald L., Adi Shamir a Leonard M. Adleman: *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*. 1977. Dostupné z: https://people.csail.mit.edu/rivest/Rsapaper.pdf.

[63] Rosický, Jiří: *Algebra*. Brno: Masarykova univerzita, 2002.

[64] Shengyu, Zhang: *Promised and Distributed Quantum Search Computing and Combinatorics*. Proceedings of the Eleventh Annual International Conference on Computing and Combinatorics, Berlin, Heidelberg, 2005.

[65] Shor, Peter W.: *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*. New York: Springer-Verlag, 1994. Dostupné z: https://arxiv.org/abs/quant-ph/9508027.

[66] Schoof, René: *Elliptic Curves Over Finite Fields and the Computation of Square Roots* mod p. Journal de Théorie des Nombres de Bordeaux 7, 1985. Dostupné z: https://www.ams.org/journals/mcom/1985-44-170/S0025-5718-1985-0777280-6/S0025-5718-1985-0777280-6.pdf.

[67] Schoof, René: *Counting points on elliptic curves over finite fields*. Journal de Théorie des Nombres de Bordeaux 7, 1995. Dostupné z: https://www.mat.uniroma2.it/~schoof/ctg.pdf.

[68] Siegel, Carl: *Über die Classenzahl quadratischer Zahlkörp*. Acta Arithmetica, 1(1), 1935.

[69] Silverman, Joseph H.: *The Arithmetic of Elliptic Curves*. New York: Springer-Verlag, 1992.

[70] Silverman, Joseph H.: *Advanced Topics in the Arithmetic of Elliptic Curves*. New York: Springer-Verlag, 1994.

[71] Rostovtsev, Alexander a Anton Stolbnov: *Public-key cryptosystem based on isogenies*. 2006. Dostupné z: http://eprint.iacr.org/2006/145/.

[72] Suchánek, Vojtěch: *Vulkány isogenií v kryptografii*. Diplomová práce. Brno: Masarykova univerzita, 2020. Dostupné z: https://is.muni.cz/th/pxawb/.

[73] Sutherland, Andrew V.: *Isogeny Volcanoes*. 2012. Dostupné z: https://arxiv.org/abs/1208.5370.

[74] Sutherland, Andrew V.: *Identifying supersingular elliptic curves*. 2012. Dostupné z: https://arxiv.org/abs/1107.1140

[75] Sutherland, Andrew V.: *Elliptic Curves*. Massachusetts Institute of Technology, 2017. Dostupné z: https://math.mit.edu/classes/18.783/2017/lectures.html.

[76] Tani, Seiichiro: *Claw Finding Algorithms Using Quantum Walk*. Theoretical Computer Science, 410(50):5285-5297, 2009.

[77] Tate, John: *Endomorphisms of Abelian Varieties over Finite Fields*. Inventiones Mathematicae, 2 (2): 134–144, Cambridge, 1966.

[78] Vélu, Jacques: *Isogénies entre courbes elliptiques*. Comptes Rendus de l'Académie des Sci-ences de Paris, 1971.

[79] Washington, Lawrence C.: *Elliptic Curves: Number theory and cryptography*. Maryland, 2008.

[80] Waterhouse, William C.: *Abelian varieties over finite fields*. Annales scientifiques de l'École Normale Supérieure, 1969.

[81] Weil, André: *L'arithmétique sur les courbes algébriques*. Acta Mathematica 52, 1929.