STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST

Obor č. 1: Matematika a statistika

Medúzy a posloupnosti průměrů

Zdeněk Pezlar
Jihomoravský kraj

Brno 2021

STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST

Obor č. 1: Matematika a statistika

Medúzy a posloupnosti průměrů

On Jellyfish and Sequences of Means

Autor: Zdeněk Pezlar
Škola: Gymnázium Brno, třída Kapitána Jaroše, p. o.
Kraj: Jihomoravský
Vedoucí: Mgr. Vojtěch Suchánek
Konzultant: 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 rekurentní 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, ?.

Na tomto místě končí článek [?], na kterém je práce založená. My jsme se rozhodli uvážit v potaz i podobné posloupnosti užívající průměry nad konečnými tělesy. Ukážeme, že jedna z nich je s AG posloupnosti téměř shodná, druhá se však liší. Grafy těchto posloupností charakterizujeme a ukážeme, že jsou ještě zajímavější, než pouhé medúzy. Ve finální části práce i tuto posloupnost propojíme s teorií dynamických systémů a eliptických křivek.

Kapitola 1

AG posloupnost nad reálnými čísly

Nejprve se budeme zabývat posloupností dvojic kladných reálných čísel, přičemž každá další je tvořena aritmetickým a geometrickým průměrem té předchozí. I v tomto jednoduchém prostředí narazíme na posloupnost v místech, kde bychom vůbec nehledali.

1.1 Seznámení s posloupností

Definice 1.1.1. Ať a, b jsou dvě kladná reálná čísla. Pak definujme *AG posloupnost* jako posloupnost $(a_n, b_n)_{n=0}^{\infty}$ tak, že $(a_0, b_0) = (a, b)$ a:

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

Jednotlivá čísla a_i a b_i nazveme *složkami* prvku (a_i, b_i) této posloupnosti.

Toto značení ponechme po zbytek sekce. První vlastnosti, které si všimněme, je monotónnost obou složek $(a_n)_{n=0}^{\infty}$ a $(b_n)_{n=0}^{\infty}$. Z *AG* nerovnosti je totiž platné $a_n \geqslant b_n$ a proto:

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

posloupnost $(b_n)_{n=0}^{\infty}$ je proto rostoucí (pokud $a_0 \neq b_0$, tak ostře rostoucí). Obdobně můžeme psát:

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

posloupnost $(a_n)_{n=0}^{\infty}$ je tedy naopak klesající. Protože průměry dvou čísel leží mezi nimi, obě posloupnosti jsou shora svírané prvkem a a zdola b. Libovolná ohraničená monotónní posloupnost konverguje, víme tedy, že obě posloupnosti $(a_n)_{n=0}^{\infty}$ a $(a_n)_{n=0}^{\infty}$ konvergují. Abychom získali nějakou představu o jejich limitách, ukážeme si pár příkladů.

Pokud si zvolíme $a = b = 5$, tak jsou obě hodnoty konstantní, to příliš zajímavě není. Zvolme si tedy například trochu zážívnější dvojici $a = 2, b = 8$. Pak můžeme psát:

a_i	b_i
2	8
5	4
4.5	4.472135955000...
4.486067977500...	4.486046343664...
4.486057160582...	4.486057160569...
4.486057160575...	4.486057160575...
4.486057160575	4.486057160575...
4.486057160575	4.486057160575...
⋮	⋮

GRAF

V tomto případě prvky *AG* posloupnosti zdárně konvergují ke společné hodnotě. Spočítejme si ještě pro jistotu jednu posloupnost, tentokrát pro dvojici $a = 1$ a $b = \sqrt{2}$. Tuto dvojici vůbec nevolíme náhodně. Vrátíme se k ní ještě za chvíli, její *AG* posloupnost lze použít k rychlému počítání čísla π.

a_i	b_i
1	1.414213562373...
1.207106781187...	1.189207115003...
1.198156948095...	1.198123521493...
1.198140234794...	1.198140234677...
1.198140234736...	1.198140234736...
1.198140234736...	1.198140234736...
1.198140234736...	1.198140234736...
⋮	⋮

Složky *AG* posloupnosti vždy konvergují ke společné hodnotě.

Věta 1.1.2. *Ať $(a_n, b_n)_{n=0}^{\infty}$ je AG posloupnost. Pak limity čísel a_n a b_n pro n jdoucí do nekonečna existují a jsou si navzájem rovné.*

Důkaz. Existenci limit jsme si ukázali výše. Jelikož platí:

$$0 \leqslant a_n - b_n = 2\left(a_n - \frac{a_n + b_n}{2}\right) = 2(a_n - a_{n+1})$$

a navíc díky existence limity $\lim_{n\to\infty} a_n - a_{n+1} = 0$, je posloupnost $(a_n - b_n)_{n=0}^{\infty}$ sevřena mezi dvěma posloupnostmi s nulovou limitou, konstantně nulovou posloupností a $(a_n - a_{n+1})_{n=0}^{\infty}$, má ji proto nulovou též. □

Definice 1.1.3. Tuto společnou limitu nazvěme *aritmeticko-geometrickým průměrem*, zkráceně *AG-průměrem*, čísel a, b. Toto číslo značme $\mathrm{AG}(a, b)$.

Následující věta shrnuje základní vlastnosti *AG* posloupnosti.

Věta 1.1.4. *Mějme $a, b, k \in \mathbb{R}^+$. Pro AG posloupnost platí:*

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

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

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

(iv) $\mathrm{AG}(1 - x, 1 + x) = \mathrm{AG}(a, b)$, *kde* $x = \frac{1}{a}\sqrt{a^2 - b^2}$.

Vraťme se zpět k příkladům, které jsme uvedli na začátku. Třetí iterace *AG* posloupnosti čísel 2 a 8 se s limitou shoduje už na čtyřech desetinných místech. Ta následující dokonce na desíti. Opravdu, *AG* posloupnost konverguje velmi rychle.

Věta 1.1.5. *Ať $(a_n, b_n)_{n=0}^{\infty}$ je AG posloupnost. Pak složky $(a_n)_{n=0}^{\infty}$ a $(b_n)_{n=0}^{\infty}$ konvergují ke společné limitě kvadraticky.*

Tzv. *řád konvergence* nám říká, jak přesně jak rychle posloupnost konverguje. Přesná definice řádu σ posloupnosti x_i konvergující k limitě L je, že pro všechna $n \in \mathbb{N}$ a nějakou konstantu C platí:

$$\frac{|x_{n+1} - L|}{|x_n - L|^{\sigma}} \leqslant C.$$

Pro $\sigma = 2$ získáme *kvadraticky konvergentní posloupnost*. U takové posloupnosti se tak v každém dalším kroku se obě čísla *přibližně* rovnají limitě na dvakrát více desetinných míst.

Důkaz. Zaveďme pomocné posloupnosti $(x_n)_{n=0}^{\infty}$ a $(\varepsilon_i)_{n=0}^{\infty}$ splňující $x_i = \frac{a_i}{b_i} = 1 + \varepsilon_i$ pro každé i. Platí $\varepsilon_i \geqslant 0$ pro každé i. Pak pro libovolné n platí:

$$x_{n+1} = \frac{a_n + b_n}{2\sqrt{a_n b_n}} = \frac{\sqrt{\frac{a_n}{b_n}} + \sqrt{\frac{b_n}{a_n}}}{2} = \frac{\sqrt{x_n} + \frac{1}{\sqrt{x_n}}}{2},$$

takže:

$$\begin{aligned} 1 + \varepsilon_{n+1} = x_{n+1} &= \frac{\sqrt{x_n} + \frac{1}{\sqrt{x_n}}}{2} \\ &= \frac{\sqrt{1 + \varepsilon_n} + \frac{1}{\sqrt{1+\varepsilon_n}}}{2}. \end{aligned}$$

Taylorova řada funkce $\sqrt{x}$ v bodě 1 je $1 + \frac{x}{2} - \frac{x^2}{8} + O(x^3)$ a Taylorova řada funkce $\sqrt{x}^{-1}$ je $1 - \frac{x}{2} + \frac{3x^2}{8} + O(x^3)$. Proto pro n dostatečně velké a tedy ε_n dostatečně malé platí:

$$1 + \varepsilon_{n+1} = 1 + \frac{\varepsilon_n^2}{8} + O(\varepsilon_n^3),$$

řád konvergence $\frac{a_i}{b_i} \to 1$ je tedy kvadratický. □

Prozatím může vypadat, že tato posloupnost leží na uzavřeném ostrůvku vzdálená od jiných oblastní matematiky. Toto zdání však nemůže být dál od pravdy. Zamysleme se přímo nad samotným průměrem, limity posloupnost. Pro čísla 2 a 8 získáváme průměr $4.48605716\ldots$. Jak takové číslo určit uzavřeně? K nalezení odpovědi budeme muset nakouknout do sféry tzv. „eliptických integrálů“.

1.2 Eliptické integrály

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

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

Tento integrál a tzv. eliptický integrál „druhé druhu“ 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:*

$$\frac{\pi}{2} \cdot \frac{1}{\mathrm{AG}(1, x)} = K\left(\sqrt{1 - x^2}\right)$$

Pokud definujeme:

$$I(a, b) := \int_0^{\pi/2} \frac{d\theta}{\sqrt{a^2 \sin^2 \theta + b^2 \cos^2 \theta}},$$

tak snadno uvidíme, že $I(a, b) = \frac{1}{a} K(x)$, kde $x = \frac{1}{a}\sqrt{a^2 - b^2}$. Takové x jsme už ale někde viděli, konkrétně ve větě 1.1.4 iv). Gaussovu větu poté můžeme díky části ii) věty 1.1.4 přepsat na:

$$\frac{\pi}{2} \frac{1}{\mathrm{AG}(a, b)} = I(a, b).$$

Skutečnosti, že se $\frac{1}{AG(1,\sqrt{2})}$ a $\frac{2}{\pi} I(1, \sqrt{2})$ shodují na 11 místech, si mladý Gauss všiml ve svém deníků již ve svých dvaadvaceti letech. [Pi and AGM] Metoda, kterou pak celou větu dokázal spočívá v důkazu výsledku $I(a, b) = I(a_1, b_1)$, ke kterému dojde po několika přiměřeně bolestných krocích, neboli jak Gauss sám pravil:

> *„After the development has been made correctly“*

Důkazem tohoto výsledku jsme hotovi, protože pak v limitním případě $I(a, b) = I(\mathrm{AG}(a, b), \mathrm{AG}(a, b)) = \frac{1}{\mathrm{AG}(a,b)} I(1, 1) = \frac{1}{\mathrm{AG}(a,b)} \cdot \frac{\pi}{2}$. Plný důkaz hledejte na [Pi and AGM].

Jelikož *AG* posloupnost konverguje kvadraticky, tato spojitost nám může pomoci počítat právě eliptické integrály velmi rychle. K čemu jinému nám ale rychlá konvergence této posloupnosti může být k užitku?

1.3 Rychlé výpočty elementárních funkcí

AG posloupnost může být využita například při počítání elementárních funkcí. Motivace použití rekurzivně definovaných posloupností může poskytnout například Newtonova metoda pro počítání odmocniny v kvadratickém čase:

Věta 1.3.1. *(Newton) Ať $N > 1$ je dané. Pak posloupnost $(x_n)_{n=0}^{\infty}$ splňující $x_0 = N$:*

$$x_{n+1} = \frac{1}{2}\left(x_n + \frac{N}{x_n}\right)$$

konverguje kvadraticky k $\sqrt{N}$.

Důkaz existence a hodnoty limity, ani řádu konvergence není obtížný. Nešlo by obdobně využít i *AG* posloupnost? Ukáže se, že ano.

Totiž přirozený logaritmus je „přirozeně“ spojen s eliptickými integrály [Borw, Pi and AGM]:

$$K(\sqrt{1-x^2}) = \left(1 + O(x^2)\right) \ln\left(\frac{4}{x}\right),$$

kde onen chybový člen lze jednoduše odhadnout []. Pro x dostatečně malé nám pak ke spočítání logaritmu velkého čísla postačí použít kvadraticky konvergující *AG* posloupnost. Dá se jednoduše ukázat, že platí vztahy:

$$\arccos(x) = \arctan\left(\frac{\sqrt{1-x^2}}{x}\right),$$
$$\arctan(x) = \mathrm{Im}(\log(1+ix)).$$

Pomocí nich a *komplexního AG*, o kterém budeme mluvit dále, pak již můžeme spočítat inverzní funkce k základním goniometrickým funkcím a proto i je samotné.

1.4 Posloupnosti s ostatními průměry

Aritmetický a geometrický průměr nám vygenerovaly posloupnost, která skýtá překvapivě mnoho praktických aplikací. S takovým úspěchem pro jednu dvojici průměrů se pak jenom nabízí vzít v potaz i nějaké další. Zapojíme proto do práce i harmonický průměr, který je pro dvě čísla definován následovně:

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

Definice 1.4.1. Ať a, b jsou dvě kladná reálná čísla. Pak definujme *HG posloupnost* $(a_n, b_n)_{n=0}^{\infty}$ tak, že $(a_0, b_0) = (a, b)$ a:

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

Obdobně definujeme *AH posloupnost* $(a_n, b_n)_{n=0}^{\infty}$ tak, že $(a_0, b_0) = (a, b)$ a:

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

Kvůli nerovnostem panujícím mezi průměry můžeme imitovat důkaz věty 1.1.2, čímž získáme, že obě posloupnosti konvergují k hodnotám $HG(a, b)$, resp. $AH(a, b)$. Abychom tyto posloupnosti porovnali s AG posloupností, spočítejme průměry pro $a = 2$ a $b = 8$. První posloupnost vypadá následovně:

a_i	b_i
2	8
3.2	4
3.555555555555...	3.577708763999...
3.566597760054...	3.566614959874...
3.566606359943...	3.566606359954...
3.566606359948...	3.566606359948...
3.566606359948...	3.566606359948...
3.566606359948...	3.566606359948...
⋮	⋮

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

Nyní přichází čas pro AH posloupnost. Bude mít něco společného s předchozími dvěma posloupnostmi? Podívejme se, jak se posloupnost chová s počátečními prvky $a_0 = 2$ a $b_0 = 8$:

a_i	b_i
2	8
5	3.2
4.1	3.902439024390...
4.001219512195...	3.998780859494...
4.000000185845...	3.999999814155...
4.000000000000...	4.000000000000...
4.000000000000...	4.000000000000...
4.000000000000...	4.000000000000...
⋮	⋮

AH posloupnost 2 a 8 tedy konverguje zjevně k číslu 4. Tento úkaz vysvětlí jednoduché pozorování, totiž že součin obou složek je přes všechny prvky posloupnosti konstantní. Platí:

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

Jelikož opět obě složky posloupnosti konvergují ke stejné hodnotě $AH(a,b)$, ta musí splňovat $AH(a,b)^2 = ab$, tedy $AH(a,b) = \sqrt{ab}$. Tento trend, kdy se *AH* drasticky liší od předchozích dvou, bude v jistém smyslu držet i v pozdějších částech práce, kdy posloupnosti uvažujeme nad konečnými tělesy. Adaptace *AG* a *GH* posloupností budou velmi spřízněné, zatímco *AH* s nimi má velmi málo společného.

Samozřejmě můžeme místo těchto třech průměrů uvažovat libovolné *mocninné průměry* a všechny takové posloupnosti budou konvergovat, to díky platným nerovnostem mezi těmito průměry. Pro mnohem více o teorii s těmito posloupnostmi vřele doporučuji knihu [AG and pi].

Na konec této sekce ještě zmiňme, že se nemusíme zastavit pouze na dvou průměrech. Zobecněná *AGH* posloupnost pro tři proměnné byla zběžně studovaná v ?, v [?] byly též studovány ještě posloupnosti čtyř a dokonce šesti čísel. Nyní se ale obraťme list a podívejme se více na vlastnosti *AG* posloupnosti v kontextu teorie čísel.

Kapitola 2

AG posloupnost nad konečnými tělesy

Když jsme nyní zodpovědně prozkoumali *AG* posloupnost nad reálnými čísly, zamysleme se, jaké informace nám *AG* může poskytnout z pohledu teorie čísel, tedy nad konečnými tělesy. Nepřekvapí nás, že v konečném případě tato posloupnost skýtá hluboká propojení se zdánlivě nesouvisejícími odvětvími matematiky, konkrétně s *eliptickými křivkami*. O nich ale až později.

2.1 Základní poznatky

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 intuitivní.

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 jsou různé prvky $\mathbb{F}_q^\times$ splňují $\phi_q(ab) = 1$. Pak definujeme $AG_{\mathbb{F}_q}(a, b)$ jako posloupnost $(a_n, b_n)_{n=0}^\infty$ 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:

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

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 *roj* (angl. *swarm*) $AG_{\mathbb{F}_q}$ 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!

Věta 2.1.4. *Graf $AG_{\mathbb{F}_q}$ čítá $(q-1)(q-3)/2$ vrcholů a stejný počet hran.*

Důkaz. Uspořádaná dvojice (a, b) náleží do $AG_{\mathbb{F}_q}$, právě pokud platí $\phi_q(ab) = 1$, tedy buď jsou a, b obě čtverci v $\mathbb{F}_q$, nebo ani jedno. Počet uspořádaných dvojic různých nenulových čtverců je roven $(q-1)/2 \cdot (q-3)/2$ a stejný počet přispívají dvojice nečtverců. Dohromady získáme $2 \cdot (q-1)(q-3)/4$ vyhovujících dvojic. Protože z každého vrcholu vychází právě jedna orientovaná hrana, počet hran je roven počtu vrcholů. □

Grafy z příkladu jsou tvořeny 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 2.1.5. Souvislý orientovaný graf G nazveme *medúzou*, pokud je tvořen jediným cyklem H a pro každý vrchol $V \in H$ existuje unikátní předchůdce mimo cyklus, který sám nemá předchůdce.

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

Lemma 2.1.6. *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 2.1.7. *Roj $AG_{\mathbb{F}_q}$ je tvořen z několika medúz.*

Důkaz. Graf je určen zobrazením $(u, v) \longmapsto (u_1, v_1) \longmapsto \ldots$ 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 1.1.4 můžeme přenásobit všechny vrcholy nějakým $k \in \mathbb{F}_q$ a získat *přátelskou* medúzu. Příklady takových medúz jsou na TOM PŘÍKLADU NA ZAČÁTKU.

Definice 2.1.8. Ať $V \in AG_{\mathbb{F}_q}$ je medúza a (a, b) její prvek. Potom nazveme libovolnou medúzu obsahující prvek (ka, kb) pro $k \in \mathbb{F}_q$ *přítelem* medúzy V.

Kolik přátel má daná medúza? Na to zodpovídá následující propozice:

Věta 2.1.9. *Ať $(a, b) \in AG_{\mathbb{F}_q}$ leží v cyklu medúzy M a i je první index takový, že existuje $k \in \mathbb{F}_q$ splňující $(a_i, b_i) = (ka, kb)$. Pak má medúza M právě:*

$$\frac{q-1}{\mathrm{ord}_q(k)}$$

přátel.

Důkaz. Je zřejmé, že všechny ostatní prvky cyklu (a_i, b_i) splňující $a_i/b_i = a/b$ jsou ve tvaru $(a_i, b_i) = (k^x a_i, k^x b_i)$. Navíc, pokud přenásobíme všechny prvky M jedním z prvků podgrupy $\mathbb{F}_q \supseteq O_k := \left(\{k, k^2, \ldots, k^{\mathrm{ord}_2(k)} = 1\}, \times\right)$, pouze otočíme medúzu.

Přesněji, máme danou akci grup $\mathbb{F}_q \times AG_{\mathbb{F}_q} \longrightarrow AG_{\mathbb{F}_q}$, která pro $k \in \mathbb{F}_q$ zobrazí prvek (a, b) na (ka, kb). Nosná množina O_k je pak stabilizátorem pro libovolný prvek medúzy M. To znamená, že existuje bijekce mezi množinou prvků $k \in \mathbb{F}_q$, které zobrazí M na

medúzu s ní spřátelenou, a faktorgrupou $\mathbb{F}_q/O_k$, která má $\frac{q-1}{\mathrm{ord}_q(k)}$ prvků. □

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

Definice 2.1.10. Ať $H \subseteq AG_{\mathbb{F}_q}$ je medúza a $H_1, \ldots, H_k$ jsou všichni její přátelé. Pak $H \cup H_1, \cup \cdots \cup H_k$ nazvěme *hejnem medúz*.

2.2 Vlastnosti grafů

Ohledně medúz je hned několik hodnot, které má cenu zkoumat. Kolik je pro dané p dohromady medúz? Kolik existuje různých hejn? A na jaké délky cyklů můžeme narazit? Pojďme se na tyto hodnoty podívat trochu podrobněji.

Asi nejdůležitější hodnotou je pro nás počet medúz v celém hejnu. Tuto hodnotu studovali autoři původního článku [?] a pomocí eliptických křivek budeme moci uvést odhady na tato čísla.

Definice 2.2.1. Ať $q \equiv 3 \pmod 4$ je mocnina prvočísla. Pak označme $d(\mathbb{F}_q)$ počet všech medúz v grafu $AG_{\mathbb{F}_q}$. Navíc, označme $s(\mathbb{F}_q)$ počet všech hejn v grafu $AG_{\mathbb{F}_q}$.

V článku, ze kterého vycházíme, se $d(\mathbb{F}_q)$ nazývá *jellyfish number*, číslo $s(\mathbb{F}_q)$ není zmíněno vůbec a obecně hejna medúz nejsou nijak značena a jsou zmíněna pouze okrajově. Protože víme z příkladu ?, že délky cyklů se přes prvočísla mohou tak lišit, tak nás nepřekvapí, že i celkový počet medúz se chová poměrně různorodě. Pro představu uveďme malou tabulku pro prvočísla $p < 100$.

p	$d(\mathbb{F}_p)$
3	9
7	1
11	3
19	8
23	5
31	10
43	7
47	4
59	7
67	30
71	25
79	18
83	6

Tato náhodná povaha se nese i dál, na následujícím grafu vidíme jednotlivé hodnoty pro prvočísla $p < 10^5$:

Graf.

I po sobě jdoucí prvočísla mohou mít disproporcionálně různé počty medúz. Na příklad pro prvočíslo 1619 je počet medúz roven $d(\mathbb{F}_{1619}) = 56$ a hned o dům dál u prvočísla 1627 nalezneme v grafu enormní počet $d(\mathbb{F}_{1627}) = 2227$ medúz, skoro čtyřicetkrát více.

Autoři původního článku ukázali, že pro libovolně malé $\varepsilon > 0$ a q dostatečně velké platí:

$$d(\mathbb{F}_q) \geqslant \left(\frac{1}{2} - \varepsilon\right)\sqrt{q},$$

pomocí teorie eliptických křivek, o kterých se budeme bavit v pozdější části práce. V závěru práce spekulují, jak optimální tento odhad je a navrhují

2.3 HG posloupnost

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?

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 jsou různé prvky $\mathbb{F}_q^\times$ splňují $\phi_q(ab) = 1$. Pak definujeme $HG_{\mathbb{F}_q}(a, b)$ jako posloupnost $(a_n, b_n)_{n=0}^\infty$ 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 $\phi_q(a_{n+1}b_{n+1}) = 1$.

Definice 2.3.2. Definujme *roj* $HG_{\mathbb{F}_q}$ 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).

PRIKLADY, GRAF.

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

Věta 2.3.3. *Graf* $HG_{\mathbb{F}_q}$ *čítá* $(q-1)(q-3)/2$ *vrcholů a stejný počet hran.*

Důkaz. Analogický k důkazu věty 2.1.4. □

Lemma 2.3.4. *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 2.3.5. *Graf $GH_{\mathbb{F}_q}$ je tvořen z několika medúz.*

Důkaz. Analogický k důkazu věty 2.1.7. □

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 $HG_{\mathbb{F}_q}$. To nám napovídá, jaké bude konkrétní propojení těchto dvou grafů.

Věta 2.3.6. *Platí isomorfismus grafů $AG_{\mathbb{F}_q} \cong HG_{\mathbb{F}_q}$.*

Důkaz. Uvažme zobrazení $\psi : AG_{\mathbb{F}_q} \longrightarrow HG_{\mathbb{F}_q}$ určené předpisem $\psi((a, b)) = (1/a, 1/b)$. Ukážeme, že toto zobrazení definuje mezi grafy isomorfismus. Opravdu, uvažme orientovanou hranu v grafu $AG_{\mathbb{F}_q}$:

$$(a, b) \longmapsto \left(\frac{a+b}{2}, \sqrt{ab}\right),$$

poté v grafu $HG_{\mathbb{F}_q}$ má $\phi_q(a, b)$ hranu:

$$\psi(a, b) = \left(\frac{1}{a}, \frac{1}{b}\right) \longmapsto \left(\frac{2/ab}{1/a + 1/b}, \sqrt{\frac{1}{ab}}\right) = \left(\frac{2}{a+b}, \frac{1}{\sqrt{ab}}\right) = \psi\left(\frac{a+b}{2}, \sqrt{ab}\right).$$

□

Kapitola 3

AH posloupnost

Zatím jsme pracovali s dvěma dvojicemi průměrů z trojice - aritmetický, geometrický a harmonický. Co se proto podívat i na tu poslední? Tentokrát již ze začátku nebude pracovat pouze nad konečným tělesem, ale i s bodem v nekonečnu. Přesto se můžeme ptát, jak souvisí tato posloupnost a její grafy s předchozími dvěma, obzvláště ve spojení s eliptickými křivkami.

Definice 3.0.1. Ať K je těleso. Pak definujeme $\mathbb{P}^1(K)$ jako $K \cap \{\infty_i | i \in \mathbb{F}_q^\times\}$, kde ∞ je *bod v nekonečnu*. Platí $\frac{1}{0} = \infty$, $\frac{1}{\infty} = 0$, $m + \infty = \infty$ a konečně $\infty_m \times 0 = m$ pro $m \in K$.

Poněkud zvláštní definice několika nekonečen nám bude vhod později.

K této ani *HG* posloupnosti nad konečnými tělesy neexistuje podle nejlepšího svědomí autora žádná literatura. Strávíme nějaký čas nad tvary grafů - případ *AH* posloupnosti je totiž na dvakrát tolik zajímavý, jako ty předchozí.

3.1 Základní poznatky

Definice 3.1.1. Ať $a, b \in \mathbb{F}_q^\times$ jsou různé. Pak definujeme $AH_{\mathbb{F}_q}(a, b)$ jako posloupnost $(a_n, b_n)_{n=0}^\infty$ s $(a_0, b_0) = (a, b)$ a:

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

pokud $a + b \neq 0$. Prvek $(a, -a)$ pro $a \in \mathbb{F}_q$ se zobrazí na $(0, \infty_k)$, $(0, \infty_k)$ se zobrazí na $(\infty_k, 0)$ a $(\infty_k, 0)$ se zobrazí sám na sebe. Zde $k = -a^2$.

Pokud $\phi_q(2) \neq 1$, tak se každý *afinní* prvek zobrazí opět na afinní prvek, tedy body, jejich některá složka je 0, tvoří vlastí komponentu. Ať je naopak pro nějaká (a_0, b_0) a n nezáporné $1/a_{n+1} + 1/b_{n+1} = 0$, pak i $a_{n+1} + b_{n+1} = 0$. Muselo pak být:

$$\frac{a_n + b_n}{2} + \frac{2a_n b_n}{a_n + b_n} = 0,$$

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

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 2 je čtvercem, se některé prvky mohou zobrazit do nekonečna. My se nejprve zaměříme na tělesa $\mathbb{F}_q$ s $q \equiv \pm 3 \pmod 8$.

Definice 3.1.2. Definujme *graf* $AH_{\mathbb{F}_q}$ jako orientovaný graf, jehož vrcholy jsou uspořádané dvojice (a, b) prvků nad $\mathbb{P}^1(\mathbb{F}_q^\times)$. Všechny orientované hrany vedou mezi vrcholem (a, b) a (a_1, b_1).

PRIKLAD

Na příkladu vidíme, že pro $q \equiv \pm 3 \pmod 8$ při vizualizaci *AH* posloupnosti získáme krom medúz i tzv. *vulkány hloubky* 2. V případě $q \equiv \pm 1 \pmod 8$ jsou tyto vulkány dokonce ještě hlubší a některé obsahují $(\infty, 0)$. Tato terminologie není vybraná autorem, setkáme se s ní v kontextu eliptických křivek.

Definice 3.1.3. Souvislý orientovaný graf V nazveme *vulkánem hloubky* k, pokud je dělen do $k + 1$ stupňů $V_0, \ldots, V_k$ a:

(i) V_0 je (možná triviální) cyklus, kde každý jeho člen má unikátního následníka mimo cyklus,

(ii) pro $0 < i < k$ má každý vrchol $W \in V_i$ unikátního předchůdce ve V_{i-1} a dva následníky ve V_{i+1},

(iii) každý prvek V_k je listem.

Všimněme si, že medúza je pouze vulkánem hloubky 1. Předtím, než ukážeme, že grafy *AH* posloupnosti pro $q = \pm 3 \pmod 8$ nabývají těchto tvarů, se pozastavme nad spojením *AH* posloupnosti s dvěma předchozími, které jsme studovali. I když větší vulkány *AG* posloupnost nikdy netvoří, pro například $p \equiv -1 \pmod 4$ získáme v některých případech *AH* posloupnosti též medúzy. Klíčové rozdělení bude na prvky (a, b), kde $\phi_q(ab)$ je fixní. Hned uvidíme, že toto číslo je pro jednotlivé souvislé komponenty stejné a dokážeme silnější tvrzení. Určeme nyní počty (afinních) dvojic v jednotlivých takových skupinách.

Věta 3.1.4. *Buď $q = p^k$ mocnina prvočísla. Pak:*

(i) počet prvků $(a, b) \in AH_{\mathbb{F}_q}$ takových, že $\phi_q(ab) = 1$, je $(q-1)(q-3)/2$,

(ii) počet prvků $(a, b) \in AH_{\mathbb{F}_q}$ takových, že $\phi_q(ab) = -1$, je $(q-1)^2/2$.

Počet hran v celém grafu vycházejících z afinních vrcholů je $(q-1)(q-2)$.

Důkaz. V případě, kdy ab je v $\mathbb{F}_q$ nenulovým čtvercem, leží v roji $AH_{\mathbb{F}_q}$ právě dvojice (a, b), až na případ, kdy $a = b$. Pokud je součin dvou prvků čtverec, tak jsou buď oba čtverce, nebo ani jeden. Počet dvojic nenulových prvků (a, b), jejichž součin je čtverec, spočítáme tedy součtem počtů dvojic různých čtverců, resp. nečtverců. Toto je $(q-1)/2 \cdot (q-3)/2 + (q-1)/2 \cdot (q-3)/2 = (q-1)(q-3)/2$.

V případě, kdy ab není v $\mathbb{F}_q$ nenulovým čtvercem, leží v roji $AH_{\mathbb{F}_q}$ právě dvojice (a, b). Takové dvojice mají jedno složku, která je čtvercem, a druhou, která není. Vyhovující počet je proto $(q-1)/2 \cdot (q-1)/2 + (q-1)/2 \cdot (q-1)/2 = (q-1)^2/2$. Konečně, z každého afinního vrcholu vychází právě jedna hrana, proto počet hran je:

$$\frac{(q-1)(q-3)}{2} + \frac{(q-1)^2}{2} = (q-1)(q-2).$$

□

Grafy $AH_{\mathbb{F}_q}$ a $AG_{\mathbb{F}_q}$ jsou velmi odlišné. Na příkladu ? vidíme, že komponenty roje $AG_{\mathbb{F}_q}$ mohou mít mnohonásobně více prvků, než je q. Zato v případě AH posloupnosti počet prvků značně omezí stejný invariant, jako v reálném případě - součin jednotlivých složek prvků. Zde poprvé využijeme naši definice nekonečna.

Lemma 3.1.5. *Uvažme graf $AH_{\mathbb{F}_q}$ a nějakou jeho souvislou komponentu V. Pro libovolnou afinní 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:

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

Toto platí i v případě, že jedním z prvků a_1, b_1 je nekonečno. □

Důsledek 3.1.6. *Každá souvislá komponenta v grafu $AH_{\mathbb{F}_q}$ obsahuje nejvýše $q-1$ afinních 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, v tělese $\mathbb{F}_{11}$ a součin roven čtyřem nevyhovuje dvojice $(2, 2)$. Lemma, které jsme zmínili před chvílí, nám též umožní zobecnit větu 2.1.9, tentokrát je totiž počet přátel grafů k dané souvislé komponentě velmi omezený.

Definice 3.1.7. Ať $(a, b) \in AG_{\mathbb{F}_q}$ leží v souvislé komponentě V. Potom nazveme libovolnou souvislou komponentu obsahující prvek (ka, kb) pro $k \in \mathbb{F}_q$ přítelem V.

Věta 3.1.8. *Ať $(a, b) \in AG_{\mathbb{F}_q}$ leží v souvislé komponentě V, která obsahuje pouze afinní vrcholy. Pak počet přátel V je roven:*

(i) $q - 1$, *pokud* $(-a, -b)$ *neleží ve* V,

(ii) $(q - 1)/2$, *pokud* $(-a, -b)$ *leží ve* V.

Důkaz. Důkaz je prakticky stejný, jako důkaz věty 2.1.9, tentokrát ale pokud pro $k \neq 1$ leží (a, b) a (ka, kb) ve stejné komponentě, podle lemmatu 3.1.5 musí platit $ab = k^2ab$, tj. $k = -1$. Nosná množina grupy O_k sestrojené analogicky k důkazu věty 2.1.9 je proto podmnožinou $\{1, -1\}$ a dojdeme k tomu, že V má právě $\frac{q-1}{\mathrm{ord}_q(\pm 1)} \in \left\{q - 1, \frac{q-1}{2}\right\}$ přátel. □

V případě, že komponenta obsahuje body v nekonečnu, pak předchůdci prvku $(0, \infty_m)$ jsou $(\pm a, \mp a)$ pro $a^2 = -m$, tedy tato komponenta má $(q - 1)/2$ přátel. Poznamenejme, že ve zdánlivé většině grafů $AH_{\mathbb{F}_q}$ se vyskytují komponenty s $q - 1$ přáteli, stejně jako jiné komponenty, které mají přátel pouze $(q - 1)/2$

Definice 3.1.9. Ať $H \subseteq AH_{\mathbb{F}_q}$ je souvislá komponenta roje a $H_1, \ldots, H_k$ jsou všichni její přátelé. Pak $H \cup H_1 \cup \cdots \cup H_k$ nazvěme *hejnem*.

3.2 Struktura grafů

AH posloupnost se od *AG* posloupnosti na několika místech principiálně liší, přesto se na jednom místě shodují. Jejich grafy mají pozoruhodně pravidelnou strukturu. V pozdějších částech práce tuto strukturu do jisté míry vysvětlíme. Bez dalšího otálení proto pojďme opravdu dokázat, že grafy $AH_{\mathbb{F}_q}$ mají tu strukturu, kterou jim připisujeme. Nejprve samozřejmě klasifikujeme, kdy má prvek předchůdce.

Lemma 3.2.1. *Afinní vrchol $(a, b) \in AH_{\mathbb{F}_q}$ má předchůdce, právě pokud $\phi_q(a^2 - ab) = 1$.*

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 3.2.2. *Roj $AH_{\mathbb{F}_q}$ vypadá následovně:*

(i) Pokud $q \equiv 3 \pmod 8$, tak:

- *sjednocení komponent obsahujících prvky (a, b) splňující $\phi_q(ab) = 1$ je tvořeno medúzami,*
- *sjednocení komponent obsahujících prvky (a, b) splňující $\phi_q(ab) = -1$ je tvořeno vulkány hloubky 2.*

(ii) Pokud $q \equiv 5 \pmod 8$, tak:

- *sjednocení komponent obsahujících prvky (a, b) splňující $\phi_q(ab) = 1$ je tvořeno vulkány hloubky 2,*
- *sjednocení komponent obsahujících prvky (a, b) splňující $\phi_q(ab) = -1$ je tvořeno medúzami.*

Vrcholy obsahující body v nekonečnu tvoří v $AH_{\mathbb{F}_q}$ samostatné komponenty.

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 $\phi_q(ab) = -1$. Nejprve zmiňme, že díky $\phi_q(2) = -1$ leží vrcholy s body v nekonečnu v $q-1$ samostatných komponentách. 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, jenž 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. Uvažme vrchol $V : (a, b)$ grafu, který má následníka, bez újmy na obecnosti

uvažme $a = 1$. Podle lemmatu je $1 - b$ čtverec v $\mathbb{F}_q$, tj. $b = 1 - x^2$ pro nějaké $x \in \mathbb{F}_q$. Nyní spočítejme dva následníky V:

$$(1, b) \longmapsto \left(\frac{b+1}{2}, \frac{2b}{b+1}\right) \longmapsto \left(\frac{b^2+6b+1}{4(b+1)}, \frac{4b(b+1)}{b^2+6b+1}\right) =: W.$$

Jádro celé charakterizace spočívá v následujícím tvrzení:

Lemma. *Vrchol W má na druhé větvi předchůdců nejvýše prarodiče.*

Důkaz. Opravdu, druhý předchůdce W je jistě:

$$Z : \left(\frac{2b}{b+1}, \frac{b+1}{2}\right).$$

ten má sám předchůdce, protože číslo:

$$\frac{2b}{b+1}\left(\frac{2b}{b+1} - \frac{b+1}{2}\right) = \frac{-b(b-1)^2}{(b+1)^2}$$

je čtvercem. Ať (X, Y) a (Y, X) jsou předchůdci Z, ti pak splňují soustavu:

$$\frac{X+Y}{2} = \frac{2b}{b+1},$$
$$\frac{2XY}{X+Y} = \frac{b+1}{2} \Rightarrow XY = b.$$

Jsou tedy kořeny kvadratické rovnice $U^2 - \frac{4b}{b+1}U + b = 0$ nad $\mathbb{F}_q$. Kořeny této rovnice spočítáme a získáme:

$$\{X, Y\} = \left\{\frac{2b + \sqrt{-b}(b-1)}{b+1}, \frac{2b - \sqrt{-b}(b-1)}{b+1}\right\}.$$

Poznamenejme, že ty leží v $\mathbb{F}_q$, protože $\phi_q(-b) = \phi_q(-1) \cdot \phi_q(b) = (-1)^2 = 1$. Konečně ukážeme, že (X, Y) nemá předchůdce, z toho jistě plyne, že i (Y, X) nemá předchůdce. K tomu nám stačí ověřit, že číslo:

$$\frac{2b + \sqrt{-b}(b-1)}{b+1} \cdot \left(\frac{2b + \sqrt{-b}(b-1)}{b+1} - \frac{2b - \sqrt{-b}(b-1)}{b+1}\right) =$$
$$\frac{2b + \sqrt{-b}(b-1)}{(b+1)^2} \cdot 2\sqrt{-b}(b-1) =$$
$$\frac{2(b-1)}{(b+1)^2} \cdot [2\sqrt{-b}b - b(b-1)] =$$
$$\frac{2b(b-1)}{(b+1)^2} \cdot [2\sqrt{-b} - (b-1)] = \frac{2b(b-1)}{(b+1)^2}(1 - \sqrt{-b})^2.$$

není v $\mathbb{F}_q$ čtvercem. Protože víme, že $\phi_q(2) = -1$, tak $2b$ je v $\mathbb{F}_q$ druhá mocnina. Číslo $b-1 = -x^2$ naopak čtverec není, protože $q \equiv -1 \pmod 4$. Levý činitel proto čtvercem není. Protože b není čtverec a $q \equiv 3 \pmod 4$, tak argument v druhé mocnina $1 - \sqrt{-b}$ leží v $\mathbb{F}_q$, tudíž pravý činitel je druhou mocninou čísla v $\mathbb{F}_q$. Dohromady získáme, že $\phi_q(X(X-Y)) = -1$, čímž je pomocné tvrzení dokázáno. □

Poznámka. Pokud bychom uvažovali tělesa, kde $\phi_q(2) = 1$, potom by měl vrchol W z obou stran alespoň praprarodiče.

Co jsme právě udělali? Ukázali jsme, že pokud nějaký vrchol, v tomto případě je to W, má na jedné větvi předků alespoň praprarodiče, tak na té druhé má už nejvýše prarodiče. Nyní již se můžeme pustit přímo do důkazu, že naše posloupnost tvoří vulkány.

Stejně jako v případě AG posloupnosti začněme s libovolným vrcholem (a, b). Pišme jeho následníky:

$$(a, b) \longmapsto (a_1, b_1) \longmapsto (a_2, b_2) \longmapsto \dots$$

Máme nekonečně definovanou posloupnost na konečné množině vrcholů, jednou proto vstoupí do cyklu, který má délku větší než jedna. Každému prvku v tomto cyklu (i kdyby byl cyklus kratší, než 4) můžeme psát nekonečně dlouho, byť periodickou, řadu předchůdců. Dejme proto tomu, že (C, D) je libovolným členem cyklu ve stejné partitě, ve které leží (a, b). Právě jsme dokázali, že na větvi předchůdců, která nezasahuje do cyklu, má právě tři předchůdce, jednoho rodiče a dva prarodiče. Toto platí pro libovolný člen cyklu. Tímto tedy získáváme, že každá partita v tomto případě tvoří vulkány hloubky 2.

□

Tato charakterizace byla poměrně pracná, přesto je pouze polovina války vyhrána. Zaprvé, co když uvážíme konečná tělesa $\mathbb{F}_q$, kde $q = p^k$ a sice platí $p \equiv 3, 5 \pmod 8$, ale k je sudé? V takovém případě je $\phi_q(2) = 1$ a v případě vulkánů má každý bývalý list nového předchůdce. Na příklad rozšiřme příklad ? nad tělesem $\mathbb{F}_{p^2}$, pak graf vypadá následovně:

Vulkán má tedy o jedna vyšší hloubky. V případě rozšíření lichého stupně jsou grafy shodné, při rozšíření sudého stupně můžeme získat alespoň jednoduché odhady na hloubku binárního stromu, který je připojen ke členu cyklu. Důkaz, že všechny listy mají stejnou hloubku přes všechny takové stromy, tedy že graf je opět vulkánem, je již nad možnosti základní teorie čísel.

Důsledek 3.2.3. *Buď $q = p^m$ a $V \subseteq AH_{\mathbb{F}_q}$ vulkán hloubky h a (a, b) nějaký jeho prvek. V grafu $AH_{\mathbb{F}_{q^k}}$ leží (a, b) ve stromu zakořeněném v cyklu. Potom výška tohoto stromu je alespoň $h + v_2(k)$.*

Důkaz. Postupujme indukcí podle $v_2(k)$. Případ k lichého pokrývá věta 3.2.2. Ať nyní věta platí pro nějaké $\ell \geqslant 0$ a všechna k s $v_2(k) = \ell$. Pokud (a, b) je list v $\mathbb{F}_{q^k}$ pro nějaké k, pak platí $\phi_{q^k}(a(a-b)) = -1$ a tedy $a(a-b)$ je čtvercem v $\mathbb{F}_{p^{2k}}$. Vrchol (a, b) má proto dva předchůdce $(a \pm x, a \mp x) \in AH_{\mathbb{F}_{q^{2k}}}$ a výšla stromu obsahujícího (a, b) má v $AH_{\mathbb{F}_{q^{2k}}}$ hloubku alespoň o jedna delší, než v $AH_{\mathbb{F}_{q^k}}$. Snadno pak získáme dokazované tvrzení. □

Vzpomeňme si na známé lemma z olympiádní matematiky, konkrétně *Lifting the Exponent lemma*, které hodnotu $v_2(k)$ ukotví k číslu $p^k - 1$.

Věta 3.2.4. *(LTE lemma) Ať p je liché a k sudé. Pak platí:*

$$v_2(p^k - 1) = v_2(p - 1) + v_2(p + 1) + v_2(k) - 1.$$

Důsledek výše spolu s větou 3.2.2 pak ukazuje, že hloubka vulkánu je určitým způsobem spojena s $v_2(q - 1)$. Toto propojení plně prozkoumáme až ke konci práce i pro tělesa s charakteristikou $p \equiv \pm 1 \pmod 8$ pomocí eliptických křivek.

3.3 Vlastnosti grafů

I v případě *AH* posloupnosti se můžeme dívat na empirická data ohledně jednotlivých parametrů.

3.4 Dynamické systémy

AH posloupnost se od dvou, které jsme studovali před chvílí, liší také 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 3.4.1. *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 3.4.2. *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?)

Kapitola 4

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 totiž popisují mnohem složitější struktury, konkrétně grafy isogenií eliptických křivek nad konečnými tělesy.

4.1 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 [],[],[].

Po celou dobu se pohybujeme v tzv. *projektivní prostoru*, tedy množině tříd nenulových vektorů $(a_0 : \cdots : a_n) \in \overline{K}^{n+1}$, kde dva vektory považujeme za shodné, pokud jsou vzájemně skalárními násobky. Tyto třídy nazveme *body*.

Definice 4.1.1. Ať $A, B, \lambda \in \mathbb{F}_q$ jsou taková, že $4A^3+27B^2 \neq 0$ a $\lambda \neq 0, 1$. Pak definujeme *eliptickou křivku ve Weierstrassově tvaru* jako množinu bodů $(x, y) \in \mathbb{F}_q$ splňujících vztah:

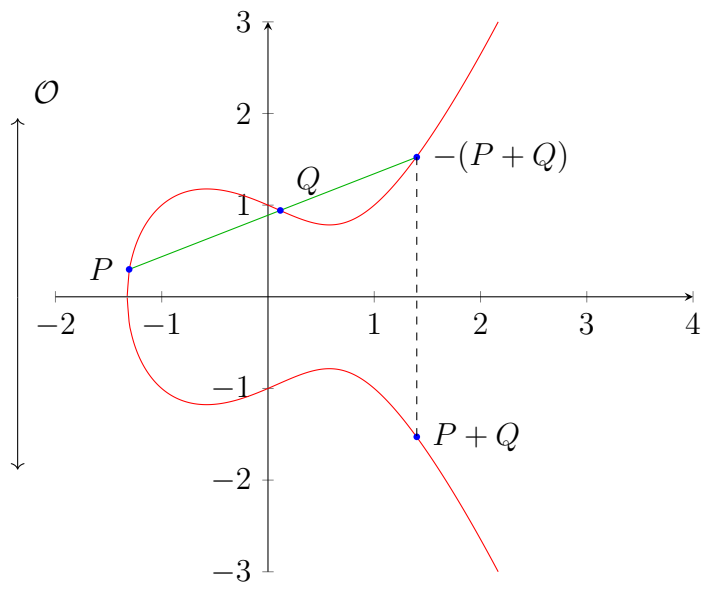
$$y^2 = x^3 + Ax + B,$$

spolu s tzv. *bodem v nekonečnu* O. Dále definujeme *eliptickou křivku v Legendrově tvaru* jako množinu $(x, y) \in \mathbb{F}_q$ splňujících:

$$y^2 = x(x - 1)(x - \lambda),$$

opět s bodem v nekonečnu.

Pokud definujeme sčítání na křivce tak, že součet každých tří kolineárních (ne-nutně různých) bodů je O, pak body na eliptické křivky tvoří grupu. V případě, že přímka PQ pro P, Q body na E degeneruje v tečnu, pak poslední průsečík této přímky s E bude dvojnásobek bodu P. Díky asociativitě sčítání na křivky můžeme pak jednoznačně definovat n-násobek bodu $[n]P = \underbrace{P + \cdots + P}_{n}$.



Obrázek 4.1: Doslova ten samej obrázek !!!!!!!

–Obrázek–

Grupa bodů definovaných nad konečným tělesem je isomorfní direktnímu součinu $\mathbb{Z}_n \times \mathbb{Z}_m$ pro vhodná celá m, n [já]. Pokud označíme $E(\mathbb{F}_q)$ množinu bodů na E definovaných nad $\mathbb{F}_q$ (včteně O), tak zmiňme důležitou *Hasseho větu*, která značně ukotví počet prvků této křivky. Ta tvrdí, že:

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

Důležité pro nás jsou zobrazení mezi křivkami, která zachovají jejich grupovou strukturu.

Definice 4.1.2. 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*. Pod jádrem $\ker \phi$ isogenie ϕ rozumíme jejímu jádru jako homomorfismu grup.

Obzvláště důležité isogenie jsou *isomorfismy*, tzn. invertibilní isogenie - isogenie dané lineárními zobrazeními $(x, y) \longmapsto (ax + by + c, dx + ey + f)$. Je jednoduché ukázat, že pro křivky ve Weierstrassově tvaru jsou isomorfismy dané zobrazením $(x, y) \longmapsto (u^2x, u^3y)$ pro $u \in \overline{K}$. Pokud je isomorfismus $\phi : E \longrightarrow E'$ definovaný nad rozšířením K, ale ne přímo nad K, pak řekneme, že je E' *twistem* křivky E. Je-li takový isomorfismus definovaný nad rozšířením $K(\sqrt{u})$, pak jej nazveme *kvadratickým twistem*.

I když ne všechny isogenie jsou invertibilní, ke každé isogenii $\phi : E \longrightarrow E'$ najdeme její *duální isogenii* $\widehat{\phi} : E' \longrightarrow E$. Můžeme proto říci, že „být isogenní“ je relace ekvivalence na množině křivek nad daným tělesem. Jak ale zjistit, kdy jsou dvě křivky isogenní? Částečný výsledek nám může poskytnout věta připisovaná *Sato a Tatovi*:

Věta 4.1.3. *(Sato-Tate) Buďte E, E' eliptické křivky nad $\mathbb{F}_q$. Pak jsou tyto křivky isogenní nad $\mathbb{F}_q$, právě pokud platí $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$.*

Problém, kdy jsou dvě křivky isogenní pod isogenií daného stupně, je již obtížnější.

4.2 Okruhy endomorfismů

4.3 AG posloupnost ve světle eliptických křivek

Kapitola 5

Eliptické křivky a 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. Přímo adaptovat jejich postup, tedy přiřadit vrcholům grafu křivky, podle nejlepšího mínění autora není pravděpodobné, protože komponenty $AH_{\mathbb{F}_q}$ mají velmi jednoduché invarianty a mají velmi málo prvků. To by znamenalo, že bychom museli vybírat ideály s malými řády v grupě tříd ideálů.

Ne, *AH* posloupnost můžeme popsat trochu jednodušeji. Přesto se ale vrátíme do světa eliptických křivek. Víceméně.

5.1 Motivace

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 $x + \frac{1}{x}$.

5.2 Montgomeryho křivky

Ve snaze adaptovat postup popsaný výše, jsem hledal křivky, na nichž existuje endomorfismus ϕ zobrazující bod $P : (x, y)$ na bod s x-ovou složkou $\frac{(x+1)^2}{4x}$. U křivek ve Weierstrassově tvaru se mi takové zobrazení najít nepodařilo. Připomeňme, že i v popisu AG posloupnosti přece pracujeme s jiným tvarem křivek, není tedy příliš překvapivé, že to bude třeba i nyní.

Hledaný endomorfismus jsem nakonec nalezl u křivek v *Montgomeryho tvaru* $By^2 = x^3 + Ax^2 + x$ pro $A, B \in \mathbb{F}_q$. Volíme zde $A \neq \pm 2$, v těchto případech je totiž křivka singulární a má mnohem jednodušší strukturu. Tyto křivky mají několik praktických výhod, proto se například používají v šifrovacím protokolu CSIDH, pro více informací doporučuji konzultovat mou předchozí práci [já].

První z takových výhod je, že třída isomorfismů Montgomeryho křivky závisí *pouze* na hodnotě parametru A. Další výhodou je, že lomené funkce udávající zobrazení [2] a [3] mají na Montgomeryho křivkách jednoduší tvary, což umožňuje pro rychlejší výpočty. Konkrétně pro bod $P = (x, y)$ je jeho dvojnásobek roven:

$$[2]P = \left(\frac{(x^2-1)^2}{4x(x^2+Ax+1)}, y\frac{(x^2-1)(x^4+2Ax^3+6x^2+2Ax+1)}{8x^2(x^2+Ax+1)^2} \right).$$

viz [karaskova]. Pokud bychom zvolili $A = -2$, tak x-ová souřadnice bodu $[2]P$ by byla právě $\frac{(x+1)^2}{4x}$, což hledáme. Toto pozorování otevírá cestu studiu AH posloupnosti pomocí eliptických křivek.

Problém ale nastává právě s hodnotou $A = -2$, pro ni je totiž křivka rovna $y^2 = x(x-1)^2$. Tato křivka ve skutečnosti není eliptická, v bodě $(1, 0)$ je singulární a nelze v něm spočítat tečnu. Všechny ostatní body při klasicky definovaném sčítání opět tvoří grupu, tentokrát je ale opravdu jednodušší, než na klasické eliptické křivce.

Definice 5.2.1. Uvažme křivku $E : y^2 = x(x-1)^2$ nad tělesem $\mathbb{F}_q$. Definujeme $E(\mathbb{F}_q)$ jako grupu bodů $(x, y) \in \mathbb{F}_q^2$ splňující $y^2 = x(x-1)^2$ a $x \neq 1$ spolu s bodem v nekonečnu $\mathcal{O}$.

ma to $p + 1$ bodů, isomorfni Z $p + 1$.

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

Serge Lang

Závěr

zu ende

Carl Friedrich Gauss aritmeticko-geometrický průměr ve svém mládí studoval hojně, v jeho deníku o této posloupnosti nalezneme hned destíku zmínek této posloupnosti mezi roky 1799 a 1800. Věnoval se i zobecnění posloupnosti nad komplexními čísly. Jak to zobecnit nad konečnýma tělesama - - p adický?

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.