STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST

Obor č. 1: Matematika a statistika

Medúzy a posloupnosti průměrů

Zdeněk Pezlar
Jihomoravský kraj

Brno 2022

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 [2], 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:

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

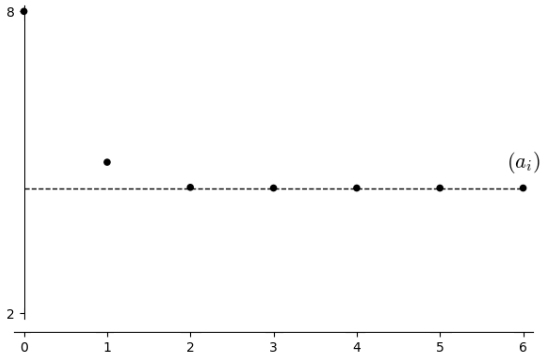
posloupnost $(b_n)_{n=0}^{\infty}$ je proto rostoucí (pokud $a_0 \neq b_0$, tak ostře rostoucí). Obdobně můžeme psát:

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

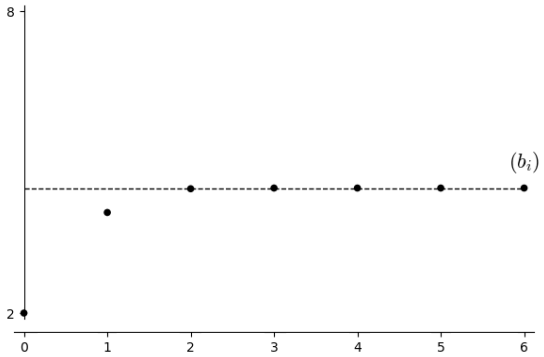
posloupnost $(a_n)_{n=0}^{\infty}$ je tedy naopak klesající. Protože aritmetický a geometrický průměr dvou čísel leží mezi nimi, jsou obě posloupnosti shora svírané prvkem a a zdola b. Libovolná ohraničená monotónní posloupnost konverguje, víme tedy, že obě posloupnosti $(a_n)_{n=0}^{\infty}$ a $(b_n)_{n=0}^{\infty}$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

Příklad 1.1.2. Pokud si zvolíme $a = b = 5$, tak jsou obě hodnoty konstantní, to příliš zajímavě není. Zvolme si tedy například trochu zážívnější dvojici $a = 8, b = 2$. Pak můžeme psát:

a_i	b_i
8	2
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...
⋮	⋮



Obrázek 1.1: složka (a_i)



Obrázek 1.2: složka (b_i)

V tomto případě prvky AG posloupnosti zdárně konvergují ke společné hodnotě. Spočítejme si ještě pro jistotu jednu posloupnost, tentokrát pro dvojici $a = \sqrt{2}$ a $b = 1$. 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
1.414213562373...	1
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. Na příkladu 1.1.2 vidíme,

že konvergují velmi rychle, jak ale takovou rychlost můžeme měřit?

Definice 1.1.3. Ať $(x_n)_{n=0}^{\infty}$ je konvergentní posloupnost. Poté *řád konvergence* σ této posloupnosti k limitě L je číslo splňující pro všechna $n \in \mathbb{N}$ a nějakou konstantu C:

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

Pro $\sigma = 2$ získáme *kvadraticky konvergentní posloupnost.*

U kvadratické posloupnosti se tak v každém dalším kroku se obě čísla *přibližně* rovnají limitě na dvakrát více desetinných míst. Na druhé posloupnosti zmíněné v příkladu 1.1.2 pozorujeme, že 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 a konverguje kvadraticky.

Věta 1.1.4. *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. Navíc složky $(a_n)_{n=0}^{\infty}$ a $(b_n)_{n=0}^{\infty}$ konvergují ke společné limitě kvadraticky.*

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 $\lim_{n\to\infty}(a_n - a_{n+1}) = 0$, platí $\lim_{n\to\infty}(a_n - b_n) = 0$. Limity posloupností (a_n) a (b_n) jsou proto shodné.

Zaveďme nyní 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. Chceme ukázat, že posloupnost (x_n) konverguje kvadraticky k 1. Platí $\varepsilon_i \geqslant 0$ pro každé i. Pak pro libovolné n platí:

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

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

$$1 + \varepsilon_{n+1} = \frac{\sqrt{1+\varepsilon_n} + \frac{1}{\sqrt{1+\varepsilon_n}}}{2}.$$

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. □

Definice 1.1.5. Ať $(a_n, b_n)_{n=0}^{\infty}$ je *AG* posloupnost. Společnou limitu složek $(a_n), (b_n)$ nazvěme *aritmeticko-geometrickým průměrem*, zkráceně *AG průměrem*, čísel a, b. Toto číslo značme $\mathrm{AG}(a, b)$.

Následující věta shrnuje základní vlastnosti *AG* průměru.

Věta 1.1.6. *Mějme $a, b, k \in \mathbb{R}^+$. Pro AG průměr 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* $x = \frac{1}{a}\sqrt{a^2 - b^2}$. *JAK SE DELA FOOTNOTE TADY???????*

Prozatím může vypadat, že *AG* posloupnost leží na uzavřeném ostrůvku vzdálená od jiných oblastní matematiky. Toto zdání však nemůže být dál od pravdy. Zamysleme se nad samotným *AG* průměrem. 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 „druhého druhu“ mají mnoho využití, například v počítání délky oblouku na elipse, ve světě fyziky zase například pomáhají najít periodu kmitu kyvadla [?].

My eliptické integrály zmiňujeme, jelikož jsou intimně spojené s *AG* posloupností, umožní nám totiž přesně vyjádřit hodnotu $AG(a, b)$. Mladý Karl Friedrich Gauss si již ve svých dvaadvaceti letech do svého deníku poznačil, že se hodnoty:

$$\frac{1}{AG\left(1, \frac{\sqrt{2}}{2}\right)} \qquad \text{a} \qquad \frac{2}{\pi} K\left(\frac{\sqrt{2}}{2}\right)$$

shodují na 11 desetinných místech. [pi and AGM] O trochu později dokázal obecný vztah, který tyto dva koncepty spojuje.

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

$$\frac{\pi}{2} \cdot \frac{1}{\mathrm{AG}(1, x)} = K\left(\sqrt{1 - x^2}\right) \tag{1.1}$$

Nyní nepatrně pozměňme integrál napravo, abychom mohli obecně popsat číslo $\mathrm{AG}(a,b)$. Definujme:

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

Snadno vidíme, že platí vztah:

$$I(a,b) = \frac{1}{a}K(x),$$

kde $x = \frac{1}{a}\sqrt{a^2-b^2}$. Takové x jsme už ale někde viděli, konkrétně ve větě 1.1.6 iv). Gaussovu větu poté můžeme díky části ii) věty 1.1.6 přepsat na:

Věta 1.2.3.

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

Příklad 1.2.4. Pojďme ověřit, že opravdu věta 1.2.3 platí. Nejprve pokud zvolíme $a = b$, tak máme:

$$I(a,a) = \int_0^{\pi/2} \frac{d\theta}{a} = \frac{\pi}{2a} = \frac{\pi}{2\,\mathrm{AG}(a,a)}.$$

Podívejme se nyní znovu na volbu $a = 8$ a $b = 2$. Určíme přibližně hodnotu $I(8,2)$ pomocí Simpsonova pravidla:

$$\begin{aligned} I(8,2)\cdot\frac{2}{\pi} &= \int_0^{\pi/2} \frac{d\theta}{\sqrt{64\sin^2\theta + 4\cos^2\theta}}\cdot\frac{2}{\pi} \\ &\approx \frac{\pi}{12}\cdot\left(\frac{1}{\sqrt{64\sin^2 0 + 4\cos^2 0}} + \frac{1}{\sqrt{64\sin^2\pi/4 + 4\cos^2\pi/4}} + \frac{1}{\sqrt{64\sin^2\pi/2 + 4\cos^2\pi/2}}\right)\cdot\frac{2}{\pi} \\ &= \frac{1}{6}\cdot\left(\frac{1}{2} + \frac{1}{\sqrt{32+2}} + \frac{1}{\sqrt{2}}\right) = 0.2297675610548\ldots. \end{aligned}$$

Převrácená hodnota tohoto čísla je:

$$\frac{\pi}{2}\cdot\frac{1}{I(8,2)} \approx 4.352224462884\ldots,$$

což při porovnání s $AG(8,2) = 4.486057160575\ldots$ není daleko od opravdové hodnoty.

Nastiňme, jakým způsobem Gauss vlastně dokázal rovnost (1.1). Jeho důkaz spočívá v důkaze mezivýsledku $I(a,b) = I(a_1,b_1)$. K němu lze dojít po několika přiměřeně bolestivých výpočteních krocích. Jak Gauss sám pravil, k tomuto výsledku dojdeme:

„After the development has been made correctly.“

Platí pak $I(a,b) = I(a_1,b_1) = \cdots = I(a_k,b_k) = \ldots$. V limitním případě získáme:

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

Jak můžeme propojení AG posloupnosti a eliptických integrálů využít? Dále si ukážeme, že eliptické integrály jsou svázané s několika elementárními funkcemi, načež je dokážeme efektivně počítat díky rychlé konvergenci AG posloupnost.

1.3 Rychlé výpočty elementárních funkcí

Motivace použití rekurzivně definovaných posloupností při počítání známých funkcí může poskytnout Newtonova metoda pro počítání odmocniny s kvadratických řádem konvergence:

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 a řádu konvergence je jednoduchý. Nešlo by obdobně využít i *AG* posloupnost? Ukáže se, že ano.

Dá se totiž ukázat, že logaritmická funkce má spojení s eliptickými integrály:

Věta 1.3.2. *Ať $x < 1$. Platí:*

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

Zde onen chybový člen lze jednoduše odhadnout []. Kvadraticky konvergující *AG* posloupnost nám tak umožní spočítat s velkou přesností logaritmus číslo $\frac{4}{x}$ pro dostatečně malé x (nebo vhodně velký argument logaritmu).

Pomocí logaritmu můžeme vyjádřit inverzní funkce ke klasických goniometrickým funkcím. Dá se totiž jednoduše ukázat [], že platí vztahy:

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

Poznámka. Všimněme si přítomnosti komplexních čísel v rovnici pro arkus tangens. Gauss a další autoři, například Legendre?, totiž studovali *AG* posloupnost i nad *komplexními čísly*. V takovém oboru není triviální zvolit správnou odmocninu a ??. Pomocí výsledků ?? pak můžeme adaptovat výpočty zmíněné výše i na komplexní čísla.

1.4 Posloupnosti s ostatními průměry

Aritmetický a geometrický průměr nám vygenerovaly posloupnost, která skýtá překvapivé praktické aplikace. 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:

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

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 1.1.4, čímž získáme, že obě posloupnosti konvergují k hodnotám $HG(a, b)$, resp. $AH(a, b)$.

Věta 1.4.2. *Ať $(a_n, b_n)_{n=0}^{\infty}$ je HG, resp. AH posloupnost. Potom limity čísel a_n, b_n pro $n \to \infty$ a existují a jsou si navzájem rovné.*

Abychom tyto posloupnosti porovnali s AG posloupností, spočítejme průměry pro $a = 2$ a $b = 8$. První z nich, HG posloupnost, vypadá následovně:

a_i	b_i
8	2
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...
⋮	⋮

Dokážeme propojit AG a HG posloupnosti. Vynásobme hodnoty $AG(8, 2)$ a $HG(8, 2)$:

$$AG(8,2) \cdot HG(8,2) \approx 4.486057160575 \cdots 3.566606359948 \cdots = 15.999999999997 \cdots \approx 8 \cdot 2.$$

Vzhledem k tomu, že $AG(a, a) \cdot HG(a, a) = a \cdot a$, vypadá to, že by mohlo platit $AG(a, b) \cdot HG(a, b) = ab$. To opravdu platí - všimněme si totiž, že můžeme psát:

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

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

Tato posloupnost je pouze AG posloupnost s převrácenými členy! Limita této posloupnosti je proto s použitím části *ii*) 1.1.6:

Věta 1.4.3.

$$HG(a,b) = \frac{1}{AG(a^{-1},b^{-1})} = \frac{ab}{AG(a,b)}.$$

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

a_i	b_i
8	2
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:

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

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 HG posloupností budou velmi spřízněné, zatímco AH s nimi má velmi málo společného.

Věta 1.4.4.

$$AH(a,b) = \sqrt{ab}.$$

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 - podíváme se na posloupnost nad konečnými tělesy. I 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 úskalí při adaptaci posloupnosti. Ne vždy totiž není součin prvků $a, b \in \mathbb{F}_q$ 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.

Tento zobecněný Legendreho symbol je podobně jako ten klasický multiplikativním charakterem na $\mathbb{F}_q$, tj. platí $\phi_q(a)\phi_q(b) = \phi_q(ab)$ pro $a, b \in \mathbb{F}_q$.

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*) $AG_{\mathbb{F}_q} = (V, E)$ jako orientovaný graf, kde $(a, b) \in V$, právě pokud platí $\phi_q(ab) = 1$, a $\big((a, b), (c, d)\big) \in E$, právě pokud platí $(c, d) = (a_1, b_1)$.

Pracujeme s orientovanými grafy, přesto se domluvme, že každou slabě souvislou komponentu souvislosti nazveme jednoduše komponentou souvislosti.

Úmluva. Ať G je orientovaný graf a $V \subseteq G$ je komponenta slabé souvislosti. Pak budeme o V říkat, že je komponenta souvislosti.

Příklad 2.1.4. Pojďme si udělat představu o grafu, se kterým pracujeme, konkrétně se podívejme na $AG_{\mathbb{F}_7}$. Zvolme dvojici $(1, 2) \in AG_{\mathbb{F}_q}$ a pišme posloupnost $AG_{\mathbb{F}_q}(1, 2)$:

$$(1, 2) \mapsto (5, 3) \mapsto (4, 1) \mapsto (6, 5) \mapsto (2, 4) \mapsto (3, 6) \mapsto (1, 2),$$

vrchol $(1, 2)$ je proto členem cyklu délky 6. Pokud máme v grafu orientovanou hranu $(a, b) \mapsto (c, d)$, tak jistě vede hrana i mezi (b, a) a (c, d), proto například vede hrana z $(2, 1)$ do $(5, 3)$ a podobně. Výpočtem lze ověřit, že prvky mimo cyklus - $(2, 1)$, $(3, 5)$ a pod., již předchůdce nemají. Komponenta obsahující vrchol $(1, 2)$ proto vypadá následovně:

Tento příklad - cyklus a listy připojené ke každému členu cyklu - je typický. Pro ilustraci se podívejme na .

Začněme zlehka, konkrétně z kolika vrcholů a hran je vlastně náš graf tvořen.

Věta 2.1.5. *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 komponent souvislosti, 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 2.1.6. 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 2.1.7. *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 2.1.8. *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. Podle analogu bodu *ii*) věty 1.1.6 můžeme přenásobit všechny vrcholy dané medúzy nějakým $k \in \mathbb{F}_q$ a získat novou medúzu, kterou nazveme jejím *přítelem*. Příklady takových medúz jsou na TOM PŘÍKLADU NA ZAČÁTKU.

Definice 2.1.9. Ať $M \subseteq AG_{\mathbb{F}_q}$ je medúza a (a, b) její prvek. Potom nazveme libovolnou medúzu obsahující prvek (ka, kb) pro $k \in \mathbb{F}_q$ *přítelem* medúzy M.

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

Věta 2.1.10. *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 $\mathbb{F}_q^\times \leqslant O_k$ generované k, 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 2.1.11. 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.

Nejdůležitější hodnotou je pro nás počet medúz v celém hejnu. Tuto hodnotu studovali autoři původního článku [2] a pomocí eliptických křivek budeme moci uvést odhady na tato čísla.

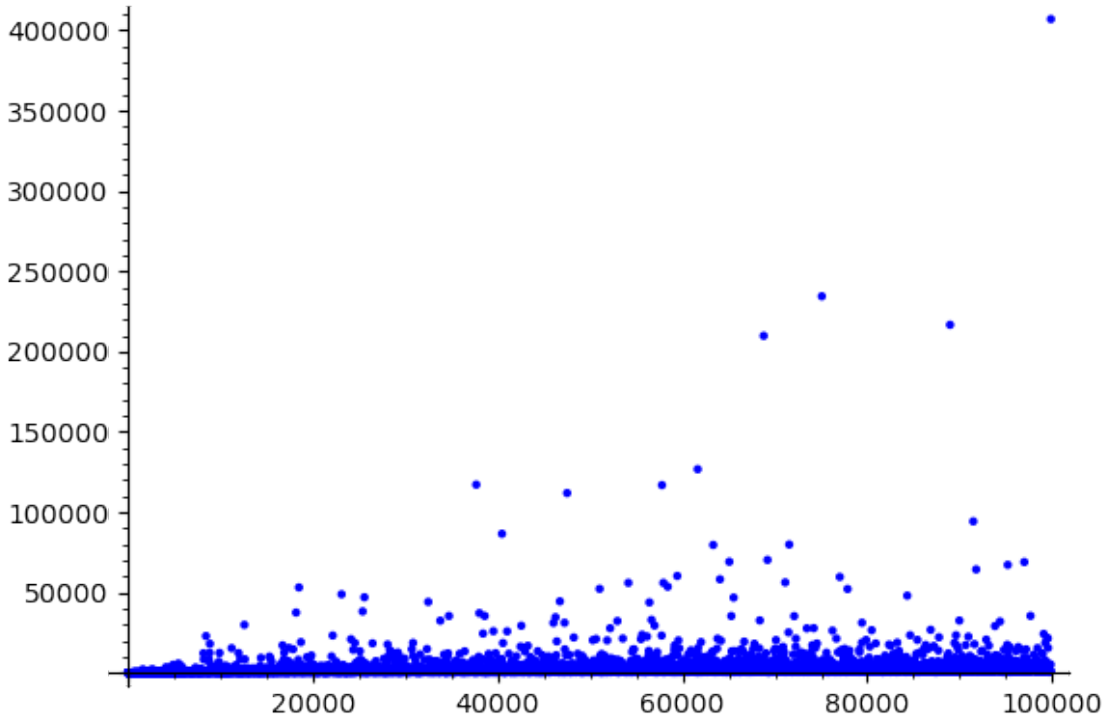
Definice 2.2.1. Ať $q \equiv 3 \pmod 4$ je mocnina prvočísla. Pak označme $d(\mathbb{F}_q)$ počet všech medúz v grafu $AG_{\mathbb{F}_q}$. Dále označme $s(\mathbb{F}_q)$ počet všech hejn v grafu $AG_{\mathbb{F}_q}$.

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	$d(\mathbb{F}_p)$	$s(\mathbb{F}_p)$
3	0	0
7	1	1
11	3	2

19	8	2
23	5	3
31	10	3
43	7	4
47	4	3
59	7	4
67	30	6
71	25	5
79	18	7
83	6	4

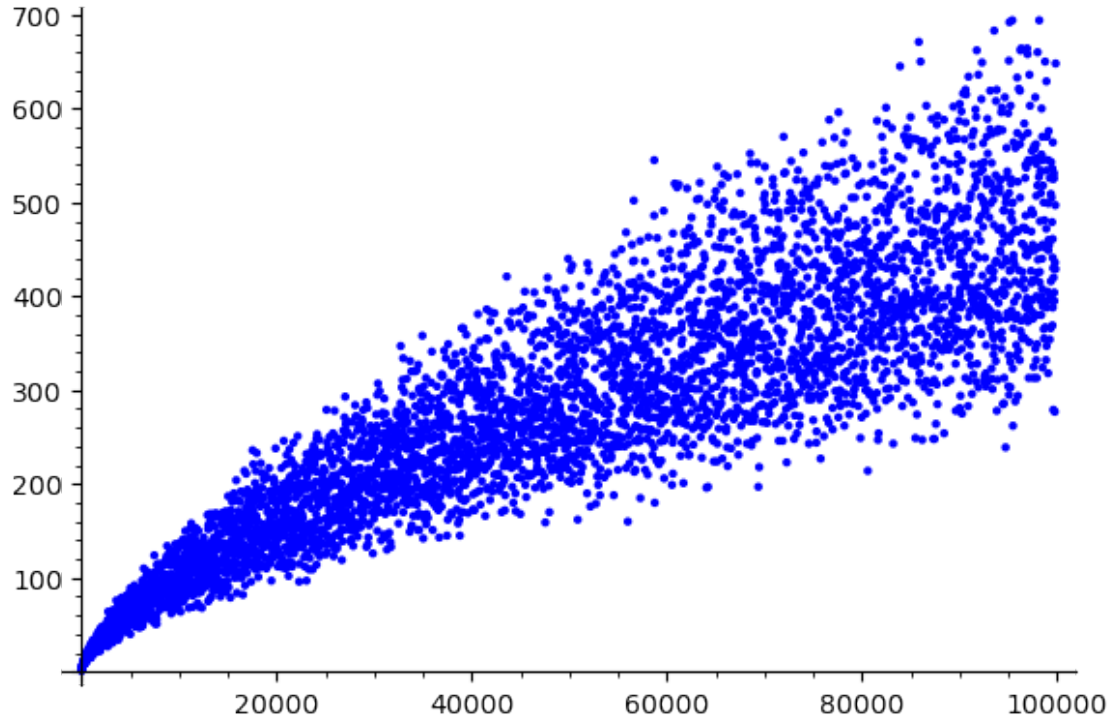
Tato náhodná povaha $d(\mathbb{F}_q)$ se nese i dál, na následujícím grafu vidíme jednotlivé hodnoty pro prvočísla $p < 10^5$:



Obrázek 2.1: Číslo $d(\mathbb{F}_p)$

Některé hodnoty $d(\mathbb{F}_p)$ jsou mnohem vyšší, než ostatní, například pro $p = 99859$ máme $d(\mathbb{F}_p) = 406954$. 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. Na grafu výše tak vidíme chování extrémních případů, ne však obecné trendy a jemné detaily. Abychom získali lepší představu o tomto čísle, tak ????.

Číslo $s(\mathbb{F}_p)$ se chová mnohem rozumněji. Případy, kdy $d(\mathbb{F}_p)$ je velké, jsou právě ty, kdy jsou hejna dostatečně velká, hodnoty $s(\mathbb{F}_q)$ stabilizují. Na následujícím grafu vidíme chování $s(\mathbb{F}_p)$ pro $p < 10^5$.



Obrázek 2.2: Číslo $s(\mathbb{F}_p)$

Autoři článku [2] propojili *AG* posloupnost s teorií eliptických křivek, těm se budeme věnovat v kapitole 4. Pomocí této teorie dokázali netriviální dolní odhad na číslo $d(\mathbb{F}_q)$, resp. jejich postup ohraničí dokonce číslo $s(\mathbb{F}_q)$. Hlavním výsledkem jejich článku je tvrzení, že pro libovolně malé $\varepsilon > 0$ a q dostatečně velké platí:

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

V závěru práce spekulují, zda je tento odhad asymptoticky optimální a navrhují odhad $d(\mathbb{F}_q) \geqslant O(\sqrt{q}\log\log q)$. Pojďme se těmto výsledkům věnovat.

Nejprve, jak optimální opravdu je odhad $s(\mathbb{F}_q)$ (resp. $d(\mathbb{F}_q)$)? Podívejme se na číslo $s(\mathbb{F}_q)$:

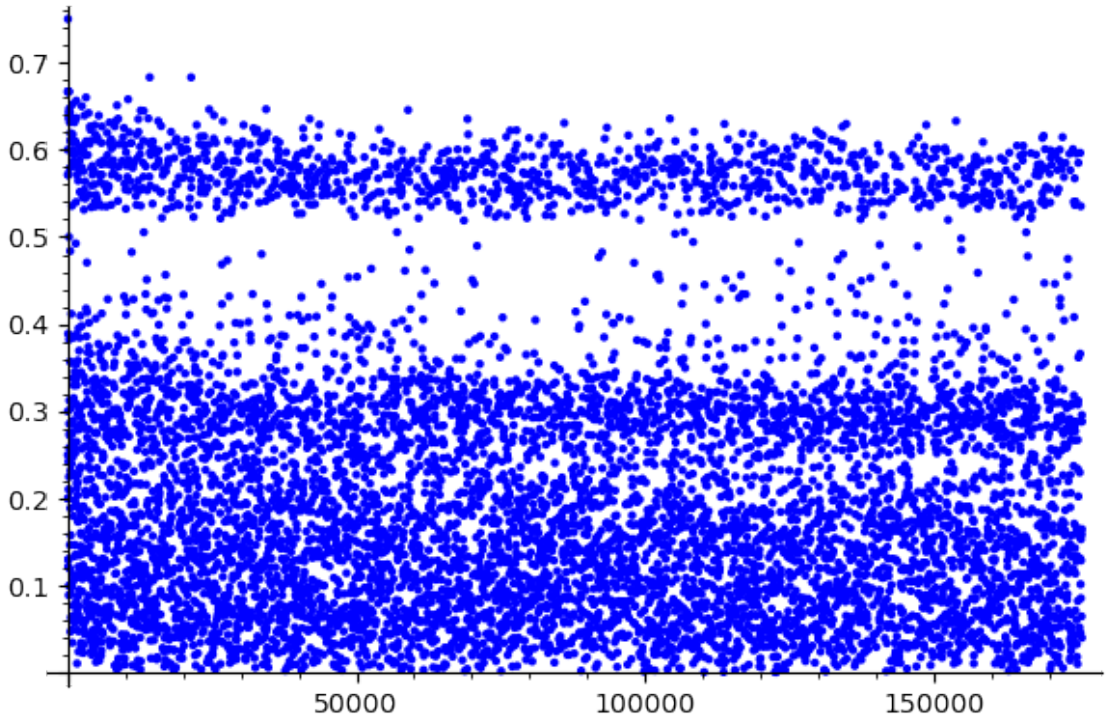
–

blabla

se to chová trochu jako nějaká funkce idk.

Další otázkou může být, jak spolu souvisí čísla $d(\mathbb{F}_q)$ a $s(\mathbb{F}_q)$. Rozhodně platí $s(\mathbb{F}_q) \geqslant d(\mathbb{F}_q)$, co lepšího ale můžeme říci? Obecný trend alespoň ze začátku zdárně neexistuje, uveďme si tabulku několika vybraných hodnot:

Tabulka
Pokud se podíváme, jak se plošně chová číslo $\frac{d(\mathbb{F}_{11})}{d(\mathbb{F}_q)}$ získáme velmi zajímavý graf:



Obrázek 2.3: Hodnoty $s(\mathbb{F}_p)/d(\mathbb{F}_p)$ pro $p < 170000$

Zaprvé, pro $p > 7$ číslo $\frac{d(\mathbb{F}_{11})}{d(\mathbb{F}_q)}$ drží pod hodnotou hodnoty 0.75 (maximální podíl nastane pro $p = 47$). To naznačuje, že libovolný horní odhad na číslo $s(\mathbb{F}_q)$ nemůže mít jako důsledek asymptoticky silnější odhad na číslo $d(\mathbb{F}_q)$. Tyto podíly se drží i pro $p \gg 10^5$, zde uveďme pár různé velkých vzorků:
-TABULKA-
Dále na grafu zjevně pozorujeme dva velké shluky hodnot, jeden v intervalu $[0.53, 0.66]$. Prvočísla $p < 10^5$, pro které hodnota $\frac{d(\mathbb{F}_{11})}{d(\mathbb{F}_q)}$ neleží v žádné z těchto mezí jsou pouze:
tabulečka.
Krom velikostí celého roje, můžeme se podívat na velikostí jednotlivých hejn, ?.
Konečně, zaměřme se na jednotlivé medúzy a podívejme se na velikosti jednotlivých medúz, resp. jejich cyklů.

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. 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 2.1.5. □

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:

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

□

Porovnejme toto lemma

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

Důkaz. Analogický k důkazu věty 2.1.8. □

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 $\psi((a, b))$ hranu:

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

Jelikož ψ se zjevně bijekce mezi $AG_{\mathbb{F}_q}$ a $HG_{\mathbb{F}_q}$, definuje mezi grafy isomorfismus. □

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.

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 K je těleso. Pak definujeme *projektivní přímku* $\mathbb{P}^1(K)$ jako $K \cup \{\infty\}$, kde ∞ je *bod v nekonečnu*. Ten pro $m \in \mathbb{F}_q$ splňuje:

(i) $\frac{1}{0} = \infty$ a $\frac{1}{\infty} = 0$,

(ii) $\infty + m = \infty$,

(iii) $\infty \cdot m = \infty$ pro $m \neq 0$,

(iv) $\infty \times \infty = \infty$.

Všimněme si, že projektivní přímka není tělesem, protože již každý prvek není jednotkou. Dále násobení není zjevně asociativní, například platí $(0 \cdot \infty) \cdot 2 = 2 \neq 1 = 0 \cdot (\infty \cdot 2)$. Pomocí projektivní přímky můžeme v plném rozsahu definovat a studovat *AH* posloupnost v konečném oboru.

Definice 3.1.2. 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:

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

Všimněme si, že prvek $(a, -a)$ pro $a \in \mathbb{F}_q$ se zobrazí na $(0, \infty)$, $(0, \infty)$ se zobrazí na $(\infty, 0)$ a $(\infty, 0)$ se zobrazí sám na sebe.

Pokud $\phi_q(2) \neq 1$, tak se každý *afinní* prvek zobrazí opět na afinní prvek. 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:

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

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 2 je čtvercem, se některé prvky mohou zobrazit do nekonečna a musíme již pracovat s projektivní přímkou. Budeme vždy pracovat pouze s posloupnostmi, které obsahují alespoň jeden afinní prvek. Nejprve zaměříme na tělesa $\mathbb{F}_q$ s $q \equiv \pm 3 \pmod 8$.

Definice 3.1.3. Definujme *roj* $AH_{\mathbb{F}_q} = (V, E)$ jako orientovaný graf, kde $(a, b) \in V$ pokud $a, b \in \mathbb{F}_q$, nebo $\{a, b\} = \{0, \infty\}$. Pro libovolná $a, b, c, d \in \mathbb{P}^1(\mathbb{F}_q)$ platí $\Big((a, b), (c, d)\Big) \in E$, právě pokud $(c, d) = (a_1, b_1)$.

Každý afinní prvek má v grafu zjevně nejvýše dva předchůdce. Toto je zdárně porušeno pro body v nekonečnu, kde prvek $(0, \infty)$ má předchůdců hned $\frac{q-1}{2}$. Čistě z důvodu elegance budeme uvažovat $\frac{q-1}{2}$ bodů $(0, \infty)$ a $(\infty, 0)$, každý příslušící jedné dvojici bodů $(a, -a)$ a $(-a, a)$.

Úmluva. Ať $a, b \in \mathbb{F}_q^\times$ splňují $a \neq \pm b$. Poté se domluvme, že body $(a, -a)$ a $(b, -b)$ neleží ve stejné komponentě souvislosti grafu $AH_{\mathbb{F}_q}$.

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 3.1.4. 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 cyklus, kde každý jeho člen má unikátního předchůdce mimo cyklus,

(ii) pro $0 < i < k$ má každý vrchol $W \in V_i$ unikátního následníka ve V_{i-1} a dva předchůdce 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 podle $\phi(ab)$ pro jednotlivé dvojice. Hned uvidíme, že toto číslo je pro jednotlivé komponenty souvislosti stejné a dokážeme silnější tvrzení. Určeme nyní počty (afinních) dvojic v jednotlivých takových skupinách.

Věta 3.1.5. *Buď $q = p^k$ mocnina prvočísla. Pak:*

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

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

(iii) 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.

Lemma 3.1.6. *Uvažme roj $AH_{\mathbb{F}_q}$ a nějakou jeho komponentu souvislosti V. Pak je přes všechny afinní dvojice $(a, b) \in V$ součin ab invariantní.*

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:

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

□

Důsledek 3.1.7. *Každá komponenta souvislosti v roji $AH_{\mathbb{F}_q}$ 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 3.1.6 mají všechny prvky jedné souvislé komponenty stejný součin prvků, je jich proto nejvýše $q-1$. □

Poznamenejme, že ze všech $q-1$ dvojic prvků s daným součinem ne nutně všechny leží v roji, například v tělese $\mathbb{F}_{11}$ pro součin roven čtyřem nevyhovuje dvojice $(2,2)$. Lemma, které jsme zmínili před chvílí, nám též umožní adaptovat větu 2.1.10, tentokrát je totiž počet přátel grafů k dané souvislé komponentě velmi omezený.

Definice 3.1.8. Ať $(a,b) \in AH_{\mathbb{F}_q}$ leží v souvislé komponentě V. Potom nazveme libovolnou souvislou komponentu obsahující prvek (ka, kb) pro $k \in \mathbb{F}_q$ přítelem V.

Věta 3.1.9. *Ať $(a,b) \in AH_{\mathbb{F}_q}$ leží v komponentě souvislosti 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 2.1.10, tentokrát ale pokud pro $k \neq 1$ leží (a,b) a (ka,kb) ve stejné komponentě, podle lemmatu 3.1.6 musí platit $ab = k^2ab$, tj. $k = -1$. Nosná množina grupy O_k sestrojené analogicky k důkazu věty 2.1.10 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 $(0,\infty)$ jsou $(\pm a, \mp a)$, 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 3.1.10. Ať $H \subseteq AH_{\mathbb{F}_q}$ je komponenta souvislosti 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 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, že (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. Podle definice roje nemůže platit $a^2 \neq a(a-b)$, tedy v $AH_{\mathbb{F}_q}$ leží vrchol $(a-x, a+x)$. Jeho následník je:

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

□

Díky tomuto tvrzení dokážeme poskytnout parciální odpověď na otázku, jak vypadají komponenty souvislosti v $AH_{\mathbb{F}_q}$. Prozatím se zaměříme na případy $q \equiv 3, 5 \pmod 8$, lemma 3.2.1 nám rozdělí práci pro tyto dva případy.

Důsledek 3.2.2. *Uvažme afinní vrchol $(a, b) \in AH_{\mathbb{F}_q}$. Potom:*

(i) pokud $\phi_q(-ab) = -1$, tak má právě jeden z vrcholů (a, b) a (b, a) v $AH_{\mathbb{F}_q}$ předchůdce,

(ii) pokud $\phi_q(-ab) = 1$, tak mají v $AH_{\mathbb{F}_q}$ předchůdce buď oba vrcholy (a, b) a (b, a), nebo ani jeden.

Důkaz. Pokud $\phi_q(-ab) = -1$, tak součin čísel:

$$a(a-b) \cdot b(b-a) = -ab(a-b)^2$$

čtverec není, tak je právě jedno z čísel $a(a-b)$ a $b(b-a)$ čtvercem, tedy díky lemmatu 3.2.1 má právě jeden z vrcholů předchůdce. Pokud naopak $\phi_q(-ab) = 1$, tak jsou buď obě čísla čtverci, nebo ani jedno, což koresponduje s počty předchůdců příslušných vrcholů. □

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. Pro $q \equiv 5$ je tato situace prohozena.

Jádro celé charakterizace grafu $AH_{\mathbb{F}_q}$ pro $q \equiv \pm 3 \pmod 8$ spočívá v následujícím tvrzení:

Lemma 3.2.3. *Ať $q \equiv 3, 5 \pmod 8$ je mocnina prvočísla. Dejme tomu, že v $AH_{\mathbb{F}_q}$ máme sled vrcholů $A \longmapsto B \longmapsto C \longmapsto D$, kde $B = (a, b)$ je bod splňující $\phi_q(-ab) = 1$. Potom každý jiný sled vrcholů v $AH_{\mathbb{F}_q}$ splňující $X \longmapsto Y \longmapsto Z \longmapsto D$ také splňuje $Z = C$.*

Důkaz. Bez újmy na obecnosti pišme $B = (1, b)$, pak požadujeme $\phi_q(-b) = 1$. Fakt, že B má předchůdce (jímž je A) díky lemmatu 3.2.1 znamená, že existuje $x \in \mathbb{F}_q$ splňující $1 - b = x^2$. Nyní si spočítejme body C, D:

$$(1, b) \longmapsto \underbrace{\left(\frac{b+1}{2}, \frac{2b}{b+1}\right)}_{C} \longmapsto \left(\frac{b^2+6b+1}{4(b+1)}, \frac{4b(b+1)}{b^2+6b+1}\right) = D.$$

Předchůdce D různý od C je roven:

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

Tento bod má sám předchůdce podle důsledku 3.2.2. Ať (X, Y) a (Y, X) jsou dva předchůdci D, ti splňují soustavu:

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

Čísla X, Y jsou tedy kořeny kvadratické rovnice $U^2 - \frac{4b}{b+1}U + b = 0$ nad $\mathbb{F}_q$. Tyto kořeny spočítáme explicitně:

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

při nějaké volbě odmocniny z $-b$, která dle předpokladů leží v $\mathbb{F}_q$. Konečně ukážeme, že (X, Y) nemá předchůdce, z toho podle důsledku 3.2.2 plyne, že i (Y, X) nemá předchůdce. K tomu nám díky lemmatu 3.2.1 stačí ověřit, že číslo $X(X - Y)$, které je rovno:

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

není v $\mathbb{F}_q$ čtvercem. Díky existenci $x \in \mathbb{F}_q$ splňujícího $x^2 = 1 - b$ pišme:

$$\phi_q(2b(b-1)) = \phi_q(2) \cdot \phi_q(b) \cdot \phi_q(b-1) = -1 \cdot \phi_q(b) \cdot \phi_q(-x^2)$$
$$= -1 \cdot \phi_q(-b) \cdot \phi_q(x^2) = -1 \cdot 1 \cdot 1 = -1.$$

Dohromady máme $\phi_q(X(X - Y)) = 1 \cdot (-1) = -1$, tedy oba předchůdci E nemají předchůdce. Pokud proto existuje sled čtyř prvků končících v D, pak předposlední člen nutně musí být C. □

Poznámka. Nad tělesy, kde $\phi_q(2) = 1$, lemma neplatí.

Nyní dokážeme hlavní větu této sekce.

Věta 3.2.4. *Ať $q \equiv 3, 5 \pmod 8$ je mocnina prvočísla. Pak roj $AH_{\mathbb{F}_q}$ vypadá následovně:*

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

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

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

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

Důkaz. Ukážeme, že komponenty souvislosti obsahující body (a, b) splňující $\phi_q(-ab) = -1$ tvoří medúzy a komponenty souvislosti obsahující (a, b) pro něž je naopak $\phi_q(-ab) = 1$ tvoří vulkány hloubky 2.

Pokud platí $\phi_q(-ab) = -1$ čtverec, tak podle důsledku 3.2.2 má právě jeden z vrcholů (a, b) a (b, a) 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. Komponenta souvislosti obsahující (c, d) je tedy medúzou.

Nyní přijde ta zajímavější část, tedy že pokud $\phi_q(-ab)$ je rovno jedné, tak komponenta souvislosti obsahující libovolný vrchol $V = (a, b)$ je vulkán. Stejně jako v případě AG posloupnosti pišme sled následníků vrcholu V:

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

Máme nekonečně definovanou posloupnost na konečné množině vrcholů, jednou proto vstoupí do cyklu, který má délku větší než jedna. Dejme tomu, že (c, d) je člen cyklu, potom mu můžeme psát nekonečnou posloupnost předků ležících v cyklu. Ať je tedy (C, D) předchůdce (c, d) neležící v cyklu. V důkaze lemmatu 3.2.3 jsme si ukázali, že (C, D) má dva rodiče a ti již rodiče nemají. Toto platí pro každý člen (c, d) libovolného cyklu. Tím tedy získáváme, že každá komponenta souvislosti 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 $p \equiv 1, 7 \pmod 8$? Nebo sice platí

$p \equiv 3, 5 \pmod 8$, ale $k = 2t$ je sudé? V takových případě je $\phi_q(2) = 1$ a navíc každý list v grafu $AH_{\mathbb{F}_{p^t}}$ má v grafu $AH_{p^k} = AH_{p^{2t}}$ předchůdce. Na příklad rozšiřme příklad ? nad tělesem $\mathbb{F}_{p^2}$, pak graf vypadá následovně:

OBR–

Vulkán má tedy o jedna vyšší hloubku. 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 3.2.5. *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 3.2.4. 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 $\mathbb{F}_{q^{2k}}$. 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. □

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

Věta 3.2.6. *(LTE lemma) Ať p je liché a k sudé. Pak platí:*

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

[citation needed] Důsledek výše spolu s větou 3.2.4 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.

Definice 3.3.1. Ať q je mocnina prvočísla. Pak označme $D(\mathbb{F}_q)$ počet všech souvislých komponent v grafu $AG_{\mathbb{F}_q}$, které obsahují alespoň jeden afinní prvek. Navíc, označme $S(\mathbb{F}_q)$ počet všech hejn v grafu $AH_{\mathbb{F}_q}$, které obsahují alespoň jeden afinní prvek.

???

Věta 3.3.2. *Platí řetězec nerovností:*

$$q - 1 \geqslant \frac{D(\mathbb{F}_q)}{S(\mathbb{F}_q)} \geqslant \frac{q-1}{2}.$$

Důkaz. Tato věta je přímým důsledkem věty 4.3.1, jelikož každé hejno přispívá buď $\frac{q-1}{2}$ nebo $q-1$ medúzami do počtu $D(\mathbb{F}_q)$. □

Lepší odhady zdánlivě nenajdeme, dále uveďme grafy $AH_{\mathbb{F}_p}$ pro $p = A$ a B, kde každá medúza je reprezentantem svého hejna a má vždy buď $q-1$ nebo $\frac{q-1}{2}$ přátel.

3.4 Dynamické systémy

AH posloupnost se od dvou, které jsme studovali před chvílí, liší také tím, že nemusíme nijak 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 $\mathbb{P}^1(\mathbb{F}_q)$. 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.

Většina vyřešených dynamických systémů se zabývá buď pouze aditivní strukturou $\mathbb{F}_q$ [] a nebo pouze jeho multiplikativní strukturou. Příklady takových systémů jsou tvaru $x \longmapsto ax$ či $x \longmapsto x + b$, případně systém $x \longmapsto ax + b$. My se zabýváme systémem, kde obě struktury kombinujeme, a proto se nemůžeme divit, že znalosti o této posloupnosti nepřijdou zdarma. Příkladem takového systému je $x \longmapsto x^2 + c$ - zobrazení, které nad komplexními čísly studovat Mandelbrot a je spojen s fraktály. Studium tohoto systému nad konečnými tělesy vedlo mimo jiné na tvorbu Pollard-Rho-ova algoritmu na rozkládání celých čísel [].

Jak přesně ale souvisí náš systém s AH posloupností?

Definice 3.4.1. Mějme $x \in \mathbb{P}^1(\mathbb{F}_q) \setminus \{1\}$. Pak definujme *orbitu* $\mathcal{O}(x)$ jako množinu:

$$\{x, f(x), f(f(x)), f(f(f(x))), \dots\},$$

kde $f \equiv \frac{(x+1)^2}{4x}$. *Dynamický systém* $D_f = (\mathbb{P}^1(\mathbb{F}_q), E)$ definujeme jako orientovaný graf takový, že pro $a, b \in \mathbb{P}^1(\mathbb{F}_q)$ platí $(a, b) \in E$, právě pokud $f(a) = b$.

Uvažme surjektivní zobrazení $g : AH_{\mathbb{F}_q} \longrightarrow \mathbb{P}^1(\mathbb{F}_q)$ dané $g(a, b) = \frac{a}{b}$. Potom se na každý nenulový prvek $x \in \mathbb{F}_q$ zobrazí právě $q-1$ prvků $AH_{\mathbb{F}_q}$, konkrétně body $(ax, a) \in AH_{\mathbb{F}_q}$ pro $a \in \mathbb{F}_q^\times$. Prvky 0 a ∞ mají každý právě jeden předobraz. Každé hejno v grafu $AH_{\mathbb{F}_q}$ se pak pod g zobrazí na jednu komponentu souvislosti v D_f. Navíc rozdělení grafů na body

(a, b) podle $\phi_q(ab)$ je zachováno. To proto, že pro bod $(a, b) \in AH_{\mathbb{F}_q}$ platí $\phi_q(ab) = 1$, právě pokud platí $\phi_q\left(\frac{a}{b}\right) = 1$.

Jelikož je D_f systém daný kvadratickou lomenou funkcí, každý prvek (vyjma 1) má buď žádného nebo dva předchůdce. Víme, že prvky $AH_{\mathbb{F}_q}$ chodí v párech - pokud (a, b) je předchůdce body (x, y), tak je jím i (b, a). Tento fakt koresponduje s tím, že funkce f je fixovaná pod involucí $x \longmapsto \frac{1}{x}$. Pokud tedy x je předchůdcem y, tak druhým předchůdcem y je $\frac{1}{x}$. Zkoumejme další pouta mezi oběma grafy.

Věta 3.4.2. *Bod $(a, b) \in AH_{\mathbb{F}_q}$ leží v cyklu, právě pokud bod $\frac{a}{b} \in D_f$ leží v cyklu.*

Důkaz. Dokážeme obměnu tvrzení. Dejme tomu, že bod (a, b) neleží v cyklu grafu $AH_{\mathbb{F}_q}$, poté dle symetrie v něm neleží ani bod $(-a, -b)$. Podle věty 3.1.6 jsou (a, b) a $(-a, -b)$ jediní možní kandidáti na body (x, y) ležící v komponentě souvislosti obsahující (a, b), které splňují $\frac{x}{y} = \frac{a}{b}$. Tj. tyto body jsou jediní kandidáti na body, které se zobrazí na prvek $\frac{a}{b} \in D_f$. Nejsou-li oba body periodické, pak $\frac{a}{b}$ nemůže být periodický též.

Naopak je-li bod (a, b) zobrazen na bod mimo cyklus, tak je $(-a, -b)$ též. To znamení, že se v orbitě $\mathcal{O}\left(\frac{a}{b}\right)$ již nebude znovu prvek $\frac{a}{b}$ vyskytovat, takže ani v posloupnosti $AH_{\mathbb{F}_q}(a, b)$ se bod (a, b) znovu nevyskytuje. Bod (a, b) proto leží mimo cyklus. □

Pokud máme posloupnost $AH(a, b)$:

$$(a, b) \longmapsto (a_1, b_1) \longmapsto \cdots \longmapsto (a_k, b_k) \longmapsto \ldots,$$

kde (a_k, b_k) je první prvek cyklu, pak v orbitě:

$$\mathcal{O}\left(\frac{a}{b}\right) = \left\{\frac{a}{b}, \frac{a_1}{b_1}, \frac{a_2}{b_2}, \ldots, \frac{a_k}{b_k}, \ldots\right\},$$

je $\frac{a_k}{b_k}$ první periodický bod. Z toho můžeme díky větám 3.2.4 a 3.4.2 odvodit následující.

Důsledek 3.4.3. *Ať $(x, y) \in AH_{\mathbb{F}_q}$ je členem cyklu a $V \subseteq AH_{\mathbb{F}_q}$ je orientovaný binární strom zakořeněný v (x, y). Dále označme $W \subseteq D_f$ orientovaný binární strom zakořeněný v prvku $\frac{a}{b} \in \mathbb{P}^1(\mathbb{F}_q)$. Potom platí $V \cong W$.*

Důsledek 3.4.4. *Ať $q \equiv 3, 5 \pmod 8$ je mocnina prvočísla. Pak graf D_f vypadá následovně:*

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

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

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

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

Jediný rozdíl tak nastává v ohledu cyklů - stejně jako v případě AG posloupnosti. Konkrétně, je-li $(a, b) \in AH_{\mathbb{F}_q}$ je členem cyklu, tak buď prvek $(-a, -b)$ leží v tom samém cyklu, potom je délka cyklu v D_f je poloviční, nebo leží v naprosto odlišném cyklu, pak je délka cyklu zachována.

Pomocí dynamických systémů můžeme znovu dokázat některé výsledky ohledně AH posloupnosti, které jsme dokázali v předchozích sekcích. Pomocí vlastností konečných těles můžeme dokázat znovu odhady, které jsou předmětem důsledku 3.2.5. Stačí nám ukázat, že pro $z \in \mathbb{F}_q$ leží každý předchůdce prvku $(z, 1) \in AH_{\overline{\mathbb{F}_q}}$ po normalizaci v $\mathbb{F}_{q^2}$.

Věta 3.4.5. *Ať $q \equiv \pm 3 \pmod 8$ je mocnina prvočísla a $x \in \overline{\mathbb{F}_q}$ je prvek splňující:*

$$\frac{(x+1)^2}{4x} \in \mathbb{F}_q.$$

Potom $x \in \mathbb{F}_{q^2}$.

Důkaz. Číslo $z \in \overline{\mathbb{F}}_q$ leží v tělese $\mathbb{F}_q$, právě pokud je kořenem polynomu $z^q - z \in \mathbb{F}_q[x]$. Protože q je mocninou charakteristiky tělesa $\mathbb{F}_q$, tak pro libovolná $a, b \in \overline{\mathbb{F}}_q$ platí kvůli binomické větě $(a+b)^q = a^q + b^q$. Speciálně:

$$\frac{(x+1)^2}{4x} = \left(\frac{(x+1)^2}{4x}\right)^q = \frac{(x^2+2x+1)^q}{4x^q} = \frac{x^{2q}+2x^q+1}{4x^q},$$
$$x^{q+1} + 2x^q + x^{q-1} = x^{2q} + 2x^q + 1,$$
$$0 = (x^{q+1} - 1)(x^{q-1} - 1).$$

Buď tedy platí $x^{q+1} = 1$ nebo $x^{q-1} = 1$. Umocněním těchto dvou vztahů na exponent po řadě $q-1$ a $q+1$ získáme, že v každém případě platí $x^{q^2-1} = 1$, tj. $x \in \mathbb{F}_{q^2}$. □

???? JE ASI MOC HARD UKAZAT, ZE DAL TO NEJDE
Nyní se věnujme otázce délek cyklů v D_f. Nejprve si všimněme, že 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. Toto koresponduje s lemmatem 3.2.1. Můžeme určit, kolik prvků v D_f není listy.

Věta 3.4.6. *Počet $a \in \mathbb{F}_q$ takových, že $\phi_q(a^2 - a) = 1$, je $\frac{q-3}{2}$.*

Důkaz. Určíme součet:

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

Bez újmy na obecnosti sčítejme přes $\mathbb{F}_q \setminus \{1\}$. 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 $x \neq 1$ existuje unikátní $a \neq 1$ splňující vztahy výše, takže:

$$\sum_a \phi_q(a^2 - a) = \sum_{a \neq 1} \phi_q(a).$$

Víme ale, že v $\mathbb{F}_q$ leží stejně kvadratických zbytků jako nezbytků, takže součet výše je roven $-\phi_q(1) = -1$.

Legendreho symbol nabývá pouze hodnot $0, 1$ a -1, přičemž v našem součtu figuruje $q-1$ sčítanců, jeden z nich nulový. To znamená, že právě $\frac{q-3}{2}$ 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 $a_1 x_1^{b_1} + \cdots + a_n x_n^{b_n} = k$ nad konečnými tělesy. Pro excelentní úvod do jejich studia doporučuji [3].

Důsledek 3.4.7. *Je-li $x \in D_f$ periodický bod, pak jeho perioda má délku nejvýše $(q-1)/4$. Jinak řečeno, každý cyklus v $AH_{\mathbb{F}_q}$ má délku nejvýše $(q-1)/2$.*

Tento výsledek je však zjevný při pohledu na původní problém. Totiž každá komponenta souvislosti obsahuje podle věty 3.1.7 nejvýše $q-1$ afinních bodů a navíc obsahuje jediný cyklus. Navíc ke každému prvku cyklu je připojen alespoň jeden další prvek, proto každý cyklus má délku nejvýše $(q-1)/2$. Můžeme ale ohraničit největší cyklus v grafu i jinak. Ohledně spodních odhadů na největší cyklus v grafu D_f již pochodíme lépe.

Dívejme se na vícenásobné aplikace lomené funkce $f \equiv \frac{(x+1)^2}{4x}$ stupně dva, její n-násobná aplikace má stupeň 2^n, přičemž stupeň čitatele je ostře větší, než stupeň jmenovatele. Podívejme se na následující rovnici:

$$\underbrace{f(f(\ldots f}_{n}(x))) = x.$$

Pokud vynásobíme rovnici jmenovatelem, získáme polynom stupně 2^n roven 0. Jelikož $\mathbb{F}_q$ je oborem integrity, rovnice má nejvýše 2^n kořenů.

Věta 3.4.8. *Buď $q \equiv \pm 3 \pmod 8$ mocnina prvočísla. Potom pro $d \in \{1, 2\}$ existuje v D_f vulkán hloubky d, jehož cyklus má délku alespoň* $\log_2((q-1)\cdot(q-3)) - d - 2$.

Důkaz. Označme $f : \mathbb{F}_q \longrightarrow \mathbb{F}_q : f(x) = \frac{(x+1)^2}{4x}$ lomenou funkci stupně dva. Potom n-násobná aplikace $f^{(n)}(x) = \underbrace{f(f(\ldots f}_{n}(x)))$ má stupeň 2^n. Prvek $x \in D_f$ tak leží v cyklu délky $D \mid n$, právě pokud $f^{(n)}(x) = x$.

Představme si, že vynásobíme lomenou funkci $f^{(n)}(x) - x$ jmenovatelem $f^{(n)}(x)$, poté získáme polynom ležící v $\mathbb{F}_q[x]$ stupně 2^n, který má nad $\mathbb{F}_q$ nejvýše 2^n kořenů. Existuje proto nejvýše 2^n prvků $x \in D_f$ ležících v cyklu délky n. Počet prvků D_f ležících v cyklu délky nejvýše n je proto roven nejvýše:

$$2 + 2^2 + \cdots + 2^n < 2^{n+1}. \tag{3.1}$$

Zvolme nyní $d \in \{1, 2\}$ a uvažme komponentu $V \subseteq D_f$ složenou ze všech vulkánů hloubky d. Ke každému členu cyklu $v \in V$ je připojen binární strom hloubky d s 2^d prvky, proto ve V je právě $|V|/2^d$ prvků ležících v cyklech. Díky větě 3.1.5 je toto číslo alespoň:

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

Označme konečně N nejvyšší délku cyklu, který ve V najdeme. Podle nerovnosti (4.3.1) musí platit:

$$2^{N+1} > \frac{(q-1)(q-3)}{2^{d+1}},$$

což jsme chtěli. □

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 [5], 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:

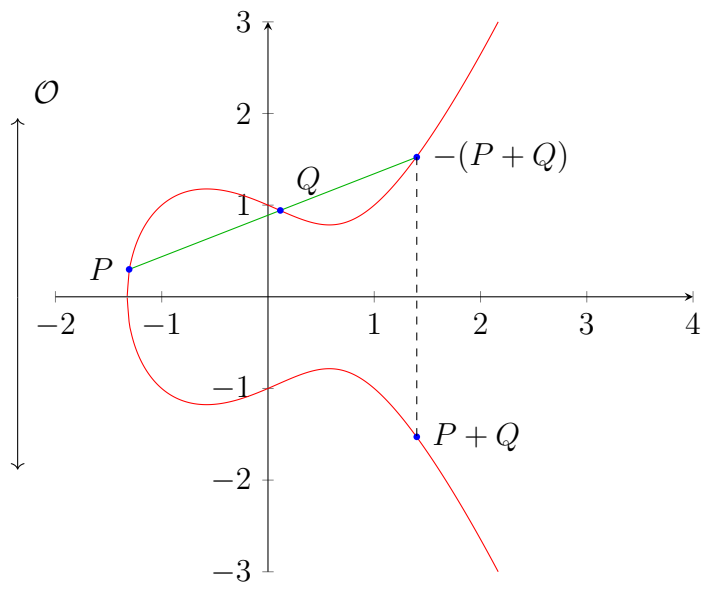
$$y^2 = x^3 + Ax + B,$$

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 $[n]P = \underbrace{P + \cdots + P}_{n}$. Definujeme $[0]P = O$.



Obrázek 4.1: Sčítání na eliptické křivce.

–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.

Věta 4.1.2. *(Hasse) Buď q mocnina lichého prvočísla a E eliptická křivka nad $\mathbb{F}_q$. Potom platí:*

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

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

Definice 4.1.3. 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 $u \in \overline{K}$. Každá Legendreho křivka má nejvýše 6 křivek s ní isomorfních a je jednoduché najít jejich koeficienty [?].

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 4.1.4. *(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

Endomorfismus na křivce E definujme jako isogenii $\phi : E \longrightarrow E$, přičemž připusťme, že $[0]$ je na E endomorfismem. Pak se sčítáním $(\phi + \psi)P = \phi P + \psi P$ a skládáním $\phi \circ \psi = \phi(\psi)$ tvoří endomorfismy na křivce okruh.

Definice 4.2.1. Buď E eliptická křivka definovaná nad $\mathbb{F}_q$. Pak označme $\mathrm{End}(E)$ okruh všech endomorfismů na E definovaných nad $\mathbb{F}_q$ s operacemi sčítáním a skládáním.

Definice 4.2.2. Buď $\phi \in \mathrm{End}(E)$. Pak definujeme jeho stopu jako:

$$\mathrm{Tr}\,\phi = \phi + \widehat{\phi}.$$

Je přímočaré ukázat, že stopa je aditivní funkce. Dále je známé, že $\phi + \widehat{\phi}$ je v okruhu endomorfismů celým číslem a navíc každý endomorfismus stupně n je nad $\mathrm{End}(E)$ kořenem kvadratické rovnice $x^2 - \mathrm{Tr}\,\phi x + n \in \mathbb{Z}[x]$.

4.3 Aplikace na AG posloupnost

Nyní aplikujeme teorii eliptických křivek na *AG* posloupnost. Konkrétně ukážeme, že medúzy, které tvoří *AG* posloupnosti, můžeme propojit s grafy isogenií Legendreho křivek.

Uvažme nějakou dvojici $(a, b) \in AG_{\mathbb{F}_q}$. Tuto dvojici ztotožníme s dvojicemi (ka, kb) pro $k \in \mathbb{F}_q^\times$ pomocí podílu $\frac{b}{a} = \lambda$. Budeme se dále zabývat pouze tímto podílem. Kvůli přítomnosti odmocniny se budeme dívat na druhou mocninu tohoto podílu při přechodu z jedné dvojice na druhé:

$$\lambda^2 = \left(\frac{b}{a}\right)^2 \longmapsto \left(\frac{2\sqrt{ab}}{a+b}\right)^2 = \frac{4ab}{(a+b)^2} = \frac{4\lambda}{(\lambda+1)^2}.$$

Chceme najít nějaké médium, ve kterém bude toto zobrazení přirozené. Autoři článku [2], na kterém je práce založena, našli velmi elegantní pohled na posloupnost pomocí Legendreho křivek. Konkrétně, pro každý podíl $\lambda = \frac{b}{a}$ definujeme Legendreho křivku:

$$E_{(a,b)} = E_{\lambda^2} : y^2 = x(x-1)\left(x - \frac{b^2}{a^2}\right).$$

Věta 4.3.1. *Graf je skoro graf isogenií.*

Pointou této definice samozřejmě je zjistit, jaký vztah spolu má dvojice (a, b) a (a_1, b_1).

Věta 4.3.2. *Mějme v grafu $AG_{\mathbb{F}_q}$ orientovanou hranu $(a,b) \longmapsto (a_1,b_1)$. Pak existuje mezi křivkami $E_{(a,b)}$ a $E_{(a_1,b_1)}$ isogenie stupně dvě definovaná nad $\mathbb{F}_q$. Tato isogenie má předpis:*

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

Důkaz. ϕ je opravdu isogenií, protože je daná lomenými funkcemi nad $\mathbb{F}_q$ (a tedy i ponechává bod v nekonečnu), postačí nám tedy ukázat, že zobrazuje jednotlivé křivky na sebe. Pokud $(x,y) \in E_{(a,b)}$ splňuje $(a,b) \neq (0,0)$, tak nám stačí ukázat, že $\phi(x,y) \in E_{(a_1,b_1)}$. To je pouze otázka výpočtu:

$$\begin{aligned}
\frac{(ax+b)^2}{x(a+b)^2} \cdot \left(\frac{(ax+b)^2}{x(a+b)^2} - 1\right)\left(\frac{(ax+b)^2}{x(a+b)^2} - \frac{b_1^2}{a_1^2}\right) = \\
\frac{(ax+b)^2}{x(a+b)^2} \cdot \left(\frac{(ax+b)^2}{x(a+b)^2} - 1\right)\left(\frac{(ax+b)^2}{x(a+b)^2} - \frac{4ab}{(a+b)^2}\right) = \\
\frac{(ax+b)^2}{x(a+b)^2} \cdot \frac{(x-1)(a^2x-b^2)}{x(a+b)^2} \cdot \frac{(ax-b)^2}{x(a+b)^2} = \\
x(x-1)\left(x - \frac{b^2}{a^2}\right) \cdot a^2 \cdot \frac{(ax-b)^2(ax+b)^2}{x^2(a+b)^6} = \left(y \cdot \frac{a(ax-b)(ax+b)}{x(a+b)^3}\right)^2.
\end{aligned}$$

Isogenie ϕ proto zobrazí $E_{(a,b)}$ na $E_{(a_1,b_1)}$. □

Jádro takové isogenie (ve smyslu homomorfismu grup) je grupa $\{(0,0), O\}$. To potvrzuje, že AG posloupnost nezobrazí žádnou dvojici na jinou dvojici s nulovou složkou.

něco svulkánama.

–

Pojďme nyní využít tento nový náhled na AG posloupnost a osvětleme zdánlivě náhodné velikosti a počty medúz. Díky větě 4.3.1 je počet skupin přátel mezi medúzami, které tvoří roj $AG_{\mathbb{F}_q}$, roven počtu různých vulkánů v grafu isogenií.

AG posloupnost sama o sobě nenabízí žádný zjevný invariant, který by mohl být sdílený mezi prvky stejné medúzy. V přechodu na grafy isogenií hledáme veličinu, která by byla sdílena křivkami na obou stranách jedné hrany. Jinak řečenu veličina, kterou sdílí isogenní křivky. Sato-Tate-ova věta 4.1.4 poskytuje takový invariant - počet prvků na křivce.

Věta 4.3.3. *souvisla komponenta ma stejnej pocet prvku*

Toto pozorování nás může zavést k odhadu počtu hejn medúz v grafu $AG_{\mathbb{F}_q}$.

Věta 4.3.4. *(Griffin, Ono, Saika, Tsai) Pro každé $\varepsilon > 0$ a dostatečně velké $q \equiv 3 \pmod 4$ platí:*

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

Nástin důkazu.

Kapitola 5

Eliptické křivky a AH posloupnost

AG posloupnost má kořeny v teorii eliptických křivek, proto jsem hledal propojení i mezi eliptickými křivkami a *AH* posloupnost. Přímo adaptovat jejich postup, tedy přiřadit vrcholům grafu křivky, podle nejlepšího mínění autora není možné. Totiž komponenty $AH_{\mathbb{F}_q}$ mají nejvýše q prvků, viz věta 3.1.7, oproti *AG* posloupnosti, kde může být až mnohonásobně více prvků, jak jsme viděli u příkladu ?. Ne, *AH* posloupnost můžeme popsat trochu jednodušeji. Opět se ale podíváme do světa eliptických křivek.

5.1 Motivace

Pro tuto sekci sledujme trochu pozorněji časovou osu studia dynamických systémů, mnohé z nich vedly směrem isogenií $\phi : E \longrightarrow E$, tzv. *endomorfismů*.

Vraťme se hned čtyři dekády nazpět, kdy Miller a Koblitz stáli u zrodu kryptografie pomocí eliptických křivek. Efektivita takového šifrování je založena na jednoduchosti vzorců pro skalární násobení, hlavně pak $[2]P$ a $[3]P$. Speciálně tito pánové navrhli práci na eliptické křivce:

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

nad konečným tělesem charakteristiky 2. Krom jejío využití v šifrování nám tato křivka může pomoci studovat mj. dynamiku funkce $x + \frac{1}{x}$ nad tělesy $\mathbb{F}_{2^n}$. V [6] je totiž ukázáno, že pro bod $P = (x, y) \in E$ a Frobeniův automorfismus $\pi : (x, y) \longmapsto (x^2, y^2)$ platí:

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

Pokud se tedy zaobíráme čistě x-ovou souřadnicí, endomorfismus $1 + \pi$ zobrazí x na prvek $x + \frac{1}{x}$. Ugolini [6, 7, 8, 9] hojně studoval podobná propojení jistých dynamických systémů a eliptických křivek, nejprominentněji právě zobrazení $x \longmapsto x + \frac{1}{x}$ nad tělesy s charakteristikou $2, 3$ a 5. V těchto případech grafy asociované s tímto zobrazením též tvoří vulkány a pomocí vlastností okruhů endomorfismů eliptických křivek dokážeme podrobněji určit vlastnosti těchto grafů. Tyto články byly hlavní inspirací pro tuto kapitolu.

5.2 Singulární Montgomeryho křivka

Ve snaze adaptovat postupy popsané 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 ani Legendrově tvaru se mi takové zobrazení najít nepodařilo.

Hledaný endomorfismus jsem nakonec nalezl u křivek v *Montgomeryho tvaru* $By^2 = x^3+Ax^2+x$ pro $A, B \in \mathbb{F}_q$. Tyto křivky mají několik praktických výhod, proto se například používají v šifrovacím protokolu CSIDH, více informací o tomto a dalších protokolech založených na isogeniích naleznete v [5].

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 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 [4]. Co by se stalo, pokud bychom zvolili $A = -2$? Pro takovou hodnotu A dostaneme pro $x \neq 1$:

$$[2]P = \left(\frac{(x+1)^2}{4x}, y\frac{x^2-1}{8x^2} \right). \tag{5.1}$$

x-ová souřadnice dvojnásobku bodu (x, y) se chová jako dynamický systém založený na AH posloupnosti! Toto pozorování otevírá cestu studiu AH posloupnosti pomocí eliptických křivek.

Problém ale nastává právě s hodnotou $A = -2$, pro ni je totiž křivka rovna:

$$E : y^2 = x(x-1)^2.$$

Tuto křivku budeme ve zbytku sekce studovat. Ve skutečnosti není křivka E 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 $(x, y) \in \mathbb{F}_q^2$ splňujících $y^2 = x(x-1)^2$ a $x \neq 1$ spolu s bodem v nekonečnu O, kde operace je sčítání na křivce.

Ihned vidíme, že pokud (x, y) leží na E, tak x je čtvercem v $\mathbb{F}_q$. Díky tomuto pozorování můžeme parametricky vyjádřit všechny body na E a charakterizovat, kdy tři body leží na přímce.

Lemma 5.2.2. *Prvky grupy $E(\mathbb{F}_q)$ můžeme vyjádřit parametricky jako:*

$$E(\mathbb{F}_q) = \{(t^2, t^3 - t) | t \in \mathbb{F}_q \setminus \{\pm 1\}\} \cup \{O\}.$$

Důkaz. Pokud (x, y) patří do $E(\mathbb{F}_q)$, tak $x \neq 1$ a platí $x = \left(\frac{y}{x-1}\right)^2$, tedy buď $(x, y) = (0, 0)$, nebo je $\phi_q(x) = 1$. Ať $x \neq 0$, potom existuje $t \in \mathbb{F}_q^\times$ takové, že $x = t^2$. Potom y splňuje:

$$y^2 = x(x-1)^2 = \left[t(t^2-1)\right]^2.$$

Tomuto vztahu vyhovují právě dvě hodnoty $y \in \{t^3 - t, (-t)^3 + t\}$. Všechny body ležící na $E(\mathbb{F}_q)$ jsou proto tvaru $(t^2, t^3 - t)$. Pro $t = \pm 1$ získáme bod, který neleží na křivce. Nyní ukážeme, že pro $t \notin \{\pm 1\}$ je každý takový bod unikátní. Opravdu, dejme tomu, že různé prvky $s, t \in \mathbb{F}_q$ splňují $(s^2, s^3 - s) = (t^2, t^3 - t)$. Platí:

$$s(s^2 - 1) = t(t^2 - 1) = t(s^2 - 1).$$

Jistě platí $st \neq 0$, proto platí $s^2 = 1 = t^2$, což je spor. Docházíme k tomu, že prvky $E(\mathbb{F}_q) \setminus \{O\}$ můžeme jednoznačně přiřadit prvkům $\mathbb{F}_q \setminus \{\pm 1\}$. □

Okamžitým důsledkem lemmatu 5.2.2 je, že počet prvků na E je $|E(\mathbb{F}_q)| = q - 1$. Podívejme se, kdy v grupě $E(\mathbb{F}_{q^k})$ leží bod s x-ovou souřadnicí $a \in \mathbb{F}_q^\times$. Leží-li bod $(a, -)$ v $E(\mathbb{F}_q)$, potom podle lemmatu 5.2.2 platí $\phi_q(a) = 1$. Je-li naopak a čtvercem v $\mathbb{F}_q$, tak podle lemmatu 5.2.2 existuje bod $P \in E(\mathbb{F}_q)$, jehož x-ová souřadnice je a. Speciálně pro $a \in \mathbb{F}_q$, které není čtvercem, leží bod $(a, -) \in E(\mathbb{F}_{q^2})$, ale takový bod už nenajdeme v $E(\mathbb{F}_q)$. Tyto poznatky shrnuje následující tvrzení.

Věta 5.2.3. *Nechť $a \in \mathbb{F}_q$. Potom:*

- *pokud $\phi_q(a) = 1$ nebo $a = 0$, pak existuje bod $(a, -) \in E(\mathbb{F}_q)$,*
- *pokud $\phi_q(a) = -1$, pak existuje bod $(a, -) \in E(\mathbb{F}_{q^2})$.*

Abychom se blíže seznámili s křivkou E, podívejme se právě jak vypadá součet dvou bodů.

Věta 5.2.4. *Uvažme dva body $P = (a^2, a^3 - a), Q = (b^2, b^3 - b) \in E(\mathbb{F}_q)$ takové, že $P \neq \pm Q$. Potom:*

$$P + Q = \left(\left(\frac{ab+1}{a+b}\right)^2, \left(\frac{ab+1}{a+b}\right)^3 - \frac{ab+1}{a+b}\right).$$

Důkaz. Dle předpokladu je $-(P + Q)$ afinní bod, označme jej $R = (c^2, c^3 - c)$ pro $c \in \mathbb{F}_q$. Potom $P + Q + R = O$ a tak P, Q a R leží na přímce. Proto platí:

$$0 = \begin{vmatrix} a^2 & a^3 - a & 1 \\ b^2 & b^3 - b & 1 \\ c^2 & c^3 - c & 1 \end{vmatrix} = (a - b)(b - c)(c - a)(ab + ac + bc + 1),$$

tedy jelikož a, b, c jsou různé, tak platí $ab + ac + bc = -1$. Proto platí $c = -\frac{ab+1}{a+b}$ a tedy $P + Q = (c^2, -c^3 + c)$. □

Důkaz výše neplatí pro $P = Q$, tento případ je pokryt rovnicí (5.1). Díky této charakterizaci můžeme přesně zjistit, jak vypadá grupa bodů na E.

Věta 5.2.5. *Ať q je lichá mocnina prvočísla. Potom platí:*

$$E(\mathbb{F}_q) \cong \mathbb{F}_q^\times.$$

Důkaz. Z lemmatu 5.2.2 implicitně plyne, že obě grupy mají stejný počet prvků, totiž $q-1$. Definujme nyní zobrazení $\psi : E \longrightarrow \mathbb{F}_q^\times$ dané $\psi(O) = 1$ a pro bod $(a^2, a^3 - a) \in E(\mathbb{F}_q)$:

$$\psi(a^2, a^3 - a) = \frac{a+1}{a-1}.$$

Ukážeme, že jde o homomorfismus grup. Nejprve, pokud pro afinní body $P, Q \in E$ platí $P + Q = O$, tak existuje $a \in \mathbb{F}_q$ takové, že $P = (a^2, a^3 - a)$ a $Q = (a^2, -a^3 + a)$. Pak:

$$\phi(a^2, a^3 - a) \cdot \phi(a^2, -a^3 + a) \cdot \phi(O) = \frac{a+1}{a-1} \cdot \frac{-a+1}{-a-1} \cdot 1 = 1.$$

Dále, ať $P = (a^2, a^3 - a), Q = (b^2, b^3 - b)$ a $R = (c^2, c^3 - c)$ jsou ne všechny stejné afinní body ležící na přímce. Podle věty 5.2.4 a rovnice (5.1) platí vztah $ab + ac + bc = -1$. Stačí nám ověřit, že za této podmínky platí:

$$\frac{a+1}{a-1} \cdot \frac{b+1}{b-1} \cdot \frac{c+1}{c-1} = 1,$$

což je triviální. Konečně, ψ je invertibilní, jelikož můžeme definovat inverzní homomorfismus s předpisem:

$$a \longmapsto \left(\left(\frac{a+1}{a-1} \right)^2, \left(\frac{a+1}{a-1} \right)^3 - \frac{a+1}{a-1} \right).$$

Funkce $\frac{x+1}{x-1}$ je involuce, tak ψ bod výše zobrazí na a. Zobrazení ψ proto definuje isomorfismus mezi oběma grupami. □

5.3 Aplikace na AH posloupnost

Studium iterací zobrazení $x \longmapsto \frac{(x+1)^2}{4x}$ na konečném tělese nás zavedlo k jedné singulární křivce. Jelikož grupa bodů na takové křivce má velmi jednoduchou strukturu, získáme mnoho informací o AH posloupnosti.

Definice 5.3.1. Označme $G_{\mathbb{F}_q} = (E(\mathbb{F}_q), F)$ orientovaný graf takový, že pro libovolné body $P, Q \in E$ platí $(P, Q) \in F$, právě pokud $[2]P = Q$.

Nejprve si uvedeme kritérium, kdy pro bod $P = (x, y) \in E(\mathbb{F}_q)$ existuje v grafu $G_{\mathbb{F}_q}$ předchůdce, tj. kdy existuje bod $Q \in E(\mathbb{F}_q)$ takový, že $[2]Q = P$. Dále ukážeme, že pokud takový bod existuje, tak už existují dva.

Věta 5.3.2. *Uvažme bod $P = (x, y) \in E(\mathbb{F}_q)$. Pak existuje bod $Q \in E(\mathbb{F}_q)$ splňující $[2]Q = P$, právě pokud platí $v_2(\operatorname{ord} P) < v_2(q-1)$.*

Důkaz. Díky větě **??** existuje hledaný bod Q, právě pokud $v_2(\operatorname{ord} P)$ je menší, než $v_2(\#E(\mathbb{F}_q))$. Protože podle věty **??** platí $\#E(\mathbb{F}_q) = q - 1$,

Věta 5.3.3. *Ať $P, Q \in E(\mathbb{F}_q)$ jsou afinní body takové, že $[2]Q = P$. Potom existuje unikátní bod $R \neq Q$ splňující $[2]R = P$ a je to právě bod splňující $Q - R = R - Q = (0,0)$.*

Důkaz. Nejprve zmiňme, že protože $P \neq O$, tak $Q \notin \{O, (0,0)\}$, jelikož jediný netriviální bod ležící ve 2-torzi je $(0,0)$. Proto body $Q, (0,0), Q - (0,0)$ a O jsou si navzájem různé.

Nyní ukážeme, že bod $R = Q + (0,0)$ splňuje $[2]R = P$. Opravdu, jelikož bod $(0,0)$ splňuje vztah $[2](0,0) = O$, tak:

$$[2]\big(Q + (0,0)\big) = [2]Q + O = P.$$

Konečně dokážeme, že Q a $Q + (0,0)$ jsou jediné body splňující $[2]X = P$. Naopak připusťme, že bod $R \neq Q$ splňuje $[2]R = P = [2]Q$. Platí pak $[2](R - Q) = O$. Jelikož bod $R - Q$ není O, tak leží ve 2-torzi a je proto roven $(0,0)$. □

Věta 5.3.3 nám říká, že každý afinní vrchol $P \in G_{\mathbb{F}_q}$ má buď dva předchůdce, nebo ani jednoho. Bod O má dva předchůdce, $(0,0)$ a sama sebe. Zamysleme se nyní, jak může souvislá komponenta grafu $G_{\mathbb{F}_q}$ vypadat - podle příkladů uvedených v kapitole 3 se můžeme domnívat, že grafy *vždy* tvoří vulkány. Jak ale rozlišíme, v jakém stupni vulkánu daný bod leží?

Předpokládejme, že komponenta souvislosti $V \subseteq G_{\mathbb{F}_q}$ je vulkán. Vrchol $P \in V_i$ má následníka $[2]P$ ležícího ve V_{i-1}. Pokud tedy bod vynásobíme dvěma, buď již leží v cyklu komponenty, nebo se přesune o stupeň výše. Veličina, kterou můžeme pomocí endomorfismu $[2]$ vhodně kontrolovat, je řád bodu P, přesněji *jeho 2-valuace*. Abychom ověřili domněnku, že úrovně vulkánu jsou dané 2-valuací řádů bodů v nich ležících, podívejme se znovu na příklad ?. Body (a, b), jejichž součin je ?, tvoří medúzy a opravdu podle věty 5.2.3 NĚCO. Naopak u vulkánu hloubky 2 si k bodům připišme jejich řády:

–OBR–

Opravdu, bod na úrovni V_2 má řád dělitelný čtyřmi, body leží ve V_1 mají řády sudé a nedělitelné čtyřmi, každý prvek V_0 má řád lichý. Pojďme si zformalizovat tato pozorování.

Podle postupu zmíněného v důkaze věty 3.2.4 víme, že každá posloupnost $AH_{\mathbb{F}_q}(a, b)$ jednou vstoupí v cyklus, to musí platit i pro posloupnost bodů $P \longmapsto [2]P \longmapsto \dots$. Podívejme se, jakou výšku budou mít stromy zakořeněné ve členech cyklu.

Věta 5.3.4. *Ať $P \in E(\mathbb{F}_q)$ je členem cyklu v grafu $G_{\mathbb{F}_q}$. Potom strom zakořeněný v P je dokonale vyvážený binární strom hloubky $v_2(q - 1)$.*

Důkaz. Fakt, že P je členem cyklu, je synonymem pro fakt, že řád P v $E(\mathbb{F}_q)$ je lichý. Pokud by totiž byl řád P sudý, tak opakovanými aplikacemi endomorfismu $[2]$ získáme posloupnost bodů, které mají ostře menší řád. Postupujme nyní ve stromu zakořeněném v P směrem k listům a sledujme vždy všechny vrcholy ve vzdálenosti k od P. Ukážeme, že 2-valuace řádu těchto bodů je rovna k. Pro $k = 0$ tvrzení platí.

Nyní předpokládejme, že pro nějaké nezáporné $k < v_2(q-1)$ tato skutečnost nastane. Potom uvažme libovolný bod Q s $v_2(\operatorname{ord} Q) = k+1$. Podle vět 5.3.2 a 5.3.3 má Q v grafu právě dva předchůdce R_1 a R_2. Ty pro $i \in \{1,2\}$ splňují $[2]R_i = Q$ a proto platí $v_2(\operatorname{ord} R_i) = v_2(\operatorname{ord} Q) + 1$. Tento postup selže až při $k = v_2(q-1) = v_2(\#E(\mathbb{F}_q))$, kdy již podle věty 5.3.2 získáme, že žádný bod $Q \in G_{\mathbb{F}_q}$ splňující $v_2(\operatorname{ord} Q) = v_2(q-1)$ nemá v grafu předchůdce. Dohromady máme, že strom zakořeněný v P je dokonale vyvážený a jeho hloubka je rovna $v_2(q-1)$. □

Důsledek 5.3.5. *Ať $P \in G_{\mathbb{F}_q}$ je libovolný bod na E. Potom komponenta souvislosti grafu $G_{\mathbb{F}_q}$ obsahující P je vulkán hloubky $v_2(q-1)$.*

Tato věta platí v případě, kdy jsou ve hře body v nekonečnu - poté je cyklus vulkánu smyčka $\infty \longmapsto \infty$. Pomocí věty 5.2.3 se můžeme vrátit zpět do roje $AH_{\mathbb{F}_q}$.

Věta 5.3.6. *Ať $q = p^k$ je mocnina prvočísla. Potom roj $AH_{\mathbb{F}_q}$ vypadá následovně:*

(i) komponenty souvislosti obsahující prvky (a,b) splňující $\phi_q(ab) = 1$ jsou vulkány hloubky $v_2(q-1)$,

(ii) komponenty souvislosti obsahující prvky (a,b) splňující $\phi_q(ab) = -1$ jsou vulkány hloubky $v_2(p+1) + v_2(k)$.

Důkaz. V případě komponent souvislosti grafu $AH_{\mathbb{F}_q}$ obsahujících prvky $\phi_q(ab)$ podle věty 5.2.3 víme, že binárních stromy zakořeněných v prvcích cyklů jsou isomorfní se stromy zakořeněnými v prvcích cyklů grafu $G_{\mathbb{F}_q}$. To znamená, že komponenty souvislosti tvoří vulkány a jejich hloubka je podle důsledku 5.3.5 rovna $v_2(q-1)$.

Poznámka. Podotkněme, že $v_2(q-1)$ lze vyjádřit pomocí $v_2(k)$ a $v_2(p \pm 1)$. Tzv. *Lifting The Exponent lemma* z olympiádní matematiky totiž říká, že pro k sudé platí:

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

Díky tomu zjišťujeme, že odhady, které byly předmětem důsledku, 3.2.5 JSOU/NEJSOU LOLOL těsné.

Konečně jsme splnili slib z kapitoly 3 - pomocí eliptických křivek plně charakterizovat, jaký tvar mají komponenty souvislosti v roji $AH_{\mathbb{F}_q}$. Pojďme toto propojení maximálně využít ve zkoumání dalších vlastností roje $AH_{\mathbb{F}_q}$.
– X = q-1 nebo q2-1 nebo tak –

Lemma 5.3.7. *Nechť jsou q mocnina prvočísla a liché číslo $k \mid q-1$. Potom počet bodů $P \in E(\mathbb{F}_q)$ takových, že k je nejmenší číslo $\ell \in \mathbb{N}$ splňující $[2^\ell]P = P$, je $\phi(k)$.*

Důkaz. Podle věty 5.2.5 platí $E(\mathbb{F}_q) \cong \mathbb{F}_q^\times$. Vzpomeňme si nyní na fakt, že multiplikativní grupa konečného tělesa je cyklická, tj. existuje *primitivní kořen* v $\mathbb{F}_q$, viz [?].
Toto tvrzení má jeden roztomilý důsledek, můžeme totiž pomocí ní dokázat novým způsobem jedno známé tvrzení.

Důsledek 5.3.8.

$$X = \sum_{k|X} \phi(k)$$

Tento vztah platí bezpodmínečně pro libovolné n:

$$n = \sum_{k|n} \phi(k).$$

Důkaz tohoto obecného tvrzení lze ? například pomocí tzv. Mobiovy inverzní formule [IR]. Blabla.

Podívejme se na nějaké $k \mid q-1$, podle věty 5.3.7 existuje $\phi(k)$ bodů, jejichž cykly jsou ?. Díky tomu můžeme vyjádřit přesně počet vulkánů obsahující tyto body.

Důsledek 5.3.9. *Nechť $k \mid X$ je liché číslo. Potom počet všech vulkánů $V \subseteq G_{\mathbb{F}_q}$ s délkou cyklu rovné k je:*

$$\frac{\phi(k)}{\mathrm{ord}_k(2)}.$$

Počet vulkánů v $E(\mathbb{F}_q)$ získáme součtem přes všechny možné vulkány s délkou cyklu $k \mid X$.s

Věta 5.3.10. *Platí:*

$$S(\mathbb{F}_q) = \sum_{\substack{k|X \\ 2\nmid k}} \frac{\phi(k)}{\mathrm{ord}_k(2)}.$$

Toto explicitní vyjádření můžeme využít na nalezení netriviálních odhadů na číslo $S(\mathbb{F}_q)$. Mnoho ohledně obecného chování řádu 2 modulo libovolné číslo k není známé, dokonce ani zda existuje nekonečně mnoho prvočísel, pro které 2 generuje grupu $\mathbb{Z}_p^\times$. Tato otázka je předmětem známé *Artinovy domněnky*. Budeme tedy používat poměrně slabé odhady.

Věta 5.3.11. *Platí řetězec nerovností:*

$$> S(\mathbb{F}_q) \geqslant$$

Důsledek 5.3.12.

$$> D(\mathbb{F}_q) \geqslant$$

Podívejme se, jak těsné tyto odhady vlastně jsou.

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
O	bod v nekonečnu křivky 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
$\langle G \rangle$	podgrupa generovaná množinou G
$E[n]$	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 $\mathbb{Q}(\theta)$
$\mathcal{O}_K$	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] De Feo, Luca: *Mathematics of Isogeny Based Cryptography*. Université de Versailles & Inria Saclay, 2017. Dostupné z: https://arxiv.org/abs/1711.04062.

[2] Griffin, Michael J., Ken Ono, Neelam Saikia a Wei-Lun Sai: *AGM and jellyfish swarms of elliptic curves*. 2021. Dostupné z:https://arxiv.org/abs/2110.12226.

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

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

[5] Pezlar, Zdeněk: *Isogenie v kryptografii*. Středoškolská odborná činnost. Brno: Masarykova univerzita, 2021. Dostupné z: https://socv2.nidv.cz/archiv43/getWork/hash/d97d25e1-9729-11eb-acaf-005056bd6e49.

[6] Ugolini, Simone: *Graphs associated with the map $x \mapsto x + x^{-1}$ in finite fields of characteristic two*. Theory and Applications of Finite Fields, Contemporary Mathematics, vol. 579, Amer. Math. Soc. 2011. Dostupné z: https://arxiv.org/abs/1107.4565.

[7] Ugolini, Simone: *Graphs associated with the map $x \mapsto x + x^{-1}$ in finite fields of characteristic three*. Journal of Number Theory, 133 (4). 2013. Dostupné z: https://arxiv.org/abs/1108.1763.

[8] Ugolini, Simone: *Graphs associated with the map $x \mapsto x + x^{-1}$ in finite fields of characteristic five*. Journal of Number Theory, 133 (4). 2013. Dostupné z: https://arxiv.org/abs/1110.0968.

[9] Ugolini, Simone: *Functional graphs of rational maps induced by endomorphisms of ordinary elliptic curves over finite fields*. Period. Math. Hung. 77(2). 2015. Dostupné z: https://arxiv.org/abs/1509.05365.