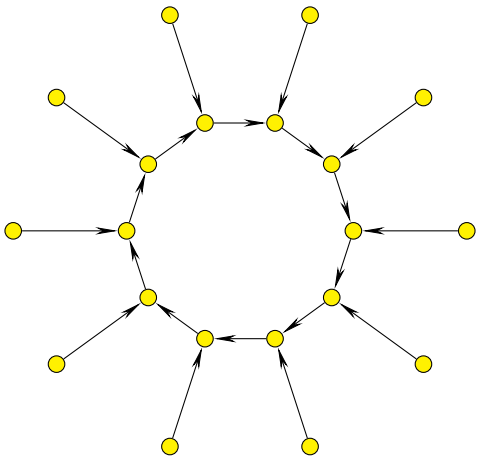
# STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST

**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**

**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

Mé díky patří všem lidem, kteří mi pomohli k dokončení práce. Zejména děkuji Vojtovi Suchánkovi za jeho ochotu vzít vedení práce a jeho nekončící trpělivost při opravách práce a konzultacích nápadů. Dále děkuji přátelům Richardu Blažkovi za podnětné debaty, které práci posunovaly, a dále Kubovi Devátovi, Martinu Dominikovi, Vojtovi Obořilovi, Danu Pravcovi a Vojtovi Stránskému za jejich pomoc při jazykových opravách. Konečně děkuji Verče za její neustálou podporu.

## Abstrakt

V práci podáváme první systematický úvod do posloupnosti průměrů nad konečnými tělesy. Nejprve se zaobíráme posloupnostmi průměrů nad reálnými čísly, jejichž studium se táhne až ke Karlu Gaussovi. V následující kapitole navazujeme na aktuální článek [1] a studujeme tři posloupnosti průměrů nad konečnými tělesy. Nejprve zkoumáme posloupnost danou aritmetickým a geometrickým průměrem a experimentálně ověřujeme odhady podané v [1]. Později v práci tuto posloupnost propojíme s teorií isogenií eliptických křivek. Hlavní přínos práce spočívá ve formulaci dvou nové posloupnosti průměrů a jejich následného studia. Zejména v závěru práce propojíme posloupnosti dané aritmetickým a harmonickým průměrem se singulární eliptickou křivkou, díky čemuž kompletně určíme strukturu grafů generovaných aritmetickým a harmonickým průměrem.

## Klíčová slova

Aritmeticko-geometrický průměr, Aritmeticko-harmonický průměr, Harmonicko-geometrický průměr, eliptické křivky, isogenie, grupa tříd ideálů, Vulkány, Medúzy

## Abstract

## Key words

Arithmetic-Geometric Mean, Arithmetic-Harmonic Mean, Harmonic-Geometric Mean, Elliptic Curves, Isogeny, Ideal Class Group, Volcanoes, Jellyfish

# Obsah

# Úvod

S aritmetickým a geometrickým průměrem se setkáváme už od základní školy. Pro libovolnou dvojici $(a, b)$ kladných čísel můžeme spočítat tuto dvojici průměrů jako:

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

Tato práce staví na jednoduché myšlence – na opakované aplikaci těchto průměrů. Přesněji definujme posloupnost $((a_n, b_n))_{n=0}^{\infty}$ s počátečním členem $(a_0, b_0) = (a, b)$ a pro každé nezáporné $n$ platí:

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

Velcí matematici jako Gauss, Legendre a Lagrange tuto tzv. *AG posloupností* studovali. Proč se však ti nejlepší z nejlepších zabývali tak zdánlivě jednoduchou posloupností? Carl Friedrich Gauss ukázal, že AG posloupnost vždy konverguje ke společné hodnotě. O co víc, posloupnost má kořeny hluboko v oblasti eliptických integrálů. O tomto propojení napsal:

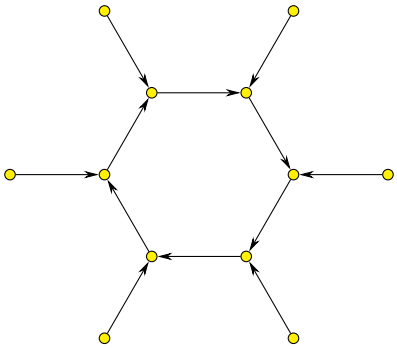
> *„This [...] will surely open up an entirely new field of analysis.“*

Přes následující století různí autoři studovali AG posloupnost a ukázali mj., že ji lze využít k rychlým výpočtů elementárních funkcí jako je $e^x$ či $\arcsin(x)$, ale i že je spojená s *modulárními funkcemi* a *modulárními formami*. Gauss měl proto pravdu.

V naší práci se na posloupnost díváme v jiném světle, konkrétně v oboru konečných těles. Jelikož pracujeme v konečném oboru je AG posloupnost vždy periodická, můžeme se proto zabývat orientovanými grafy generovanými AG posloupností. Všechny komponenty slabé souvislosti, které získáme, mají typický tvar cyklu, kde ke každému prvku cyklu je připojena jediná hrana. Takový graf nazveme *medúzou*.

Pokud se podíváme na medúzy obsažené v takových grafech pro různá $p$ tak zjistíme, že se jejich počty i velikosti chovají zdánlivě náhodně. Pomocí efektivní implementace v jazyku Sage poskytujeme rozsáhlé grafy hodnot spojených s AG posloupností. Dále experimentálně ověřujeme a navrhujeme odhady položené ve článku [1] a zavádíme nové struktury, které nám pomohou ve studiu posloupnosti.

Ve čtvrté kapitole osvětlíme sporadické chování AG posloupnosti nad konečnými tělesy. Ukážeme totiž, že posloupnost popisuje tzv. *vulkány* eliptických křivek nad konečnými



tělesy a že velikosti medúz jsou úzce spojené s grupou tříd ideálů jistých imaginárních kvadratických těles.

Hlavní přínos práce spadá do kapitol 3 a 5. Ve třetí kapitole definujeme předtím nestudovanou AH posloupnost nad konečným tělesem a teoreticky i experimentálně určíme jejich vlastnosti, zejména pozoruhodné jsou tvary grafů, které generuje. Krom medúz totiž grafy udávající AH posloupnost tvoří i hlubší vulkány a pro některá tělesa přesně určíme jejich hloubku. Vyvrcholení nastane v páté kapitole, kde ukážeme, že posloupnost můžeme popsat pomocí skalárních násobků na jisté singulární eliptické křivce. Díky tomuto propojení určíme plnou strukturu komponent souvislosti a poskytneme netriviální odhady na jejich počty.

# 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 $a \geqslant b$ 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:

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

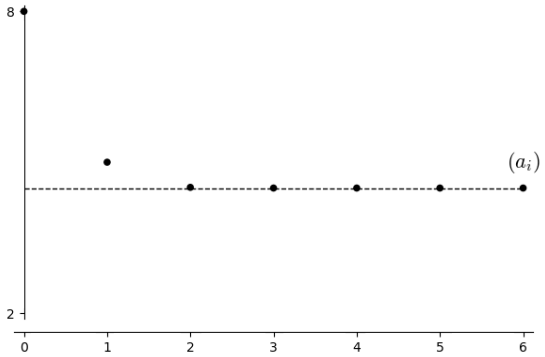
posloupnost $(b_n)_{n=0}^{\infty}$ je proto rostoucí (pokud $a_0 \neq b_0$, tak ostře rostoucí). Obdobně můžeme psát:

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

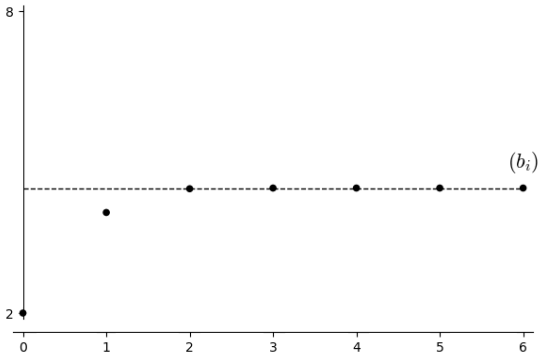
posloupnost $(a_n)_{n=0}^{\infty}$ je tedy naopak klesající. Protože aritmetický a geometrický průměr dvou čísel leží mezi nimi, jsou obě posloupnosti shora svírané prvkem $a$ a zdola $b$. Libovolná ohraničená monotónní posloupnost konverguje, víme tedy, že obě posloupnosti $(a_n)_{n=0}^{\infty}$ a $(b_n)_{n=0}^{\infty}$ 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 $b = 1$.

| $a_i$ | $b_i$ |
|---|---|
| 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* $\sigma$ 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 kvadraticky konvergující 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 složek $(a_n)_{n=0}^{\infty}$ a $(b_n)_{n=0}^{\infty}$ pro $n$ jdoucí do nekonečna existují a jsou si navzájem rovné. Navíc tyto složky konvergují ke společné limitě kvadraticky.*

*Důkaz.* Existenci limit složek 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 $\varepsilon_n$ 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* $x = \frac{1}{a}\sqrt{a^2 - b^2}$.[1]

Prozatím může vypadat, že *AG* posloupnost leží n 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 [4].

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:

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

shodují na 11 desetinných místech [2]. O trochu později dokázal obecný vztah, který tyto dva koncepty spojuje.

[1] Tato vlastnost nám přijde vhod v následující sekci.

**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:

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

Pomocí goniometrické jedničky $\sin^2\theta + \cos^2\theta = 1$ 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 v části *iv)* věty 1.1.6. 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 pro numerickou integraci:

$$\begin{aligned} I(8,2)\cdot\frac{2}{\pi} &= \int_0^{\pi/2} \frac{d\theta}{\sqrt{64\cos^2\theta + 4\sin^2\theta}} \cdot \frac{2}{\pi} \\ &\approx \frac{\pi}{12}\cdot\left(\frac{1}{\sqrt{64\cos^2 0 + 4\sin^2 0}} + \frac{4}{\sqrt{64\cos^2\pi/4 + 4\sin^2\pi/4}} + \frac{1}{\sqrt{64\cos^2\pi/2 + 4\sin^2\pi/2}}\right)\cdot\frac{2}{\pi} \\ &= \frac{1}{6}\cdot\left(\frac{1}{8} + \frac{4}{\sqrt{32+2}} + \frac{1}{2}\right) = 0.2184990567617\ldots. \end{aligned}$$

Převrácená hodnota tohoto čísla je:

$$\frac{\pi}{2}\cdot\frac{1}{I(8,2)} \approx 4.576678795876\ldots,$$

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

Obdobně můžeme ověřit:

$$\begin{aligned} I\left(\sqrt{2},1\right)\cdot\frac{2}{\pi} &= \int_0^{\pi/2}\frac{d\theta}{\sqrt{2\cos^2\theta+1\sin^2\theta}}\cdot\frac{2}{\pi} \\ &\approx \frac{\pi}{12}\cdot\left(\frac{1}{\sqrt{2\cos^2 0+\sin^2 0}}+\frac{4}{\sqrt{2\cos^2\pi/4+\sin^2\pi/4}}+\frac{1}{\sqrt{2\cos^2\pi/2+\sin^2\pi/2}}\right)\cdot\frac{2}{\pi} \\ &= \frac{1}{6}\left(\frac{1}{\sqrt{2}}+\frac{4}{\sqrt{1+1/2}}+1\right) = 0.8288488508162\ldots \end{aligned}$$

Převrácená hodnota tohoto čísla je $\approx 1.2064925939\cdots > \mathrm{AG}(\sqrt{2},1) = 1.198140234736\ldots$.

Eliptické integrály nedokážeme nijak „hezky“ vyjádřit, můžeme ale využít numerické techniky, abychom je aproximovali. Obecně Simpsonova metoda dává následující odhad.

**Věta 1.2.5.** *Buďte $a, b$ kladná čísla. Pak platí:*

$$\mathrm{AG}(a,b) \approx 6\left(\frac{1}{a}+\frac{4\sqrt{2}}{\sqrt{a^2+b^2}}+\frac{1}{b}\right)^{-1}.$$

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 výpočetních krocích. Jak Gauss sám pravil, k tomuto výsledku dojdeme:

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

Podrobnosti jsou k nalezení na [2, Ch. 2 Sec. 3]. 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 spolu s větou 1.2.2, že logaritmická funkce má spojení s eliptickými integrály:

**Věta 1.3.2.** *Ať $x < 1$. Platí:*

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

Zde onen chybový člen lze jednoduše odhadnout [2, Ch 1, Sec 3, Exc. 4]. Známe-li hodnotu $\pi$, tak nám kvadraticky konvergující *AG* posloupnost umožní spočítat s velkou přesností logaritmus číslo $4/x$ pro dostatečně malé $x$ (nebo vhodně velký argument logaritmu).

Chtěli bychom využít rychlý algoritmus pro logaritmus pro počítání ostatních elementárních funkcí. K tomu zmíníme, ale pouze okrajově, že Gauss, Legendre a další nestudovali *AG* posloupnost pouze nad oborem reálných čísel, ale dokonce komplexních. V takovém oboru není triviální volit správnou odmocninu z čísla, v kladných číslech jsme jednoduše brali tu kladnou. Lze ukázat [3], že pouze některé, tzv. *správné*, volby vyústí v netriviální konvergence a právě ty nás zajímají. Dokážeme pak počítat efektivně logaritmus komplexních čísel.

Pomocí algoritmu pro počítání logaritmus komplexních čísel můžeme vyjádřit inverzní funkce ke klasických goniometrickým funkcím. Dá se totiž jednoduše ukázat [2, Ch. 7], že platí vztahy:

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

Po spočítání inverze k těmto funkcím pak dokážeme pomocí *AG* posloupnosti počítat kvadraticky funkce jako například sinus či cosinus. Díky *AG* posloupnost též dokážeme počítat v kvadratickém čase čísla jako $\pi$ či $e$. V prvním případě nám stačí spočítat číslo $4\tan(1) = \pi$ pomocí komplexního *AG*. Číslo $e$ spočítáme jako kořen rovnice $\ln(x) - 1$, což dokážeme efektivně s pomocí Newtonovy metody a algoritmu pro $\ln(x)$ pomocí *AG* posloupnosti.

## 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 $\mathrm{HG}(a, b)$, resp. $\mathrm{AH}(a, b)$.

**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 $\mathrm{AG}(8, 2)$ a $\mathrm{HG}(8, 2)$:

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

Vzhledem k tomu, že $\mathrm{AG}(a, a)\cdot\mathrm{HG}(a, a) = a^2$, vypadá to, že by mohl platit vztah $\mathrm{AG}(a, b)\cdot\mathrm{HG}(a, b) = ab$. To opravdu platí - všimněme si totiž, že můžeme psát:

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

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

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

**Věta 1.4.3.** *Pro libovolná $a, b \in \mathbb{R}^+$ platí:*

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

Nyní přichází čas pro *AH* posloupnost. Má něco společného s předchozími dvěma posloupnostmi? Podívejme se, jak se posloupnost chová pro počáteční 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 $\mathrm{AH}(a,b)$, ta musí splňovat $\mathrm{AH}(a,b)^2 = ab$, 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.** *Pro libovolná $a, b \in \mathbb{R}^+$ platí:*

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

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 [2].

Na konec této sekce ještě zmiňme, že se nemusíme zastavit pouze na dvou průměrech. Zobecněná *AGH* posloupnost pro tři proměnné byla zběžně studovaná v [5] a uvažovaná jejich spojení s tzv. *elipsoidálními plošnými integrály*. 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 v kapitole 4.

## 2.1 Základní poznatky

Hned ze začátku narážíme na první úskalí při adaptaci posloupnosti. Ne vždy totiž je součin prvků $a, b \in \mathbb{F}_q$ čtvercem v $\mathbb{F}_q$, tj. můžeme totiž narazit na případ, kdy nemůže psát další prvek. Navíc i pokud je $ab$ čtverec, v $\mathbb{F}_q$ z něj existují z dvě odmocniny. Jak rozlišíme tu správnou odmocninu? Kvůli tomuto problému se zaměříme na tělesa $\mathbb{F}_q$ s $q = p^k \equiv -1 \pmod 4$, pak v $\mathbb{F}_q$ neexistuje odmocnina z $-1$. Díky tomu, že pro nenulové $x$ je právě jeden z prvků $x, -x$ čtverec, 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. Volíme tedy odmocninu kladnou, jelikož následující prvek je opět kladným číslem.

**Definice 2.1.1.** Definujme „zobecněný Legendreho symbol“ $\phi_q$ 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 $\mathbb{F}_q$ [7, Ch. 8.], tj. platí $\phi_q(a)\phi_q(b) = \phi_q(ab)$ pro $a, b \in \mathbb{F}_q$. Pro každé $x \in \mathbb{F}_q$ platí $\phi_q(x) = x^{\frac{q-1}{2}}$. Každý prvek $\mathbb{F}_q$ je totiž kořenem polynomu $x^q - x = x\left(x^{\frac{q-1}{2}} - 1\right)\left(x^{\frac{q-1}{2}} + 1\right) \in \mathbb{F}_q[x]$. Pro každý z $\frac{q-1}{2}$ nenulových čtverců $y = a^2 \in \mathbb{F}_q$ je číslo $y$ kořenem polynomu $x^{\frac{q-1}{2}} - 1 \in \mathbb{F}_q[x]$. Konečné těleso $\mathbb{F}_q$ je oborem

integrity, proto má polynom $x^{\frac{q-1}{2}} - 1 \in \mathbb{F}_q[x]$ právě $\frac{q-1}{2}$ kořenů - všechny nenulové čtverce v $\mathbb{F}_q$. To znamená, že kořeny polynomu $x^{\frac{q-1}{2}} + 1$ jsou právě nečtverce v $\mathbb{F}_q$.

**Definice 2.1.2.** Ať $a, b$ jsou různé prvky $\mathbb{F}_q^\times$ splňující $\phi_q(ab) = 1$. Pak definujeme $\mathrm{AG}_{\mathbb{F}_q}(a, b)$ 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 $\phi_q(a_{n+1}b_{n+1}) = 1$.

Vysvětleme, proč je naše posloupnost je dobře definovaná. Nejprve si všimněme, že $a_n$ a tedy ani $b_n$ je vždy nenulové. Pokud by totiž bylo $a_{n+1} = 0$, tak musí být $a_n + b_n = 0$ a tedy by platilo $\phi_q(a_n b_n) = \phi_q(-a_n^2) = -1$, jelikož předpokládáme $\phi_q(-1) = -1$. To je však spor s konstrukcí posloupnosti.

Vždy si též můžeme zvolit hodnotu $b_n$ tak, aby $b_{n+1}$ bylo definované. Je-li $\phi_q(a_n b_n) = 1$, tak jedna z navzájem opačných odmocnin z $a_n b_n$ je v $\mathbb{F}_q$ nenulovým čtvercem, opět díky předpokladu $\phi_q(-1) = -1$. Můžeme pak zvolit $b_{n+1}$ takové, že platí $\phi_q(a_{n+1}b_{n+1}) = 1$.

Sjednocení všech posloupností $\mathrm{AG}_{\mathbb{F}_q}(a, b)$ budeme reprezentovat jako orientovaný graf.

**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 $(c, d) = (a_1, b_1)$, kde $(a_0, b_0) = (a, b)$.

**Úmluva.** U orientovaných grafů rozlišujeme komponenty *slabé* a *silné souvislosti*. My se v textu budeme zabývat pouze komponentami slabé souvislosti. Pro stručnost a lepší čitelnost budeme tyto komponenty nazývat jednoduše komponenty souvislosti.

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

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

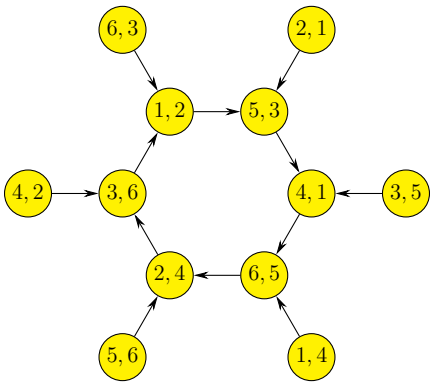
vrchol $(1, 2)$ je proto členem cyklu délky 6. Pokud máme v grafu orientovanou hranu $(a, b) \mapsto (c, d)$, tak jistě vede hrana i mezi $(b, a)$ a $(c, d)$, proto například vede hrana z $(2, 1)$ do $(5, 3)$ a podobně. Výpočtem lze ověřit, že prvky mimo cyklus - $(2, 1)$, $(3, 5)$ a podobně, již předchůdce nemají. Toto je jediná komponenta souvislosti grafu $\mathrm{AG}_{\mathbb{F}_7}$.

Podívejme se nyní na graf $\mathrm{AG}_{\mathbb{F}_{11}}$. Zvolme dvojice $(1, 3)$, $(1, 5)$ a $(10, 6)$ a pišme jejich posloupnosti:

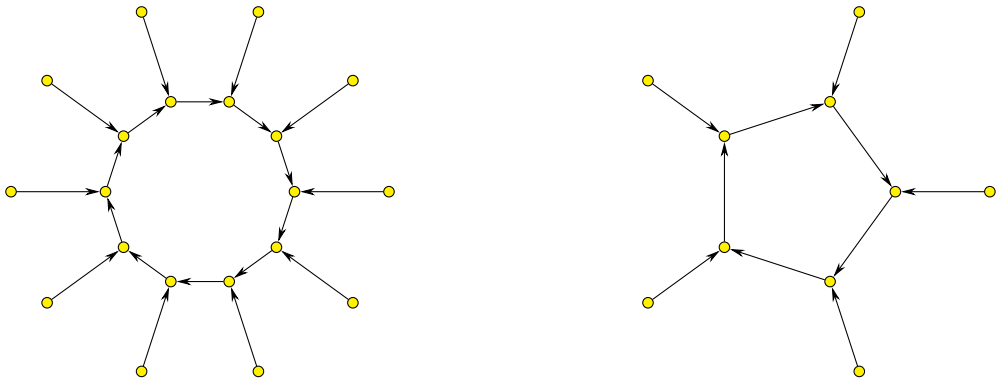
$$\begin{aligned}(1,3) \mapsto (2,6) \mapsto (4,1) \mapsto (8,2) \mapsto (5,4) \mapsto (10,8) \mapsto (9,5) \mapsto (7,10) \mapsto (3,9) \mapsto (6,7) \mapsto (1,3),\\ (1,5) \mapsto (3,4) \mapsto (9,1) \mapsto (5,3) \mapsto (4,9) \mapsto (1,5),\\ (10,6) \mapsto (8,7) \mapsto (2,10) \mapsto (6,8) \mapsto (7,2) \mapsto (10,6).\end{aligned}$$

Opět platí, že v každém z těchto případů mají všechny prvky cyklu právě jednoho předchůdce mimo cyklus. Tito předchůdci jsou už listy. Tyto tři komponenty souvislosti

tvoří celý graf $\mathrm{AG}_{\mathbb{F}_{11}}$. Všimněme si, že pokud vezmeme druhou posloupnost a vynásobíme každý prvek $-1$, tj. $1 \longmapsto 10, 2 \longmapsto 9$, tak získáme přesně posloupnost třetí. Komponenty souvislosti obsahující prvky $(1, 5)$ a $(10, 6)$ jsou proto isomorfní.




Obrázek 2.1: Roj $\mathrm{AG}_{\mathbb{F}_7}$.



Obrázek 2.2: Neisomorfní komponenty souvislosti roje $\mathrm{AG}_{\mathbb{F}_{11}}$.

Nyní se podíváme na vlastnosti grafu $\mathrm{AG}_{\mathbb{F}_q}$. Začněme zlehka, konkrétně z kolika vrcholů a hran je vlastně náš graf tvořen.

**Věta 2.1.5.** *Graf* $\mathrm{AG}_{\mathbb{F}_q}$ *čítá* $(q-1)(q-3)/2$ *vrcholů a stejný počet hran.*

*Důkaz.* Uspořádaná dvojice $(a, b)$ náleží do $\mathrm{AG}_{\mathbb{F}_q}$, 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 jediná hrana. 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 navíc pro každý vrchol $W \in H$ existuje unikátní předchůdce[2] mimo cyklus, který sám nemá předchůdce a žádného jiného následníka.

Ukážeme si, že komponenty souvislosti grafu $\mathrm{AG}_{\mathbb{F}_q}$ jsou medúzami. Nejprve si charakterizujme, které vrcholy mají v $\mathrm{AG}_{\mathbb{F}_q}$ předchůdce.

**Lemma 2.1.7.** *Vrchol $(a, b) \in \mathrm{AG}_{\mathbb{F}_q}$ má předchůdce, právě pokud platí $\phi_q(a^2 - b^2) = 1$.*

*Důkaz.* Nejprve předpokládejme, že vrchol $(a, b) \in \mathrm{AG}_{\mathbb{F}_q}$ 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:

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

□

**Věta 2.1.8.** *Roj $\mathrm{AG}_{\mathbb{F}_q}$ je tvořen z několika medúz.*

*Důkaz.* Graf má konečný počet vrcholů, proto každý nekonečný sled $(u, v) \longmapsto (u_1, v_1) \longmapsto \ldots$ obsahuje cyklus délky větší než 1.

Dejme tomu, že $(c, d)$ je členem nějakého cyklu a jeho předchůdce v cyklu je $(C, D)$. Platí vztahy $C + D = 2c$ 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 předchůdci vrcholu $(c, d)$ v $\mathrm{AG}_{\mathbb{F}_q}$ jsou proto $(C, D)$ a $(D, C)$.

Jedno z čísel $\phi_q(C^2 - D^2)$ a $\phi_q(D^2 - C^2)$ je kvůli $\phi_q(-1) = -1$ rovno 1 a to druhé $-1$, podle lemmatu 2.1.7 proto má právě jeden z vrcholů $(C, D)$ a $(D, C)$ předchůdce, ten je jistě taky součástí cyklu. Každý vrchol, který není členem cyklu, proto nemá předchůdce a každá komponenta souvislosti $\mathrm{AG}_{\mathbb{F}_q}$ je proto medúzou. □

[2] Označme $G = (V, E)$. Předchůdce vrcholu $X \in V$ je libovolný vrchol $W \in V$ splňující $(W, X) \in E$. V tomto případě je $X$ následníkem $W$.

**Příklad 2.1.9.** Délky cyklů medúz se mohou přes různá prvočísla drasticky lišit. Z příkladu 2.1.4 víme, že pro $p = 7$ nalezneme v grafu $\mathrm{AG}_{\mathbb{F}_p}$ medúzu s délkou cyklu rovnou 6 a pro $p = 11$ jsou délky cyklů rovné po řadě 5 a 10. Například v grafu $\mathrm{AG}_{\mathbb{F}_{67}}$ máme mimo jiné medúzy s délkami cyklů po řadě 9 a 198.

$$(1,17) \mapsto (9,33) \mapsto (21,37) \mapsto (29,24) \mapsto \cdots \mapsto (65,15) \mapsto (40,29) \mapsto (1,17),$$
$$(1,9) \mapsto (5,33) \mapsto (4,22) \mapsto (13,50) \mapsto \cdots \mapsto (21,26) \mapsto (57,12) \mapsto (1,9).$$

V grafu $\mathrm{AG}_{\mathbb{F}_{79}}$ jsou jediné přípustné délky cyklů velké, po řadě 205 a 410.

Pojďme si 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 medúzy v $\mathrm{AG}_{\mathbb{F}_{11}}$ obsahující vrcholy $(1,5)$ a $(10,6) = (-1,-5)$ z příkladu 2.1.4.

**Definice 2.1.10.** Ať $M \subseteq \mathrm{AG}_{\mathbb{F}_q}$ je medúza a v ní leží vrchol $(a,b)$. Potom nazveme libovolnou medúzu obsahující vrchol $(ka,kb)$ pro $k \in \mathbb{F}_q$ *přítelem* medúzy $M$.

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

**Věta 2.1.11.** *Ať $(a,b) \in \mathrm{AG}_{\mathbb{F}_q}$ leží v cyklu medúzy $M$ a $(a_i,b_i) \in \mathrm{AG}_{\mathbb{F}_q}(a,b)$ je první vrchol takový, že existuje $k \in \mathbb{F}_q$ splňující $(a_i,b_i) = (ka,kb)$. Pak počet přátel medúzy $M$ je právě:*

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

*Důkaz.* Je zřejmé, že všechny ostatní prvky cyklu $(a_i,b_i)$ splňující $a_i/b_i = a/b$ jsou ve tvaru $(a_i,b_i) = (k^x a_i, k^x b_i)$. Označme $O_k$ podgrupu grupy $\mathbb{F}_q^\times$ generovanou $k$. Pokud přenásobíme $M$ libovolným prvkem z $O_k$, získáme opět $M$.

Přesněji, máme danou akci grup $\mathbb{F}_q \times \mathrm{AG}_{\mathbb{F}_q} \longrightarrow \mathrm{AG}_{\mathbb{F}_q}$, která pro $k \in \mathbb{F}_q$ zobrazí prvek $(a,b)$ na $(ka,kb)$. Podgrupa $O_k$ 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 jejího přítele, a faktorgrupou $\mathbb{F}_q/O_k$, která má $\frac{q-1}{\mathrm{ord}_q(k)}$ prvků. □

Je-li jediné vyhovující $k$ rovno 1, tak medúza má $q-1$ přátel a pro $(a_i,b_i) \in \mathrm{AG}_{\mathbb{F}_q}(a,b)$ platí $a_i/b_i = a_j/b_j$ právě pokud $(a_i,b_i) = (a_j,b_j)$. Pro taxonomické účely se nám hodí tyto spřátelené medúzy uskupit dohromady, zaveďme proto pojem *hejno*.

**Definice 2.1.12.** 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 roji, případně počet hejn v roji. Tyto hodnoty studovali autoři původního článku [1] a pomocí eliptických křivek budeme moci na tato čísla uvést odhady.

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

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 2.1.9, že délky cyklů se přes prvočísla mohou hodně lišit, tak nás nepřekvapí, že i celkový počet medúz se chová poměrně různorodě. Pro představu uveďme malou tabulku pro prvočísla $p < 100$.

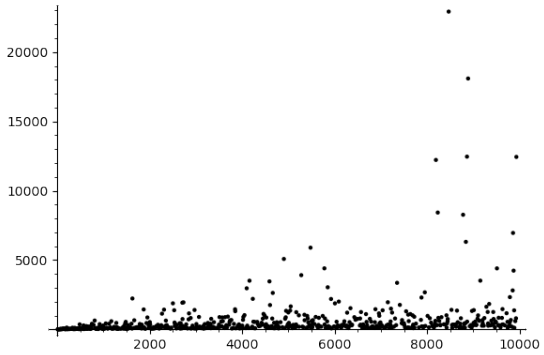
| $p$ | $d(\mathbb{F}_p)$ | $s(\mathbb{F}_p)$ |
|---|---|---|
| 3 | 0 | 0 |
| 7 | 1 | 1 |
| 11 | 3 | 2 |
| 19 | 8 | 2 |
| 23 | 5 | 3 |
| 31 | 10 | 3 |
| 43 | 7 | 4 |
| 47 | 4 | 3 |
| 59 | 7 | 4 |
| 67 | 30 | 6 |
| 71 | 25 | 5 |
| 79 | 18 | 7 |
| 83 | 6 | 4 |

Obrázek 2.3: Tabulka hodnot $d(\mathbb{F}_p)$ a $s(\mathbb{F}_p)$ pro $p < 100$

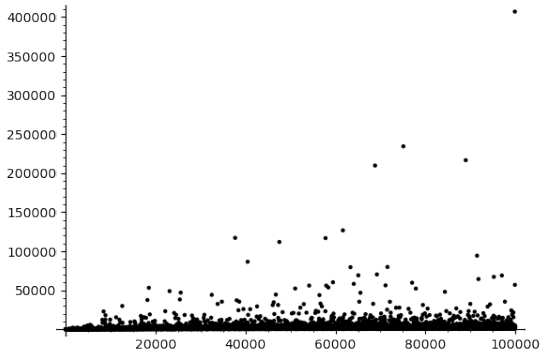
Tato náhodná povaha $d(\mathbb{F}_q)$ se nese i dál, na obrázcích 2.4 a 2.5 vidíme jednotlivé hodnoty pro prvočísla $p < 10^4$ a $p < 10^5$.

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, žádné zjevné trendy se nevyskytují.

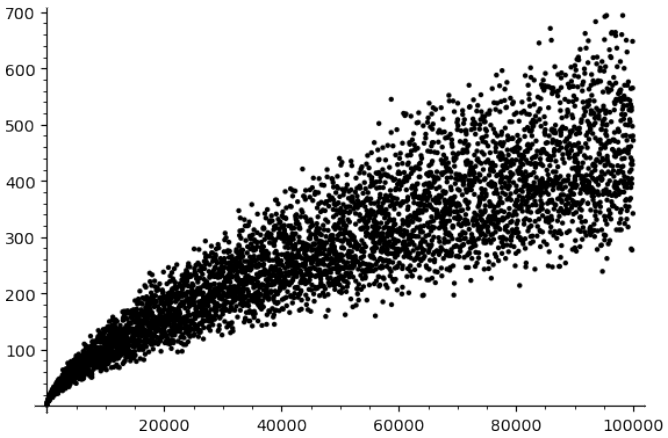
Číslo $s(\mathbb{F}_p)$ se chová mnohem rozumněji. Případy, kdy $d(\mathbb{F}_p)$ je velké, jsou právě ty, kdy jsou hejna malá, a proto mezi hodnotami $s(\mathbb{F}_q)$ nenacházíme odlehlé hodnoty. Na obrázku 2.6 vidíme chování $s(\mathbb{F}_p)$ pro $p < 10^5$.




Obrázek 2.4: Číslo $d(\mathbb{F}_p)$ pro $p < 10^4$




Obrázek 2.5: Číslo $d(\mathbb{F}_p)$ pro $p < 10^5$




Obrázek 2.6: Číslo $s(\mathbb{F}_p)$ pro $p < 10^5$

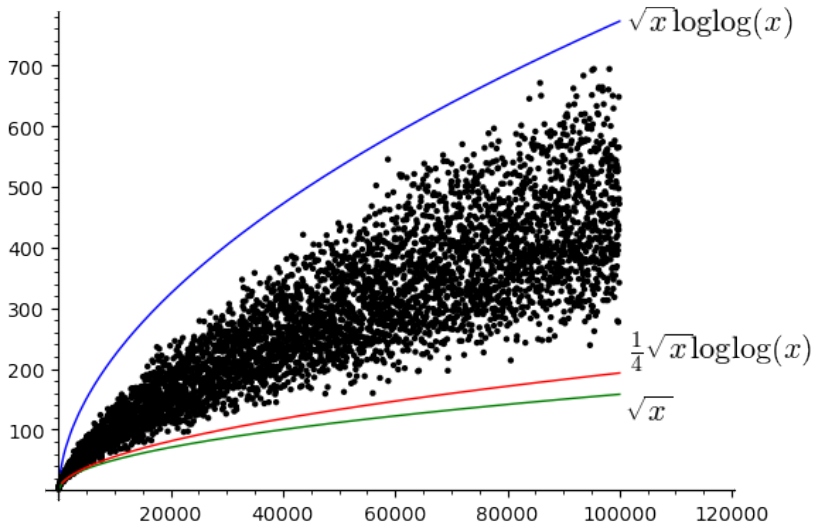
Autoři článku [1] propojili *AG* posloupnost s teorií eliptických křivek, těm se budeme věnovat v kapitole 4. Pomocí této teorie dokázali netriviální dolní odhad na číslo $d(\mathbb{F}_q)$, resp. jejich postup ohraničí dokonce číslo $s(\mathbb{F}_q)$. Hlavním výsledkem jejich článku je tvrzení, že pro 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 $d(\mathbb{F}_q) \geqslant O(\sqrt{q}\log\log q)$. Tento odhad není nijak podložen. Pojďme se těmto odhadům věnovat.

Nejprve, jak optimální opravdu je odhad $s(\mathbb{F}_q)$ (resp. $d(\mathbb{F}_q)$)? Porovnejme číslo $s(\mathbb{F}_q)$ s funkcí $\sqrt{q}$:

Těsnější odhad získáme, pokud uvážíme funkce $f \in O(\sqrt{q}\log\log q)$, podle návrhu v [1]. I když se autoři horním odhadům na číslo $s(\mathbb{F}_q)$ nevěnovali, zdánlivě jej můžeme též odhadnout funkcí tvaru $c\sqrt{q}\log\log q$.



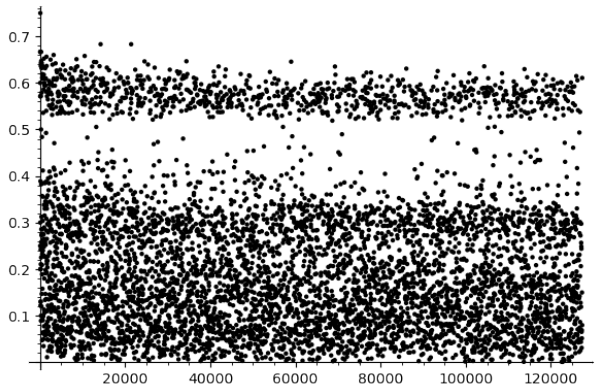

Obrázek 2.7: Porovnání $s(\mathbb{F}_p)$ s funkcemi $\sqrt{p}$, $\sqrt{p}\log\log p$ a $\frac{1}{4}\sqrt{p}\log\log p$.

**Domněnka 2.2.2.** *Existuje $c \in \mathbb{R}^+$ takové, že pro dostatečně velké $q$ platí:*

$$c\sqrt{q}\log\log q \geqslant s(\mathbb{F}_q) \geqslant \frac{1}{4}\sqrt{q}\log\log q.$$

Spočítali jsme hodnoty $d(\mathbb{F}_q)$ a $s(\mathbb{F}_q)$ pro vybrané hodnoty $p < 10^6$. Pro tato prvočísla platí $s(\mathbb{F}_p) > \frac{1}{4}\sqrt{p}\log\log p$, pro $p = 350431$ platí $s(\mathbb{F}_p) = 1571 > \sqrt{p}\log\log p \approx 1507.6$.

Další otázkou může být, jak spolu souvisí čísla $d(\mathbb{F}_q)$ a $s(\mathbb{F}_q)$. Zjevně platí nerovnost $s(\mathbb{F}_q) \geqslant d(\mathbb{F}_q)$. Co lepšího můžeme říci? Pokud se podíváme, jak se plošně chová číslo $\frac{s(\mathbb{F}_q)}{d(\mathbb{F}_q)}$ získáme velmi zajímavý graf, viz obrázek 2.8. Vidíme, že pro $p > 7$ se číslo $\frac{s(\mathbb{F}_q)}{d(\mathbb{F}_q)}$ drží pod hodnotou 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 $d(\mathbb{F}_q)$.




Obrázek 2.8: Hodnoty $s(\mathbb{F}_p)/d(\mathbb{F}_p)$ pro $p < 1.2 \cdot 10^5$

## 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 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* $\mathrm{HG}_{\mathbb{F}_q} = (V, E)$ 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 $(c, d) = (a_1, b_1)$, kde $(a_0, b_0) = (a, b)$.

**Příklad 2.3.3.** Podívejme se na roje $HG_{\mathbb{F}_p}$ pro $p = 7$ a 11. Pro $p = 7$ je jediná komponenta medúza, jejíž cyklus je následující:

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

V roji $\mathrm{HG}_{\mathbb{F}_{11}}$ zvolme dvojice $(3, 1)$ a $(5, 1)$ a pišme jejich posloupnosti:

$$\begin{aligned}(3,1) \mapsto (7,6) \mapsto (9,3) \mapsto (10,7) \mapsto (5,9) \mapsto (8,10) \mapsto (4,5) \mapsto (2,8) \mapsto (1,4) \mapsto (6,2) \mapsto (3,1),\\ (5,1) \mapsto (9,4) \mapsto (3,5) \mapsto (1,9) \mapsto (4,3) \mapsto (5,1),\\ (6,10) \mapsto (2,7) \mapsto (8,6) \mapsto (10,2) \mapsto (7,8) \mapsto (6,10).\end{aligned}$$

Tyto tři cykly jsou cykly všech medúz v $\mathrm{HG}_{\mathbb{F}_q}$. Druhé dvě z těchto medúz jsou přátelé, stejně jako v případě roje $\mathrm{AG}_{\mathbb{F}_{11}}$.

Z příkladu 2.3.3 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 2.3.4.** *Graf* $\mathrm{HG}_{\mathbb{F}_q}$ *čítá* $(q-1)(q-3)/2$ *vrcholů a stejný počet hran.*

*Důkaz.* Analogický k důkazu věty 2.1.5. □

**Lemma 2.3.5.** *Vrchol* $(a,b) \in \mathrm{HG}_{\mathbb{F}_q}$ *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:

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

□

**Důsledek 2.3.6.** *Graf* $\mathrm{HG}_{\mathbb{F}_q}$ *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 $\mathrm{AG}_{\mathbb{F}_q}$ a $\mathrm{HG}_{\mathbb{F}_q}$ díky lemmatům 2.1.7 a 2.3.5. To a nebo věta 1.4.3 nám napovídají, jaké bude konkrétní propojení těchto dvou grafů.

**Věta 2.3.7.** *Platí isomorfismus grafů* $\mathrm{AG}_{\mathbb{F}_q} \cong \mathrm{HG}_{\mathbb{F}_q}$.

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

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

poté v grafu $\mathrm{HG}_{\mathbb{F}_q}$ 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 $\psi$ se zjevně bijekce mezi $\mathrm{AG}_{\mathbb{F}_q}$ a $\mathrm{HG}_{\mathbb{F}_q}$, definuje mezi grafy isomorfismus. □

# Kapitola 3

# AH posloupnost

Zatím jsme pracovali s dvěma dvojicemi průměrů z trojice – aritmetický, geometrický a harmonický. V této kapitole se proto podíváme i na tu poslední – aritmetický a harmonický průměr. 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

Tentokrát již ze začátku nebudeme pracovat pouze nad konečným tělesem, ale i s bodem v nekonečnu.

**Definice 3.1.1.** Ať $K$ je těleso. Pak definujeme *projektivní přímku* $\mathbb{P}^1(K)$ jako množinu tříd nenulových vektorů $(a_1 : a_2) \in K^2$ s relací ekvivalence $(a : b) \sim (c : d)$, právě pokud existuje $\lambda \in K$ splňující $(a, b) = \lambda(c, d)$.

Pro třídu $(a : b)$ pro $b \neq 0$ zvolíme reprezentanta $\left(\frac{a}{b} : 0\right)$ a identifikujeme třídu $(a : b)$ s číslem $\frac{a}{b} \in \mathbb{F}_q$. Jediná třída, která takto není pokryta, je třída $(1 : 0)$, tu ztotožníme s *bodem v nekonečnu* $\infty$. 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) $\infty \times \infty = \infty$.

Pomocí projektivní přímky můžeme v plném rozsahu definovat a studovat $AH$ posloupnost nad konečným tělesem.

**Definice 3.1.2.** Ať $a, b \in \mathbb{F}_q^\times$ jsou různé. Pak definujeme $\mathrm{AH}_{\mathbb{F}_q}(a,b)$ 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 následník bodu $(a, -a)$ pro $a \in \mathbb{F}_q$ je $(0, \infty)$ a následník $(0, \infty)$ je $(\infty, 0)$. Bod $(\infty, 0)$ je následník sama sebe.

Pokud $\phi_q(2) \neq 1$, tak se každý *afinní*[3] bod zobrazí opět na afinní bod. Připusťme, že pro nějaká $(a_0, b_0)$ a $n$ nezáporné platí $1/a_{n+1} + 1/b_{n+1} = 0$, pak i $a_{n+1} + b_{n+1} = 0$. Musí 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, mohou některé posloupnosti $\mathrm{AH}_{\mathbb{F}_q}(a,b)$ obsahovat body v nekonečny a musíme již pracovat s projektivní přímkou. Budeme vždy pracovat pouze s posloupnostmi, které obsahují alespoň jeden afinní prvek. Nejprve podíváme na tělesa $\mathbb{F}_q$ s $q \equiv \pm 3 \pmod 8$.

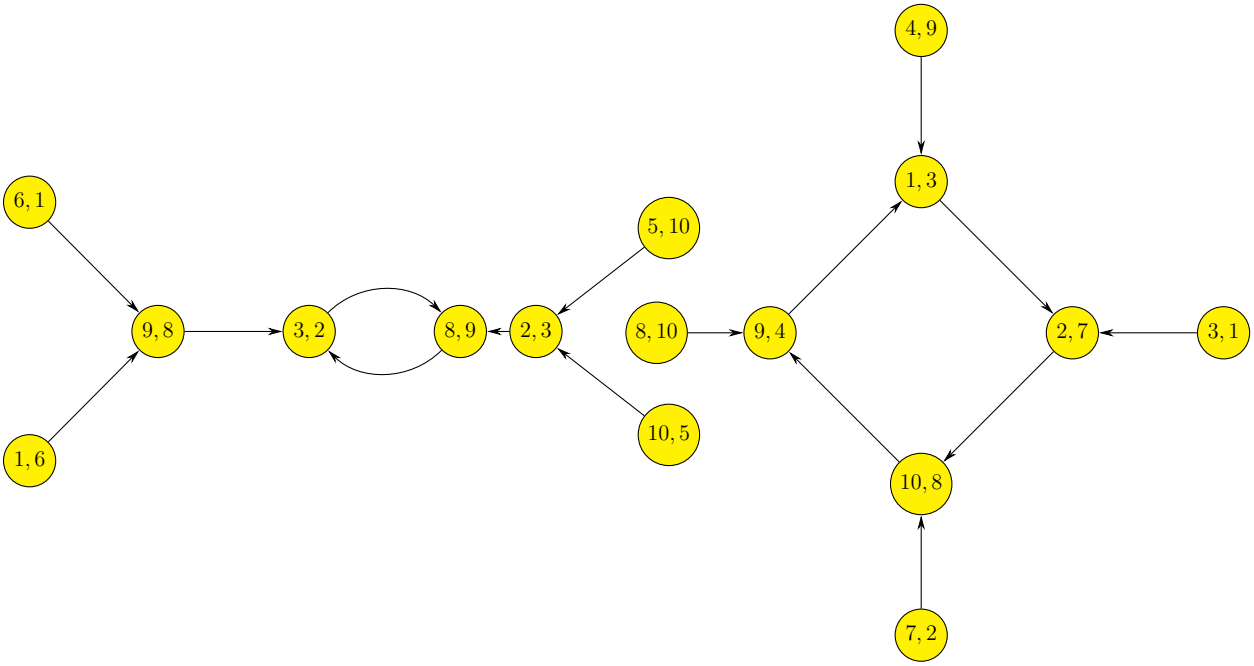
**Definice 3.1.3.** Definujme *roj* $\mathrm{AH}_{\mathbb{F}_q} = (V, E)$ jako orientovaný graf, kde $(a, b) \in V$ pokud $a, b \in \mathbb{F}_q$, nebo $\{a, b\} = \{0, \infty\}$. Pro libovolná $a, b, c, d \in \mathbb{P}^1(\mathbb{F}_q)$ platí $\Big((a, b), (c, d)\Big) \in E$, právě pokud $(c, d) = (a_1, b_1)$, kde $(a_0, b_0) = (a, b)$.

**Úmluva.** Každý afinní bod má v grafu zjevně nejvýše dva předchůdce. Toto je zdárně porušeno pro body v nekonečnu, kde bod $(0, \infty)$ má předchůdců hned $q-1$ – body $(a, -a)$, viz příklad 3.1.4. Čistě z důvodu elegance, která se prokáže v kapitole 5, budeme uvažovat $\frac{q-1}{2}$ bodů $(0, \infty)$ a $(\infty, 0)$, každý příslušící jedné dvojici bodů $(a, -a)$ a $(-a, a)$. Domluvíme se tedy, že pro $a, b \in \mathbb{F}_q^\times$ splňující $a \neq \pm b$ body $(a, -a)$ a $(b, -b)$ neleží ve stejné komponentě souvislosti grafu $\mathrm{AH}_{\mathbb{F}_q}$. Naopak uvažujme, že body $(a, -a)$ a $(-a, a)$ ve stejné komponentě souvislosti leží.

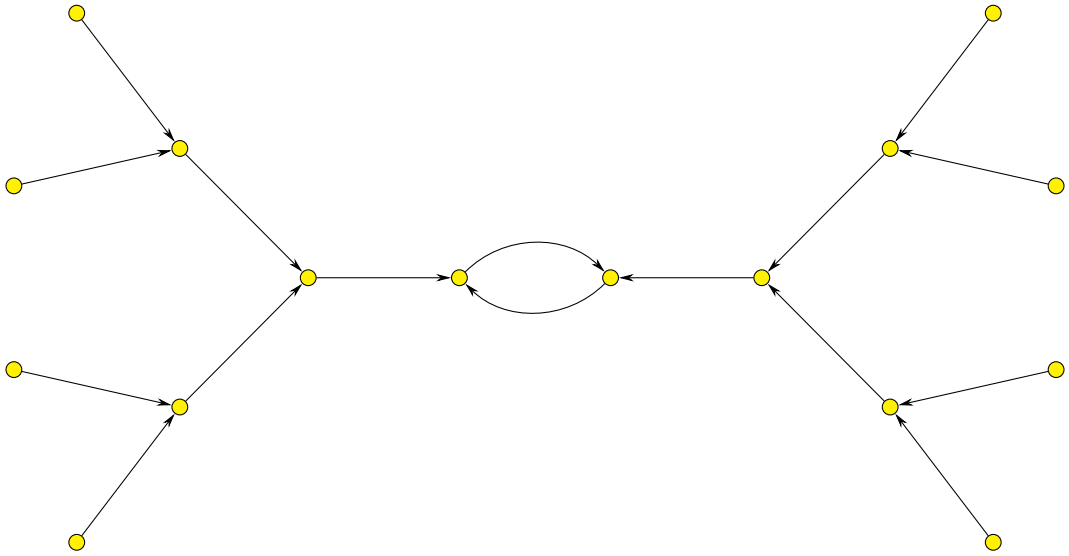
**Příklad 3.1.4.** Podívejme se na graf $\mathrm{AH}_{\mathbb{F}_{11}}$ a dva prvky, $(1, 3)$ a $(3, 2)$. Komponenta souvislosti obsahující $(1, 3)$ je medúza, komponenta obsahující $(3, 2)$ je tvořena z cyklu, ke každému prvku cyklu je připojen vyvážený binární strom hloubky 2.

Dále se podívejme na graf $\mathrm{AH}_{\mathbb{F}_{23}}$. Zde pro nás jsou zajímavé dvě komponenty souvislosti, konkrétně ty obsahující body $(1, 5)$ a $(1, -1) \in \mathrm{AH}_{\mathbb{F}_q}$. Ty vypadají následovně.

[3] Bod $(a, b) \in \mathrm{AH}_{\mathbb{F}_q}$ takový, že $a, b \in \mathbb{F}_q$, nazveme afinním.

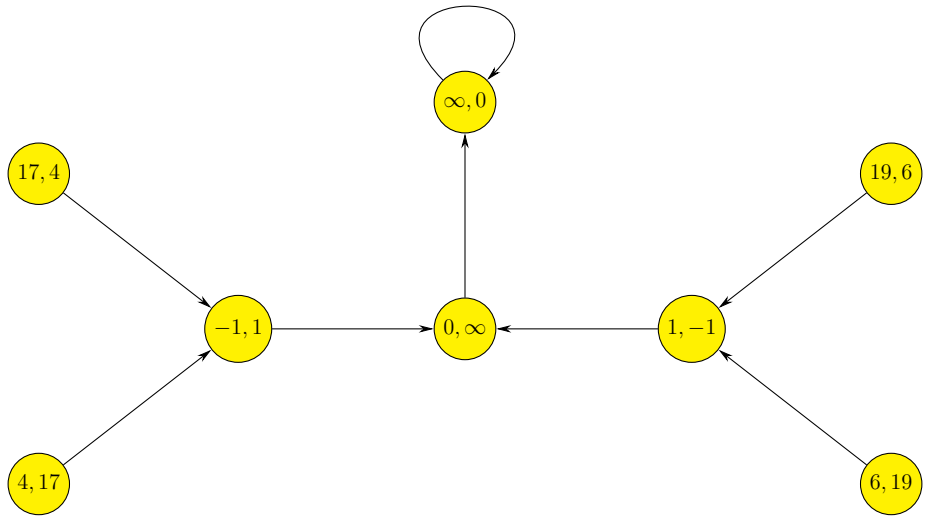



Obrázek 3.1: Komponenty souvislosti grafu $\mathrm{AH}_{\mathbb{F}_{11}}$.



Obrázek 3.2: Komponenta roje $\mathrm{AH}_{\mathbb{F}_{23}}$ obsahující $(1, 5)$.

Na příkladu 3.1.4 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 [10].




Obrázek 3.3: Komponenta roje $\mathrm{AH}_{\mathbb{F}_{23}}$ obsahující $(1, -1)$.

**Definice 3.1.5.** Souvislý orientovaný graf $V$ nazveme *vulkánem hloubky* $k$, pokud lze jeho vrcholy rozdělit do $k+1$ disjunktních množin $V_0, \ldots, V_k$ a:

(i) Podgraf grafu $V$ obsahující $V_0$ 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 posloupnostmi, 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.

**Věta 3.1.6.** *Buď $q = p^k$ mocnina prvočísla. Pak:*

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

*(ii) počet afinních vrcholů $(a, b) \in \mathrm{AH}_{\mathbb{F}_q}$ 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 $\mathrm{AH}_{\mathbb{F}_q}$ 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 $\mathrm{AH}_{\mathbb{F}_q}$ všechny 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 $\mathrm{AH}_{\mathbb{F}_q}$ a $\mathrm{AG}_{\mathbb{F}_q}$ jsou velmi odlišné. Na příkladu 2.1.9 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 3.1.7.** *Uvažme roj* $\mathrm{AH}_{\mathbb{F}_q}$ *a nějakou jeho komponentu souvislosti* $V$*. Pak je přes všechny afinní vrcholy* $(a, b) \in V$ *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 3.1.8.** *Každá komponenta souvislosti v roji* $\mathrm{AH}_{\mathbb{F}_q}$ *obsahuje nejvýše* $q-1$ *afinních vrcholů.*

*Důkaz.* Pro dané nenulové $k \in \mathbb{F}_q$ 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 3.1.7 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 2.1.11, tentokrát je totiž počet přátel grafů k dané souvislé komponentě velmi omezený.

**Definice 3.1.9.** Ať $(a, b) \in \mathrm{AH}_{\mathbb{F}_q}$ leží v souvislé komponentě $V$. Potom nazveme libovolnou souvislou komponentu obsahující prvek $(ka, kb)$ pro $k \in \mathbb{F}_q$ přítelem $V$.

**Věta 3.1.10.** *Ať $(a, b) \in \mathrm{AH}_{\mathbb{F}_q}$ 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 2.1.11, tentokrát ale pokud pro $k \neq 1$ leží $(a, b)$ a $(ka, kb)$ ve stejné komponentě, podle lemmatu 3.1.7 musí platit $ab = k^2ab$, tj. $k = -1$. Nosná množina grupy $O_k$ sestrojené analogicky k důkazu věty 2.1.11 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 $\mathrm{AH}_{\mathbb{F}_q}$ se vyskytují komponenty s $q - 1$ přáteli, stejně jako jiné komponenty, které mají přátel pouze $(q - 1)/2$.

**Definice 3.1.11.** Ať $H \subseteq \mathrm{AH}_{\mathbb{F}_q}$ 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 $\mathrm{AH}_{\mathbb{F}_q}$ mají tu strukturu, kterou jim připisujeme. Nejprve klasifikujeme, kdy má prvek předchůdce.

**Lemma 3.2.1.** *Afinní vrchol $(a, b) \in \mathrm{AH}_{\mathbb{F}_q}$ 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 $\mathrm{AH}_{\mathbb{F}_q}$ leží vrchol $(a - x, a + x)$. Jeho následník je:

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

□

**Poznámka.** Lemma 3.2.1 pro $a = -b$ nám říká, že vrchol $(a, -a) \in \mathrm{AH}_{\mathbb{F}_q}$ má předchůdce, právě pokud platí $\phi_q(2) = 1$.

Díky tomuto tvrzení dokážeme poskytnout parciální odpověď na otázku, jak vypadají komponenty souvislosti v $\mathrm{AH}_{\mathbb{F}_q}$. 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 $(a, b) \in \mathrm{AH}_{\mathbb{F}_q}$. Potom:*

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

*(ii) pokud $\phi_q(-ab) = 1$, tak mají v $\mathrm{AH}_{\mathbb{F}_q}$ 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 $\mathrm{AH}_{\mathbb{F}_q}$ 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. Připusťme, že v $\mathrm{AH}_{\mathbb{F}_q}$ máme sled afinních 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 $\mathrm{AH}_{\mathbb{F}_q}$ 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:

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

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

$$\begin{aligned}
\phi_q(2b(b-1)) &= \phi_q(2) \cdot \phi_q(b) \cdot \phi_q(b-1) = -1 \cdot \phi_q(b) \cdot \phi_q(-x^2) \\
&= -1 \cdot \phi_q(-b) \cdot \phi_q(x^2) = -1 \cdot 1 \cdot 1 = -1.
\end{aligned}$$

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, viz např. obrázek 3.2.

Nyní dokážeme hlavní větu této sekce.

**Věta 3.2.4.** *Ať $q \equiv 3, 5 \pmod 8$ je mocnina prvočísla. Pak roj $\mathrm{AH}_{\mathbb{F}_q}$ 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 $W = (a, b)$ je vulkán. Stejně jako v případě $AG$ posloupnosti pišme sled následníků vrcholu V:

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

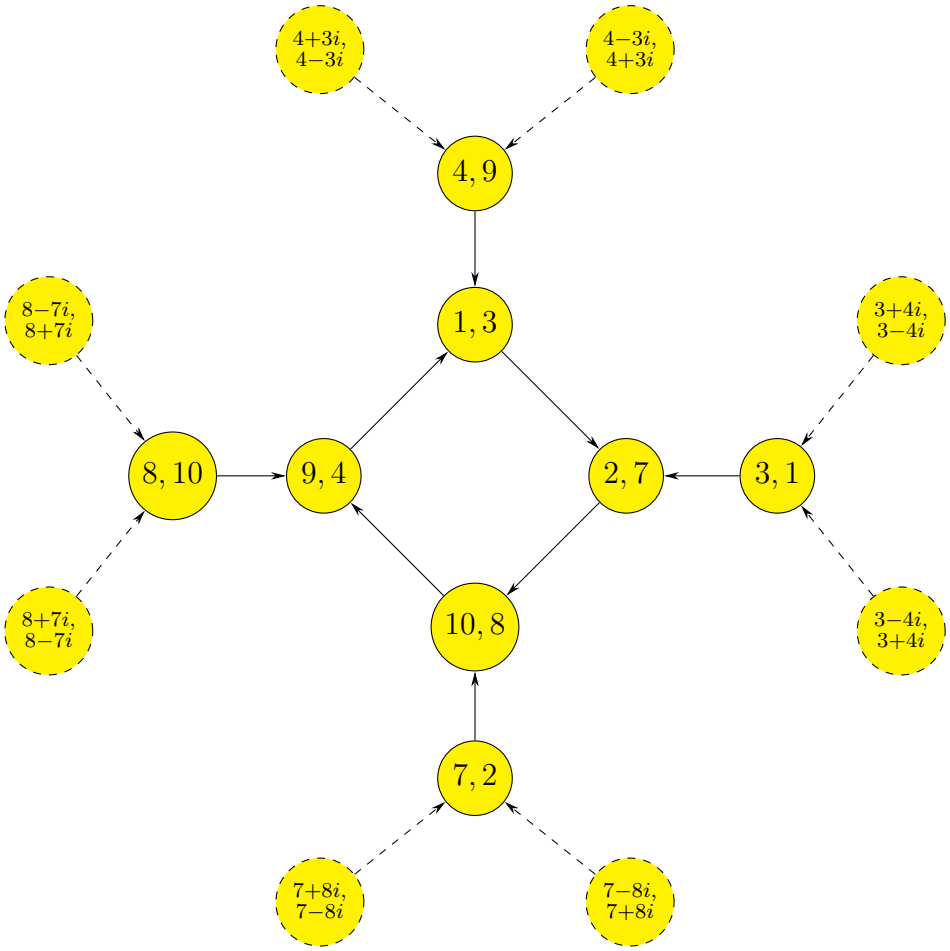
Máme nekonečně definovanou posloupnost na konečné množině vrcholů, jednou proto vstoupí do cyklu, který má délku větší než jedna. Dejme tomu, že $(c, d)$ je člen cyklu, potom mu můžeme psát nekonečnou posloupnost předků ležících v cyklu. Ať je tedy $(C, D)$ předchůdce $(c, d)$ neležící v cyklu. V důkaze lemmatu 3.2.3 jsme si ukázali, že $(C, D)$ má dva předchůdce a ti již předchůdce 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 je charakteristika tělesa $p \equiv 3, 5 \pmod 8$, ale $q = p^k$? je čtverec? V takových případě platí $\phi_q(2) = 1$ a navíc každý list v grafu $\mathrm{AH}_{\mathbb{F}_{p^t}}$ má v grafu $\mathrm{AH}_{p^k} = \mathrm{AH}_{p^{2t}}$ předchůdce. Na příklad rozšiřme komponentu obsahující $(1, 3)$ z příkladu 3.1.4 nad tělesem $\mathbb{F}_{11^2}$, pak získáme komponentu v obrázku 3.4.

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* $V \subseteq \mathrm{AH}_{\mathbb{F}_q}$ *vulkán hloubky* $h$ *a* $(a, b)$ *nějaký jeho prvek. V grafu* $\mathrm{AH}_{\mathbb{F}_{q^k}}$ *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




Obrázek 3.4: Rozšíření příkladu 3.1.4 nad $\mathbb{F}_{11^2} = \mathbb{F}_{11}[i]$

$k$, 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 $(a \pm x, a \mp x) \in \mathrm{AH}_{\mathbb{F}_{q^{2k}}}$ a výšla stromu obsahujícího $(a,b)$ má v $\mathrm{AH}_{\mathbb{F}_{q^{2k}}}$ hloubku alespoň o jedna delší, než v $\mathrm{AH}_{\mathbb{F}_{q^k}}$. 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 $a$ je liché a $k$ sudé. Pak platí:*

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

*Důkaz.* Využijeme vzorec $a^k - 1 = (a-1)(a^{k-1} + \cdots + 1)$. Pokud je $k$ liché a $a$ též, tak ve druhé závorce sčítáme lichý počet lichých členů, získáme tedy liché číslo a platí $v_2(a^k - 1) = v_2(a-1)$. Stačí nám tedy uvažovat případ, kdy $k = 2^t$ je mocnina dvojky. Pak rozložíme:

$$a^{2^t} - 1 = (a^{2^t} + 1)(a^{2^{t-1}} + 1) \cdots (a^2 + 1)(a+1)(a-1).$$

Kvadratické zbytky modulo 4 jsou pouze 0 a 1, tedy každá až na poslední dvě závorky je sudá a nedělitelná čtyřmi. Tyto závorky proto do 2-valuace čísla $a^k - 1$ přispívají po jedné a jelikož jich je $t - 1 = v_2(k) - 1$, jsme hotovi. □

Důsledek výše spolu s větou 3.2.4 pak ukazuje, že hloubka vulkánu je určitým způsobem spojena s $v_2(q-1)$.

## 3.3 Vlastnosti grafů

I v případě *AH* posloupnosti se můžeme dívat na empirická data ohledně jednotlivých parametrů. Ukázali jsme, že pro $q \equiv 3, 5 \pmod 8$ jsou komponenty souvislosti v roji $\mathrm{AH}_{\mathbb{F}_q}$ vulkány hloubky 1 a 2. V kapitole 5 ukážeme, že i pro ostatní mocniny prvočísel $q$ tvoří komponenty souvislosti roje $\mathrm{AH}_{\mathbb{F}_q}$ vulkány. Jakou hloubku mají tyto vulkány pro komponenty obsahující body $(a, b)$ splňující $\phi_q(ab) = 1$, resp. $\phi_q(ab) = -1$? Ukažme si malou tabulku těchto hloubek.

| $p$ | hloubka vulkánů obsahující prvky $(a, b)$ s $\phi_q(ab) = 1$ | hloubka vulkánů obsahující prvky $(a, b)$ s $\phi_q(ab) = -1$ |
|---|---|---|
| 3 | – | 2 |
| 5 | 2 | 1 |
| 7 | 1 | 3 |
| 11 | 1 | 2 |
| 13 | 2 | 1 |
| 17 | 4 | 1 |
| 19 | 1 | 2 |
| 23 | 1 | 3 |
| 29 | 2 | 1 |
| 31 | 1 | 5 |
| 37 | 2 | 1 |

Obrázek 3.5: Tabulka hloubek vulkánů pro $p < 40$.

Všimneme si dvou věcí, nejprve zdárně vždy buď komponenty souvislosti obsahující body $(a, b)$ s $\phi_q(ab) = 1$ nebo komponenty obsahující body $(a, b)$ s $\phi_q(ab) = -1$ jsou vulkány hloubky 1, tj. medúzy. Kvůli hloubkám vulkánů pro po řadě $p = 17$ a $p = 31$ se můžeme dovtípit, jaká hloubka nastane v obecném případě.

**Domněnka 3.3.1.** *Komponenty souvislosti roje* $\mathrm{AH}_{\mathbb{F}_p}$ *obsahující body* $(a, b)$ *splňující* $\phi_p(ab) = 1$ *jsou vulkány hloubky* $v_2(p-1)$. *Komponenty souvislosti obsahující body* $(a, b)$ *splňující* $\phi_p(ab) = 1$ *jsou vulkány hloubky* $v_2(p+1)$.

V kapitole 5 tuto domněnku dokážeme a určíme hloubku vulkánů pro libovolné konečné těleso $\mathbb{F}_q$ liché charakteristiky. Vzhledem k tomu, že hloubky grafů se mohou prvočíslo od prvočísla zásadně lišit, tak se nebudeme v této sekci věnovat heuristikám ohledně počtu komponent, resp. počtu hejn. Podíváme se ale, jak tato dvě čísla souvisí spolu.

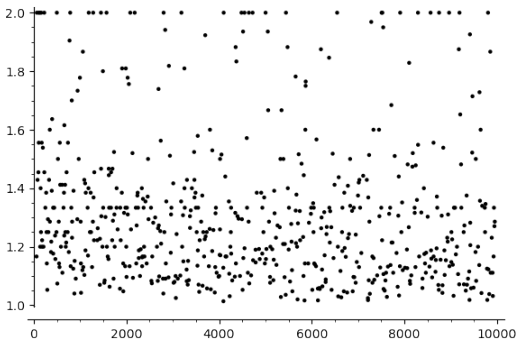
**Definice 3.3.2.** Ať $q$ je mocnina prvočísla. Pak označme $D(\mathbb{F}_q)$ počet všech souvislých komponent v grafu $\mathrm{AH}_{\mathbb{F}_q}$, které obsahují alespoň jeden afinní prvek. Navíc, označme $S(\mathbb{F}_q)$ počet všech hejn v grafu $\mathrm{AH}_{\mathbb{F}_q}$, které obsahují alespoň jeden afinní prvek.

**Věta 3.3.3.** *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 4.3.3, jelikož každé hejno přispívá buď $\frac{q-1}{2}$ nebo $q-1$ medúzami do počtu $D(\mathbb{F}_q)$. □

Silnější odhady zdánlivě nenajdeme. Pro například $p = 11$ platí $D(\mathbb{F}_{11}) = 10$ a $S(\mathbb{F}_{11}) = 2$, tj. $D(\mathbb{F}_{11}) = S(\mathbb{F}_{11}) \cdot \frac{11-1}{2}$. Obdobné vztahy platí pro $p = 19, 67, 107, 131, \ldots$. Na druhou stranu rovnost $D(\mathbb{F}_p) = (p-1)S(\mathbb{F}_p)$ nenastane pro $p < 10^5$. Pro $p = 11243$ nastane $D(\mathbb{F}_p) = 753214$ a $S(\mathbb{F}_p) = 68$, tj. $\frac{S(\mathbb{F}_p)\cdot(p-1)}{D(\mathbb{F}_p)} = 1.015\ldots$.




Obrázek 3.6: Číslo $\frac{S(\mathbb{F}_p)\cdot(p-1)}{D(\mathbb{F}_p)}$ pro $p < 10^4$

## 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 Pollardova-Rho 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 $g : \mathrm{AH}_{\mathbb{F}_q} \longrightarrow \mathbb{P}^1(\mathbb{F}_q)$ dané $g(a, b) = \frac{a}{b}$. Potom se na každý nenulový prvek $x \in \mathbb{F}_q$ zobrazí právě $q - 1$ prvků $\mathrm{AH}_{\mathbb{F}_q}$, konkrétně body $(ax, a) \in AH_{\mathbb{F}_q}$ pro $a \in \mathbb{F}_q^\times$. Prvky 0 a $\infty$ 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 $(a, b) \in \mathrm{AH}_{\mathbb{F}_q}$ 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 $\mathrm{AH}_{\mathbb{F}_q}$ 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 $(a, b) \in \mathrm{AH}_{\mathbb{F}_q}$ 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 $\mathrm{AH}_{\mathbb{F}_q}$, poté dle symetrie v něm neleží ani bod $(-a, -b)$. Podle věty 3.1.7 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 $\mathrm{AH}_{\mathbb{F}_q}(a, b)$ se bod $(a, b)$ znovu nevyskytuje. Bod $(a, b)$ proto leží mimo cyklus. □

Pokud máme posloupnost $\mathrm{AH}_{\mathbb{F}_q}(a,b)$:

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

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 $(x,y) \in \mathrm{AH}_{\mathbb{F}_q}$ je členem cyklu a $V \subseteq \mathrm{AH}_{\mathbb{F}_q}$ 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 $(a,b) \in \mathrm{AH}_{\mathbb{F}_q}$ 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.

**Poznámka.** ?

Pomocí dynamických systémů můžeme znovu dokázat některé výsledky ohledně *AH* posloupnosti, které jsme dokázali v předchozích sekcích. Vlastnosti konečných těles poskytnou nový důkaz odhadů, které jsou předmětem důsledku 3.2.5. Stačí nám ukázat, že pro $z \in \mathbb{F}_q$ leží každý předchůdce prvku $z \in D_f$ 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:

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

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. $x \in \mathbb{F}_{q^2}$. □

Dokázali jsme, že list $(a, b) \in \mathrm{AH}_{\mathbb{F}_q}$ má v grafu $\mathrm{AH}_{\mathbb{F}_{q^2}}$ dva předchůdce. Bohužel ukázat, že tyto dva vrcholy již předchůdce nemají, je obtížnější. Abychom ukázali, že pro $q \equiv 1, 7 \pmod 8$ tvoří komponenty souvislosti grafu $\mathrm{AH}_{\mathbb{F}_q}$ hlubší vulkány, využijeme v kapitole 5 teorii spojenou s eliptickými křivkami.

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 $\phi_q$ 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 $a_1x_1^{b_1} + \cdots + a_nx_n^{b_n} = k$ nad konečnými tělesy. Pro excelentní úvod do jejich studia doporučuji [7].

**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 3.1.8 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:

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

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 3.1.6 je toto číslo alespoň:

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

Označme konečně $N$ nejvyšší délku cyklu, který ve $V$ najdeme. Podle nerovnosti (4.3.3) 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 [9], excelentní cizojazyčné zdroje jsou například [12, 17, 10]

Po celou dobu se pohybujeme v tzv. *projektivní prostoru* $\mathbb{P}^n(K)$, 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 $(x : y : z) \in \mathbb{P}^2(\overline{\mathbb{F}_q})$ splňujících vztah:

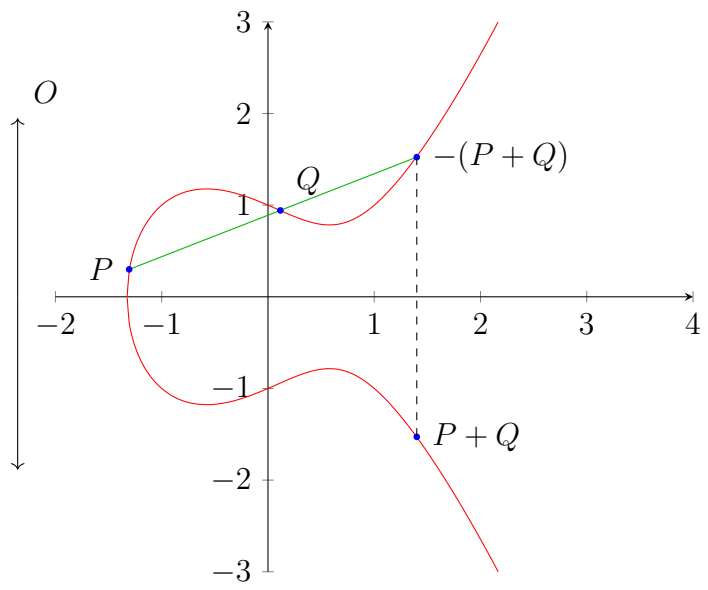
$$Y^2Z = X^3 + AXZ^2 + BZ^3,$$

spolu s tzv. *bodem v nekonečnu* $O$. Dále definujeme *eliptickou křivku v Legendrově tvaru* jako množinu $(x : y : z) \in \mathbb{P}^2(\overline{\mathbb{F}_q})$ splňujících:

$$Y^2Z^2 = X(X - Z)(X - \lambda Z),$$

opět s bodem v nekonečnu. Značíme $E/\mathbb{F}_q$, je-li $E$ definovaná nad tělesem $\mathbb{F}_q$.

Můžeme přejít na tzv. *afinní souřadnice*, kde body $(X : Y : Z)$ sjednotíme s body $(X/Z : Y/Z : 1)$. Jediný *bod v nekonečnu* $(0 : 1 : 0)$ nemá afinní vyjádření. Na eliptické křivce můžeme definovat sčítání viz obrázek 4.1. S tímto sčítáním tvoří body na eliptické křivce abelovskou grupu. Definujeme pak $n$-násobek bodu $[n]P = \underbrace{P + \cdots + P}_{n}$, kde $[0]P = O$.




Obrázek 4.1: Sčítání na eliptické křivce.

Označme $E(\mathbb{F}_q)$ množinu bodů na $E$ definovaných nad $\mathbb{F}_q$ (včteně $O$). Zmiňme pak důležitou *Hasseho větu*, která tvrdí, že počet bodů na křivce ne příliš liší od $q$.

**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*. Označme navíc $\ker \phi$ jádro isogenie $\phi$.

Příklady isogenií jsou například právě skalární násobení $[n]$ a nebo tzv. *Frobeniův automorfismu* daný předpisem $\pi : (X : Y : Z) \longmapsto (X^p : Y^p : Z^p)$. 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 $u \in \overline{K}$.

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 $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$.*

## 4.2 Okruhy endomorfismů

Endomorfismus na křivce $E$ definujme jako isogenii $\phi : E \longrightarrow E$, přičemž připusťme, že $[0]$ je na $E$ endomorfismem. Můžeme definovat součet resp. složení dvou isogenií jako isogenii, která pro každé $P \in E$ splňuje $(\phi + \psi)(P) = \phi(P) + \psi(P)$, resp. $(\phi \circ \psi)(P) = \phi(\psi(P))$. S takto definovaným sčítáním a skládáním 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.

Dá se ukázat, že každý endomorfismus $\phi \in \mathrm{End}(E)$ je kořenem kvadratického polynomu $x^2 + ax + b \in \mathrm{End}(E)[x]$. Nás bude obzvláště zajímat Frobeniův automorfismus, který je kořenem polynomu:

$$x^2 - [t]x + [q] \in \mathrm{End}(E)[x],$$

kde $t = q + 1 - \#E(\mathbb{F}_q) \in [-2\sqrt{q}, 2\sqrt{q}]$ je *stopa Frobenia*. Legendreho křivky jsou tzv. *obyčejné křivky*, což znamená, že okruh endomorfismů Legendreho křivky můžeme umístit do kvadratického tělesa [12, Thm. 13.17.].

**Věta 4.2.2.** *Buď $E$ Legendreho křivka a $t$ jako výše. Označme $K = \mathbb{Q}(\pi) \cong \mathbb{Q}(\sqrt{t^2 - 4q})$ imaginární kvadratické těleso. Poté okruh $\mathrm{End}(E)$ je pořádek*[1] *v $K$.*

Věta 4.2.2 říká, že endomorfismy na dané Legendreho křivce $E$ můžeme ztotožnit s prvky pořádků $\mathcal{O}$ v jistém číselném tělesem $K$. Přesněji je můžeme sjednotit s *hlavními ideály* v tomto pořádku [9, Lemma 4.3.3]. Isogenie $\phi : E \longrightarrow E'$, které nejsou endomorfismy, můžeme přiřadit nehlavním ideálům v $\mathcal{O}$ [9, Def. 4.3.1].

Důležitou strukturou spojenou s okruhy celých algebraických čísel a pořádky v číselném tělese je *grupa tříd ideálů* $Cl(\mathcal{O})$ pořádku $\mathcal{O}$. Tu zde nebudeme precizně definovat, berme ji jako faktorgrupu jistých grup ideálů v pořádku $\mathcal{O}$ s operací násobení ideálů. Neutrální prvek grupy tříd ideálů je podgrupa obsahující právě hlavní ideály pořádku $\mathcal{O}$. Tato grupa je konečná, její řád označme $h_{\mathcal{O}}$, tzv. *třídové číslo*. Grupa tříd ideálů a třídové číslo jsou propojené s jednoznačností rozkladu v $\mathcal{O}$, viz [9, Věta 3.6.10].

Grupa tříd ideálů nám pomůže blíže popsat korespondenci isogenií vycházejících z $E$ a ideálů pořádku $\mathcal{O} \cong \mathrm{End}(E)$. Konkrétně všechny ideály z jedné třídy $Cl(\mathcal{O})$ jsou v korespondenci se třídou isogenií vycházejících z $E$, které jsou všechny shodné *až na složení s endomorfismem* [9, Věta 4.3.9]. Toto propojení využijeme při studiu $AG$ posloupnosti.

## 4.3 Aplikace na AG posloupnost

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

[1] Volný $\mathbb{Z}$-modul ranku $n$ $\mathcal{O} \subseteq \mathcal{O}_K$ v číselném tělese $K$ stupně $n$ nazveme pořádkem.

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 [1], 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:

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

**Definice 4.3.1.** Označme $\mathrm{Ell}(\mathbb{F}_q) = (V, F)$ orientovaný graf, kde $V = \{E_{\lambda^2} | \lambda \in \mathbb{F}_q^\times \setminus \{\pm 1\}\}$ a $(E, E') \in F$, právě pokud existuje vrchol $(a, b) \in \mathrm{AG}_{\mathbb{F}_q}$ splňující $E = E_{(a,b)}$ a $E' = E_{(a_1,b_1)}$.

**Definice 4.3.2.** Definujme zobrazení $\Psi : \mathrm{AG}_{\mathbb{F}_q} \longrightarrow \mathrm{Ell}(\mathbb{F}_q)$ dané $\Psi : (a, b) \longmapsto E_{(a,b)}$.

Následující věta nám ukáže, jak přesně souvisí grafy $\mathrm{AG}_{\mathbb{F}_q}$ a $\mathrm{Ell}(\mathbb{F}_q)$.

**Věta 4.3.3.** *Ať $V \subseteq \mathrm{AG}_{\mathbb{F}_q}$ je medúza obsahující vrchol $(a, b)$, jejíž cyklus má délku $d$. Dále ať $V \in W \subseteq \mathrm{AG}_{\mathbb{F}_q}$ je hejno, které čítá $N$ medúz. Poté $\Psi(W)$ je medúza, jejíž cyklus má délku:*

$$\frac{dN}{q-1}.$$

*Důkaz.* Zjevně $\Psi(W)$ je medúza. Ať $(a_j, b_j) \in \mathrm{AG}_{\mathbb{F}_q}(a, b)$ je první vrchol roje $\mathrm{AG}_{\mathbb{F}_q}$ splňující $(a_j, b_j) = (ka, kb)$, tj. délka cyklu $\Psi(W)$ je $j$. Délka cyklu medúzy $V$ je rovna $d = j \operatorname{ord}_q(k)$ a podle věty 2.1.11 platí:

$$N = \frac{q-1}{\operatorname{ord}_q(k)},$$

tedy délka medúzy $\Psi(W)$ je rovna:

$$j = \frac{dN}{q-1}.$$

□

Jak pro danou křivku $E \in \mathrm{Ell}(\mathbb{F}_q)$ určíme, zda leží v cyklu medúzy? Ukáže se, že tato vlastnost závisí právě na tom, jaký je okruh endomorfismů $E$. Jelikož $t^2 - 4q \equiv 1 \pmod 4$, tak díky větě 4.2.2 a [9, Věta 3.2.10] je okruh celých algebraických čísel tělesa $K$ z věty 4.2.2 $\mathcal{O}_K \cong \mathbb{Z}\left[\frac{1+\pi}{2}\right]$. Můžeme říci, že platí $\mathbb{Z}[\pi] \subseteq \mathrm{End}(E)$, jelikož všechny skalární násobky $[n]$ a Frobeniův automorfismus $\pi$ leží v $\mathrm{End}(E)$. Platí proto $\mathbb{Z}[\pi] \subseteq \mathrm{End}(E) \subseteq \mathbb{Z}\left[\frac{1+\pi}{2}\right]$. Následující věta odpovídá na to, kdy nastane který z případů.

**Věta 4.3.4.** *Ať $V \subseteq \mathrm{Ell}(\mathbb{F}_q)$ je medúza. Poté křivka $E \in V$ splňuje $\mathrm{End}(E) = \mathbb{Z}\left[\frac{1+\pi}{2}\right]$, právě pokud $E$ je členem cyklu ve $V$.*

Důkaz je podán v [10, Lemma 98].

Můžeme přesně konstruovat isogenii, která na sebe převádí křivky $E_{(a,b)}$ a $E_{(a_1,b_1)}$.

**Věta 4.3.5.** *Mějme vrchol $(a,b) \in \mathrm{AG}_{\mathbb{F}_q}$. 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.* $\phi$ 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 $\phi$ 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.

Pojďme nyní využít tento nový náhled na *AG* posloupnost a osvětleme zdánlivě náhodné velikosti a počty medúz v roji $\mathrm{AG}_{\mathbb{F}_q}$.

**Věta 4.3.6.** *Buď $V \subseteq \mathrm{Ell}(\mathbb{F}_q)$ medúza. Označme $d$ délka cyklu $V$ a $\mathcal{O} \cong \mathbb{Z}\left[\frac{1+\pi}{2}\right]$ pořádek v tělese $K$. Pak existuje ideál $\mathfrak{a} \subseteq \mathcal{O}$ takový, že řád třídy $[\mathfrak{a}]$ v $Cl(\mathcal{O})$ je roven $d$.*

Důkaz je podán v [18, Thm. 4.5].

Věta 4.3.6 tvrdí, že délka cyklu každé medúzy dělí třídové číslo $h_{\mathcal{O}}$, kde $\mathcal{O} \cong \mathbb{Z}\left[\frac{1+\pi}{2}\right]$ je pořádek v kvadratickém tělese $K = \mathbb{Q}(t^2 - 4q)$. Určení velikost grupy tříd ideálů je známý a těžký problém a její velikost se liší divoce od tělesa k tělesu.

*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 řečeno veličina, kterou sdílí isogenní křivky. Sato-Tateova věta 4.1.4 poskytuje takový invariant – počet prvků na křivce.

**Věta 4.3.7.** *Ať $V \subseteq \mathrm{Ell}(\mathbb{F}_q)$ je medúza. Pak existuje $t \in \mathbb{N}$ takové, že pro všechny křivky $E \in V$ platí $\#E(\mathbb{F}_q) = q + 1 - t$.*

Věta 4.3.7 vede na hlavní výsledek článku [1], odhad počtu hejn medúz v grafu $AG_{\mathbb{F}_q}$.

**Věta 4.3.8.** *(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.* Důkaz podaný v [1] postupuje tak, že autoři hledají $s \in [q+1-2\sqrt{q}, q+1+2\sqrt{q}]$ taková, že existuje Legendreho křivka v $\mathrm{Ell}(\mathbb{F}_q)$ mající právě $s$ prvků. Ukazují, že mohou sestrojit Legendreho křivky, jejichž počet prvků $\#E(\mathbb{F}_q) = s$ splňuje $s \in [q+1-2\sqrt{q}, q+1+2\sqrt{q}]$ a platí $s \equiv q+1 \pmod 8$. Každá z těchto přibližně $(1/2-\varepsilon)\sqrt{q}$ křivek leží podle věty 4.3.7 v jiné medúze v grafu $\mathrm{Ell}(\mathbb{F}_q)$ a tedy podle věty 4.3.3 platí:

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

□

Tento odhad zdánlivě není optimální, jak jsme si ukázali v sekci 2.2. Ne vždy totiž dvě křivky se stejným počtem prvků leží ve stejném vulkánu v grafů isogenií. Obecně určit, zda dvě eliptické křivky leží ve stejném vulkánu závisí na tzv. *modulárním polynomu* a i algoritmicky to vůbec není snadný problém. Pro více informací se odkazujeme na [11].

# 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 $\mathrm{AH}_{\mathbb{F}_q}$ mají nejvýše $q$ prvků, viz věta 3.1.8, oproti *AG* posloupnosti, kde může být až mnohonásobně více prvků, jak jsme viděli u příkladu 2.1.9. 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 jejího využití v šifrování nám tato křivka může pomoci studovat mj. dynamiku funkce $x + \frac{1}{x}$ nad tělesy $\mathbb{F}_{2^n}$. 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 [13, 14, 15, 16] 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 $\phi$ 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 [9].

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 [8]. 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, $\psi$ 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 $\psi$ bod výše zobrazí na $a$. Zobrazení $\psi$ 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 studujme předchůdce vrcholů ve grafu $G_{\mathbb{F}_q}$. Nejprve ukážeme, že pokud pro daný bod $P \in G_{\mathbb{F}_q}$ existuje bod $Q \in G_{\mathbb{F}_q}$ splňující $[2]Q = P$, pak již existují dva. Díky tomu pak určíme, kdy vlastně má daný bod předchůdce.

**Věta 5.3.2.** *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 splňující $[2]P = O$ 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.** *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.* Dejme tomu, že existuje bod $Q$ splňující $[2]Q = P$. Vysvětleme, proč bod $Q$ splňující $[2]Q = P$ pro $v_2(\operatorname{ord} P) > 0$ musí splňovat $\operatorname{ord} Q = 2 \operatorname{ord} P$. Platí $[2 \operatorname{ord} P]Q = [\operatorname{ord} P]P = O$, tj. $\operatorname{ord} Q \mid 2 \operatorname{ord} P$. Pokud označíme $r$ libovolný prvodělitel čísla $2 \operatorname{ord} P$, pak:

$$\left[\frac{2 \operatorname{ord} P}{r}\right] Q = \begin{cases} (0,0), & \text{pokud } r = 2, \\ \left[\frac{\operatorname{ord} P}{r}\right] P \neq O, & \text{pokud } r > 2. \end{cases}$$

Je proto $\operatorname{ord} Q = 2 \operatorname{ord} P$. To znamená, že:

$$v_2(\operatorname{ord} P) + 1 = v_2(\operatorname{ord} Q) \leqslant v_2(\#E(\mathbb{F}_q)) = v_2(q-1).$$

Nyní předpokládejme, že platí $v_2(\operatorname{ord} P) < v_2(q-1)$. Využijeme větu 5.2.5. Je známé [7, Ch.7 Thm. 1], že grupa $\mathbb{F}_q^\times$ je cyklická, tj. existuje prvek $g \in \mathbb{F}_q^\times$, který ji generuje. To znamená, že pokud nejvyšší mocnina dvojky dělící řád $P$ je ostře menší, než $v_2(q-1)$, pak má $P$ předchůdce. □

Věta 5.3.2 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 5.3.3 a 5.3.2 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 5.3.3 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 $\mathrm{AH}_{\mathbb{F}_q}$ 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 $v_2(q+1)$.*

*Důkaz.* V případě komponent souvislosti grafu $\mathrm{AH}_{\mathbb{F}_q}$ obsahujících body $(a,b)$ splňující $\phi_q(ab) = 1$. 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 $v_2(q-1)$.

Nyní se podívejme na komponenty souvislosti v $\mathrm{AH}_{\mathbb{F}_q}$ obsahující list $(a,b)$ s $\phi_q(ab) = -1$. Všimněme, že pokud $k = 2t$ je sudé, tak vždy platí:

$$\phi_q(a(a-b))\phi_q(b(b-a)) = \phi_q(-ab)\phi_q((a-b)^2) = \phi_q(-ab) = -1.$$

Podle věty 3.2.2 jsou komponenty obsahující body $(a, b)$ s $\phi(ab) = -1$ medúzy. Opravdu, $-1$ není kvadratický zbytek modulo 4, proto $q+1 = p^{2t}+1 \equiv 2 \pmod 4$. Jediný „zajímavý“ případ proto nastane, pokud stupeň rozšíření $[\mathbb{F}_q : \mathbb{F}_p]$ je lichý a pokud nastane $\phi_q(-1) = -1$. To nastane, právě pokud $q = p^k \equiv -1 \pmod 4$.
Podle věty 5.2.3 leží v $E(\mathbb{F}_{q^2})$ bod $\left(\frac{a}{b}, -\right)$. ?????????????????????????????????????????????
!!! !! ! ! !! ! ! ! ! ! ! ! ! !SPRAVIT

Takový bod ztotožníme pro $z = \frac{a}{b}$ s bodem $z \in D_f$, platí $\phi_q(z) = -1$. Podle věty 5.2.3 existuje bod $(z, y) \in E(\mathbb{F}_{q^2})$. Tento bod je díky větě 3.4.2 jistě v grafu $G_{\mathbb{F}_{q^2}}$ listem. Podle věty 5.3.5 leží ve binárním stromu hloubky $v_2(q^2 - 1) = v_2(q - 1) + v_2(q + 1)$.

**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 těsné.

Konečně jsme splnili slib z kapitoly 3 - pomocí eliptických křivek plně charakterizovat, jaký tvar mají komponenty souvislosti v roji $\mathrm{AH}_{\mathbb{F}_q}$. Pojďme toto propojení maximálně využít ve zkoumání dalších vlastností roje $\mathrm{AH}_{\mathbb{F}_q}$.

**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 $P$ má řád $k$, 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 [7, Ch.4 Thm.2]. To jistě znamená, že se v $\mathbb{F}_q^\times$ a následně v $E(\mathbb{F}_q)$ nachází právě $\phi(k)$ prvků lichého řádu $k \mid q - 1$. □

**Věta 5.3.8.** *Nechť jsou $q$ mocnina prvočísla a liché číslo $k \mid q - 1$. Potom počet vulkánů $V \subseteq G_{\mathbb{F}_q}$ obsahující body s řádem $P$ rovným $k$, je:*

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

*Důkaz.* Uvažme bod $P \in G_{\mathbb{F}_q}$ s řádem $k$. Pak je členem cyklu:

$$P \mapsto [2]P \mapsto \cdots \mapsto [2^t]P = P,$$

kde $t = \mathrm{ord}_k(2)$. Spolu s větou 5.3.7 pak získáme dokazované. □

Věta 5.3.8 má jeden roztomilý důsledek, můžeme totiž pomocí ní dokázat novým způsobem jedno známé tvrzení.

**Důsledek 5.3.9.** *Označme $t = v_2(q-1)$ nejvyšší mocninu dělící $q-1$. Pak platí:*

$$\frac{q-1}{2^t} = \sum_{k \mid \frac{q-1}{2^t}} \phi(k).$$

Tento vztah platí bezpodmínečně pro libovolné $n$:

$$n = \sum_{k \mid n} \phi(k). \tag{5.2}$$

Důkaz tohoto obecného tvrzení lze vést například pomocí tzv. *Möbiovy inverzní formule* [7, Ch.3 Thm 2.]. O něco důležitější důsledek věty 5.3.8 je následující.

**Důsledek 5.3.10.** *Uvažme komponentu roje $H \subseteq \mathrm{AH}_{\mathbb{F}_q}$ obsahující všechny komponenty souvislosti, jejichž prvky jsou body $(a,b) \in \mathrm{AH}_{\mathbb{F}_q}$ splňující $\phi_q(ab) = 1$. Dále označme $\{d_1, \ldots, d_s\}$ multimnožinu*[1] *délek cyklů vulkánů $V \subseteq H$. Potom existují $\varepsilon_i \in \{1,2\}$ splňující:*

$$\left\{ \frac{d_1}{\varepsilon_1}, \ldots, \frac{d_s}{\varepsilon_s} \right\} = \left\{ \mathrm{ord}_1(2), \ldots, \underbrace{\mathrm{ord}_k(2), \ldots, \mathrm{ord}_k(2)}_{\frac{\phi(k)}{\mathrm{ord}_k(2)}}, \ldots \;\middle|\; k \mid q-1 \right\}$$

Díky ??, můžeme podat netriviální odhady na čísla $S(\mathbb{F}_q)$ a $D(\mathbb{F}_q)$.

**Věta 5.3.11.** *Platí:*

$$\sum_{\substack{k \mid q^2-1 \\ 2 \nmid k}} \frac{\phi(k)}{\mathrm{ord}_k(2)} \geqslant S(\mathbb{F}_q) \geqslant \sum_{\substack{k \mid q-1 \\ 2 \nmid k}} \frac{\phi(k)}{\mathrm{ord}_k(2)}.$$

Toto 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 5.3.12.** *Označme $t = v_2(q-1)$ a $s = v_2(q+1)$. Platí řetězec nerovností:*

$$\frac{q^2-1}{2^{s+t}} \geqslant S(\mathbb{F}_q) \geqslant \frac{q-1}{2^t \,\mathrm{ord}_X(2)},$$

*kde $X = \frac{q-1}{2^t}$.*

*Důkaz.* Jistě pro každé $k$ platí $\mathrm{ord}_k(2) \geqslant 1$, proto:

$$S(\mathbb{F}_q) \leqslant \sum_{\substack{k \mid q^2-1 \\ 2 \nmid k}} \frac{\phi(k)}{\mathrm{ord}_k(2)} \leqslant \sum_{\substack{k \mid q^2-1 \\ 2 \nmid k}} \phi(k) = \frac{q^2-1}{2^{v_2(q^2-1)}} = \frac{q^2-1}{2^{s+t}},$$

[1] co toje

kde využíváme vztah (5.2). Pro druhou stranu nerovnosti použijeme nerovnost $\mathrm{ord}_k(2) \leqslant \mathrm{ord}_{\frac{q-1}{2^t}}(2)$ platnou pro libovolné $k \mid q-1$ liché a poté znovu využijeme vztah (5.2). □

**Důsledek 5.3.13.** *Označme $t = v_2(q-1)$ a $s = v_2(q+1)$. Platí řetězec nerovností:*

$$\frac{(q-1)^2(q+1)}{2^{s+t}} \geqslant D(\mathbb{F}_q) \geqslant \frac{(q-1)^2}{2^{t+1}\,\mathrm{ord}_X(2)},$$

*kde $X = \frac{q-1}{2^t}$.*

*Důkaz.* Přímý důsledek vět 5.3.12 a 3.3.3. □

# 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 $E$ |
| $\pi, \pi_E$ | Frobeniův endomorfismus |
| $\widehat{\phi}$ | isogenie duální k $\phi$ |
| $\deg \phi$ | stupeň isogenie $\phi$ |
| $\ker \phi$ | jádro isogenie $\phi$ |
| $\langle G \rangle$ | 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 $\phi$, 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 $\ell$ |

# Literatura


[1] 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.

[2] Borwein, Jonathan M a Peter B. Borwein: *Pi and the AGM: A study in analytic number theory and computational complexity*. Canadian mathematical society series of monographs and advanced texts, 1998.

[3] Cox, David A.: *Gauss and the Arithmetic-Geometric Mean*. Department of Mathematics and Statistics, Amherst College. CTNT, 2016. Dostupné z: https://ctnt-summer.math.uconn.edu/wp-content/uploads/sites/1632/2016/02/coxctnt.pdf.

[4] Crawford, James A.: *Pendulums and Elliptic Integrals*. 2004. Dostupné z: http://ed.quantum-bg.org/elliptic-integrals.pdf

[5] Dalpatadu, Rohan J,: *The Arithmetic-Harmonic-Geometric Mean*. Department of Mathematical Sciences, University of Nevada, Las Vegas, 2014. Dostupné z: https://www.jscimedcentral.com/Mathematics/mathematics-1-1002.pdf.

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

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

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

[9] 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.

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

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

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

[13] 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.

[14] 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.

[15] 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.

[16] 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.

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

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