FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

BACHELOR THESIS

Natália Bátorová

Arithmetic-geometric mean sequences and elliptic curves over finite fields

Department of Algebra

Supervisor of the bachelor thesis: doc. Mgr. Vítězslav Kala, Ph.D.
Study programme: Mathematics for information technologies

Prague 2024

I declare that I carried out this bachelor thesis on my own, and only with the cited sources, literature and other professional sources. I understand that my work relates to the rights and obligations under the Act No. 121/2000 Sb., the Copyright Act, as amended, in particular the fact that the Charles University has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 subsection 1 of the Copyright Act.

In .... date ....

Author's signature

I would like to thank my supervisor doc. Mgr. Vítězslav Kala, Ph.D. for his help with choosing the theme and giving me useful advice.

I also thank my consultant Stevan Gajović, Ph. D. for his patience, willingness, and time dedicated to me. I appreciate his kind and friendly attitude during consultations while answering my questions, and leading me to do my own little research.

Finally, thanks to all my friends and family for support.

Title: Arithmetic-geometric mean sequences and elliptic curves over finite fields

Author: Natália Bátorová

Department: Department of Algebra

Supervisor: doc. Mgr. Vítězslav Kala, Ph.D., Department of algebra

Consultant: Stevan Gajović, Ph. D.

Abstract: In the thesis we introduce arithmetic geometric mean sequences, firstly over real numbers and then over finite fields $\mathbb{F}_q$ such that $q \equiv 3 \pmod 4$. We connect the sequences with graphs and prove some properties over general finite fields for these graphs. We also extend arithmetic geometric mean sequences over $\mathbb{F}_q$ such that $q \equiv 5 \pmod 8$ and we show a connection between elliptic curves and arithmetic geometric mean sequences over $\mathbb{F}_q$ such that $q \equiv 3 \pmod 4$.

Keywords: arithmetic-geometric mean sequences, finite fields, jellyfish swarms, elliptic curves

Název práce: Posloupnosti aritmeticko-geometrických průměrů a eliptické křivky nad konečnými tělesy

Autor: Natália Bátorová

Katedra: Katedra algebry

Vedoucí bakalářské práce: doc. Mgr. Vítězslav Kala, Ph.D., Katedra algebry

Konzultant: Stevan Gajović, Ph. D.

Abstrakt: V práci najskôr predstavíme postupnosti aritmeticko-geometrických priemerov nad reálnymi číslami a následne definujeme tieto postupnosti nad konečnými telesami $\mathbb{F}_q$ takými, kde $q \equiv 3 \pmod 4$. Ďalej zavedieme grafy znázorňujúce tieto postupnosti a dokážeme pre ne pár vlastností. Taktiež rozšírime definíciu postupností aritmeticko-geometrických priemerov pre konečné telesá $\mathbb{F}_q$ také, že $q \equiv 5 \pmod 8$ a ukážeme súvislosť medzi eliptickými krivkami a týmito postupnosťami nad telesami $\mathbb{F}_q$, kde $q \equiv 3 \pmod 4$.

Klíčová slova: postupnosti aritmeticko-geometrických priemerov, konečné telesá, húfy medúz, eliptické krivky

Contents

Introduction

The arithmetic geometric mean sequence (AGM) is a sequence of ordered pairs where the first element of the pair is the arithmetic mean of previous pair and the second element of the pair is the geometric mean of previous pair. AGM over positive real numbers was firstly discovered by Lagrange and rediscovered by Gauss a few years later. There were also discovered some algorithms based on AGM to count digits of π. AGM sequences can be considered over finite fields too. For example, Michael J. Griffin, Ken Ono, Neelam Saikia and Wei-Lun Tsai [Gri+23] introduced AGM over finite fields with q elements such that $q \equiv 3 \pmod 4$. In this case they made a natural definition of infinite AGM for $q > 3$. In this thesis we recall their results and extend the definition over finite fields with q elements such that $q \geq 29$ and $q \equiv 5 \pmod 8$.

One can also show the connection between AGM and elliptic curves. Elliptic curves and its properties has been studied for long since the second or third century. Elliptic curves are important as they appear in lots of areas of mathematics and its applications, for example, they are used in cryptography. One can look at [BM14] for more information about the history of elliptic curves.

In the thesis in Chapter 1 we start with the arithmetic and geometric means over positive real numbers. We define the sequences and show some basic properties as well as the use of AGM for counting digits of π. Namely, we prove the AM-GM inequality for two positive real numbers and prove that both components of AGM have the same limit.

Chapter 2 begins with some definitions and theorems about finite fields. We define quadratic residues and quadratic residue symbol and show that it is a homomorphism. Then we count the number of quadratic residues and show how to compute the quadratic residue symbol. In Section 2.1 we add some graph terminology and finally start with specification of AGM over finite fields. We consider it as a directed graph where there is an edge between two vertices if and only if they are two consecutive elements of AGM sequence. Then we explain some properties of these graphs, see Theorems 26 and 27 and Corollary 28.

In Chapter 3 we describe the case of finite fields with q elements such that $q \equiv 3 \pmod 4$ giving more details than in [Gri+23, Section 1]. We define AGM in this case, define a corresponding directed graph, and describe how it looks like and its components. We also add some examples for better understanding of the results and in the end we count the number of vertices of the graph and the number of components.

Then in Chapter 4 we give some original results for finite fields with q elements such that $q \equiv 5 \pmod 8$. We state that for $q \geq 29$ there is always a component with the cycle hence we can define some infinite AGM for these fields too, see Theorem 44. However, the graph is more complicated in this case and we describe it in detail concluding with Theorem 41 where we describe its components.

Chapter 5 is just a brief and informal chapter about the connection between AGM over finite fields such that $q \equiv 3 \pmod 4$ and elliptic curves. The connection is described in Theorem 51. Finally, we state in Theorem 52 a lower bound of the number of components of the directed graphs of AGM.

Now, we state the contribution of the author in the thesis.

In Chapter 1 we define AGM (Definition 1) more formally than in the article [Gri+23]. We also add a proof of Theorem 4 and mention the sequence 1.1 based on AGM, which converges to π. There was a mistake in this sequence in the older version of article [Gri+23], which we independently fixed. The mistake was fixed in the current version of the article.

In Section 2.1 we generalise the definitions and lemmas with its proofs which were originally formulated only for finite fields $\mathbb{F}_q$ such that $q \equiv 3 \pmod 4$. In Lemma 23, Lemma 24 and Theorem 26 we give more details and slightly generalise results from [Gri+23]. Theorem 27 and Corollary 28 are author's own results.

In Chapter 3 we add the proof of Lemma 29 and formalise the definition of AGM in Definition 31. We also add some details in the proof of Lemma 32 and bring an illustrative example.

The main contribution of the thesis is Chapter 4 where author gives own results for AGM over finite fields with q elements such that $q \equiv 5 \pmod 8$. The intention is to submit these results to some mathematical journal.

In Chapter 5 we briefly introduce elliptic curves and add the definition of an isogeny (Definition 49). We also add one more example of the connection between elliptic curves and AGM. However, we recall that this chapter is informal.

For the purpose of the thesis, namely to count number of components and draw graphs for $\mathbb{F}_q$ where $q \equiv 3 \pmod 4$ or $q \equiv 5 \pmod 8$, a code in Python was written.

1 Arithmetic and geometric means over $\mathbb{R}$

We firstly look at sequences and some properties of arithmetic and geometric means over real numbers.

Definition 1. *Let a, b be positive real numbers, then we define the sequence $AGM_{\mathbb{R}}(a, b) = ((a_n, b_n))_{n=0}^{\infty}$, consisting of arithmetic and geometric means inductively, where $a_0 = a$, $b_0 = b$ and then*

$$a_n := \frac{a_{n-1} + b_{n-1}}{2}, \qquad\qquad b_n : = \sqrt{a_{n-1} b_{n-1}}.$$

Lemma 2. *The sequence $AGM(a, b)$ from Definition 1 is well-defined and*

$$\forall (a_n, b_n) \in AGM(a, b) : a_n > 0, b_n > 0.$$

Proof. We need to show that $\forall (a_n, b_n) \in AGM(a, b) : a_n b_n \geq 0$, so $\sqrt{a_n b_n} \in \mathbb{R}$. This holds if a_n, b_n are positive real numbers, which we will show by induction induction by n. From the definition it holds that a_0 and b_0 are positive real numbers. For the inductive step, suppose a_{n-1}, b_{n-1} are positive real numbers, then $a_n = \frac{a_{n-1}+b_{n-1}}{2} > 0$ as the numerator is a positive real number. As $a_{n-1} b_{n-1} > 0$, b_n is defined and it is a positive real number. □

Now we prove the arithmetic-geometric inequality for two numbers, see [Cve12, p. 9].

Lemma 3. *Let $(a_n, b_n) \in AGM(a, b)$, then $a_n \geq b_n$ for all n natural numbers. This inequality is called arithmetic-geometric mean inequality (AM-GM inequality).*

Proof. Let us take some $(a_n, b_n) \in AGM(a, b), n \in \mathbb{N}$. From Lemma 2 we know, that a_{n-1}, b_{n-1} are positive real numbers, so

$$\begin{aligned} (a_{n-1} - b_{n-1})^2 &\geq 0 \\ a_{n-1}^2 - 2a_{n-1}b_{n-1} + b_{n-1}^2 &\geq 0 \\ a_{n-1}^2 + 2a_{n-1}b_{n-1} + b_{n-1}^2 &\geq 4a_{n-1}b_{n-1} \\ (a_{n-1} + b_{n-1})^2 &\geq 4a_{n-1}b_{n-1}. \\ a_{n-1} + b_{n-1} &\geq 2\sqrt{a_{n-1}b_{n-1}} \\ \frac{a_{n-1} + b_{n-1}}{2} &\geq \sqrt{a_{n-1}b_{n-1}} \\ a_n &\geq b_n. \end{aligned}$$

□

In general, one can show by induction that for any $n - tuple$ of positive real numbers it holds that the arithmetic mean is greater than the geometric mean,

$$\frac{a_1 + a_2 + \cdots + a_n}{n} \geq \sqrt[n]{a_1 a_2 \cdots a_n}.$$

The proof of the general AM-GM inequality is not hard and can be made by mathematical induction[Cve12, p.49]. We will not prove it as for our purpose we will use the inequality only for ordered pairs.

Theorem 4. *Let $AGM(a,b) = ((a_n, b_n))_{n=0}^{\infty}$, then the sequences $(a_n)_{n=0}^{\infty}$ and $(b_n)_{n=0}^{\infty}$ converge. Moreover, they have the same limit.*

Proof. For $n \in \mathbb{N}$, we have the AM-GM inequality $a_n \geq b_n$ from Lemma 3. As a_n, b_n are positive real numbers from Lemma 2, it holds that $b_{n+1} = \sqrt{a_n b_n} \geq \sqrt{b_n b_n} = b_n$ and $a_{n+1} = \frac{a_n + b_n}{2} \leq \frac{a_n + a_n}{2} = a_n$. This means that b_n is non-decreasing sequence and a_n is non-increasing sequence. Then we have

$$a_1 \geq a_2 \geq \cdots \geq a_n \geq b_n \geq b_{n-1} \cdots \geq b_1,$$

so both sequences are bounded by b_1 and a_1. As they are monotonous sequences, they have a limit. Let $\lim_{n\to\infty} a_n = A$, then for given $\varepsilon \in \mathbb{R}$ such that $\varepsilon > 0$ we will find $n_0 \in \mathbb{N} : \forall n \in \mathbb{N}, n \geq n_0 : |a_n - A| < \frac{\varepsilon}{3}$. Then also

$$\begin{aligned} |b_n - A| &= |2 \cdot a_{n+1} - a_n - A| = |2 \cdot a_{n+1} - 2A + A - a_n| \\ &\leq |2 \cdot a_{n+1} - 2A| + |A - a_n| \\ &< \frac{2\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon, \end{aligned}$$

so $\lim_{n\to\infty} b_n = A = \lim_{n\to\infty} a_n$.

□

One can use $AGM_{\mathbb{R}}$ for rapidly computing digits of π. The following algorithm was based on Gauss work and was discovered by Brent and Salamin independently.

Let $\tilde{a}_0 = 1$ and $\tilde{b}_0 = \frac{1}{\sqrt{2}}$. Define

$$\pi_n := \frac{2\tilde{a}_{n+1}^2}{1 - \sum_{i=0}^{n} 2^i (\tilde{a}_i^2 - \tilde{b}_i^2)}, \tag{1.1}$$

where $\tilde{a_n}$, $\tilde{b_n}$ are computed by the AGM. Then π_n increases monotonically to π. We won't prove it as the proof needs some non-trivial results from mathematical analysis. One can find the proof in [BBB87, p.48] with the theory needed on previous pages.

If we start with $(a_0, b_0) = (\sqrt{2}\tilde{a}_0, \sqrt{2}\tilde{b}_0) = (\sqrt{2}, 1)$, we can show by induction by n, that for all non-negative integers n, $a_n = \sqrt{2}\tilde{a}_n$, $b_n = \sqrt{2}\tilde{b}_n$. It holds for $n = 0$ from the definition. Then suppose that it holds for some $n-1$ such that $n \in \mathbb{N}$. We have

$$a_n = \frac{a_{n-1} + b_{n-1}}{2} = \frac{\sqrt{2} \cdot \tilde{a}_{n-1} + \sqrt{2} \cdot \tilde{b}_{n-1}}{2} = \sqrt{2} \cdot \tilde{a}_n$$

$$b_n = \sqrt{a_{n-1} b_{n-1}} = \sqrt{\sqrt{2} \cdot \tilde{a}_{n-1} \cdot \sqrt{2} \cdot \tilde{b}_{n-1}} = \sqrt{2} \cdot \tilde{b}_n.$$

Therefore we can rewrite the sequence π_n as following:

$$\pi_n = \frac{2\tilde{a}_{n+1}^2}{1 - \sum_{i=0}^{n} 2^i (\tilde{a}_i^2 - \tilde{b}_i^2)} = \frac{a_{n+1}^2}{1 - \sum_{i=0}^{n} 2^{i-1} (a_i^2 - b_i^2)}.$$

That is the formula stated in [Gri+23, p. 1]

2 Finite fields and arithmetic-geometric means

We recall some facts about finite fields. We will follow [Lan05, Section V.5] and [Sta22, p.49-51]. We will denote $\mathbb{F}_q$ the finite field with q elements.

- There exists a finite field $\mathbb{F}_q$ with q elements if and only if $q = p^n$, where p is a prime number and $n \in \mathbb{N}$.
- We have $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$. We will use this to represent elements of $\mathbb{F}_p$ as elements from the set $\{0, \pm 1, \pm 2, \cdots, \pm \frac{p-1}{2}\}$.
- The finite field $\mathbb{F}_{p^n}$, $n > 1$, is constructed in the following way $\mathbb{F}_{p^n} \simeq \mathbb{F}_p[x]/f_n$, where $f_n \in \mathbb{F}_p[x]$ is an irreducible polynomial of degree n.
- The multiplicative group of $\mathbb{F}_q$ - $\mathbb{F}_q^\times$ is cyclic and $|\mathbb{F}_q^\times| = q - 1$.

In the whole chapter we will consider a prime $p \neq 2$. For this fields we know, that $0 \neq 2 \in \mathbb{Z}/p\mathbb{Z}$, so $2 \in \mathbb{F}_q$ hence $2^{-1} \in \mathbb{F}_q$ too.

Definition 5. *Let $x \in \mathbb{F}_q^\times$, then x is a quadratic residue if there exists $y \in \mathbb{F}_q$ such that*

$$y^2 = z.$$

If there is not such y, x is a quadratic non-residue. We will also call quadratic residues squares and non-residues non-squares.

Definition 6. *Let $\phi_q \colon \mathbb{F}_q^\times \to \mathbb{F}_q^\times$ such that for every $a \in \mathbb{F}_q$ the following holds:*

$$\phi_q(a) = \begin{cases} 1 & \textit{if } a \textit{ is a quadratic residue}; \\ -1 & \textit{if } a \textit{ is a quadratic non-residue.} \end{cases}$$

Lemma 7. *Let $a \in \mathbb{F}_q^\times$ and let g be the generator of $\mathbb{F}_q^\times$. Let $d \in \mathbb{N}$ such that $d \mid q - 1$.*

- *Then $a = b^d$ where $b \in \mathbb{F}_q^\times$ if and only if $a = g^n$, such that $d \mid n$.*
- *Let $D = \{a \in \mathbb{F}_q^\times : a = b^d, b \in \mathbb{F}_q^\times\}$, then $|D| = \frac{q-1}{d}$.*

Proof. If $a = b^d$, then as $b \in \mathbb{F}_q^\times$ we can write $b = g^m,\ m \in \mathbb{N}$ and

$$a = b^d = (g^m)^d = g^{md}.$$

If $n = md$, let $b = g^m$, then $b \in \mathbb{F}_q^\times$ and then

$$a = g^n = g^{md} = (g^m)^d = b^d.$$

Hence,

$$D = \{g^{md} \mid m \in \mathbb{N}\} = \{g^{md} \mid md \leq q - 1\}$$

as $\mathbb{F}_q^\times$ is a cyclic group and

$$g^{m_1 d} \neq g^{m_2 d} \qquad \text{where} \qquad m_1 < m_2 \leq \frac{q-1}{d}.$$

If $g^{m_1 d} = g^{m_2 d}$, then $g^{d(m_2 - m_1)} = 1$. As $d(m_2 - m_1) < q - 1$, it is a contradiction as the order of g must be $q - 1$. Hence, $|D| = \frac{q-1}{d}$. □

Corollary 8. *Let $a \in \mathbb{F}_q^\times$ and let g be the generator of $\mathbb{F}_q^\times$.*

(a) If $a = g^n$, then $\phi_q(a) = (-1)^n$.

(b) ϕ_q is a homomorphism.

Proof. To prove (a), we note that $\phi_q(a) = 1$ if and only if a is a square which by Lemma 7 happens if and only if n is even. For (b), let $a, b \in \mathbb{F}_q^\times$. Then we can write $a = g^n$ and $b = g^m$ for some natural numbers m, n. Then

$$\phi_q(a)\phi_q(b) = (-1)^n(-1)^m = (-1)^{m+n} = \phi_q(ab).$$

□

Corollary 9. *Let $a \in \mathbb{F}_q^\times$, then a^{-1} is quadratic residue if and only if a is quadratic residue.*

Proof. We can write $1 = 1^2$ and compute

$$1 = \phi_q(1) = \phi_q(a \cdot (a^{-1})) = \phi_q(a) \cdot \phi_q(a^{-1}),$$

which is equivalent to a^{-1} is quadratic residue if and only if a is quadratic residue. □

Corollary 10. *In $\mathbb{F}_q^\times$, the number of squares and non-squares is the same.*

Proof. Let $D = \{a \in \mathbb{F}_q^\times \mid a = b^2,\ b \in \mathbb{F}_q^\times\}$, then the number of squares is $|D| = \frac{q-1}{2}$ by Lemma 7. Hence, the number of non-squares if $q - 1 - \frac{q-1}{2} = \frac{q-1}{2}$. □

Theorem 11. *(Lagrange) Let $a \in \mathbb{F}_q^\times$. Then $a^{|\mathbb{F}_q^\times|} = 1$.*

This theorem is a consequence of the Lagrange theorem about groups. For the proof one can see [Lan05, Proposition 2.2, Proposition 4.1].

Corollary 12. *Let $a \in \mathbb{F}_q^\times$. Then $a^{\frac{|\mathbb{F}_q|}{2}}$ is equal to 1 or -1.*

Proof. $a^{\frac{|\mathbb{F}_q|}{2}}$ is a root of the polynomial $x^2 - 1$, which has roots ±1. □

Theorem 13. *Let $a \in \mathbb{F}_q^\times$. Then*

$$\phi_q(a) = a^{\frac{|\mathbb{F}_q|}{2}} = a^{\frac{q-1}{2}}.$$

Proof. Let g be a generator of $\mathbb{F}_q^\times$ and write $a = g^n$. Then $\phi_q(a) = (-1)^n$ by Corollary 8(a). Also, $a^{\frac{q-1}{2}} = g^{n\frac{q-1}{2}} = (-1)^n$ because $g^{\frac{q-1}{2}}$ is equal to ±1 by Corollary 12, and since g is a generator of $\mathbb{F}_q^\times$ and $\frac{q-1}{2} < q - 1$, we have that $g^{\frac{q-1}{2}} = -1$. Thus, $\phi_q(a) = (-1)^n = a^{\frac{q-1}{2}}$.

□

2.1 AGM as a directed graph over finite fields

Recall that in the whole section we will consider finite fields $\mathbb{F}_q$ such that $q = p^n$ for a prime $p \neq 2$ and a natural number n. Also, recall that $0 \neq 2 \in \mathbb{F}_q$, so $2^{-1} \in \mathbb{F}_q$. We recall some facts about graph theory from [MNK09, p. 111 - 118].

Definition 14. *A graph G is an ordered pair $G = (V, E)$ such that V is a non-empty set and E is a set of 2 - element sets $\{u, v\}$ such that $u \neq v$ and $u, v \in V$. When E is a set of ordered pairs (u, v), we call G a directed graph. We will call elements of the set V vertices and elements of the set E edges.*

Definition 15. *An isomorphism f between graphs $G = (V, E)$ and $G' = (V', E')$ is the mapping*

$$f\colon V \to V',$$

such that f is a bijection and

$$\{x, y\} \in E \text{ if and only if } \{f(x), f(y)\} \in E'.$$

If $G = G'$ we call f an automorphism.

Definition 16. *Let $H = (V_H, E_H)$ and $G = (V_G, E_G)$ be graphs. Then H is a subgraph of G if $V_H \subset V_G$ and $E_H \subset E_G$.*

Definition 17. *A path in the graph is a subgraph such that $V = \{v_1, \dots, v_n\}$ and $E = \{\{v_{i-1}, v_i\}; i \in \mathbb{N}\}$ or $E = \{(v_{i-1}, v_i); i \in \mathbb{N}\}$ if G is directed.*

Definition 18. *Consider a directed graph $G = (V, E)$. We will construct an undirected graph $G' = (V', E')$ such that*

$$V' = V \text{ and } \{u, v\} \in E' \iff (u, v) \in E \text{ or } (v, u) \in E.$$

We call the graph G weakly connected if G' is connected, so for all $u, v \in V'$ there exists a path connecting u and v.

Definition 19. *A component of directed graph is every maximal weakly connected subgraph.*

Definition 20. *A directed cycle of directed graph G is a subgraph such that $V = \{v_1, v_2, \dots, v_n\}$ and $E = \{(v_1, v_2), (v_2, v_3), \dots, (v_{n-1}, v_n), (v_n, v_1)\}$.*

Definition 21. *Let u, v be vertices in an oriented graph. Then we will call u a parent of v if there is an edge $u \to v$. We will call u a son of v if there is an edge $v \to u$.*

Now we are able to define a directed graph which will represent the AGM sequences in finite fields.

Definition 22. *Let us have a directed graph $\mathcal{J}_{\mathbb{F}_q} = (V, E)$ where $V = \{(a, b) \in \mathbb{F}_q^{\times 2} \mid \phi_q(ab) = 1, a \neq \pm b\}$ and $(a, b) \to (c, d)$ is an edge if and only if*

$$c = \frac{a+b}{2} \qquad\qquad d^2 = ab.$$

We will denote the components of $\mathcal{J}_{\mathbb{F}_q}$ as J_i and the number of components $d(\mathbb{F}_q)$.

Lemma 23. *Let (a,b) be a vertex of $\mathcal{J}_{\mathbb{F}_q}$. Then (a,b) has a parent if and only if a^2-b^2 is a square. Furthermore, if (a,b) has a parent (A,B) then the other parent is (B,A) and these are the only parents of (a,b). Namely, the parents of (a,b) are $(a+S,a-S)$ and $(a-S,a+S)$, such that $S^2=a^2-b^2$.*

Proof. Suppose (a,b) has some parent (A,B). We have $A+B=2a$ and $AB=b^2$. Suppose the polynomial $x^2-2ax+b^2=(x-A)(x-B)$. Then A and B are roots of $x^2-2ax+b^2$ and as it has exactly two roots, there are exactly two parents, (A,B) and (B,A). Furthermore, $(A-B)^2=4a^2-4b^2$, and so $\phi_q(a^2-b^2)=1$.

On the other hand, if $\phi_q(a^2-b^2)=1$, then there exist $S\in\mathbb{F}_q$ such that

$$S^2=a^2-b^2\neq 0.$$

Hence $S\neq 0$ and we can consider the vertex $(a+S,a-S)$ as $a+S\neq\pm(a-S)$ and

$$\phi_q\left((a+S)(a-S)\right)=\phi_q(a^2-S^2)=\phi_q(a^2-(a^2-b^2))=\phi_q(b^2)=1.$$

Consider a son of this vertex, then we have

$$\frac{(a+S)+(a-S)}{2}=a$$

and

$$(a+S)(a-S)=b^2,$$

hence $(a+S,a-S)$ is a parent of (a,b). □

Lemma 24. *Every $\alpha\in\mathbb{F}_q^\times$ induces a distinct graph automorphism*

$$\begin{aligned}\varphi_\alpha\colon \mathcal{J}_{\mathbb{F}_q}&\to\mathcal{J}_{\mathbb{F}_q}\\ (a,b)&\mapsto(\alpha a,\alpha b).\end{aligned}$$

Proof. Consider the edge $(a,b)\to(c,d)$ and the mapping φ_α. Then

- $\phi_q(\alpha a\alpha b)=\phi_q(ab)=1$
- $\alpha a\pm\alpha b=\alpha(a\pm b)\neq 0$ as $\alpha\neq 0$ and $a\pm b\neq 0$. So, $\alpha a\neq\pm\alpha b$,

so it maps vertices of the graph to vertices. What's more, $\frac{\alpha a+\alpha b}{2}=c\cdot\alpha$ and $\alpha a\alpha b=\alpha^2d^2$, so there is an edge $(\alpha a,\alpha b)\to(\alpha c,\alpha d)$, so it preserves edges. φ_α is injective as $\alpha a=\alpha b$ means $a=b$. Number of vertices (and edges) is finite hence φ_α is surjective and it is an automorphism.

Finally we will show the distinction of automorphisms. If $\varphi_\alpha=\varphi_\beta$ then e.g. $\varphi_\alpha(1,\cdot)=\varphi_\beta(1,\cdot)$ which implies $\alpha\cdot 1=\beta\cdot 1$, so $\alpha=\beta$. □

Lemma 25. $G=\{\varphi_\alpha\mid\alpha\in\mathbb{F}_q^\times\}\simeq\mathbb{F}_q^\times$ *is a group.*

This lemma can be proved in the same way as Lemma 24.

Theorem 26. *Let N_n denote the number of components of $\mathcal{J}_{\mathbb{F}_q}$ with n vertices. Then $(q-1)|nN_n$. Moreover, if in the component is an oriented cycle of the length c and N_c denotes the number of components with an oriented cycle of the length c, then $(q-1)|cN_c$*

Proof. Consider G, the group of graph automorphisms φ_α such that $\alpha \in \mathbb{F}_q^\times$. This group acts on the $\mathcal{J}_{\mathbb{F}_q}$, it permutes the vertices of components which have the same number of vertices and in the graph $\mathcal{J}_{\mathbb{F}_q}$ there is nN_n these vertices. Every orbit of a *vertex* has size $q-1$ as this automorphisms are distinct. Hence, $(q-1)|nN_n$. Furthermore, the vertex from the cycle has to be mapped to the vertex from the cycle. It implies that $q-1$ divides the number of all vertices which are in the cycles of the same length. Hence, $q-1 \mid cN_c$. □

We can make one more observation. We will call the vertex (a,b) a square vertex if a and b are both squares. The other vertices are non-square.

Theorem 27.

- *If the edge in the component connects two square vertices, then all the vertices in the component are square nodes.*
- *If the edge in the component connects two non-square vertices, then all the vertices in the component are non-square.*
- *If the edge in the component connects square vertex and non-square vertex, then in the component the square and non-square vertices alternate, so there is no edge in this component connecting two square vertices or two non-square vertices.*

Proof. Consider the path $(a,b) \to (c,d) \to (e,f)$ and suppose (a,b) is a square vertex, so $a = A^2$ and $b = B^2$. Then

$$c = \frac{A^2+B^2}{2} \qquad\qquad d^2 = A^2B^2,$$

which means that either $d = AB$ or $d = -AB$ which gives

$$e = \frac{c+d}{2} \implies e = \frac{A^2+B^2+2AB}{4} = \left(\frac{A+B}{2}\right)^2$$

or

$$e = \frac{A^2+B^2-2AB}{4} = \left(\frac{A-B}{2}\right)^2.$$

Then by Definition 22, f is a square. Hence (e,f) is a square vertex and we see, that every second vertex is also a square vertex. Now suppose (a,b) is non-square vertex, then let us take $\alpha \in \mathbb{F}_q^\times$ a non-square and consider the graph automorphism φ_α. Then

$$(a,b) \to (c,d) \to (e,f) \qquad \mapsto \qquad \varphi_\alpha((a,b)) \to \varphi_\alpha((c,d)) \to \varphi_\alpha((e,f))$$

and as $\varphi_\alpha((a,b)) = (\alpha a, \alpha b)$, $\phi_q(\alpha a) = (-1)(-1) = 1$, so $\varphi_\alpha((a,b))$ is a square vertex. Then $\varphi_\alpha((e,f))$ is a square vertex and as $\varphi_\alpha((e,f)) = (\alpha e, \alpha f)$, $\phi_q(e) = -1$. So, the theorem holds.

□

Corollary 28. *Let us consider a component of graph $\mathcal{J}_{\mathbb{F}_q}$ with the directed cycle. Let c be the number of nodes in the cycle of the component. If c is odd, then there is a component made of non-square vertices and another component made of square vertices, so N_c is even.*

3 AGM over $\mathbb{F}_q$, where $q \equiv 3 \pmod 4$

In the whole chapter we will work with finite fields $\mathbb{F}_q$, with $q \equiv 3 \pmod 4$.

Lemma 29. *When $q \equiv 3 \pmod 4$, -1 is a quadratic non-residue in $\mathbb{F}_q$.*

Proof. We count $\phi_q(-1) = (-1)^{\frac{q-1}{2}} = -1$ as $q \equiv 3 \pmod 4$, so $\frac{q-1}{2} \equiv 1 \pmod 2$. □

Lemma 30. *Let $\varepsilon \in \{\pm 1\}$, $x \in \mathbb{F}_q^\times$. If $\phi_q(x) = 1$, then $\exists! y \in \mathbb{F}_q^\times$ such that $y^2 = x$ and $\phi_q(y) = \varepsilon$. We will denote ${}_\varepsilon\sqrt{x} = y$.*

Proof. Suppose $\phi_q(x) = 1$. Then the polynomial $p(t) = t^2 - x$ has solution $\pm y$. As -1 is not a square, exactly one from $\{y, -y\}$ is square so the other is non-square. □

Definition 31. *Let $a, b \in \mathbb{F}_q^\times$ such that $\phi_q(ab) = 1$ and $a \neq \pm b$. We define a sequence $AGM_{\mathbb{F}_q}(a, b) = ((a_n, b_n))_{n=0}^\infty$ such that $a_0 = a$, $b_0 = b$ and*

$$a_n = \frac{a_{n-1} + b_{n-1}}{2} \qquad \varepsilon = \phi_q(a_n) \qquad b_n = {}_\varepsilon\sqrt{a_{n-1}b_{n-1}}.$$

Lemma 32. *$AGM_{\mathbb{F}_q}(\cdot, \cdot)$ is an infinite sequence consisting of $(a_n, b_n) \in {\mathbb{F}_q^\times}^2$, such that $a_n \neq \pm b_n$.*

Proof. We need to show, that for all non-negative integers n it holds that $\phi_q(a_n b_n) = 1$, so the sequence can continue, hence to be infinite and that $a_n \neq \pm b_n$ and $(a_n, b_n) \in {\mathbb{F}_q^\times}^2$.

We will show it by induction. From the definition of a_0, b_0 we know that it holds. Suppose it holds for $n - 1$, we want to show, that it also holds for n. From the definition of a_n and b_n we have

$$a_n = \frac{a_{n-1} + b_{n-1}}{2}$$

$$b_n = {}_\varepsilon\sqrt{a_{n-1}b_{n-1}}$$

and as $a_{n-1} \neq b_{n-1}$, $a_n, b_n \in \mathbb{F}_q^\times$. If $a_n = \pm b_n$ then $0 = a_n^2 - b_n^2 = \frac{(a_{n-1}+b_{n-1})^2}{4} - a_{n-1}b_{n-1} = \frac{(a_{n-1}-b_{n-1})^2}{4}$ which is a contradiction as $a_{n-1} \neq b_{n-1}$.

Finally, $\phi_q(a_n b_n) = \phi_q(a_n) \cdot \phi_q(b_n) = \varepsilon \cdot \phi_q({}_\varepsilon\sqrt{a_{n-1}b_{n-1}}) = \varepsilon^2 = 1$. □

Example. Let us have a look at $q = 3$. We have $\mathbb{F}_q^\times = \{1, -1\}$ so there is no (a, b) such that $a \neq \pm b$.

Example. Consider $q = 11$. Then,

$$\begin{aligned} AGM_{\mathbb{F}_{11}}(4,1) = (&\overline{(4,1),(8,2),(5,4),(10,8),(9,5),(7,10),(3,9),}\\ &\overline{(6,7),(1,3),(2,6)}) \end{aligned}$$

$$\begin{aligned} AGM_{\mathbb{F}_{11}}(1,4) = (&(1,4),\overline{(8,2),(5,4),(10,8),(9,5),(7,10),(3,9),}\\ &\overline{(6,7),(1,3),(2,6),(4,1)}) \end{aligned}$$

$$AGM_{\mathbb{F}_{11}}(9,1) = (\overline{(9,1),(5,3),(4,9),(1,5),(3,4)})$$

$$AGM_{\mathbb{F}_{11}}(1,9) = ((1,9),\overline{(5,3),(4,9),(1,5),(3,4),(9,1)}),$$

where the line above a sequence means it is a repeating period.

Now, let us have a look on the graph of $\mathcal{J}_{\mathbb{F}_q}$. We will see, that the components have a special shape, which is not a coincidence.

Example. For $q = 11$, $\mathcal{J}_{\mathbb{F}_q}$ consists of 3 connected components:

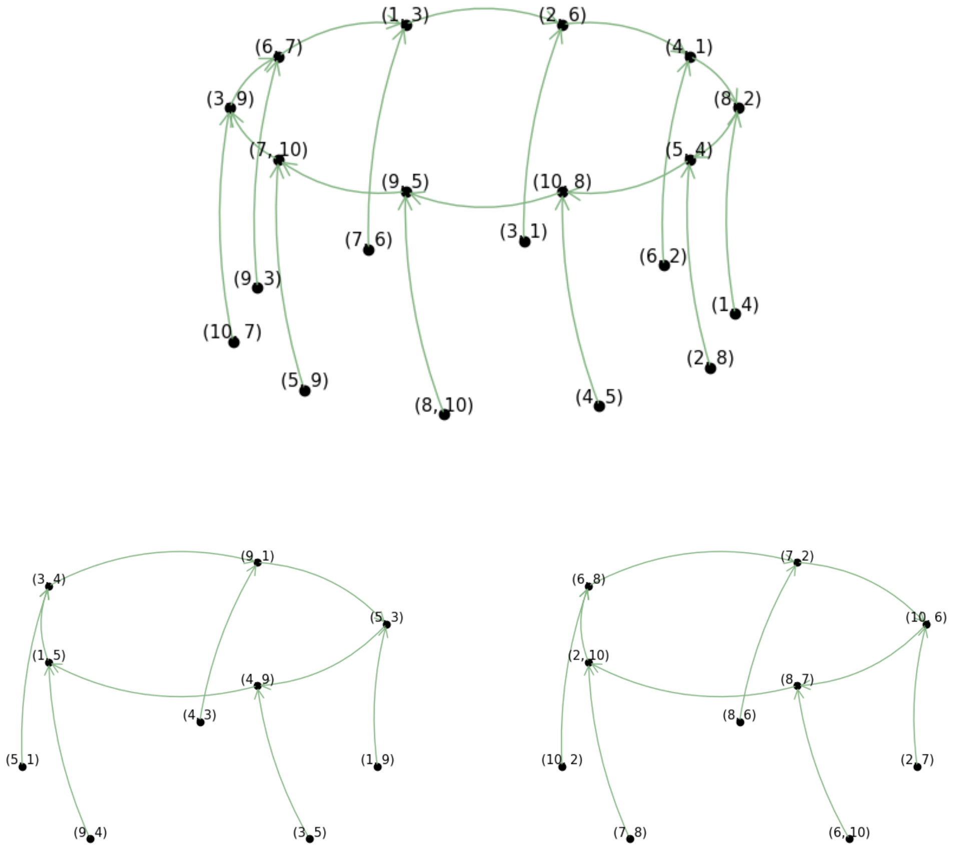

Figure 3.1 Components of $\mathcal{J}_{\mathbb{F}_{11}}$

Theorem 33. *(1) $\mathcal{J}_{\mathbb{F}_q}$ has $(q-1)(q-3)/2$ vertices.*

(2) Every component of $\mathcal{J}_{\mathbb{F}_q}$ consists of the directed cycle and there lead an oriented path of the length 1 to every vertex of that cycle. There are no other cycles (even undirected).

Proof. (1) We compute the number of vertices. Consider a vertex (a, b). There are $q - 1$ choices for a, as $a \in \mathbb{F}_q^\times$. We need $b \neq \pm a$ and $b \in \mathbb{F}_q^\times$ which is $q - 3$ choices. Let $B = \{b \in \mathbb{F}_q^\times \mid b \neq \pm a\}$ and let us take $b \in B$. We need $\phi_q(b) = \phi_q(a)$ and as we know from Lemma 30 either $\phi_q(b) = \phi_q(a)$ or $\phi_q(-b) = \phi_q(a)$. So we have $\frac{q-3}{2}$ choices for b. All in all, there is $\frac{(q-1)(q-3)}{2}$ vertices.

(2) Let (a, b) be a vertex of some component J of $\mathcal{J}_{\mathbb{F}_q}$. As we have shown in Lemma 32, the sequence $AGM_{\mathbb{F}_q}(a, b)$ is infinite, but we have only finitely many vertices, so there is a directed cycle in J. Now, suppose (a, b) is in the directed cycle. Let us consider (A, B) as the parent of (a, b), which is in the cycle too. Then from Lemma 23 (a, b) has another parent (B, A). As (A, B) is in the cycle, it has some parent, so $A^2 - B^2 = -(B^2 - A^2)$ is a square which implies $(B^2 - A^2)$ is not a square hence (B, A) doesn't have parents.

□

When we draw the component of $\mathcal{J}_{\mathbb{F}_q}$ in the plane, it looks like bell head with tentacles. Hence the components of $\mathcal{J}_{\mathbb{F}_q}$ are playfully called jellyfishes and the graph $\mathcal{J}_{\mathbb{F}_q}$ is jellyfish swarm in [Gri+23].

Example. Recall the notation $\mathrm{d}(\mathbb{F}_q)$ from Definition 22. Here is a table of some numbers of components for $q \equiv 3 \pmod 4$ prime numbers.

q	3	7	11	19	23	31	43	47	59	67	71	79
$d(\mathbb{F}_q)$	0	1	3	8	5	10	7	4	7	30	25	18
q	83	103	107	127	131	139	151	163	167	179	191	199
$d(\mathbb{F}_q)$	6	41	9	54	46	33	45	38	11	14	14	101
q	211	223	227	239	251	263	271	283	307	311	331	347
$d(\mathbb{F}_q)$	120	18	12	40	31	17	34	35	32	33	117	19

Table 3.1 Table of numbers of components $d(\mathbb{F}_q)$ for some $q \equiv 3 \pmod 4$

4 AGM over $\mathbb{F}_q$, where $q \equiv 5 \pmod 8$

In the whole chapter we suppose $q = p^n$ for a prime p and natural number n and $q \equiv 5 \pmod 8$.

Lemma 34. *When $q \equiv 5 \pmod 8$, then*

- *the number -1 is a quadratic residue. Suppose $i \in \mathbb{F}_q$ such that $i^2 = -1$. Then i is a quadratic non-residue.*
- *the number 2 is a quadratic non-residue.*

Proof. We compute $\phi_q(-1) = (-1)^{\frac{q-1}{2}} = 1$ as $q \equiv 1 \pmod 4$ so $\frac{q-1}{2} \equiv 0 \pmod 2$. Now we can compute $\phi_q(i) = i^{\frac{q-1}{2}} = (i^2)^{\frac{q-1}{4}} = (-1)^{\frac{q-1}{4}} = -1$ as $q \equiv 5 \pmod 8$ so $\frac{q-1}{4} \equiv 1 \pmod 2$.

It remains to compute $\phi_q(2)$. We can write $(i+1)^2 = 2i$, hence

$$1 = \phi_q(2i) = \phi_q(2)\phi_q(i) = -\phi_q(2),$$

so $\phi_q(2) = -1$. □

Lemma 35. *Let (a, b) be a vertex of $\mathcal{J}_{\mathbb{F}_q}$ such that $\phi(ab) = 1$. Then (a, b) has either 2 or 0 sons.*

Proof. Suppose (a, b) has some son (A, B), so $\phi(AB) = 1$ which implies that $\phi(A \cdot (-B)) = 1$, because -1 is a square. Therefore $(A, -B)$ is the other son. The equation $x^2 - ab = 0$ has only this two solutions (B and $-B$). □

Recall that (a, b) has either 2 or 0 parents from Lemma 23.

Theorem 36. *Let E be the set of edges of $\mathcal{J}_{\mathbb{F}_q}$. If $E \neq \emptyset$, then there is a cycle in $\mathcal{J}_{\mathbb{F}_q}$.*

Proof. Consider the edge $(a, b) \to (A, B)$ from $\mathcal{J}_{\mathbb{F}_q}$. Then the next son of (a, b) is $(A, -B)$. Consider the pairs (c, d) and (e, f) (which do not have to be vertices of $\mathcal{J}_{\mathbb{F}_q}$) such that

$$c = \frac{A+B}{2} \qquad d^2 = AB$$
$$e = \frac{A-B}{2} \qquad f^2 = -AB.$$

Then either $d = if$ or $d = -if$, $i \in \mathbb{F}_q$: $i^2 = -1$. Suppose $d = if$ and let us compute

$$\phi_q(cdef) = \phi_q(ce)\phi_q(if^2) = \phi_q\left(\frac{A^2 - B^2}{4}\right) \cdot (-1) = \phi_q\left(\left(\frac{a-b}{4}\right)^2\right) \cdot (-1) = -1.$$

We obtain the same if $d = -if$. As $cdef$ is a quadratic non-residue, exactly one of cd and ef is a quadratic residue, so exactly one of (c, d), (e, f) is a vertex. So, we can make the path longer and continue analogously for either (A, B) or $(A, -B)$, not both. As we can continue like this in every step and the number of vertices is finite, there must be a cycle. □

Theorem 37. *Let C be the cycle in $\mathcal{J}_{\mathbb{F}_q}$, then there are more than two vertices in C.*

Proof. Consider that in $\mathcal{J}_{\mathbb{F}_q}$ there is a cycle with only two vertices, so there are edges $(a,b) \to (c,d)$ and $(c,d) \to (a,b)$. Then, it must hold that

$$\begin{aligned} c &= \frac{a+b}{2}, & d^2 &= ab, \\ a &= \frac{c+d}{2}, & b^2 &= cd. \end{aligned}$$

Then we get

$$\begin{aligned} a+c &= \frac{a+b+c+d}{2} & \implies && a+c &= b+d, \\ b^2d^2 &= abcd & \implies && ac &= bd. \end{aligned}$$

Let us denote $A = a+c = b+d$ and $B = ac = bd$ and consider a polynomial $p(x) \in \mathbb{F}_q[x]$, such that $p(x) = x^2 - Ax + B$. Then $p(x) = (x-a)(x-c) = (x-b)(x-d)$ and as we work with a finite field, it must have at most 2 roots. Hence, either $a = b, c = d$ or $a = d, b = c$.

Recall Definition 22, then $a = b$ is a contradiction, hence suppose $a = d, b = c$. So, we have an edge $(a,b) \to (b,a)$ which gives us $b = \frac{a+b}{2}$, hence $b = a$ which is again a contradiction. □

Corollary 38. *Let $C \subset V$ be the set of vertices in a cycle. Then every $c \in C$ has exactly 2 sons, one is a part of the cycle and the other does not have any son.*

Proof. Suppose $c_1 \in C$, it has exactly two sons, c_2 and d_2. Suppose c_2 is in the cycle, so it has exactly two sons, $c_3 = (a_c, b_c)$ and c_3'. If d_2 had a son $d_3 = (a_d, b_d)$, then

$$\phi_q(a_cb_ca_db_d) = \phi_q(a_cb_c)\phi(a_db_d) = 1 \cdot 1 = 1,$$

which would be a contradiction as we know from the proof of Theorem 36 that $\phi_q(a_cb_ca_db_d) = -1$. □

Theorem 39. *Consider the path $(a,b) \to (c,d) \to (e,f)$, then there is another path $(g,h) \to (d,c) \to (e,f)$ and exactly one of the vertices $(a,b),(g,h)$ has some parents.*

Proof. From Lemma 23 we know, that

$$\begin{aligned} a &= c - x & b &= c + x & &\text{where } x^2 = c^2 - d^2 \\ g &= d - y & h &= d + y & &\text{where } y^2 = d^2 - c^2, \end{aligned}$$

which means $x^2 = -y^2$, so $x = iy$ or $x = -iy$ and $\phi_q(xy) = -1$. We can compute

$$\begin{aligned} \phi_q((a^2-b^2)(g^2-h^2)) &= \phi_q\left(\left((c-x)^2 - (c+x)^2\right)\left((d-y)^2 - (d+y)^2\right)\right) \\ &= \phi_q(4cx \cdot 4dy) = \phi_q(16)\phi_q(cd)\phi_q(xy) = \phi_q(xy) \\ &= -1, \end{aligned}$$

which implies that either $(a^2 - b^2)$ or $(g^2 - h^2)$ is a quadratic residue, so either (a,b) or (g,h) has parents and the other does not have. □

Corollary 40. *Let $C \subset V$ be the set of vertices in a cycle. Then every $c \in C$ has exactly 2 parents, one is the part of the cycle C and the other is not part of any cycle.*

Proof. Suppose $c \in C$ and recall Theorem 37 the length of cycle is at least 3, so we can consider the path $c_1 \to c_2 \to c$ of vertices from the cycle. As c has another parent $c_3{}'$, by Theorem 39 we know there is another path$c_1{}' \to c_2{}' \to c$, hence exactly one of the vertices c_1 and c'_1 has parents. As $c_1 \in C$, it has parents, hence c'_2 does not have parents.

□

When we join all the previous claimings about $\mathcal{J}_{\mathbb{F}_q}$ together, we obtain the following theorem.

Theorem 41. *Every component of $\mathcal{J}_{\mathbb{F}_q}$ is made either of single vertex or of the cycle $c_1 \to c_2 \to \cdots \to c_n$, vertices u_i such that $c_i \to u_{i+1}$, vertices v_i such that $v_i \to c_i$ and $v_i \to u_i$ and vertices w_i such that $w_i \to v_i$, $w_{n+i} \to v_i$ and vertices x_i such that $w_i \to x_i$, $w_{n+i} \to x_i$. These are all edges and vertices of the component of $\mathcal{J}_{\mathbb{F}_q}$.*

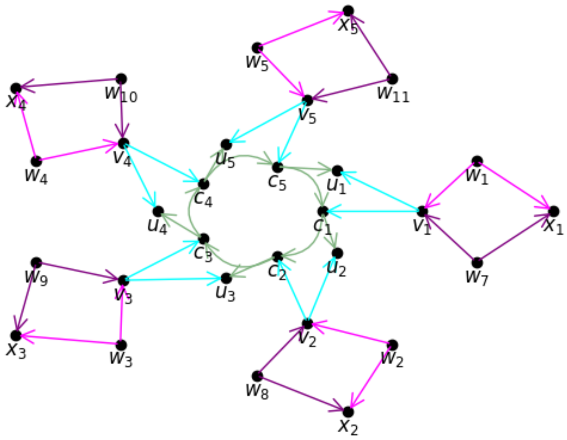

Figure 4.1 A general nontrivial component of $\mathcal{J}_{\mathbb{F}_q}$ such that $q \equiv 5 \pmod 8$

Definition 42. *Let $q \equiv 5 \pmod 8$ and $(a,b) \in \mathbb{F}_q^{\times 2}$ such that $\phi_q(ab) = 1$ and there exist $c, d \in \mathbb{F}_q^{\times}$ such that*

$$c = \frac{a+b}{2}, \qquad d^2 = ab, \qquad \phi_q(cd) = 1.$$

Let C be the component of $\mathcal{J}_{\mathbb{F}_q}$ which contains the vertex (a,b) and suppose it contains a cycle of the length n. Then, using the notation from Theorem 41, without loss of generality, $(a,b) \in \{c_1, v_1, w_1, w_{1+n}\}$. Hence we define an infinite *arithmetic-geometric mean sequence*

$$AGM_{\mathbb{F}_q}(a,b) = \begin{cases} (\overline{c_1, c_2, \ldots, c_n}) & \text{if } (a,b) = c_1, \\ (v_1, \overline{c_1, c_2, \ldots, c_n}) & \text{if } (a,b) = v_1, \\ (w_1, v_1, \overline{c_1, c_2, \ldots, c_n}) & \text{if } (a,b) = w_1, \\ (w_{1+n}, v_1, \overline{c_1, c_2, \ldots, c_n}) & \text{if } (a,b) = w_{1+n}. \end{cases}$$

Recall that we denote the repeating period by line over elements of sequence.

Theorem 43. *If $q > 13$ and $q \equiv 5 \pmod 8$, then there is at least one nontrivial component (component with some edges).*

Proof. Recall Theorem 36, it suffices to prove that the set of edges is non-empty. This holds if and only if in $\mathcal{J}_{\mathbb{F}_q}$ there is a vertex (a,b) which has parents, hence $\phi_q(a^2 - b^2) = 1$ by Lemma 23. Also notice, that if (a,b) is a vertex, then $a^2 - b^2 = (a-b)(a+b) \neq 0$.

Suppose g is the generator of the group $\mathbb{F}_q^\times$. Then g is not a square and order of g is $q-1$. Then $g^{\frac{q-1}{2}} = -1$ by Theorem 13.

As $q > 13$, $g^2, g^4, g^6 \notin \{1, -1\}$ hence we can consider vertices $(g^2, 1)$, $(g^4, 1)$, $(g^6, 1)$. If any of

$$(g^2)^2 - 1^2 = g^4 - 1, \qquad (g^4)^2 - 1^2 = g^8 - 1, \qquad (g^6)^2 - 1^2 = g^{12} - 1$$

is a square, we found the vertex with parents, so we finished. Suppose none of them is a square, then

$$\begin{aligned} -1 &= \phi_q(g^8 - 1) = \phi_q((g^4 - 1)(g^4 + 1)) = \phi_q(g^4 - 1)\phi_q(g^4 + 1) \\ &= -\phi(g^4 + 1) \implies \phi(g^4 + 1) = 1 \\ -1 &= \phi_q(g^{12} - 1) = \phi_q((g^4 - 1)(g^8 + g^4 + 1)) = \phi_q(g^4 - 1)\phi_q(g^8 + g^4 + 1) \\ &= -\phi_q(g^8 + g^4 + 1) \implies \phi_q(g^8 + g^4 + 1) = 1, \end{aligned}$$

so we can write $a^2 = g^4 + 1 \neq 0$ and $b^2 = g^8 + g^4 + 1 \neq 0$. Then

$$\begin{aligned} a^4 - b^2 &= g^8 + 2g^4 + 1 - (g^8 + g^4 + 1) = g^4 \\ a^4 - g^4 &= b^2. \end{aligned}$$

We can see that $\phi_q(a^2 g^2) = 1$ as they are both squares. Furthermore, $a^2 \neq \pm g^2$ as $0 \neq b^2 = a^4 - g^4 = (a^2 - b^2)(a^2 + b^2)$. Hence, (a^2, g^2) is the vertex of $\mathcal{J}_{\mathbb{F}_q}$ which has parents.

□

We can show that for any less q there are not any nontrivial components.

Theorem 44. *There is $\frac{(q-1)(q-5)}{2}$ vertices.*

Proof. There are $\frac{q-1}{2}$ squares which we can pair with $\frac{q-1}{2} - 2 = \frac{q-5}{2}$ squares. The same is for non-squares, so together we have $\frac{(q-1)(q-5)}{2}$ vertices. □

Example. Now, we can see that for $q = 5$ we do not have any vertices.

Example. Suppose $q = 13$, then the vertices which contain 1 are

$$(1,4), (4,1), (1,9), (9,1), (1,3), (3,1)(1,10), (10,1)$$

but none of them is part of any edge. When we use the homomorphism φ_α, we can obtain that there are no edges.

Corollary 45. *The smallest q with nontrivial graph components is 29.*

Example. Consider $q = 29$. Then there is one cycle of length 28 and 4 cycles of length 7.

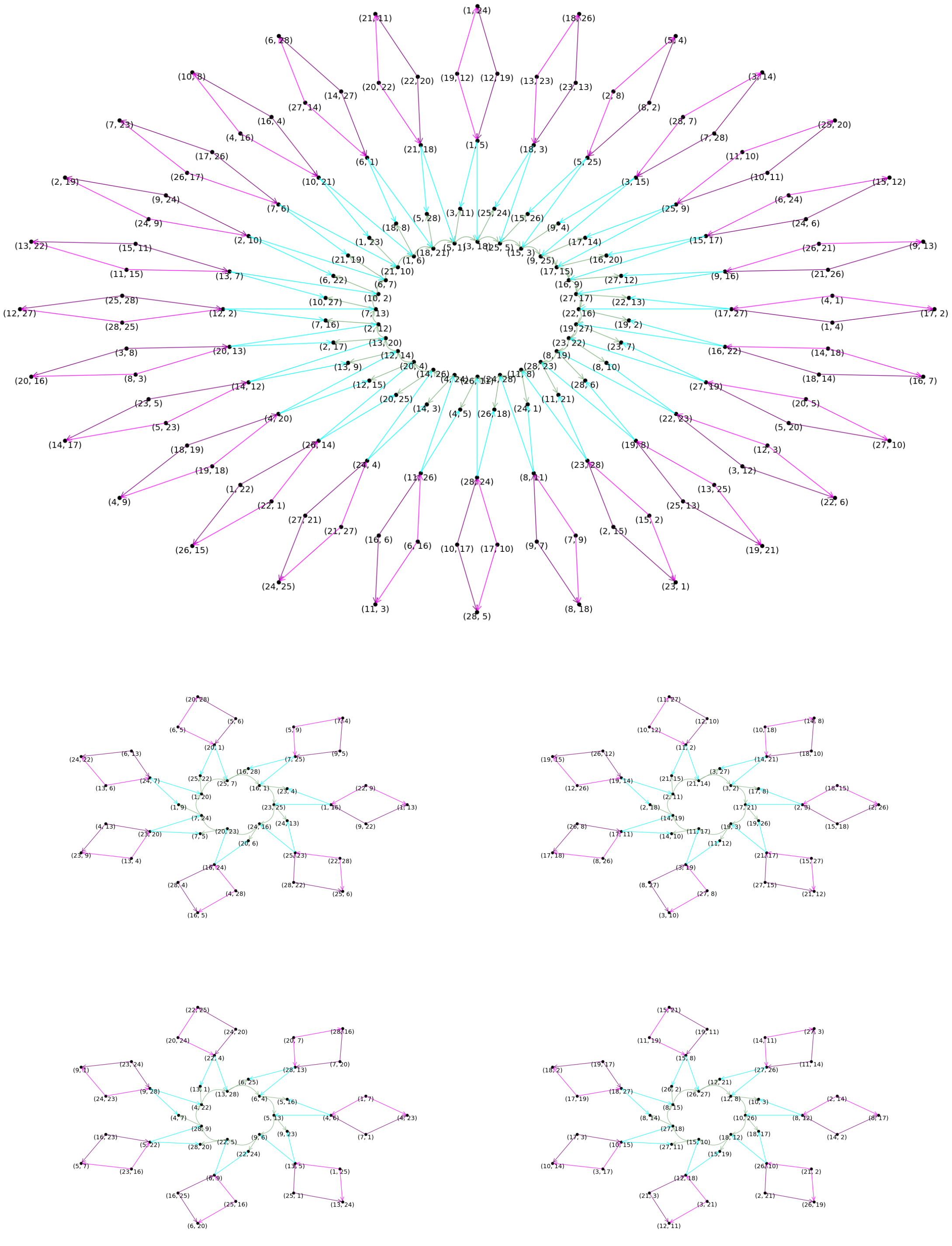

Figure 4.2 The components of $\mathcal{J}_{\mathbb{F}_{29}}$

5 Elliptic curves and $AGM_{\mathbb{F}_q}$

This is an informal chapter which gives a brief view of the connection between elliptic curves and arithmetic-geometric mean sequences. One can use this connection to give a lower bound on the number of components in the graph $\mathcal{J}_{\mathbb{F}_q}$. In the whole chapter we follow [Gri+23, p. 4-9] $\mathbb{F}_q$ such that $q \equiv 3 \pmod 4$.

Definition 46. *Let E be a curve over field $\mathbb{F}$ given by the equation*

$$y^2 = f(x) = x^3 + ax^2 + bx + c,$$

where $a, b, c \in \mathbb{F}$ and $f(x)$ has distinct roots in the algebraic closure $\bar{\mathbb{F}}$. Then E; seen as a projective curve is an elliptic curve.

As we informally introduce elliptic curves, let us briefly explain that E as a projective curve means that E contains of an affine part given by the equation $y^2 = f(x)$ and of one point, which we call the point at infinity. We denote this point O. Then, if we want to be more precise, the curve E together with the point O is called an elliptic curve. For more details, see [Was03, Chapter 2 and 4].

Definition 47. *Let*

$$E(\mathbb{F}) = \{(x, y) \in \mathbb{F}^2 \colon y^2 = f(x)\} \cup \{O\},$$

then $E(\mathbb{F})$ is the set of $\mathbb{F}$-rational points on E.

Lemma 48. *There is a way to define an abelian group law on the set $E(\mathbb{F})$.*

One can find more details about the group law in [ST15, Chapter 1].

Definition 49. *[Was03, p. 236] An isogeny is a homomorphism between groups $E_1(\overline{\mathbb{F}})$ and $E_2(\overline{\mathbb{F}})$ given by rational functions.*

Recall $\mathcal{J}_{\mathbb{F}_q}$ is a directed graph with the components of special shape.

Definition 50. *Let $\mathbb{F}_q$ such that $q = p^n$ where $n \in \mathbb{N}$ and $p \neq 2$. We define Legendre curves E_λ, such that $\lambda \in \mathbb{F}_q \setminus \{0, 1\}$ and*

$$E_\lambda \colon y^2 = x(x-1)(x-\lambda).$$

Theorem 51. *[Gri+23, p.6] Let $\mathbb{F}_q$ such that $q \equiv 3 \pmod 4$ $q = p^n$ where $n \in \mathbb{N}$ and $p \geq 7$. Let $\mathcal{E}_{\mathbb{F}_q}$ be the set of Legendre curves over $\mathbb{F}_q$ and J_i be the components of $\mathcal{J}_{\mathbb{F}_q}$. We define the map $\Psi_{\mathbb{F}_q} \colon \mathcal{J}_{\mathbb{F}_q} \to \mathcal{E}_{\mathbb{F}_q}$ such that*

$$\Psi_{\mathbb{F}_q}((a, b)) := E_{\lambda(a,b)},$$

where $\lambda(a, b) := \frac{b^2}{a^2}$. Then the following are true:

- *We have that*
$$\Psi_{\mathbb{F}_q}(\mathcal{J}_{\mathbb{F}_q}) = \{E_{\lambda^2} \colon \lambda \in \mathbb{F}_q \setminus \{0, \pm 1\}\}$$
and each $E_{\lambda^2} \in \mathcal{E}_{\mathbb{F}_q}(\mathcal{J}_{\mathbb{F}_q})$ has $q - 1$ preimages.

- *For each $1 \leq i \leq d(\mathbb{F}_q)$, we have that $\Psi_{\mathbb{F}_q}(J_i)$ is a connected graph, where an edge $(a_n, b_n) \to (a_{n+1}, b_{n+1}) \in J_i$ transforms to the isogeny $\Phi_n \colon E_{\lambda(a_n,b_n)} \to E_{\lambda(a_{n+1},b_{n+1})}$ defined by*

  $$\Phi_n(x, y) := \left(\frac{(a_n x + b_n)^2}{x(a_n + b_n)^2}, -\frac{a_n y(a_n x - b_n)(a_n x + b_n)}{x^2(a_n + b_n)^3} \right).$$

  Moreover, we have that $ker(\Phi_n) = \langle (0,0) \rangle$.

Example. Consider $q = 11$, than we obtain

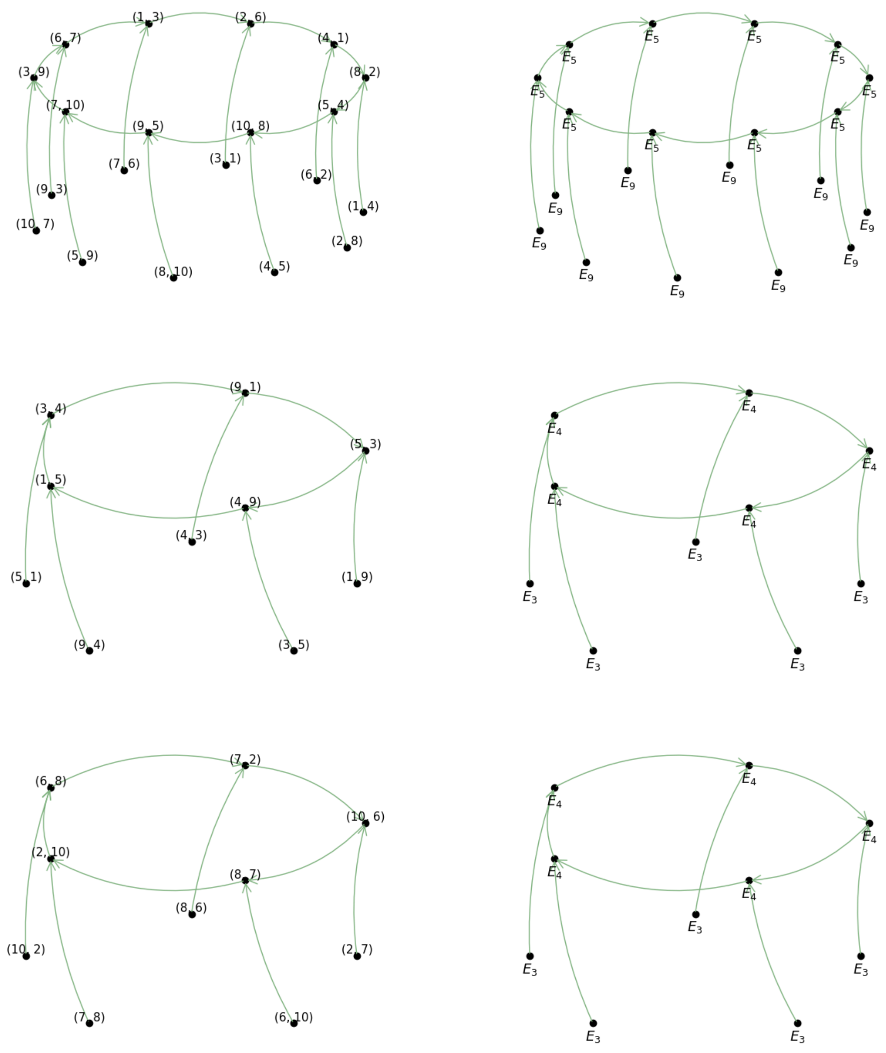

Figure 5.1 AGM and Legendre curves in $\mathbb{F}_{11}$

Example. Consider $q = 19$, then $d(\mathbb{F}_{19}) = 8$ and we obtain

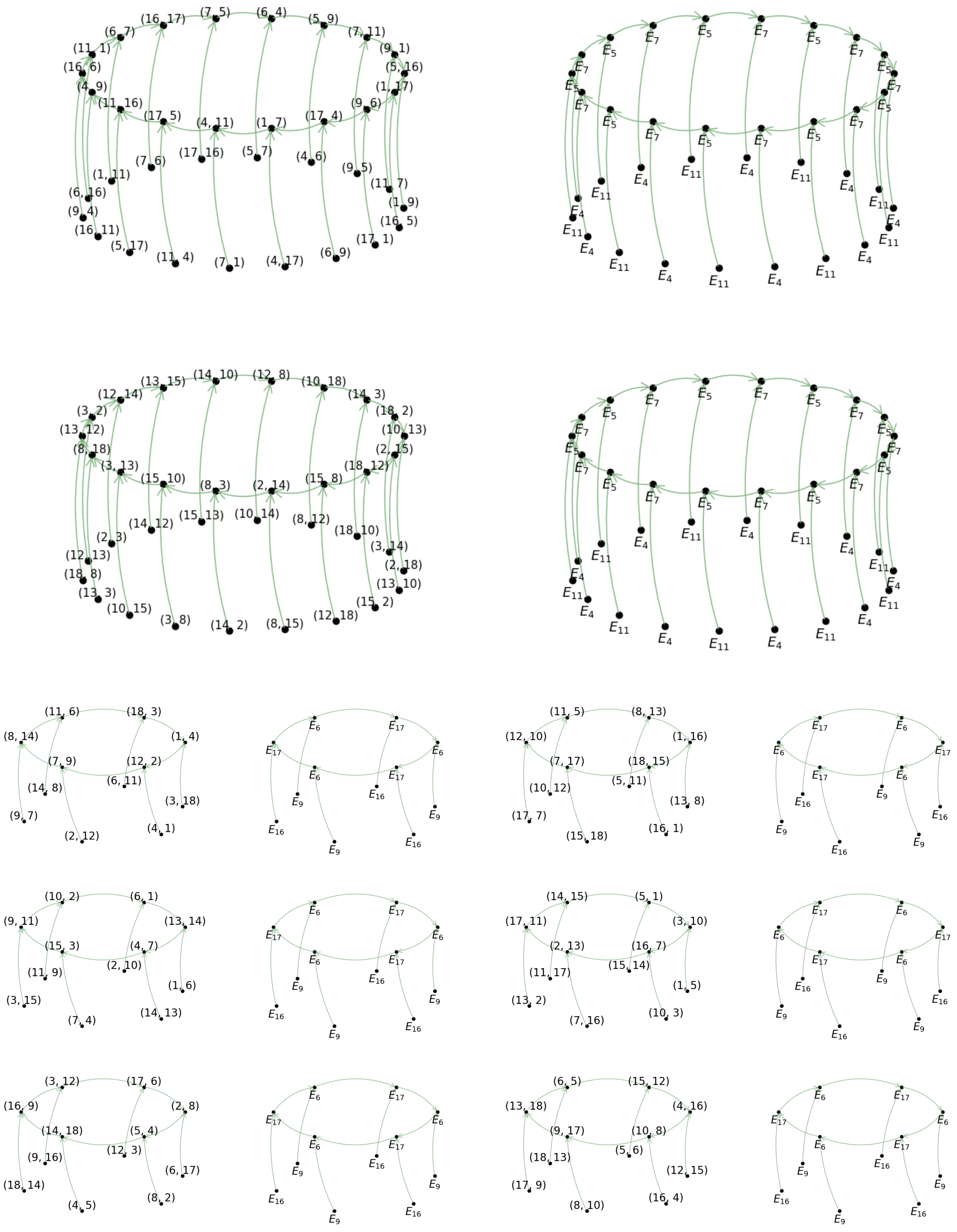

Figure 5.2 AGM and Legendre curves in $\mathbb{F}_{19}$

Theorem 51 gives the connection between elliptic curves and AGM. One can use the connection between elliptic curves and arithmetic geometric means to give the lower bound of $d(\mathbb{F}_q)$.

Theorem 52. *[Gri+23, Theorem 5] Let $\varepsilon > 0$, then for sufficiently large $q \equiv 3 \pmod 4$ we have*

$$d(\mathbb{F}_q) \geq (\frac{1}{2} - \varepsilon) \cdot \sqrt{q}.$$

One can ask if this lower bound is close to the truth values. When we view some examples

$$\begin{aligned}
d(\mathbb{F}_{47}) &= 4 > \frac{\sqrt{47}}{2} \approx 3.4278, \\
d(\mathbb{F}_{383}) &= 14 > \frac{\sqrt{383}}{2} \approx 9.7851, \\
d(\mathbb{F}_{983}) &= 25 > \frac{\sqrt{983}}{2} \approx 15.6764, \\
d(\mathbb{F}_{1907}) &= 38 > \frac{\sqrt{1907}}{2} \approx 21.8346, \\
d(\mathbb{F}_{7703}) &= 87 > \frac{\sqrt{7703}}{2} \approx 43.8833,
\end{aligned}$$

it looks as if this lower bound was not much smaller than an optimal bound, which perhaps might be of the form $\sqrt{q}\log\log(q)$ by [Gri+23, p. 9].

Bibliography

[BBB87] Borwein, Jonathan M. Borwein, and Peter B. *Pi and the AGM: a study in the analytic number theory and computational complexity.* USA: Wiley-Interscience, 1987, pp. 48–49. ISBN: 0471831387.

[BM14] Minal Wankhede Barsagade and Suchitra Meshram. "Overview of History of Elliptic Curves and its use in cryptography". In: *International Journal of Scientific & Engineering Research* 5.4 (2014), pp. 467–471. ISSN: 2229-5518.

[Cve12] Z. Cvetkovski. *Inequalities: Theorems, Techniques and Selected Problems.* SpringerLink : Bücher. Springer Berlin Heidelberg, 2012. ISBN: 9783642237928.

[Gri+23] Michael J. Griffin, Ken Ono, Neelam Saikia, and Wei-Lun Tsai. "AGM and Jellyfish Swarms of Elliptic Curves". In: *The American Mathematical Monthly* 130.4 (2023), pp. 355–369. URL: `https://doi.org/10.1080/00029890.2022.2160157`.

[Lan05] S. Lang. *Algebra.* Graduate Texts in Mathematics. Springer New York, 2005. ISBN: 9780387953854.

[MNK09] J. Matoušek, J. Nešetřil, and Univerzita Karlova. *Kapitoly z diskrétní matematiky.* Karolinum, 2009. ISBN: 9788024617404.

[ST15] Joseph H. Silverman and John T. Tate. *Rational Points on Elliptic Curves.* 2nd. Springer Publishing Company, Incorporated, 2015. ISBN: 331918587X.

[Sta22] David Stanovský. *Učební text algebra 2021/2022.* 2022. URL: `https://www.karlin.mff.cuni.cz/~stanovsk/vyuka/2122/algebra22.pdf`.

[Was03] L.C. Washington. *Elliptic Curves: Number Theory and Cryptography.* Discrete Mathematics and Its Applications. Taylor & Francis, 2003. ISBN: 9781584883654.