AGM and jellyfish swarms of elliptic curves

Michael J. Griffin, Ken Ono, Neelam Saikia, and Wei-Lun Tsai

Abstract. The classical AGM produces wonderful infinite sequences of arithmetic and geometric means with common limit. For finite fields $\mathbb{F}_q$, with $q \equiv 3 \pmod 4$, we introduce a finite field analogue $\mathrm{AGM}_{\mathbb{F}_q}$ that spawns directed finite graphs instead of infinite sequences. The compilation of these graphs reminds one of a *jellyfish swarm*, as the 3D renderings of the connected components resemble *jellyfish* (i.e., tentacles connected to a bell head). These swarms turn out to be more than the stuff of child's play; they are taxonomical devices in number theory. Each jellyfish is an isogeny graph of elliptic curves with isomorphic groups of $\mathbb{F}_q$-points, which can be used to prove that each swarm has at least $(1/2-\varepsilon)\sqrt{q}$ jellyfish. Additionally, this interpretation gives a description of the *class numbers* of Gauss, Hurwitz, and Kronecker which is akin to counting types of spots on jellyfish.

1. ARITHMETIC AND GEOMETRIC MEANS. Beginning with positive real numbers $a_1 := a$ and $b_1 := b$, the $\mathrm{AGM}_{\mathbb{R}}$ inductively produces a sequence of pairs $\mathrm{AGM}_{\mathbb{R}}(a,b) := \{(a_1,b_1),(a_2,b_2),\dots\}$, consisting of arithmetic and geometric means. Namely, for $n \geq 2$, we let

$$a_n := \frac{a_{n-1}+b_{n-1}}{2} \quad \text{and} \quad b_n := \sqrt{a_{n-1}b_{n-1}}.$$

For $n \geq 2$, we have the elementary inequality $a_n \geq b_n$. At a deeper level, the classical theory of the $\mathrm{AGM}_{\mathbb{R}}$ (for example, see Chapter 1 of [**3**]) establishes that these rapidly converging sequences have a common limit $\lim_{n\to+\infty} a_n = \lim_{n\to+\infty} b_n$.

In 1748, Euler [**3**] employed $\mathrm{AGM}_{\mathbb{R}}(\sqrt{2},1)$ as a remarkable device for rapidly computing digits of π. Namely, he showed that $\pi = \lim_{n\to+\infty} p_n$, where

$$p_n := \frac{a_n^2}{\sum_{i=1}^{n} 2^{i-2}(a_i^2-b_i^2)}.$$

Although the first three terms $p_1 = 4,\ p_2 = 3.18767\dots,$ and $p_3 = 3.14168\dots$ are quite satisfying, the next two terms

$$p_4 = 3.14159265389\dots \quad \text{and} \quad p_5 = 3.14159265358979323846\dots$$

are even more astounding as they give 11 and 20 decimal places of π respectively.

Is there a finite field analogue of $\mathrm{AGM}_{\mathbb{R}}$? If so, what number theoretic secrets does it reveal? The non-existence of many square-roots in $\mathbb{F}_q$ poses an obvious obstacle. One solution would be to consider a process where the finite fields grow in size, allowing for the existence of square-roots. However, a second issue arises. Namely, what defines the correct choice of square-root? Over $\mathbb{R}$, the convention of taking positive square-roots guarantees that $\mathrm{AGM}_{\mathbb{R}}$ never ventures beyond $\mathbb{R}$, and so over finite fields we seek situations where there are unique choices of square-root that similarly avoid the need for field extensions.

These requirements hold for finite fields $\mathbb{F}_q$, where $q = p^m \equiv 3 \pmod 4$ with p prime. These fields enjoy the property that -1 is not a square, which corresponds to the

fact that $i = \sqrt{-1}$ is not a real number. For such a field $\mathbb{F}_q$, we let $\phi_q(\cdot)$ be its quadratic residue symbol (the usual Legendre symbol $\left(\frac{\cdot}{p}\right)$ when $q = p$ is prime). We then define $\mathrm{AGM}_{\mathbb{F}_q}(a, b)$ for pairs $a, b \in \mathbb{F}_q^\times := \mathbb{F}_q \setminus \{0\}$, with $a \neq \pm b$ and $\phi_q(ab) = 1$. This input data gives $a_1 := a$ and $b_1 := b$, and for $n \geq 2$ we let

$$a_n := \frac{a_{n-1} + b_{n-1}}{2} \quad \text{and} \quad b_n := \sqrt{a_{n-1} \cdot b_{n-1}}, \tag{1.1}$$

where b_n is the unique square-root with $\phi_q(a_n b_n) = 1$. Although $a_{n-1}b_{n-1}$ has two square-roots, only one choice satisfies $\phi_q(a_n b_n) = 1$ as $\phi_q(-1) = -1$. Therefore, we obtain a sequence of pairs

$$\mathrm{AGM}_{\mathbb{F}_q}(a, b) := \{(a_1, b_1), (a_2, b_2), \dots\}.$$

Let's consider the case of $\mathbb{F}_7$. Half of the 12 pairs that appear in some $\mathrm{AGM}_{\mathbb{F}_7}(a, b)$ form a single AGM-orbit

$$\mathrm{AGM}_{\mathbb{F}_7}(1, 2) = \{\overline{(1, 2), (5, 3), (4, 1), (6, 5), (2, 4), (3, 6)}, \dots\}$$

(Note. The overlined pairs form a repeating orbit.). The other 6 pairs lead to this orbit after a single step. For example, we have

$$\mathrm{AGM}_{\mathbb{F}_7}(6, 3) = \{(6, 3), \overline{(1, 2), (5, 3), (4, 1), (6, 5), (2, 4), (3, 6)}, \dots\}. \tag{1.2}$$

The compilation $\mathcal{J}_{\mathbb{F}_7}$ of all such sequences forms a connected directed graph.

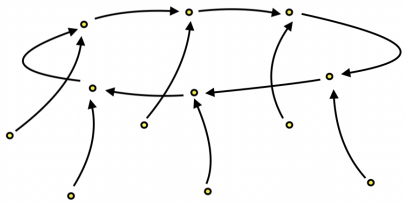

Figure 1: 3D rendering of $\mathcal{J}_{\mathbb{F}_7}$

This example is typical. The compilation of the $\mathrm{AGM}_{\mathbb{F}_q}$ sequences is always a disjoint union of connected directed graphs. The nodes are *admissible ordered pairs*[1] (a, b), where $a, b \in \mathbb{F}_q^\times$, with $a \neq \pm b$, and $\phi_q(ab) = 1$. Moreover, $(a, b) \mapsto (c, d)$ is an edge if and only if

$$c = \frac{a + b}{2} \quad \text{and} \quad d = \sqrt{ab},$$

with $\phi_q(cd) = 1$. These connected components are like *jellyfish*, as their 3D renderings turn out to be unit length tentacles leading to a *bell head* cycle. Hence, we playfully refer to the compilation of the $\mathrm{AGM}_{\mathbb{F}_q}$ sequences

$$\mathcal{J}_{\mathbb{F}_q} := J_1 \sqcup J_2 \sqcup \cdots \sqcup J_{d(\mathbb{F}_q)} \tag{1.3}$$

[1]There are no loops (i.e., $(a, b) \mapsto (a, b)$) as nodes of the form (a, a) are not allowed.

as the *jellyfish swarm* for $\mathbb{F}_q$, where the $J_1, J_2, \ldots, J_{d(\mathbb{F}_q)}$ are the individual jellyfish which make up the swarm.

Let's summarize some basic facts about $\mathrm{AGM}_{\mathbb{F}_q}$ and the jellyfish swarms $\mathcal{J}_{\mathbb{F}_q}$.

Theorem 1.1. *If $\mathbb{F}_q$ is a finite field with $q \equiv 3 \pmod 4$, then the following are true.*

(1) The $\mathrm{AGM}_{\mathbb{F}_q}$ algorithm is well-defined.

(2) The jellyfish swarm $\mathcal{J}_{\mathbb{F}_q}$ has $(q-1)(q-3)/2$ nodes.

(3) Every jellyfish has a bell head with length one tentacles pointing to each node.

(4) If $N_n(\mathbb{F}_q)$ denotes the number of jellyfish with n nodes, then $(q-1) \mid nN_n(\mathbb{F}_q)$.

Proof of Theorem 1.1.

(1) If (a, b) is admissible, then we must show that the next pair (c, d) generated by $\mathrm{AGM}_{\mathbb{F}_q}$ is also admissible. It is clear that $cd \neq 0$ since $ab \neq 0$ and $a \neq \pm b$. If $c = \pm d$, then

$$(a-b)^2 = a^2 - 2ab + b^2 = 4c^2 - 4d^2 = 0,$$

which in turn implies the contradiction that $a = b$. Therefore, $\mathrm{AGM}_{\mathbb{F}_q}$ is well-defined.

(2) We compute the number of admissible pairs (a, b). There are $q-1$ choices for a, and $(q-3)/2$ choices of b with $a \neq \pm b$ which additionally satisfy the quadratic residue condition $\phi_q(ab) = 1$.

(3) Each $\mathrm{AGM}_{\mathbb{F}_q}$ sequence eventually enters a repeating cycle (i.e., the bell head). Suppose that (a, b) is in this orbit. Reversing $\mathrm{AGM}_{\mathbb{F}_q}$ to find its parents, say (A, B), we have $A + B = 2a$ and $AB = b^2$. Therefore, $(A-B)^2 = 4a^2 - 4b^2$, and so $\phi_q(a^2 - b^2) = 1$ with two square-roots. If (A, B) is the parent in the cycle, then the other solution is (B, A), and is not in the cycle. Therefore, (a, b) has exactly one attached tentacle. To see that this tentacle has length 1, we use the assumption that (A, B) is in the cycle, and so has a parent of its own. Repeating the argument above, we have $\phi_q(A^2 - B^2) = 1$, which in turn gives $\phi_q(B^2 - A^2) = -1$. This means that (B, A) does not have a parent.

(4) Each $\alpha \in \mathbb{F}_q^\times$ induces an automorphism on $\mathcal{J}_{\mathbb{F}_q}$ defined by $(a, b) \mapsto (\alpha a, \alpha b)$, as $\alpha \cdot \mathrm{AGM}_{\mathbb{F}_q}(a, b) = \mathrm{AGM}_{\mathbb{F}_q}(\alpha a, \alpha b)$. As there are no fixed admissible pairs provided that $\alpha \neq 1$, we find that the orbit of a node under these automorphisms has size $q-1$. As these automorphisms permute the jellyfish with fixed size, the claim follows. ∎

Theorem 1.1 inspires many natural questions. For example, how small (resp. large) are the jellyfish in a general swarm? This appears to be a very difficult question. For instance, there are $\mathrm{AGM}_{\mathbb{F}_q}$-orbits that are much shorter than q, such as the length 9

$$\mathrm{AGM}_{\mathbb{F}_{67}}(1, 17) = \{\overline{(1, 17), (9, 33) \ldots, (65, 15), (40, 29)}, \ldots\},$$

as well as those that are much longer than q, such as the length 410

$$\mathrm{AGM}_{\mathbb{F}_{83}}(1, 3) = \{\overline{(1, 3), (2, 13), \ldots, (37, 12), (66, 19)}, \ldots\}.$$

These examples correspond to a tiny 18 node jellyfish in $\mathcal{J}_{\mathbb{F}_{67}}$, and a gigantic 820 node jellyfish in $\mathcal{J}_{\mathbb{F}_{83}}$. As another question, what can be said about $d(\mathbb{F}_q)$, the number of jellyfish in $\mathcal{J}_{\mathbb{F}_q}$? Table 1 illustrates the oscillatory behavior of $d(\mathbb{F}_q)$. This erratic

sequence does not appear to settle into a predictable pattern as $q \to +\infty$. Indeed, there are many astonishing examples of disproportionate consecutive values, such as $d(\mathbb{F}_{479}) = 18$ and $d(\mathbb{F}_{487}) = 359$. The only clear observation is that the $d(\mathbb{F}_{p^m})$ grow rapidly with m when p is fixed. For instance, we have

$$\begin{aligned} d(\mathbb{F}_3) = 0 &\to d(\mathbb{F}_{3^3}) = 39 \to d(\mathbb{F}_{3^5}) = 1210, \\ d(\mathbb{F}_7) = 1 &\to d(\mathbb{F}_{7^3}) = 1539 \to d(\mathbb{F}_{7^5}) = 876713, \\ d(\mathbb{F}_{11}) = 3 &\to d(\mathbb{F}_{11^3}) = 8778 \to d(\mathbb{F}_{11^5}) = 25558635. \end{aligned}$$

We shall see that the theory of elliptic curves offers deep insight into these questions.

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

Table 1. $d(\mathbb{F}_q)$ for pimes q

2. JELLYFISH SWARMS ORGANIZE ELLIPTIC CURVES. Computing arithmetic and geometric means over $\mathbb{F}_q$ might seem like mere child's play. However, it turns out that this arithmetic process is a taxonomical device in number theory which organizes elliptic curves.

An *elliptic curve* E over a field $\mathbb{F}$ can be thought of as a cubic equation of the form

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

where $a, b, c \in \mathbb{F}$, and f has non-zero discriminant. If $E(\mathbb{F})$ denotes the $\mathbb{F}$-rational points of E, including the identity "point at infinity" O, then $E(\mathbb{F})$ naturally forms an abelian group via the well-known "chord-tangent law." The group law can be described by asserting that three colinear points on an elliptic curve sum to the identity O. Number theorists are deeply interested in these groups of rational points.

If F is a number field (i.e., a field which has finite degree over $\mathbb{Q}$), then a classical theorem by Mordell and Weil asserts that $E(\mathbb{F})$, the Mordell-Weil group of $E/\mathbb{F}$, is finitely generated. The special case where $\mathbb{F} = \mathbb{Q}$ is the subject of two frequently cited *Monthly* articles. The beautiful 1993 article by Silverman [**17**] on the representation of positive integers as sums of two rational cubes describes the intimate relationship between Ramanujan's taxi-cab numbers and positive rank elliptic curves (i.e., curves with infinitely many $\mathbb{Q}$-rational points). The famous 1991 article by Mazur [**12**] promotes the conjectured "Modularity" of elliptic curves over $\mathbb{Q}$ (formerly known as the Taniyama-Weil Conjecture). This conjecture is now known to be true, largely thanks to the work of Wiles and Taylor [**20, 23**], which was a celebrated ingredient in the proof of Fermat's Last Theorem.

Turning to the case of finite fields, it turns out that the jellyfish swarms $\mathcal{J}_{\mathbb{F}_q}$ organize elliptic curves. One can think of the nodes as spots on the jellyfish, and these spots will be mapped to curves. These swarms are coverings of networks of special Legendre elliptic curves when $q \equiv 3 \pmod 4$ and $p \geq 7$. To be precise, for $\lambda \in \mathbb{F}_q \setminus \{0, 1\}$, we recall the *Legendre normal form* elliptic curve

$$E_\lambda : \ y^2 = x(x-1)(x-\lambda). \tag{2.1}$$

Isomorphism classes of elliptic curves are distinguished by their j*-invariants*, and for E_λ we have

$$j(E_\lambda) = 2^8 \cdot \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}. \tag{2.2}$$

For an introduction to elliptic curves over finite fields, the reader may consult Chapter 4 of [**22**].

The jellyfish swarm $\mathcal{J}_{\mathbb{F}_q}$ organizes elliptic curves via the map $\Psi_{\mathbb{F}_q} : \mathcal{J}_{\mathbb{F}_q} \mapsto \mathcal{E}_{\mathbb{F}_q}$, where $\mathcal{E}_{\mathbb{F}_q}$ is the set of Legendre curves over $\mathbb{F}_q$, and

$$\Psi_{\mathbb{F}_q}(a, b) := E_{\lambda(a,b)}, \tag{2.3}$$

where $\lambda(a, b) := b^2/a^2$. For instance, example (1.2) gives

$$\begin{aligned}\Psi_{\mathbb{F}_7}(\mathrm{AGM}_{\mathbb{F}_7}(6, 3)) &= \Psi_{\mathbb{F}_7}\left(\{(6, 3), \overline{(1, 2), (5, 3), (4, 1), (6, 5), (2, 4), (3, 6)}, \dots\}\right) \\ &= \left\{E_2, \overline{E_4, E_4, E_4, E_4, E_4, E_4}, \dots\right\} = \left\{E_2, \overline{E_4}, \dots\right\}.\end{aligned}$$

As the values $\lambda(a, b) = b^2/a^2$ cover the squares in $\mathbb{F}_q \setminus \{0, 1\}$, it is natural ask what special features are shared by curves of the form E_{λ^2}. It turns out that these curves are distinguished by the 2-Sylow subgroups of their $\mathbb{F}_q$-rational points.

Lemma 2.1. *Suppose that $\mathbb{F}_q$ is a finite field with $q \equiv 3 \pmod 4$. If $\lambda \in \mathbb{F}_q \setminus \{0, 1\}$, then the 2-Sylow subgroup of $E_{\lambda^2}(\mathbb{F}_q)$ is of the form $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{2+b}\mathbb{Z}$, where $b \geq 0$.*

Proof. Elliptic curves with four 2-torsion points (i.e., including the identity) can be written in the form

$$E : \ y^2 = (x - \alpha)(x - \beta)(x - \gamma).$$

The non-trivial 2-torsion points correspond to the roots of the cubic. They are the points $(\alpha, 0), (\beta, 0)$ and $(\gamma, 0)$. For such curves, the classical *2-descent lemma* (see p. 47-49 of [**10**] or p. 315 of [**16**]) says that a non-zero point $P = (x_0, y_0) \in E(\mathbb{F}_q)$ satisfies $P = 2Q$, where $Q \in E(\mathbb{F}_q)$, if and only if

$$x_0 - \alpha, \ \ x_0 - \beta, \ \ x_0 - \gamma \in \mathbb{F}_q^2.$$

Here we have $\alpha = 0, \beta = 1$, and $\gamma = \lambda^2$. Since $q \equiv 3 \pmod 4$, then exactly one of $(1, 0)$ and $(\lambda^2, 0)$ is in $2E_{\lambda^2}(\mathbb{F}_q)$, as exactly one of $\pm(1 - \lambda^2)$ is a square. On the other hand, $(0, 0) \notin 2E_{\lambda^2}(\mathbb{F}_q)$ by the 2-descent lemma because -1 is not a square. Therefore, the $\mathbb{Z}/4\mathbb{Z}$ rank of $E(\mathbb{F}_q)$ is 1, which means that $E(\mathbb{F}_q)$ contains $\mathbb{Z}/4\mathbb{Z}$ but not $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. ∎

The $\mathcal{J}_{\mathbb{F}_q}$ organize the curves in $\Psi_{\mathbb{F}_q}(\mathcal{J}_{\mathbb{F}_q})$ as unions of explicit *isogeny graphs*. An *isogeny* between two elliptic curves is a special map Φ (called a *morphism*) that preserves the identity element, is given by rational functions $\Phi = (u(x, y), v(x, y))$, and is a homomorphism on $\mathbb{F}_q$-points with finite kernel. The isogeny graph structure of $\Psi_{\mathbb{F}_q}(\mathcal{J}_{\mathbb{F}_q})$ is provided by the following theorem.

Theorem 2.2. *If $\mathbb{F}_q$ is a finite field with $q \equiv 3 \pmod 4$ and $\mathrm{char}(\mathbb{F}_q) = p \geq 7$, then the following are true.*

(1) We have that

$$\Psi_{\mathbb{F}_q}(\mathcal{J}_{\mathbb{F}_q}) = \{E_{\alpha^2}/\mathbb{F}_q \ : \ \alpha \in \mathbb{F}_q \setminus \{0, \pm 1\}\}.$$

Moreover, each $E_{\alpha^2} \in \Psi_{\mathbb{F}_q}(\mathcal{J}_{\mathbb{F}_q})$ has $q - 1$ preimages.

(2) For each $1 \leq i \leq d(\mathbb{F}_q)$, we have that $\Psi_{\mathbb{F}_q}(J_i)$ is a connected graph[2], where an edge $(a_n, b_n) \to (a_{n+1}, b_{n+1}) \in J_i$ is the isogeny $\Phi_n : E_{\lambda(a_n,b_n)} \to E_{\lambda(a_{n+1},b_{n+1})}$ 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 $\ker(\Phi_n) = \langle (0, 0) \rangle$.

Proof of Theorem 2.2.

(1) For an admissible pair (a, b), we have $a, b \in \mathbb{F}_q^\times$, and $a \neq \pm b$. Therefore, $b/a \in \mathbb{F}_q \setminus \{0, \pm 1\}$ and

$$\Psi_{\mathbb{F}_q}(\mathcal{J}_{\mathbb{F}_q}) \subset \{E_{\alpha^2}/\mathbb{F}_q \ : \ \alpha \in \mathbb{F}_q \setminus \{0, \pm 1\}\}.$$

On the other hand, if $\alpha \in \mathbb{F}_q \setminus \{0, \pm 1\}$, then one can choose (a, b) such that $a = \pm 1$ and $b = \pm\alpha$ with $\phi_q(ab) = 1$, giving $\lambda(a, b) = \alpha^2$. Furthermore, each admissible pair (a, b), produces the $q - 1$ further admissible pairs (ka, kb), all mapping to E_{b^2/a^2}. Hence, each $E_{\lambda(a,b)}$ has $q - 1$ preimages.

(2) If $(x, y) \neq (0, 0) \in E_{\lambda(a_n,b_n)}$, then a brute force calculation gives

$$\frac{(a_n x + b_n)^2}{x(a_n + b_n)^2} \left(\frac{(a_n x + b_n)^2}{x(a_n + b_n)^2} - 1 \right) \left(\frac{(a_n x + b_n)^2}{x(a_n + b_n)^2} - \frac{b_{n+1}^2}{a_{n+1}^2} \right) = \frac{a_n^2 y^2 (a_n x - b_n)^2 (a_n x + b_n)^2}{x^4 (a_n + b_n)^6}.$$

This proves that $\Phi_n(x, y) \in E_{\lambda(a_{n+1},b_{n+1})}$. To verify that the map preserves the identity $O = [0, 1, 0]$ (the point at infinity in projective space), we consider the projectivized form $\Phi_n(x, y, z) := [\varphi_1(x, y, z), \varphi_2(x, y, z), \varphi_3(x, y, z)]$, where

$$\begin{aligned}
\varphi_1 &:= (a_n + b_n) \\
&\quad \times (a_n^4 x y^2 + (a_n^4 + a_n^2 b_n^2) x^3 + 2a_n^3 b_n y^2 z + (2a_n^3 b_n + 2a_n b_n^3) x^2 z - 2a_n b_n^3 x z^2), \\
\varphi_2 &:= 2a_n^3 b_n^2 x y z - a_n^5 y^3 - (a_n^5 + a_n^3 b_n^2) x^2 y, \\
\varphi_3 &:= (a_n + b_n)^3 (a_n^2 y^2 z + (a_n^2 + b_n^2) x^2 z - b_n^2 x z^2).
\end{aligned}$$

[2]The proof of Theorem 2.2 shows that the swarms are graphs of 2-isogenies. We point interested readers to Sutherland's expository article [**19**] for more on the theory of isogeny graphs.

One sees that $\Phi_n(x, y, z)$ preserves the point at infinity O. Furthermore, as $a_n + b_n = 2a_{n+1} \neq 0$, we find by inspection that Φ_n is an isogeny with $\ker(\Phi_n) = \langle (0, 0) \rangle$. ∎

What features are shared by the elliptic curves corresponding to the nodes of a single jellyfish? The next corollary offers the answer.

Corollary 2.3. *For each $1 \leq i \leq d(\mathbb{F}_q)$, the following are true.*
(1) There is an abelian group G such that for all $(a_n, b_n) \in J_i$ we have

$$E_{\lambda(a_n,b_n)}(\mathbb{F}_q) \cong G.$$

Moreover, the 2-Sylow subgroup of G is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{2+b_q(i)}\mathbb{Z}$, where $b_q(i) \geq 0$.
(2) There is a fixed "trace of Frobenius" $a_q(i)$ such that for all $(a_n, b_n) \in J_i$ we have

$$|E_{\lambda(a_n,b_n)}(\mathbb{F}_q)| = q + 1 - a_q(i).$$

Proof of Corollary 2.3.
(1) For adjacent pairs $(a_n, b_n), (a_{n+1}, b_{n+1}) \in J_i$, Theorem 2.2 (2) gives an isogeny

$$\Phi_n : E_{\lambda(a_n,b_n)} \mapsto E_{\lambda(a_{n+1},b_{n+1})},$$

with $\ker(\Phi_n) = \langle (0, 0) \rangle \cong \mathbb{Z}/2\mathbb{Z}$. It is well-known (for example, see Exercise 5.4 on p. 153 of [**16**]) that isogenous elliptic curves over finite fields have the same number of rational points. In particular, the 2-Sylow subgroups of the groups of $\mathbb{F}_q$ rational points of these two curves have the same order. Therefore, since $\Phi_n(E_{\lambda(a_n,b_n)}(\mathbb{F}_q))$ is an index 2 subgroup of $E_{\lambda(a_{n+1},b_{n+1})}(\mathbb{F}_q)$, then as abstract groups we find that

$$E_{\lambda(a_n,b_n)}(\mathbb{F}_q) \cong E_{\lambda(a_{n+1},b_{n+1})}(\mathbb{F}_q).$$

(2) By Theorem 2.2 (2), we have that $\Psi_{\mathbb{F}_q}(J_i)$ is a connected isogeny graph. As mentioned above, isogenous curves over finite fields have the same number of rational points. Hence, there is a fixed integer $a_q(i)$, known as the trace of Frobenius, such that

$$|E_{\lambda(a_n,b_n)}(\mathbb{F}_q)| = q + 1 - a_q(i)$$

for each $(a_n, b_n) \in J_i$. ∎

Example. By Theorem 1.1, $\mathcal{J}_{\mathbb{F}_{19}}$ has 144 nodes. and it turns out that

$$\mathcal{J}_{\mathbb{F}_{19}} = J_1 \sqcup J_2 \sqcup \cdots \sqcup J_6 \sqcup J_7 \sqcup J_8$$

(i.e., $d(\mathbb{F}_{19}) = 8$), where the jellyfish can be ordered so that $J_1, J_2, \ldots, J_6$ have bell heads with cycle length 6, and J_7 and J_8 have bell heads with cycle length 18. By Theorem 2.2 (1), the nodes in $\mathcal{J}_{\mathbb{F}_{19}}$ map to the eight Legendre curves with 18 preimages each. The 6 smaller jellyfish give the isogeny graph depicted below.

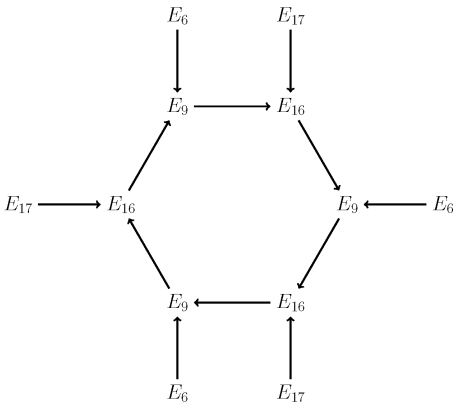

Figure 2: 2D rendering of the isogeny graph of each $J \in \{J_1, \ldots, J_6\}$

This defines the 3-to-1 covering $\Psi_{\mathbb{F}_{19}}(J_1) = \cdots = \Psi_{\mathbb{F}_{19}}(J_6) = \{E_6, E_9, E_{16}, E_{17}\}$. These Legendre curves satisfy

$$E_6(\mathbb{F}_{19}) \cong E_9(\mathbb{F}_{19}) \cong E_{16}(\mathbb{F}_{19}) \cong E_{17}(\mathbb{F}_{19}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}.$$

We have $a_{19}(1) = \cdots = a_{19}(6) = 19 + 1 - |\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}| = -4$. For J_7 and J_8, we obtain the 9-to-1 covering $\Psi_{\mathbb{F}_{19}}(J_7) = \Psi_{\mathbb{F}_{19}}(J_8) = \{E_4, E_5, E_7, E_{11}\}$, with

$$E_4(\mathbb{F}_{19}) \cong E_5(\mathbb{F}_{19}) \cong E_7(\mathbb{F}_{19}) \cong E_{11}(\mathbb{F}_{19}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}.$$

Therefore, we have $a_{19}(7) = a_{19}(8) = 19 + 1 - |\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}| = 4$.

This example shows that individual jellyfish generally include many non-isomorphic curves, as the j-invariants (see (2.2)) for the smaller (resp. larger) jellyfish are $j(E_9) = j(E_{17}) = 5$ and $j(E_6) = j(E_{16}) = 15$ (resp. $j(E_7) = j(E_{11}) = 5$ and $j(E_4) = j(E_5) = 15$). We shall show that the number of different j-invariants, like counting types of spots on jellyfish, has taxonomic significance.

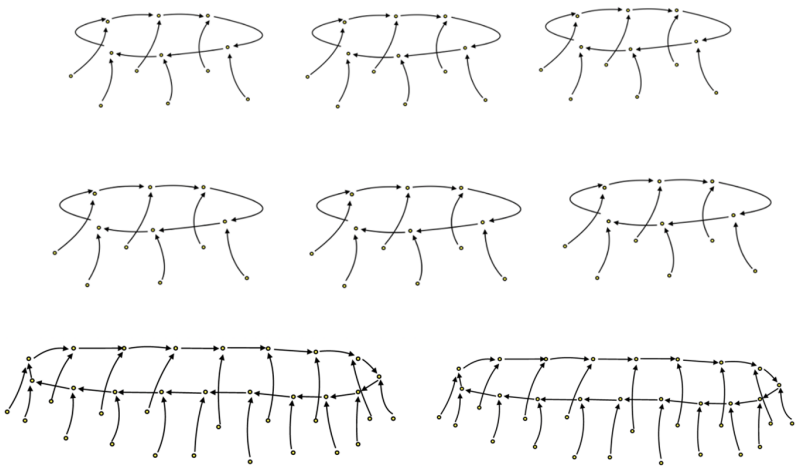

Figure 3: $\mathcal{J}_{\mathbb{F}_{19}}$ swarm

Thanks to the deeper insight offered by Corollary 2.3, we are able to revisit the baffling numbers $d(\mathbb{F}_q)$, and offer a non-trivial lower bound.

Theorem 2.4. *If $\varepsilon > 0$, then for sufficiently large $q \equiv 3 \pmod 4$ we have*

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

Remark. Is this lower bound close to the truth? In view of examples such as

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

it is tempting to speculate that this lower bound is not much smaller than an optimal bound which perhaps might be of the form $\gg \sqrt{q}\log\log(q)$.

Proof of Theorem 2.4. Corollary 2.3 guarantees that $d(\mathbb{F}_q)$ is at least as large as the number of distinct groups G for which $E_{\lambda^2}(\mathbb{F}_q) \cong G$ for some $\lambda \in \mathbb{F}_q \setminus \{0,1\}$. For a group G, the proof of Theorem 3.1 establishes the existence of such a curve provided $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \subseteq G$ and there is an $E/\mathbb{F}_q$ for which $E(\mathbb{F}_q) \cong G$.

We can construct many such groups. If $-2\sqrt{q} \leq s \leq 2\sqrt{q}$ and $s \equiv q+1 \pmod 8$, then let $m_q(s) := (q+1-s)/2 \equiv 0 \pmod 4$. A classical theorem of Rück and Voloch [**15, 21**] guarantees that one can take $G := \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/m_q(s)\mathbb{Z}$. For large q, this represents approximately one eighth of the integers in $[-2\sqrt{q}, 2\sqrt{q}]$. Therefore, if $\varepsilon > 0$, then for sufficiently large q we have

$$d(\mathbb{F}_q) \geq \left(\frac{1}{2} - \varepsilon\right)\sqrt{q}. \tag{2.4}$$

■

3. JELLYFISH SWARMS AND GAUSS' CLASS NUMBERS. The swarms $\mathcal{J}_{\mathbb{F}_q}$ offer new descriptions of the *class numbers* studied by Gauss, Hurwitz and Kronecker (see [**5**] for more on class numbers). To make this precise, recall that an *integral binary quadratic form* is a homogeneous degree 2 polynomial

$$f(x,y) := ax^2 + bxy + cy^2 \in \mathbb{Z}[x,y].$$

The *discriminant*[3] of f is $D := b^2 - 4ac$. If $a > 0$ and $D < 0$, then $f(x,y)$ is called *positive definite*. Furthermore, f is *primitive* if $\gcd(a,b,c) = 1$. For negative discriminants D, the group $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathcal{Q}_D$, the set of positive definite binary quadratic forms of discriminant D. More precisely, for any $\gamma = \left(\begin{smallmatrix} u & v \\ r & s \end{smallmatrix}\right)$, we have

$$(f \circ \gamma)(x,y) := f(ux+vy, rx+sy).$$

[3]Discriminants always satisfy $D \equiv 0, 1 \pmod 4$.

Although there are infinitely many primitive binary quadratic forms with discriminant D, Gauss proved that their number of $\mathrm{SL}_2(\mathbb{Z})$-orbits is finite, and this number is known as *Gauss' class number* $h(D)$.

Gauss' class numbers lead to the more general *Hurwitz-Kronecker class numbers.* If $N \equiv 0, 3 \pmod 4$, then the Hurwitz-Kronecker class number $H(N)$ is the class number of positive definite integral binary quadratic forms of discriminant $-N$, where each class C is counted with multiplicity $1/\mathrm{Aut}(C)$. If $-N = Df^2$, where D is a negative fundamental discriminant (i.e., the discriminant of the ring of integers of an imaginary quadratic field), then $H(N)$ is related to $h(D)$ by (for example, see p. 273 of [**5**])

$$H(N) = \frac{h(D)}{w(D)} \sum_{d|f} \mu(d) \left(\frac{D}{d}\right) \sigma_1(f/d).$$

Here $w(D)$ is half the number of integral units in $\mathbb{Q}(\sqrt{D})$, and $\sigma_s(n)$ denotes the sum of the s^{th} powers of the positive divisors of n, and $\left(\frac{D}{\cdot}\right)$ is the quadratic Dirichlet character with conductor D.

Class numbers have a long and rich history. For example, class numbers play a central role in the study of quadratic forms. Indeed, if $r_3(n)$ denotes the number of representations of an integer n as a sum of three squares, then Gauss proved that

$$r_3(n) = \begin{cases} 12H(4n) & \text{if } n \equiv 1, 2 \pmod 4, \\ 24H(n) & \text{if } n \equiv 3 \pmod 8, \\ r_3(n/4) & \text{if } n \equiv 0 \pmod 4, \\ 0 & \text{if } n \equiv 7 \pmod 8. \end{cases}$$

Class numbers play even deeper roles in algebraic and analytic number theory, as they are the orders of ideal class groups of rings of integers and orders of imaginary quadratic fields. These groups themselves are the Galois groups of Hilbert class fields. For brevity, we simply say that the study of class numbers continues to drive cutting edge research today.

The jellyfish swarms $\mathcal{J}_{\mathbb{F}_q}$ offer a new interpretation of these class numbers. As the nodes are jellyfish spots, it is quite gratifying to discover that class numbers represent the number of types of spots that appear in a family of jellyfish. In this analogy, the j-invariants distinguish these types of spots. Namely, for integers s, let $M_{\mathbb{F}_q}(s)$ be the number of distinct j-invariants of curves in the union of jellyfish with $a_q(i) = s$, the "Frobenius trace s family." We have the following attractive description which follows from a well-known theorem of Schoof.

Theorem 3.1. *Suppose that $\mathbb{F}_q$ is a finite field with $q \equiv 3 \pmod 4$ and $p \geq 7$. If $-2\sqrt{q} \leq s \leq 2\sqrt{q}$ is a non-zero integer with $s \equiv q + 1 \pmod 8$, then we have*

$$H\left(\frac{4q - s^2}{4}\right) = M_{\mathbb{F}_q}(s).$$

Example. We revisit the example of $\mathcal{J}_{\mathbb{F}_{19}}$, where $J_1, \ldots, J_6$ (resp. J_7 and J_8) are the smaller (resp. larger) jellyfish. We found earlier that the Frobenius trace -4 family is

$$\Psi_{\mathbb{F}_{19}}(J_1) \cup \cdots \cup \Psi_{\mathbb{F}_{19}}(J_6) = \{E_6, E_9, E_{16}, E_{17}\}.$$

One checks (using (2.2) that $j(E_9) = j(E_{17}) = 5$ and $j(E_6) = j(E_{16}) = 15$, giving $M_{\mathbb{F}_{19}}(-4) = 2$. We also found that the Frobenius trace 4 family is

$$\Psi_{\mathbb{F}_{19}}(J_7) \cup \Psi_{\mathbb{F}_{19}}(J_8) = \{E_4, E_5, E_7, E_{11}\}.$$

As $j(E_7) = j(E_{11}) = 5$, and $j(E_4) = j(E_5) = 15$, we also have $M_{\mathbb{F}_{19}}(4) = 2$. Therefore, since $M_{\mathbb{F}_{19}}(\pm 4) = 2$, Theorem 3.1 gives

$$H\left(\frac{76 - (\pm 4)^2}{4}\right) = H(15) = 2.$$

Proof of Theorem 3.1. Let $E/\mathbb{F}_q$ be an elliptic curve for which $|E(\mathbb{F}_q)| \equiv 0 \pmod 8$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \subseteq E(\mathbb{F}_q)$. We automatically have $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \subseteq E(\mathbb{F}_q)$, because these groups can always be described as a direct product of at most 2 cyclic groups. Moreover, a standard application of the 2-descent lemma (for example, see Proposition 3.3 of [**1**]) implies that there is an $\alpha \in \mathbb{F}_q \setminus \{0, \pm 1\}$ for which $E_{\alpha^2} \cong_{\mathbb{F}_q} E$. Conversely, every $E_{\lambda(a,b)}$ is such an E thanks to Corollary 2.3. Therefore, $\mathcal{J}_{\mathbb{F}_q}$ encodes the isomorphism classes of elliptic curves $E/\mathbb{F}_q$ with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \subseteq E(\mathbb{F}_q)$, with the additional property that $q \equiv s + 1 \pmod 8$, where $s := q + 1 - \#E(\mathbb{F}_q)$.

We consider the $\mathbb{F}_q$ isomorphism classes of such curves with fixed non-zero trace of Frobenius s. If $(a, b), (a', b') \in \mathcal{J}_{\mathbb{F}_q}$ satisfies $j(E_{\lambda(a,b)}) = j(E_{\lambda(a',b')})$, then either $E_{\lambda(a,b)} \cong_{\mathbb{F}_q} E_{\lambda(a',b')}$, or they are non-trivial twists of each other (see Chapter X of [**16**]). In the latter case, the traces of Frobenius differ in sign.

Combining these facts, we have that $M_{\mathbb{F}_q}(s)$ is the number of isomorphism classes of elliptic curves $E/\mathbb{F}_q$ with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \subseteq E(\mathbb{F}_q)$ and trace of Frobenius s. The rich theory of complex multiplication for elliptic curves is the bridge which connects the counts of such classes with equivalence classes of binary quadratic forms. Indeed, a well-known deep theorem of Schoof (see Section 4 of [**18**]) asserts that $H\left(\frac{4q-s^2}{4}\right)$ equals the number of such isomorphism classes of elliptic curves. Invoking this theorem completes the proof.

■

4. ANALOGIES BETWEEN HYPERGEOMETRIC FUNCTIONS. Does the classical $\mathrm{AGM}_{\mathbb{R}}$ have more in common with its finite field analogues than the inductive rules

$$a_n := \frac{a_{n-1} + b_{n-1}}{2} \quad \text{and} \quad b_n := \sqrt{a_{n-1}b_{n-1}}\,?$$

This is indeed the case. It turns out that the results offered above are a byproduct of remarkable analogies between complex hypergeometric functions and their finite field analogues. Let us explain.

Hypergeometric functions and $\mathrm{AGM}_{\mathbb{R}}$. The theory underlying $\mathrm{AGM}_{\mathbb{R}}$ (see Chapter 1 of [**3**]) is a story involving special integrals and their relationship with Gauss' hypergeometric functions. To make this precise, for $a > b > 0$, we let

$$I_{\mathbb{R}}(a, b) := \frac{1}{2a} \int_1^\infty \frac{dx}{\sqrt{x(x-1)(x-(1-b^2/a^2))}}, \tag{4.1}$$

where the polynomial in the square-root in the denominator of the integrand is tantalyzingly[4] close to the cubic in the Legendre curve

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

It is straightforward to check that $I_{\mathbb{R}}(a,b) = I_{\mathbb{R}}\left(\frac{a+b}{2}, \sqrt{ab}\right)$, which in turn implies that $\mathrm{AGM}_{\mathbb{R}}(a,b) = \{(a_1,b_1),(a_2,b_2),\dots\}$ satisfies

$$I_{\mathbb{R}}(a_1,b_1) = I_{\mathbb{R}}(a_2,b_2) = \cdots = I_{\mathbb{R}}(a_n,b_n) = \cdots. \tag{4.2}$$

Gauss discovered a beautiful formula for $I_{\mathbb{R}}(a,b)$ in terms of hypergeometric functions. For $\alpha_1,\alpha_2,\dots\alpha_n$ and $\beta_1,\dots,\beta_{n-1} \in \mathbb{C}$, these functions are defined by

$${}_nF_{n-1}^{\text{class}}\left(\begin{matrix}\alpha_1, & \alpha_2, & \dots, & \alpha_n \\ & \beta_1, & \dots, & \beta_{n-1}\end{matrix} \mid t\right) := \sum_{k=0}^{\infty} \frac{(\alpha_1)_k(\alpha_2)_k\cdots(\alpha_n)_k}{(\beta_1)_k\cdots(\beta_{n-1})_k}\frac{t^k}{k!}, \tag{4.3}$$

where $(x)_k$ is the Pochhammer symbol defined by

$$(x)_k = \begin{cases} 1 & \text{if} \quad k=0 \\ x(x+1)\cdots(x+k-1) & \text{if} \quad k>0. \end{cases}$$

Gauss' theory of elliptic integrals [**9**, p. 182] gives

$$I_{\mathbb{R}}(a,b) = \frac{\pi}{2a}\cdot {}_2F_1^{\text{class}}\left(\begin{matrix}\frac{1}{2}, & \frac{1}{2} \\ & 1\end{matrix} \mid 1-\frac{b^2}{a^2}\right), \tag{4.4}$$

which, by letting $a \mapsto (a+b)/2$ and $b \mapsto \sqrt{ab}$, also gives

$$I_{\mathbb{R}}\left(\frac{a+b}{2}, \sqrt{ab}\right) = \frac{\pi}{a+b}\cdot {}_2F_1^{\text{class}}\left(\begin{matrix}\frac{1}{2}, & \frac{1}{2} \\ & 1\end{matrix} \mid \frac{(a-b)^2}{(a+b)^2}\right). \tag{4.5}$$

Equating these expressions, we find that $\mathrm{AGM}_{\mathbb{R}}$ leads to the identity

$${}_2F_1^{\text{class}}\left(\begin{matrix}\frac{1}{2}, & \frac{1}{2} \\ & 1\end{matrix} \mid 1-\frac{b^2}{a^2}\right) = \frac{2a}{a+b}\cdot {}_2F_1^{\text{class}}\left(\begin{matrix}\frac{1}{2}, & \frac{1}{2} \\ & 1\end{matrix} \mid \frac{(a-b)^2}{(a+b)^2}\right),$$

which relates $1-b^2/a^2$ with $\lambda(a+b,a-b) = (a-b)^2/(a+b)^2$. This identity is a special case (i.e., $\alpha=\beta=1/2$ and $t=(a-b)/(a+b)$) of the far more general quadratic transformation formula (see [**2**, (3.1.11)])

$$\begin{aligned} &{}_2F_1^{\text{class}}\left(\begin{matrix}\alpha, & \beta \\ & 2\alpha\end{matrix} \mid \frac{4t}{(1+t)^2}\right) \\ &\qquad = (1+t)^{2\beta}\cdot {}_2F_1^{\text{class}}\left(\begin{matrix}\beta+\frac{1}{2}-\alpha, & \beta \\ & \alpha+\frac{1}{2}\end{matrix} \mid t^2\right). \end{aligned} \tag{4.6}$$

[4]These models are actually -1 quadratic twists of each other.

Hypergeometric functions and $\mathrm{AGM}_{\mathbb{F}_q}$. In view of the previous discussion, we seek a finite field analog of

$$I_{\mathbb{R}}(a,b) := \frac{1}{2a}\int_1^\infty \frac{dx}{\sqrt{x(x-1)(x-(1-b^2/a^2))}}.$$

To this end, one can replace the integral over $\mathbb{R}$ by a sum over $\mathbb{F}_q$, and replace the square-root with the quadratic character $\phi_q(\cdot)$, and we can naively declare the finite field analogue to be the sum

$$I_{\mathbb{F}_q}(a,b) := \sum_{x\in\mathbb{F}_q} \phi_q(x)\phi_q(x-1)\phi_q(x-(1-b^2/a^2)). \tag{4.7}$$

We hope that such sums are values of hypergeometric-type functions.

In his important 1984 Ph.D thesis [**7**], Greene defined the *finite field hypergeometric functions* that do the trick (see [**13, 14**] for applications). For multiplicative characters[5] $A_1, A_2, \ldots, A_n$ and $B_1, B_2, \ldots, B_{n-1}$ of $\mathbb{F}_q^\times$, he defined

$${}_nF_{n-1}\left(\begin{matrix} A_1, & A_2, & \ldots, & A_n \\ & B_1, & \ldots, & B_{n-1}\end{matrix} \mid t\right)_{\mathbb{F}_q} :=$$
$$\frac{q}{q-1}\sum_{\chi}\binom{A_1\chi}{\chi}\binom{A_2\chi}{B_1\chi}\cdots\binom{A_n\chi}{B_{n-1}\chi}\chi(t),$$

where the sum is over the multiplicative characters of $\mathbb{F}_q^\times$, and $\binom{A}{B}$ is the normalized Jacobi sum

$$\binom{A}{B} := \frac{B(-1)}{q}J(A,\overline{B}) := \frac{B(-1)}{q}\sum_{t\in\mathbb{F}_q} A(t)\overline{B}(1-t).$$

This definition was meant to resemble (4.3), and is based on analogies between Gauss sums and the complex Γ-function, which interpolates factorials, and the classical Gauss sum expression for Jacobi sums (when $\chi\psi$ is nontrivial)

$$J(\chi,\Psi) = \frac{G(\chi)G(\psi)}{G(\chi\psi)},$$

which in turn emulates binomial coefficients.

These functions take an attractive form when $n = 2$ (see p. 82 of [**8**]). If A, B and C are characters of $\mathbb{F}_q$ and $t \in \mathbb{F}_q^\times$, then

$${}_2F_1\left(\begin{matrix} A, & B \\ & C\end{matrix} \mid t\right)_{\mathbb{F}_q} = \frac{BC(-1)}{q}\cdot\sum_{x\in\mathbb{F}_q} B(x)\cdot\overline{B}C(1-x)\cdot\overline{A}(1-xt).$$

In particular, if $A = B = \phi_q(\cdot)$ and $\varepsilon_q(\cdot)$ is trivial, then a change of variables gives

$${}_2F_1(\lambda)_{\mathbb{F}_q} := {}_2F_1\left(\begin{matrix} \phi_q, & \phi_q \\ & \varepsilon_q\end{matrix} \mid \lambda\right)_{\mathbb{F}_q} = -\frac{\phi_q(-1)}{q}\cdot\sum_{x\in\mathbb{F}_q}\phi_q(x(x-1)(x-\lambda)). \tag{4.8}$$

[5]For multiplicative characters χ, we adopt the convention that $\chi(0) := 0$.

In analogy with Gauss' integral formulas, which give *periods* of elliptic curves, Greene's functions compute traces of Frobenius over $\mathbb{F}_q$. Indeed, if $\mathrm{char}(\mathbb{F}_q) > 3$ and $\lambda \in \mathbb{F}_q \setminus \{0, 1\}$, then (4.8) gives

$$|E_\lambda(\mathbb{F}_q)| = q + 1 + q\phi_q(-1) \cdot {}_2F_1(\lambda)_{\mathbb{F}_q}. \tag{4.9}$$

In terms of the desired analogy, if $q \equiv 3 \pmod 4$, then (4.7) and (4.8) gives the counterpart of (4.4)

$$I_{\mathbb{F}_q}(a, b) = q \cdot {}_2F_1(1 - b^2/a^2)_{\mathbb{F}_q}.$$

To complete the analogy, we require a quadratic transformation law which plays the role of (4.6). We conclude by stating this recent theorem of Evans and Greene (see Th. 2 of [**6**]), which precisely offers the desired analogous transformation.

Theorem 4.1. [Th. 2 of [**6**]] *Suppose that A, $A^2\overline{B}$, and $\phi_q A\overline{B}$ are all nontrivial characters of $\mathbb{F}_q^\times$. If $t \in \mathbb{F}_q \setminus \{-1\}$, then*

$$\begin{aligned} &{}_2F_1\left(\begin{matrix} A, & B \\ & A^2 \end{matrix} \;\middle|\; \frac{4t}{(1+t)^2}\right)_{\mathbb{F}_q} \\ &= \frac{\overline{A}(4)\phi_q B(-1)G(A^2\overline{B}) \cdot G(\phi_q \overline{A}B)}{G(\phi_q)G(A)} \cdot B^2(1+t)\,{}_2F_1\left(\begin{matrix} \phi_q\overline{A}B, & B \\ & \phi_q A \end{matrix} \;\middle|\; t^2\right)_{\mathbb{F}_q}. \end{aligned}$$

5. EPILOGUE. We hope that the reader agrees that the story presented here is a beautiful amalgamation of facts about elliptic curves over $\mathbb{C}$ and over finite fields. It is quite marvelous to find that the hypergeometric functions of Gauss (in the case of $\mathbb{R}$) and of Greene (in the case of $\mathbb{F}_q$) underlie different features in the theory of elliptic curves that are captured by sequences of arithmetic and geometric means. We hope that this story encourages readers to learn more about the theory of Gauss' class numbers, elliptic curves, and hypergeometry. We highly recommend D. Cox's book "Primes of the form $x^2 + ny^2$" [**5**] and "Pi and the AGM" [**3**] by P. Borwein and J. Borwein.

We aim to entice readers with the following tantalizing problems.

Problems.

(1) What can one prove about the sizes of the jellyfish in $\mathcal{J}_{\mathbb{F}_q}$? This question is intimately connected to the unproven Cohen-Lenstra heuristics on the expected behavior of class groups of imaginary quadratic orders.

(2) Determine an "optimal" function $D(q)$ for which

$$d(\mathbb{F}_q) \geq D(q).$$

In particular, how close to optimal is the lower bound in Theorem 2.4? Is the correct lower bound more like $\gg \sqrt{q}\log\log(q)$?

(3) It would be very interesting to define variants of AGM *in situations where choices of square-root are not well-defined, such as the complex field $\mathbb{C}$ and the finite fields $\mathbb{F}_q$ with $q \not\equiv 3 \pmod 4$.*

To conclude, we must confess that the $\mathrm{AGM}_{\mathbb{F}_q}$ jellyfish are merely alluring examples of creatures that inhabit the magnificent kingdom formed out of elliptic curves over finite fields. The beautiful $\mathrm{AGM}_{\mathbb{F}_q}$ sequences innocently offer glimpses of the

fascinating theory of isogenies for elliptic curves over finite fields, which form networks, dubbed *isogeny volcanoes*. The jellyfish are examples arise from "2-volcanoes of height 1." Isogeny volcanoes play important roles in computational number theory and cryptography. They are often employed as a means of accelerating number theoretic algorithms. They have even been used to quickly compute values of Euler's partition function [**4**]. This important theory has its origins in David Kohel's 1996 PhD thesis [**11**]. We invite interested readers to read the delightful expository article [**19**] by Sutherland.

ACKNOWLEDGMENT. The authors thank the referees, Jennifer Balakrishnan, Hasan Saad, and Drew Sutherland for comments and suggestions that improved this article. The second author thanks the Thomas Jefferson Fund and the NSF (DMS-2002265 and DMS-2055118) for their generous support, as well as the Kavli Institute grant NSF PHY-1748958. The third author is grateful for the support of a Fulbright Nehru Postdoctoral Fellowship.

REFERENCES

1. S. Ahlgren and K. Ono, *Modularity of a certain Calabi-Yau threefold*, Montash. Math. **129** (3) (2000), 177–190. 11
2. G. Andrews, R. Askey and R. Roy, *Special functions*, encyclopedia of mathematics and its applications, **71**, Cambridge University Press, (2001). 12
3. J. Borwein and P. Borwein, *Pi and the AGM: A study in analytic number theory and computational complexity*, Canadian mathematical society series of monographs and advanced texts, **4**, John Wiley and Sons, 1998. 1, 11, 14
4. J. H. Bruinier, K. Ono, and A. V. Sutherland, *Class polynomials for nonholomorphic modular functions*, J. Number Th. **161** (2016), 204-229. 15
5. D. A. Cox, *Primes of the form $x^2 + ny^2$. Fermat, class field theory, and complex multiplication*, John Wiley and Sons, Hoboken, N.J., 2013. 9, 10, 14
6. R. Evans and J. Greene, *A quadratic hypergeometric ${}_2F_1$ transformation over finite fields*, Proc. Amer. Math. Soc. **145** (2017), 1071-1076. 14
7. J. Greene, *Character sum analogues for hypergeometric and generalized hypergeometric functions over finite fields*, Thesis (Ph.D.)-University of Minnesota, 1984. 13
8. J. Greene, *Hypergeometric functions over finite fields*, Trans. Amer. Math. Soc. **301** (1) (1987), 77–101. 13
9. D. Husemöller, *Elliptic curves*, Springer, GTM Vol. 111 (2004). 12
10. N. Koblitz, *Introduction to elliptic curves and modular forms*, 2nd. edition, Springer-Verlag, New York, 1993. 5
11. D. Kohel, *Endomorphism rings of elliptic curves over finite fields*, PhD thesis, Univ. California (Berkeley), 1996. 15
12. B. Mazur, *Number theory as gadfly*, Amer. Math. Monthly **98** (7) (1991), 593-610. 4
13. K. Ono, *Values of Gaussian hypergeometric series*, Trans. Amer. Math. Soc. **350** (3) (1998), 1205–1223. 13
14. K. Ono, *The web of modularity: Arithmetic of the coefficients of modular forms and q-series*, CBMS, Regional Conference series in Mathematics, 102, Amer. Math. Soc., Providence, 2004. 13
15. H.-G. Rück, *A note on elliptic curves over finite fields*, Math. Comp. **49** (1987), 301-304. 9
16. J. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Springer Verlag, New York, 2009. 5, 7, 11
17. J. Silverman, *Taxicabs and sums of two cubes*, Amer. Math. Monthly **100** (1993), no. 4, 331-340. 4
18. R. Schoof, *Nonsingular plane cubic curves over finite fields*, J. Comb. Theory Ser. A **46** (2) (1987), 183-211. 11
19. A. V. Sutherland, *Isogeny volcanoes*, ANTS X- Proc. Algorithmic Number Theory Symposium, Open Book Ser. 1, Math. Sci. Publ., Berkeley, 2013, 507-530. 6, 15
20. R. Taylor and A. Wiles, *Ring theoretic properties of certain Hecke algebras*, Ann. of Math. **141** (1995), 553-572. 4
21. J. F. Voloch, *A note on elliptic curves over finite fields*, Bull. Soc. Math. France **116** (1988), 455-458. 9
22. L. C. Washington, *Elliptic curves, number theory, and cryptography*, Chapman & Hall, Boca Raton, FL. 2008. 5
23. A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Ann. of Math. (2) **141** (1995), 443-551. 4

MICHAEL J. GRIFFIN *Department of Mathematics, 275 TMCB, Brigham Young University, Provo, UT 84602*
mjgriffin@math.byu.edu

KEN ONO *Department of Mathematics, University of Virginia, Charlottesville, VA 22904*
ken.ono691@virginia.edu

NEELAM SAIKIA *Department of Mathematics, University of Virginia, Charlottesville, VA 22904*
nlmsaikia1@gmail.com

WEI-LUN TSAI *Department of Mathematics, University of Virginia, Charlottesville, VA 22904*
wt8zj@virginia.edu