Experimental Mathematics, 21(1):1–10, 2012
Copyright © Taylor & Francis Group, LLC
ISSN: 1058-6458 print / 1944-950X online
DOI: 10.1080/10586458.2012.632754

On Group Structures Realized by Elliptic Curves over a Fixed Finite Field

Reza Rezaeian Farashahi and Igor E. Shparlinski

CONTENTS

2000 AMS Subject Classification: 11G05, 11G20, 14H52
Keywords: elliptic curve, finite field, group structure

We obtain explicit formulas for the number of nonisomorphic elliptic curves with a given group structure (considered as an abstract abelian group) and the number of distinct group structures of all elliptic curves over a finite field. We use these formulas to derive some asymptotic estimates and tight upper and lower bounds for various counting functions related to classification of elliptic curves according to their group structure. Finally, we present results of some numerical tests that exhibit several interesting phenomena in the distribution of group structures.

1. INTRODUCTION

1.1. Background

Let $\mathbb{F}_q$ be the finite field of characteristic p with $q = p^k$ elements. An elliptic curve E over a finite field $\mathbb{F}_q$ is given by the *Weierstrass equation*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad (1–1)$$

where the coefficients a_1, a_2, a_3, a_4, a_6 are in $\mathbb{F}_q$.

It is well known that elliptic curves are a versatile cryptographic tool, and in particular, that their group structure plays a crucial role in such applications; see [Avanzi et al. 05].

Let $E(\mathbb{F}_q)$ be the group of $\mathbb{F}_q$-rational points on elliptic curve E including the point at infinity, denoted by $\mathcal{O}$. We recall (see [Avanzi et al. 05, Silverman 95, Washington 08]) that

$$|\#E(\mathbb{F}_q) - q - 1| \le 2\sqrt{q} \quad \text{and} \quad E(\mathbb{F}_q) \simeq \mathbb{Z}_m \times \mathbb{Z}_n,$$

where the unique integers m, n satisfy

$$m \mid n \quad \text{and} \quad m \mid q - 1. \qquad (1–2)$$

Let $G(q; m, n)$ be the number of distinct elliptic curves E over $\mathbb{F}_q$ (up to isomorphism over $\mathbb{F}_q$) such that $E(\mathbb{F}_q) \simeq \mathbb{Z}_m \times \mathbb{Z}_n$. Moreover, let $F(q)$ be the number of distinct group structures of all elliptic curves over the finite field $\mathbb{F}_q$. In this paper, we give explicit formulas for $G(q; m, n)$ and $F(q)$, for all prime powers q and all possible values of m, n. We use these formulas to derive tight upper and lower bounds on $F(q)$ and also an asymptotic formula for the average value of $F(q)$ over prime powers $q \le Q$ as $Q \to \infty$.

We also present some numerical results concerning the frequency of the "most common" group structure over $\mathbb{F}_q$, that is, for

$$G(q) = \max_{n,m} G(q; m, n). \tag{1–3}$$

These results reveal several interesting phenomena in the behavior of $G(q)$ and the parameters m, n, and $t = p + 1 - mn$ at which this value is achieved.

Finally, we note that the distribution of group structures generated by all elliptic curves over all finite fields $\mathbb{F}_q$ has been studied in [Banks et al. 12].

1.2. Notation

Throughout the paper, p always denotes a prime, and $q = p^k$ always denotes a prime power. As usual, we use $d(s)$ and $\varphi(s)$ to denote the number of positive integer divisors and the Euler function of s, respectively. We write $E/\mathbb{F}$ if an elliptic curve E is defined over a field $\mathbb{F}$.

Let t be an integer such that $\gcd(t, p) = 1$ and $t^2 \le 4q$. Let $\Delta = t^2 - 4q$ and let c_t be the largest integer such that

$$c_t^2 \mid \Delta \quad \text{and} \quad \Delta/c_t^2 \equiv 0 \text{ or } 1 \pmod 4.$$

Let s_t be the largest integer such that $s_t^2 \mid q + 1 - t$ and $s_t \mid q - 1$. We note that $s_t \mid c_t$.

For each positive divisor m of s_t, let

$$\mathcal{M}_t(m) = \{e \in \mathbb{N} : m \mid e,\ e \mid c_t\}$$

and

$$\mathcal{S}_t(m) = \mathcal{M}_t(m) \setminus \bigcup_{\substack{l \in \mathbb{N},\, l > m \\ m \mid l,\, l \mid s_t}} \mathcal{M}_t(l).$$

Moreover, for every negative integer D with $D \equiv 0$ or $1 \pmod 4$ we denote by $h(D)$ the class number of some quadratic order of discriminant D.

For $p > 2$, let χ_p be the quadratic character modulo p. Moreover, for $p = 2$, we define $\chi_p(x)$ as 0, 1, or -1 if $x \equiv 0 \pmod 2$, $x \equiv \pm 1 \pmod 8$, or $x \equiv \pm 3 \pmod 8$, respectively. We also define

$$\alpha_p = \frac{1 - \chi_p(-1)}{2}, \quad \beta_p = \chi_p(-3), \quad \gamma_p = \chi_p(-4).$$

The implied constants in the symbols O, $\ll$, and $\gg$ are absolute. We recall that the notations $U = O(V)$, $U \ll V$, and $V \gg U$ are all equivalent to the assertion that the inequality $|U| \le cV$ holds for some constant $c > 0$.

2. OUR RESULTS

2.1. Explicit Formulas

Here we give some explicit formulas for $G(q; m, n)$ and $F(q)$.

Theorem 2.1. *Let $q = p^k$ be a power of a prime p. Let m, n be positive integers. Let $t = q + 1 - mn$ and $\Delta = t^2 - 4q$. Then $G(q; m, n)$ equals:*

(1) $\sum_{l \in \mathcal{S}_t(m)} h\left(\frac{\Delta}{l^2}\right)$ *if* $\gcd(t, p) = 1$, $t^2 \le 4q$, $m \mid n$, *and* $m \mid q - 1$;

(2) $h(-4p)$ *if k is odd,* $m = 1$, *and* $n = q + 1$;

(3) $h(-p)$ *if k is odd,* $p \equiv 3 \pmod 4$, $m = 2$, *and* $n = (q + 1)/2$;

(4) 1 *if k is odd,* $p = 2$ *or* 3, $m = 1$, *and* $n = q + 1 \pm \sqrt{pq}$;

(5) $1 - \gamma_p$ *if k is even,* $m = 1$, *and* $n = q + 1$;

(6) $1 - \beta_p$ *if k is even,* $m = 1$ *and* $n = q + 1 \pm \sqrt{q}$;

(7) $(p + 6 - 4\beta_p - 3\gamma_p)/12$ *if k is even, and* $m = n = \sqrt{q} \pm 1$;

(8) 0 *otherwise.*

The following result gives explicit formulas for the number $F(q)$ of distinct group structures of all elliptic curves over $\mathbb{F}_q$.

Theorem 2.2. *Let $q = p^k$ be a power of a prime p. For the number $F(q)$ of distinct group structures of all elliptic curves over $\mathbb{F}_q$, we have*

$$F(q) = \sum_{\substack{t \in \mathbb{Z},\ t^2 \le 4q, \\ \gcd(t,p)=1}} d(s_t) + \begin{cases} 1 + \alpha_p, & \text{if } k \text{ is odd, } p > 3, \\ 3 + \alpha_p, & \text{if } k \text{ is odd, } p = 2, 3, \\ 3 + \alpha_p - \beta_p, & \text{if } k \text{ is even, } p > 3, \\ 5, & \text{if } k \text{ is even, } p = 2, 3. \end{cases}$$

2.2. Estimates and Average Values

We now present explicit upper and lower bounds on $F(q)$.

Theorem 2.3. *Let $q = p^k$ be a power of a prime p. For the number $F(q)$ of distinct group structures of all elliptic* *curves over* $\mathbb{F}_q$*, we have*

$$\frac{2\pi^2}{3}\sqrt{q}\left(1-\frac{1}{p}\right)+d(q-1)+5>F(q)$$
$$>\begin{cases}2\sqrt{q}+2, & \text{if } p=2,\\ 5\sqrt{q}\,(1-1/p)-2, & \text{if } p\ge 3.\end{cases}$$

We also show that the bounds of Theorem 2.3 are asymptotically tight.

Theorem 2.4. *As* $q=p^k\to\infty$ *via the set of prime powers, we have*

$$\limsup_{q\to\infty}\frac{F(q)}{\sqrt{q}\,(1-1/p)}=\frac{2\pi^2}{3}, \qquad (2\text{–}1)$$

$$\liminf_{\substack{q\to\infty\\ q\ \text{odd}}}\frac{F(q)}{\sqrt{q}\,(1-1/p)}=5, \qquad (2\text{–}2)$$

$$\liminf_{k\to\infty}\frac{F(2^k)}{2^{k/2}}=2. \qquad (2\text{–}3)$$

Finally, we derive an asymptotic formula for the average value of $F(q)$.

Theorem 2.5. *For* $Q\to\infty$*, as q runs over the set of prime powers, we have*

$$\sum_{q\le Q}F(q)=(\vartheta+o(1))\frac{Q^{3/2}}{\log Q},$$

where

$$\vartheta=\frac{8}{3}\sum_{m=1}^{\infty}\frac{1}{m^2\varphi(m)}=3.682609\ldots.$$

Our argument can also be used to obtain an explicit bound on the error term in Theorem 2.5.

3. PRELIMINARIES

3.1. Endomorphism Rings

For an elliptic curve $E/\mathbb{F}_q$, let $N=\#E(\mathbb{F}_q)$ and $t=q+1-N$. Let π denote the *Frobenius endomorphism* on E, given by

$$\pi:(x,y)\mapsto(x^q,y^q).$$

We note that π is the root of the characteristic polynomial X^2-tX+q in the ring of $\mathbb{F}_q$-endomorphisms of E. This ring is denoted by $\mathrm{End}_{\mathbb{F}_q}(E)$. Moreover, by $\mathrm{End}(E)=\mathrm{End}_{\overline{\mathbb{F}}_q}(E)$ we denote the full endomorphism ring, that is, the ring of $\overline{\mathbb{F}}_q$-endomorphisms of E. Let $\Delta=t^2-4q$ be the discriminant of the characteristic polynomial of E.

Suppose $\gcd(t,p)=1$. Then E is called an ordinary elliptic curve. We have $\mathrm{End}(E)=\mathrm{End}_{\mathbb{F}_q}(E)$. Moreover, $\mathrm{End}(E)$ is isomorphic to some order O in the quadratic imaginary field $K=\mathbb{Q}(\sqrt{\Delta})$. In particular, if O_K denotes the maximal order in K, that is, the ring of algebraic integers of K, then

$$\mathbb{Z}[\pi]=\mathbb{Z}\left[\frac{\Delta+\sqrt{\Delta}}{2}\right]\subseteq\mathrm{End}(E)\subseteq O_K.$$

Let $c_t=[O_K:\mathbb{Z}[\pi]]$ be the conductor of $\mathbb{Z}[\pi]$, that is, the largest integer such that $\Delta/c_t^2\equiv 0,1 \pmod 4$. Then $\Delta_K=\Delta/c_t^2$, called the fundamental discriminant, is the discriminant of the field K. Also, $O_K=\mathbb{Z}\left[\frac{\Delta_K+\sqrt{\Delta_K}}{2}\right]$. We note that $O=\mathbb{Z}+cO_K$, where the conductor $c=[O_K:O]$ is a divisor of c_t. Furthermore, $c^2\Delta_K$ is the discriminant of O, so the order O is uniquely determined by its discriminant and denoted by $O(\Delta)$.

Now suppose $p\mid t$. Then E is called a supersingular elliptic curve. Let $\mathbb{Q}_{\infty,p}$ denote the unique quaternion algebra over $\mathbb{Q}$ that is ramified only at p and ∞. Then $\mathrm{End}_{\mathbb{F}_q}(E)$ is either a quadratic order in $K=\mathbb{Q}(\sqrt{\Delta})$ or a maximal order in $\mathbb{Q}_{\infty,p}$. Moreover, $\mathrm{End}(E)$ is a maximal order in $\mathbb{Q}_{\infty,p}$; see [Schoof 87, Silverman 95, Waterhouse 69].

3.2. Isogeny Classes

Two elliptic curves over $\mathbb{F}_q$ are called *isogenous* over $\mathbb{F}_q$ if they have the same number of points over $\mathbb{F}_q$. The number of $\mathbb{F}_q$-rational points of the elliptic curve $E/\mathbb{F}_q$ satisfies the Hasse–Weil bound. On the other hand, the Deuring–Waterhouse theorem, see [Washington 08, Waterhouse 69], describes all possible values of N that can be the cardinality of $E(\mathbb{F}_q)$ for some elliptic curve $E/\mathbb{F}_q$.

Lemma 3.1. *Let* $q=p^k$ *be a power of a prime p. Let* $t\in\mathbb{Z}$ *and let* $N=q+1-t$*. The integer N is the cardinality of* $E(\mathbb{F}_q)$ *for some elliptic curve* $E/\mathbb{F}_q$ *if and only if one of the following conditions is satisfied:*

(1) $t^2\le 4q$ *and* $\gcd(t,p)=1$*;*

(2) *k is odd and* $t=0$*;*

(3) *k is odd,* $t=\pm\sqrt{pq}$*,* $p=2$ *or* 3*;*

(4) *k is even,* $t=0$*,* $p\not\equiv 1 \pmod 4$*;*

(5) *k is even,* $t=\pm\sqrt{q}$*,* $p\not\equiv 1 \pmod 3$*;*

(6) *k is even,* $t=\pm 2\sqrt{q}$*.*

Let Δ be a negative integer with $\Delta \equiv 0$ or 1 (mod 4) and let c be the largest integer such that $c^2 \mid \Delta$ and $\Delta/c^2 \equiv 0$ or 1 (mod 4). Let $H(\Delta)$ denote the Kronecker class number of Δ. We have

$$H(\Delta) = \sum_{l \mid c,\ l>0} h\left(\frac{\Delta}{l^2}\right).$$

Let $I(q;N)$ be the number of distinct elliptic curves $E/\mathbb{F}_q$ (up to isomorphism over $\mathbb{F}_q$) such that $\#E(\mathbb{F}_p) = N$. By [Schoof 87, Theorem 4.6] we have the following result.

Lemma 3.2. *Let $q = p^k$ be a power of a prime p. Let $t \in \mathbb{Z}$ and let $N = q + 1 - t$. Then $I(q;N)$ equals:*

(1) $H(t^2 - 4q)$, *if* $t^2 \le 4q$ *and* $\gcd(t,p) = 1$;

(2) $H(-4p)$, *if k is odd and $t = 0$;*

(3) 1, *if k is odd, $t = \pm\sqrt{pq}$, $p = 2$ or 3;*

(4) $1 - \gamma_p$, *if k is even, $t = 0$, $p \not\equiv 1 \pmod 4$;*

(5) $1 - \beta_p$, *if k is even, $t = \pm\sqrt{q}$, $p \not\equiv 1 \pmod 3$;*

(6) $(p + 6 - 4\beta_p - 3\gamma_p)/12$, *if k is even, $t = \pm 2\sqrt{q}$;*

(7) 0, *otherwise.*

3.3. Group Structures

The group of $\mathbb{F}_q$-rational points on the elliptic curve $E/\mathbb{F}_q$ is isomorphic to the group $\mathbb{Z}_m \times \mathbb{Z}_n$, with unique integers m, n such that $m \mid n$ and $m \mid q-1$. We note that every group $\mathbb{Z}_m \times \mathbb{Z}_n$ with integers m, n satisfying the above conditions can occur as the group $E(\mathbb{F}_q)$ for some elliptic curve $E/\mathbb{F}_q$. The following theorem describes the possible group structures for elliptic curves over finite fields; see [Rück 87, Tsfasman and Vlăduţ 91, Voloch 88].

Lemma 3.3. *Let $q = p^k$ be a power of a prime p. Let m, n be positive integers with $m \le n$. Let $t = q + 1 - mn$. There is an elliptic curve $E/\mathbb{F}_q$ such that $E(\mathbb{F}_q) \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ if and only if one of the following holds:*

(1) $\gcd(t,p) = 1$, $t^2 \le 4q$, $m \mid n$, *and* $m \mid q-1$;

(2) *k is odd, $t = 0$, $p \not\equiv 3 \pmod 4$, and $m = 1$;*

(3) *k is odd, $t = 0$, $p \equiv 3 \pmod 4$, and $m = 1$ or 2;*

(4) *k is odd, $t = \pm\sqrt{pq}$, $p = 2$ or 3, and $m = 1$;*

(5) *k is even, $t = 0$, $p \not\equiv 1 \pmod 4$, and $m = 1$;*

(6) *k is even, $t = \pm\sqrt{q}$, $p \not\equiv 1 \pmod 3$, and $m = 1$;*

(7) *k is even, $t = \pm 2\sqrt{q}$, and $m = n = \sqrt{q} \mp 1$.*

We note that case (1) in Lemma 3.3 corresponds to ordinary elliptic curves, and the other cases correspond to supersingular elliptic curves.

As usual, we let $E[l]$ be the set of l-torsion points of the elliptic curve $E/\mathbb{F}_q$, that is,

$$E[l] = \left\{P : P \in E(\overline{\mathbb{F}}_q),\ lP = \mathcal{O}\right\}.$$

Lemma 3.4. *For an ordinary elliptic curve $E/\mathbb{F}_q$, the following are equivalent:*

(1) $m = \max\{l : l \in \mathbb{N},\ \gcd(l,q) = 1,\ E[l] \subseteq E(\mathbb{F}_q)\}$,

(2) $m = \max\left\{l : l \in \mathbb{N},\ \ l \mid q-1,\ \ l^2 \mid \#E(\mathbb{F}_q),\ \ O\left(\frac{\Delta}{l^2}\right) \subseteq \mathrm{End}(E)\right\}$,

(3) $E(\mathbb{F}_q) \simeq \mathbb{Z}_m \times \mathbb{Z}_n$, *where $m \mid n$ and $m \mid q-1$.*

Proof. We recall that for all positive integers l with $\gcd(l,q) = 1$, we have $E[l] \subseteq E(\mathbb{F}_q)$ if and only if $l \mid q-1$, $l^2 \mid \#E(\mathbb{F}_q)$, and $O\left(\frac{\Delta}{l^2}\right) \subseteq \mathrm{End}(E)$; see [Schoof 87, Proposition 3.7]. Thus, the values of m in cases (1) and (2) are the same.

Moreover, for all positive integers l with $\gcd(l,q) = 1$, we have $E[l] \simeq \mathbb{Z}_l \times \mathbb{Z}_l$. Suppose $E(\mathbb{F}_q) \simeq \mathbb{Z}_m \times \mathbb{Z}_n$, where $m \mid n$ and $m \mid q-1$. Then for all l with $\gcd(l,q) = 1$, we have $E[l] \subseteq E(\mathbb{F}_q)$ if and only if $l \mid m$. Hence cases (1) and (3) are also equivalent. □

We recall the definition of c_t and s_t and the sets $\mathcal{S}_t(m)$, given in Section 1.

Lemma 3.5. *Let E be an ordinary elliptic curve over $\mathbb{F}_q$. Assume that m, n are positive integers with $m \mid n$, $m \mid q-1$, and $mn = \#E(\mathbb{F}_q) = q + 1 - t$. Then we have $E(\mathbb{F}_q) \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ if and only if for some $l \in \mathcal{S}_t(m)$, we have*

$$\mathrm{End}(E) = O\left(\frac{\Delta}{l^2}\right).$$

Proof. We note that

$$\mathrm{End}(E) = O\left(\frac{\Delta}{l^2}\right),$$

where l is some positive divisor of c_t. By assumption, m is a divisor of s_t. From Lemma 3.4, we have $E(\mathbb{F}_q) \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ if and only if m is the largest divisor of s_t satisfying $O\left(\frac{\Delta}{m^2}\right) \subseteq \mathrm{End}(E) = O\left(\frac{\Delta}{l^2}\right)$. The latter is equivalent to $l \in \mathcal{S}_t(m)$, which completes the proof. □

3.4. Primes in Arithmetic Progressions

For a real $z \geq 2$ and integers $s > r \geq 0$, we denote by $\pi(z; s, r)$ the number of primes $p \leq z$ such that $p \equiv r \pmod{s}$ and recall that by the Siegel–Walfisz theorem, see [Crandall and Pomerance 05, Theorem 1.4.6], we have the following.

Lemma 3.6. *For every fixed $A > 0$ there exists $C > 0$ such that for $z \geq 2$ and for all positive integers $s \leq (\log z)^A$,*

$$\max_{\gcd(r,s)=1} \left| \pi(z; s, r) - \frac{\operatorname{li} z}{\varphi(s)} \right| = O\left(z \exp\left(-C\sqrt{\log z} \right) \right),$$

where

$$\operatorname{li} z = \int_2^z \frac{du}{\log u}.$$

4. PROOFS

4.1. Proof of Theorem 2.1

We note that $G(q; m, n) \neq 0$ if and only if m, n satisfy one of the cases given by Lemma 3.3, and we study these cases separately.

For case (1), we assume that $\gcd(t, p) = 1$ and $t^2 \leq 4q$. From Lemma 3.3, we see that $G(q; m, n) \neq 0$ if and only if $m \mid n$ and $m \mid q - 1$. So let m, n be positive integers satisfying such conditions. From Lemma 3.5, for all elliptic curves $E/\mathbb{F}_q$, we have $E(\mathbb{F}_q) \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ if and only if $\operatorname{End}(E) = O(\Delta/l^2)$ for some $l \in \mathcal{S}_t(m)$. We also note that all orders $O(\Delta/l^2)$ with $l \in \mathcal{S}_t(m)$ will occur as the endomorphism ring of some elliptic curves over $\mathbb{F}_q$; see [Waterhouse 69, Theorem 4.2]. Moreover, the number of $\mathbb{F}_q$ isomorphism classes of elliptic curves with $\operatorname{End}(E) = O(\Delta/l^2)$ is $h\left(\Delta/l^2\right)$ (see, e.g., [Waterhouse 69, Theorem 4.5], [Schoof 87]). Therefore, we have

$$G(q; m, n) = \sum_{l \in \mathcal{S}_t(m)} h\left(\frac{\Delta}{l^2}\right).$$

For case (2), we have $t = 0$. Moreover, $G(q; m, n)$ with $m = 1$ is the number of cyclic supersingular elliptic curves over $\mathbb{F}_q$ with trace 0 (up to $\mathbb{F}_q$-isomorphism), that is, $h(-4p)$; see [Schoof 87, Lemma 4.8].

For case 3, we have $t = 0$ and $q \equiv 3 \pmod{4}$. Also, $G(q; m, n)$ with $m = 2$ is the number of noncyclic supersingular elliptic curves over $\mathbb{F}_q$ with trace 0 (up to $\mathbb{F}_q$-isomorphism). This is $H(-4p) - h(-4p) = h(-p)$.

For cases (4)–(7), we have $t^2 = q, 2q, 3q, 4q$. Also, all supersingular elliptic curves in the corresponding isogeny class are cyclic. Then $G(q; m, n)$ with $m = 1$ is the isogeny class number given by Lemma 3.2.

4.2. Proof of Theorem 2.2

The possible group structures of elliptic curves over $\mathbb{F}_q$ are the groups isomorphic to $\mathbb{Z}_m \times \mathbb{Z}_n$, for some values m, n described by Lemma 3.3. For an integer t, let $f(q; t)$ be the number of distinct group structures of elliptic curves over $\mathbb{F}_q$ with trace t. Let t be a positive integer with $|t| \leq 2\sqrt{q}$. From Lemma 3.3, we consider the following cases for t:

Case 1. Suppose $\gcd(t, p) = 1$. Let $N = q + 1 - t$. Then $\mathbb{Z}_m \times \mathbb{Z}_n$, for $1 \leq m \leq n$, is the group structure of some elliptic curve $E/\mathbb{F}_q$ with trace t if and only if (1–2) holds and $mn = N$. This is equivalent to having $m^2 \mid N$, $m \mid q - 1$, and $mn = N$. As before, let s_t be the greatest integer such that $s_t^2 \mid N$ and $s_t \mid q - 1$. Therefore, there is a one-to-one correspondence between the group structures of ordinary elliptic curves over $\mathbb{F}_q$ with trace t and positive integer divisors of s_t. So

$$f(q; t) = d(s_t). \qquad (4–1)$$

Case 2. Suppose $t \mid p$. Then we may have $t^2/q = 0$, 1, 2, 3, or 4. From Lemma 3.3, we see that

$$f(q; t) = \begin{cases} 1 + \alpha_p, & \text{if } k \text{ is odd, } t = 0, \\ 1, & \text{if } k \text{ is odd, } p = 2 \text{ or } 3,\ t^2 = pq. \\ \alpha_p, & \text{if } k \text{ is even, } p \neq 2,\ t = 0, \\ 1, & \text{if } k \text{ is even, } p = 2,\ t = 0, \\ (1 - \beta_p)/2, & \text{if } k \text{ is even, } p \neq 3,\ t^2 = q, \\ 1, & \text{if } k \text{ is even, } p = 3,\ t^2 = q, \\ 1, & \text{if } k \text{ is even, } t^2 = 4q, \\ 0, & \text{otherwise.} \end{cases} \qquad (4–2)$$

Now we sum up $g(q; t)$ over all possible integer values of t. We have

$$F(q) = \sum_{t \in \mathbb{Z},\ t^2 \leq 4q} f(q; t).$$

Using (4–1) and (4–2), we obtain the explicit formulas for $F(q)$.

4.3. Proof of Theorem 2.3

Let $\mathcal{H}_q$ be the set of integers of the Hasse–Weil interval, that is,

$$\mathcal{H}_q = \left\{ N : N \in \mathbb{N},\ q - 2\sqrt{q} + 1 \leq N \leq q + 2\sqrt{q} + 1 \right\}.$$

We recall from the proof of Theorem 2.2 that for every $N \in \mathcal{H}_q$ with $\gcd(N - 1, p) = 1$, there is a bijection between the set of group structures of isogenous elliptic curves $E/\mathbb{F}_q$ with order N and the set of positive divisors m of $q-1$ with $m^2 \mid N$.

For a positive integer divisor m of $q-1$, let $g(q;m)$ be the number of distinct group structures $\mathbb{Z}_m \times \mathbb{Z}_n$ of elliptic curves over $\mathbb{F}_q$ for some $n \in \mathbb{N}$. In other words, $g(q;m)$ is the cardinality of the set of positive integers n such that there exists some elliptic curve $E/\mathbb{F}_q$ with $E(\mathbb{F}_q) \simeq \mathbb{Z}_m \times \mathbb{Z}_n$. Clearly, we have

$$F(q) = \sum_{m \mid q-1} g(q;m). \tag{4–3}$$

Here, we express $g(q;m)$ by counting the number of multiples of m^2 in $\mathcal{H}_q$. For a positive integer divisor m of $q-1$, let

$$\mathcal{H}_q(m) = \left\{N : N \in \mathcal{H}_q,\ \gcd(N-1,p) = 1,\ m^2 \mid N\right\}.$$

From the proof of Theorem 2.2 and by Lemma 3.3, for all positive divisors m of $q-1$, we have

$$g(q;m) = \#\mathcal{H}_q(m) + \delta_q(m), \tag{4–4}$$

where

$$\delta_q(m) = \begin{cases} 1, & \text{if } k \text{ is odd, } p \neq 2,3,\ m = 1, \\ 1 + \alpha_p - \beta_p, & \text{if } k \text{ is even, } p \neq 2,3,\ m = 1, \\ 3, & \text{if } p = 2 \text{ or } 3,\ m = 1, \\ \alpha_p, & \text{if } k \text{ is odd, } m = 2, \\ 1, & \text{if } k \text{ is even, } m = \sqrt{q} \pm 1, \\ 0, & \text{otherwise.} \end{cases}$$

Next, using (4–3) and (4–4), we obtain

$$F(q) = \sum_{m \mid q-1} \#\mathcal{H}_q(m) + \delta_q(m). \tag{4–5}$$

We note that $\#\mathcal{H}_q = 2\left[2\sqrt{q}\right] + 1$. Moreover, for all divisors m of $q-1$, if $m \geq \sqrt{q}+1$, then $\#\mathcal{H}_q(m) = 0$, and if $m < \sqrt{q}+1$, then

$$\left[\frac{4\sqrt{q}}{m^2}\right] - \left[\frac{4\sqrt{q}}{m^2 p}\right] - 1 \leq \#\mathcal{H}_q(m) \leq \left[\frac{4\sqrt{q}}{m^2}\right] - \left[\frac{4\sqrt{q}}{m^2 p}\right] + 1,$$

and so

$$\frac{4\sqrt{q}}{m^2}\left(1 - \frac{1}{p}\right) - 2 < \#\mathcal{H}_q(m) < \frac{4\sqrt{q}}{m^2}\left(1 - \frac{1}{p}\right) + 2. \tag{4–6}$$

Therefore, to obtain an upper bound for $F(q)$, we write

$$\begin{aligned} &\sum_{m \mid q-1} \#\mathcal{H}_q(m) \\ &\quad = \sum_{\substack{m \mid q-1, \\ m < \sqrt{q-1}}} \#\mathcal{H}_q(m) + \sum_{\substack{m \mid q-1, \\ \sqrt{q-1} \leq m < \sqrt{q}+1}} \#\mathcal{H}_q(m) \\ &\quad < \sum_{m \mid q-1} \frac{4\sqrt{q}}{m^2}\left(1 - \frac{1}{p}\right) + \sum_{\substack{m \mid q-1, \\ m < \sqrt{q-1}}} 2 \\ &\qquad + \sum_{\substack{m \mid q-1, \\ \sqrt{q-1} \leq m < \sqrt{q}+1}} \#\mathcal{H}_q(m). \end{aligned}$$

One can see that

$$\sum_{\substack{m \mid q-1, \\ \sqrt{q-1} \leq m < \sqrt{q}+1}} \#\mathcal{H}_q(m) + \sum_{m \mid q-1} \delta_q(m) \leq 5.$$

Then from (4–5), we have

$$\begin{aligned} F(q) &< 4\sqrt{q}\left(1 - \frac{1}{p}\right) \sum_{m \in \mathbb{N}} \frac{1}{m^2} + d(q-1) + 5 \\ &= \frac{2\pi^2}{3}\sqrt{q}\left(1 - \frac{1}{p}\right) + d(q-1) + 5. \end{aligned}$$

Now we provide the lower bound for $F(q)$. If $p = 2$, then using (4–5), we write

$$F(q) \geq \#\mathcal{H}_q(1) + \sum_{m \mid q-1} \delta_q(m) \geq [2\sqrt{q}] + 3 > 2\sqrt{q} + 2.$$

For $p \geq 3$, using (4–5), we write

$$F(q) \geq \#\mathcal{H}_q(1) + \#\mathcal{H}_q(2) + \sum_{m \mid q-1} \delta_q(m).$$

We now use (4-6) with $m = 1, 2$. Also note that

$$\#\mathcal{H}_q(2) > \sqrt{q}\left(1 - \frac{1}{p}\right) - 1$$

if $q \equiv 1 \pmod 4$. Since

$$\sum_{m \mid q-1} \delta_q(m) \geq \begin{cases} 1, & \text{for } q \equiv 1 \pmod 4, \\ 2, & \text{for } q \equiv 3 \pmod 4, \end{cases}$$

we complete the proof.

4.4. Proof of Theorem 2.4

To prove (2–1), we choose a sufficiently large integer L, and let M be the least common multiple of all positive integers $m \leq L$.

We now choose a prime $p \equiv 1 \pmod M$ and put $q = p$. Using (4–3) and (4–4), we derive

$$F(q) \ge \sum_{\substack{m\,|q-1\\ m\le L}} g(q;m) = \sum_{m\le L} g(q;m) = \sum_{m\le L} \left(\#\mathcal{H}_q(m) + O(1)\right).$$

Since by (4–6) for $q = p$ we have $\#\mathcal{H}_q(m) = 4\sqrt{q}/m^2 + O(1)$, we now derive

$$F(q) \ge \sum_{m\le L} \left(\frac{4\sqrt{q}}{m^2} + O(1)\right) = 4\sqrt{q}\left(\frac{\pi^2}{6} + O(1/L)\right) + O(L).$$

Since by the prime number theorem we have $q \ge M \ge \exp\left((1+o(1))L\right)$, then taking $L \to \infty$, we obtain

$$F(q) = \left(\frac{2\pi^2}{3} + o(1)\right)\sqrt{q} = \left(\frac{2\pi^2}{3} + o(1)\right)\sqrt{q}\left(1 - \frac{1}{p}\right)$$

for the above sequence of $q = p$.

For (2–2), we recall [Heath-Brown 86, Lemma 1], which asserts that there are infinitely many primes p such that either $p = 2\ell + 1$ for a prime ℓ or $p = 2\ell_1\ell_2 + 1$ for primes $\ell_1, \ell_2 \ge p^\rho$ for some $\rho > 1/4$ (one can take $\rho = 0.276\ldots$; see the proof of the cited lemma). Using (4–3) and (4–4), we see that for each such prime p and $q = p$, we have

$$\begin{aligned} F(q) &= \sum_{m\,|q-1} g(q;m) = \sum_{m\,|q-1} \left(\#\mathcal{H}_q(m) + O(1)\right) \\ &= \#\mathcal{H}_q(1) + \#\mathcal{H}_q(2) + O(1) = 5\sqrt{q} + O(1) \\ &= 5\sqrt{q}\left(1 - \frac{1}{p}\right) + O(1). \end{aligned}$$

Finally to prove (2–3), we recall that if $q = 2^r$, where r is prime, then all prime divisors ℓ of $q-1$ satisfy $\ell \equiv 1 \pmod r$ (since r is the multiplicative order of 2 modulo ℓ, and thus $r \mid \ell - 1$). In particular, for any $m \mid q-1$ with $m > 1$, we have $m > r$. Hence as before, and also recalling (4–6), for $q = 2^r$ we obtain

$$\begin{aligned} F(q) &= \#\mathcal{H}_q(1) + \sum_{\substack{m\,|q-1\\ m>1}} \left(\#\mathcal{H}_q(m) + O(1)\right) \\ &= \#\mathcal{H}_q(1) + O\Bigg(\sum_{\substack{m\,|q-1\\ m>r}} \left(q^{1/2}m^{-2} + 1\right)\Bigg) \\ &= \#\mathcal{H}_q(1) + O\left(q^{1/2}r^{-1} + d(q-1)\right) \\ &= (2+o(1))\,q^{1/2}, \end{aligned}$$

which concludes the proof.

4.5. Proof of Theorem 2.5

Since there are $O(Q^{1/2})$ prime powers $q = p^k \le Q$ with $k \ge 2$, using the upper bound of Theorem 2.3, we obtain

$$\sum_{q\le Q} F(q) = \sum_{p\le Q} F(p) + O(Q).$$

We see from (4–5) and the well-known estimate on the divisor function

$$d(s) = s^{o(1)}, \quad s \to \infty, \tag{4–7}$$

see [Hardy and Wright 79, Theorem 317], that

$$\begin{aligned} \sum_{p\le Q} F(p) &= 4\sum_{p\le Q}\Bigg(\sqrt{p}\sum_{m\,|p-1}\frac{1}{m^2} + O(d(p-1))\Bigg) \\ &= 4\sum_{m\le Q}\frac{1}{m^2}\sum_{\substack{p\le Q\\ p\equiv 1 \pmod m}} \sqrt{p} + O\left(Q^{1+o(1)}\right). \end{aligned}$$

By Lemma 3.6 and partial summation, we see that for $m \le \log Q$, we have

$$\begin{aligned} \sum_{\substack{p\le Q\\ p\equiv 1 \pmod m}} \sqrt{p} &= \left(\frac{2}{3} + o(1)\right) Q^{1/2}\frac{\operatorname{li} Q}{\varphi(m)} \\ &= \left(\frac{2}{3} + o(1)\right)\frac{Q^{3/2}}{\varphi(m)\log Q}. \end{aligned}$$

Furthermore, for $m > \log Q$, we use the trivial estimate

$$\sum_{\substack{p\le Q\\ p\equiv 1 \pmod{m}}} \sqrt{p} \le Q^{1/2}\sum_{\substack{2\le n\le Q\\ n\equiv 1 \pmod{m}}} 1 = O(Q^{3/2}m^{-1}).$$

The result now follows.

5. DISTRIBUTION OF THE MOST FREQUENT GROUP STRUCTURES

5.1. Preliminaries

In our study of $G(q)$, given by (1–3), we concentrate only on prime values $q = p$. First of all, we note that for any N, we have

$$\sum_{\substack{m,n\ge 1\\ mn=N}} G(p;m,n) = I(p;N),$$

where as before, $I(p;N)$ is the number of distinct isomorphism classes of elliptic curves $E/\mathbb{F}_p$ (up to isomorphism over $\mathbb{F}_p$) such that $\#E(\mathbb{F}_p) = N$ (see Lemma 3.2). In particular,

$$\max_N I(p;N)/d(N) \le G(p) \le \max_N I(p;N). \tag{5–1}$$

It is well known that the bounds on the Kronecker class number imply that $I(p;N) \ll p^{1/2}\log p(\log\log p)^2$, and

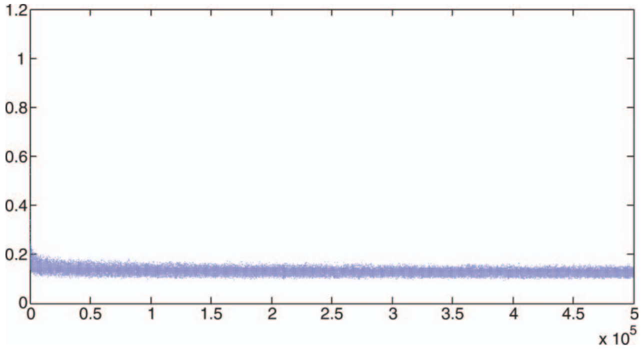

FIGURE 1. Distribution of $G(p)/p^{1/2}\log p$ for primes $p < 500\,000$ (color figure available online).

for all $N \in [p+1-p^{1/2}, p+1+p^{1/2}]$, except at most two of them, we have $I(p;N) \gg p^{1/2}/\log p$; see, for example, [Lenstra 87, Proposition 1.9]. Thus, from (4–7) and (5–1), we derive that

$$G(p) = p^{1/2+o(1)}. \tag{5–2}$$

5.2. Numerical Data

We see from (5–2) that it is natural to study the values of $G(p)$ scaled by $p^{1/2}$. In fact, our experiments with 41 538 primes $p < 500\,000$ show that scaling by $p^{1/2}\log p$ is more natural, and the ratio $G(p)/p^{1/2}\log p$ stabilizes in a reasonably narrow strip between roughly 0.1 and 0.2; see Figure 1.

We also notice that for all primes checked, the value of $G(p)$ is always achieved for (m,n) with $m = 1$ (that is, for curves with cyclic group of points). Moreover, for some primes, the same value is also achieved for some pairs (m,n) with $m = 2$. In our experiments, the value of $G(p)$ has never been achieved with $m \ge 3$. In Figure 2, we compare $G(p)$ with $I(p) = \max_N I(p;N)$.

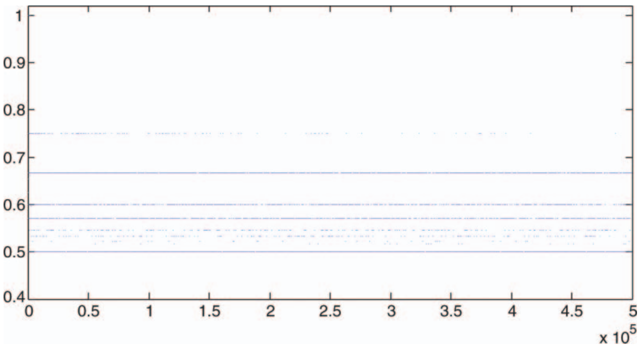

FIGURE 3. Distribution of $G(p)/I(p)$ achieved for the same value of t for primes $p < 500\,000$ (color figure available online).

For primes $p < 500\,000$ where we have computed $G(p)/I(p)$, the ratio 1 was achieved for $p = 2, 5, 7, 17, 29, 41, 101, 1009, 1109, 1879, 4289$, where $G(p)$ and $I(p)$ are achieved with the same value of t with $s_t = 1$. Also, only four times (for $p = 37591$, 187651, 246391, 397591) was the value of $G(p)/I(p)$ below 0.5. Unfortunately, these extreme values of both types are invisible in Figure 2. We do not know whether these primes are just some sporadic exceptions or whether there are infinitely many such primes. More generally, it would certainly be interesting to evaluate or at least obtain nontrivial theoretic estimates for

$$\limsup_{p\to\infty} G(p)/I(p) \quad \text{and} \quad \liminf_{p\to\infty} G(p)/I(p).$$

This may also help to explain the presence of several horizontal lines in Figure 2 (slightly emphasized there to improve their visibility).

Clearly, one expects the value of $G(p)$ to be achieved for (m,n) for which $t = p+1-N$, where $N = mn$, is small, so that $\Delta = t^2 - 4p$ has a large absolute value, which leads to a large value of $I(p;N)$. However, this

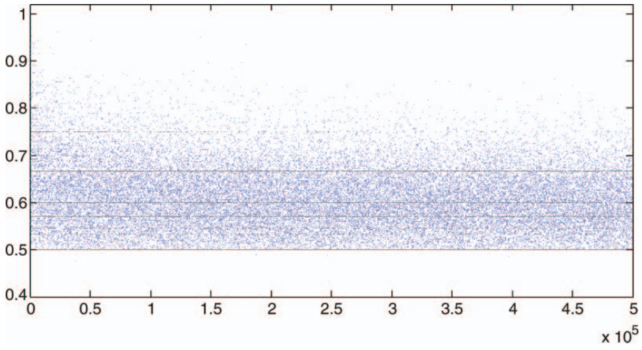

FIGURE 2. Distribution of $G(p)/I(p)$ for primes $p < 500\,000$ (color figure available online).

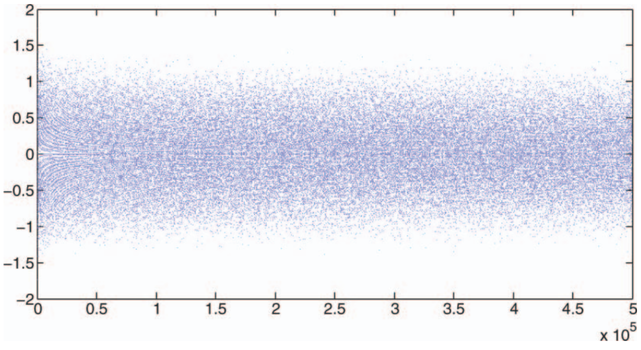

FIGURE 4. Distribution of $t/p^{1/2}$, where $t \in \mathcal{T}_{\max}$, for primes $p < 500\,000$ (color figure available online).

Ratio $\frac{G(p)}{I(p)}$	$\frac{1}{2}$	$\frac{2}{3}$	$\frac{3}{5}$	$\frac{4}{7}$	$\frac{6}{11}$	$\frac{5}{8}$	$\frac{8}{15}$	$\frac{3}{4}$	$\frac{12}{23}$	$\frac{17}{26}$	$\frac{16}{31}$	$\frac{45}{68}$	$\frac{28}{47}$	1
Number of primes p in Figure 2	2933	2300	1287	1236	329	292	268	258	71	45	39	28	15	11
Number of primes p in Figure 3	2931	1968	883	1012	220	1	161	139	32	1	19	1	1	11

TABLE 1. Ratios of $G(p)/I(p)$ for primes $p < 500\,000$.

is offset by the fact that for N having many divisors, the value of $I(p;N)$ is "split" between $d(s_t)$ values of $G(p;m,n)$. This effect is observed in the numerical results presented below, which show that if $G(p;m,n) = G(p)$, then $t = p+1-mn$ is small but not necessarily very small. In particular, most of the time, $G(p)$ and $I(p)$ are achieved for different values of t, namely in about 82.2% of the cases within the above range of primes p (more precisely, for 34 158 primes out of the total number 41 538 of primes $p < 500\,000$). Furthermore, it seems that the remaining 7380 cases in which $G(p)$ and $I(p)$ are achieved at the same value of t are those that are mainly (but not entirely) responsible for the presence of horizontal lines in Figure 2. Indeed, the same lines are clearly visible in Figure 3, where the ratios $G(p)/I(p)$ are plotted only if they come from the same value of t.

We also summarize this result in Table 1, which gives the number of points on horizontal lines in Figures 2 and 3 (ordered by the total number of points).

Let $\mathcal{T}_{\max}(p)$ be the set of traces corresponding to the most "popular" group structure, that is,

$$\mathcal{T}_{\max}(p) = \{t \ : \ t = p+1-mn, \ G(p;m,n) = G(p)\}\,.$$

In Table 2, we give some data about the distribution of $\#\mathcal{T}_{\max}(p)$ for primes $p < 500\,000$. In particular, $\#\mathcal{T}_{\max}(p) = 1$ in about 52% of the cases.

We also remark that the set $\mathcal{T}_{\max}(p)$ is symmetric around 0 (that is, $\mathcal{T}_{\max}(p) = -\mathcal{T}_{\max}(p)$) for 20 020 primes out of the total number 41 538 of primes $p < 500\,000$.

Figure 4 presents the scaled values $t/p^{1/2}$ for $t \in \mathcal{T}_{\max}(p)$ and $p < 500\,000$.

As we have mentioned, we do not have any solid theoretical explanation for the observed facts.

$\#\mathcal{T}_{\max}(p)$	1	2	3	4	5	6	7	10
Number of primes p	21638	19087	230	524	19	36	3	1

TABLE 2. Distribution of $\#\mathcal{T}_{\max}(p)$ for primes $p < 500\,000$.

REFERENCES

[Avanzi et al. 05] R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, and F. Vercauteren, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. CRC Press, 2005.

[Banks et al. 12] W. D. Banks, F. Pappalardi, and I. E. Shparlinski, "On Group Structures Realized by Elliptic Curves over Arbitrary Finite Fields." *Exp. Math.* 21 (2012), 11–25.

[Crandall and Pomerance 05] R. Crandall, and C. Pomerance. *Prime Numbers: A Computational Perspective*, 2nd edition. Springer, 2005.

[Hardy and Wright 79] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford Univ. Press, 1979.

[Heath-Brown 86] D. R. Heath-Brown. "Artin's Conjecture for Primitive Roots." *Quart. J. Math.* 37 (1986), 27–38.

[Lenstra 87] H. W. Lenstra. "Factoring Integers with Elliptic Curves." *Ann. of Math.* 126 (1987), 649–673.

[Rück 87] H.-G. Rück. "A Note on Elliptic Curves over Finite Fields." *Math. Comp.* 49 (1987), 301–304.

[Schoof 87] R. Schoof. "Nonsingular Plane Cubic Curves over Finite Fields." *J. of Combin. Theory* 46 (1987), 183–211.

[Silverman 95] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 1995.

[Tsfasman and Vlăduţ 91] M. Tsfasman and S. G. Vlăduţ. *Algebraic Geometric Codes*. Kluwer, 1991.

[Voloch 88] J. F. Voloch. "A Note on Elliptic Curves over Finite Fields." *Bull. Soc. Math. Franc.* 116 (1988), 455–458.

[Washington 08] L. C. Washington. *Elliptic Curves: Number Theory and Cryptography*. CRC Press, 2008.

[Waterhouse 69] W. C. Waterhouse. "Abelian Varieties over Finite Fields." *Ann. Sc. Ec. Norm. Sup. (4)* 2 (1969), 521–560.

Reza Rezaeian Farashahi, Department of Computing, Macquarie University, Sydney, NSW 2109, Australia (reza.farashahi@mq.edu.au) and Isfahan University of Technology, Department of Mathematical Sciences, P.O. Box 85145, Isfahan, Iran

Igor E. Shparlinski, Department of Computing, Macquarie University, Sydney, NSW 2109, Australia (igor.shparlinski@mq.edu.au)

Received March 14, 2010; accepted October 19, 2010.