2007

Some properties of the distribution of the numbers of points on elliptic curves over a finite prime field

Saiying He
Trinity College, Hartford Connecticut

James McLaughlin
West Chester University of Pennsylvania, jmclaughlin2@wcupa.edu

SOME ELEMENTARY PROPERTIES OF THE DISTRIBUTION OF THE NUMBERS OF POINTS ON ELLIPTIC CURVES OVER A FINITE PRIME FIELD

SAIYING HE AND J. MC LAUGHLIN

Abstract. Let $p \geq 5$ be a prime and for $a, b \in \mathbb{F}_p$, let $E_{a,b}$ denote the elliptic curve over $\mathbb{F}_p$ with equation $y^2 = x^3 + a\,x + b$. As usual define the trace of Frobenius $a_{p,\,a,\,b}$ by

$$\#E_{a,b}(\mathbb{F}_p) = p + 1 - a_{p,\,a,\,b}.$$

We use elementary facts about exponential sums and known results about binary quadratic forms over finite fields to evaluate the sums $\sum_{t\in\mathbb{F}_p} a_{p,\,t,\,b}$, $\sum_{t\in\mathbb{F}_p} a_{p,\,a,\,t}$, $\sum_{t=0}^{p-1} a_{p,\,t,\,b}^2$, $\sum_{t=0}^{p-1} a_{p,\,a,\,t}^2$ and $\sum_{t=0}^{p-1} a_{p,\,t,\,b}^3$ for primes p in various congruence classes.

As an example of our results, we prove the following: Let $p \equiv 5 \pmod 6$ be prime and let $b \in \mathbb{F}_p^*$. Then

$$\sum_{t=0}^{p-1} a_{p,\,t,\,b}^3 = -p\left((p-2)\left(\frac{-2}{p}\right) + 2p\right)\left(\frac{b}{p}\right).$$

1. Introduction

Let $p \geq 5$ be a prime and let $\mathbb{F}_p$ be the finite field of p elements. For $a, b \in \mathbb{F}_p$, let $E_{a,b}$ denote the elliptic curve over $\mathbb{F}_p$ with equation $y^2 = x^3 + a\,x + b$. Denote by $E_{a,\,b}(\mathbb{F}_p)$ the set of $\mathbb{F}_p$– rational points on the curve $E_{a,\,b}$ and define the trace of Frobenius, a_p, by the equation

$$\#E_{a,\,b}(\mathbb{F}_p) = p + 1 - a_p.$$

A simple counting argument makes it clear that

$$a_p = -\sum_{x\in\mathbb{F}_p}\left(\frac{x^3 + a\,x + b}{p}\right), \tag{1.1}$$

where $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol. We recall some of the arithmetic properties of the distribution of a_p. The following theorem is due to Hasse [4]:

Theorem 1. *The integer a_p satisfies*

$$-2\sqrt{p} \leq a_p \leq 2\sqrt{p}.$$

Date: August 13th, 2004.
1991 *Mathematics Subject Classification.* 11G20.
Key words and phrases. Elliptic Curves, Finite Fields.

Since we wish to look at how a_p varies as the coefficients a and b of the elliptic curve vary, it is convenient for our purposes to write a_p for the elliptic curve $E_{a,b}$ as $a_{p,\,a,\,b}$. The following result is well known (an easy consequence of the remarks on page 36 of [3], for example).

Proposition 1. *Let the function* $f : \mathbb{Z} \to \mathbb{N}_0$ *be defined by setting*

$$f(k) = \#\{(a,b) \in \mathbb{F}_p^* \times \mathbb{F}_p^* : a_{p,\,a,\,b} = k\}. \tag{1.2}$$

Then for each integer k,

$$\frac{p-1}{2}\bigg| f(k).$$

The following result can be found in [2] (page 57).

Proposition 2. *Define the function* $f_1 : \mathbb{Z} \to \mathbb{N}_0$ *by setting*

$$f_1(k) = \#\{(a,b) \in \mathbb{F}_p \times \mathbb{F}_p \setminus \{(0,0)\} : a_{p,\,a,\,b} = k\}. \tag{1.3}$$

Then for each integer k,

$$f_1(k) = f_1(-k).$$

The following result is also known ([3], page 37, for example).

Proposition 3. *Let* v *be a quadratic non-residue modulo* p. *Then*

$$a_{p,\,a,\,b} = -a_{p,\,v^2a,\,v^3b}.$$

To better understand the distribution of the $a_{p,\,a,\,b}$ it makes sense to study the moments. The j *-invariant* of the elliptic curve $E_{a,b}$ is defined by

$$j = \frac{2^8 3^3 a^3}{4a^3 + 27b^2},$$

provided $4a^3 + 27b^2 \neq 0$. Michel showed in [7] that if $\{E_{a(t),\,b(t)} : t \in \mathbb{F}_p\}$ is a one-parameter family of elliptic curves with $a(t)$ and $b(t)$ polynomials in t such that

$$j(t) := \frac{2^8 3^3 a(t)^3}{4a(t)^3 + 27b(t)^2},$$

is non-constant, then

$$\sum_{t \in \mathbb{F}_p} a^2_{p,\,a(t),\,b(t)} = p^2 + O(p^{3/2}).$$

In [2] Birch defined

$$S_R(p) = \sum_{a,\,b=0}^{p-1} \left[\sum_{x=0}^{p-1} \left(\frac{x^3 - ax - b}{p} \right) \right]^{2R}$$

for integral $R \geq 1$, and proved

Theorem 2. [1] *For $p \geq 5$,*

$$\begin{aligned}
S_1(p) &= (p-1)p^2,\\
S_2(p) &= (p-1)(2p^3-3p),\\
S_3(p) &= (p-1)(5p^4-9p^2-5p),\\
S_4(p) &= (p-1)(14p^5-28p^3-20p^2-7p),\\
S_5(p) &= (p-1)(42p^6-90p^4-75p^3-35p^2-9p-\tau(p)),
\end{aligned}$$

where $\tau(p)$ is Ramanujan's τ-function.

Theorem 2 evaluates sums of the form $\sum_{a,\,b=0}^{p-1} a_{p,\,a,\,b}^{2R}$ in terms of p and these results were derived by Birch as consequences of the Selberg trace formula .

In this present paper we instead use elementary facts about exponential sums and known results about binary quadratic forms over finite fields to evaluate the sums $\sum_{t\in\mathbb{F}_p} a_{p,\,t,\,b}$, $\sum_{t\in\mathbb{F}_p} a_{p,\,a,\,t}$, $\sum_{t=0}^{p-1} a_{p,\,t,\,b}^2$, $\sum_{t=0}^{p-1} a_{p,\,a,\,t}^2$ and $\sum_{t=0}^{p-1} a_{p,\,t,\,b}^3$, for primes p in particular congruence classes. In particular, we prove the following theorems.

Theorem 3. *Let $p \geq 5$ be a prime, and a, $b \in \mathbb{F}_p$. Then*
(i) $\sum_{t\in\mathbb{F}_p} a_{p,\,t,\,b} = -p\left(\frac{b}{p}\right)$,
(ii)$\sum_{t\in\mathbb{F}_p} a_{p,\,a,\,t} = 0$.

This result is elementary but we prove it for the sake of completeness.

Theorem 4. *Let $p \equiv 5 \pmod 6$ be prime and let $b \in \mathbb{F}_p^*$. Then*

$$\sum_{t=0}^{p-1} a_{p,\,t,\,b}^2 = p\left(p-1-\left(\frac{-1}{p}\right)\right). \tag{1.4}$$

Theorem 5. *Let $p \geq 5$ be prime and let $a \in \mathbb{F}_p^*$. Then*

$$\sum_{t=0}^{p-1} a_{p,\,a,\,t}^2 = p\left(p-1-\left(\frac{-3}{p}\right)-\left(\frac{-3a}{p}\right)\right). \tag{1.5}$$

Theorem 4 and Theorem 5 could be deduced from Theorem 2, but we believe it is of interest to give elementary proofs that do not use the Selberg trace formula.

Theorem 6. *Let $p \equiv 5 \pmod 6$ be prime and let $b \in \mathbb{F}_p^*$. Then*

$$\sum_{t=0}^{p-1} a_{p,\,t,\,b}^3 = -p\left((p-2)\left(\frac{-2}{p}\right)+2p\right)\left(\frac{b}{p}\right).$$

[1]In [2], Birch incorrectly omitted the factor of $p-1$ in his statement of Theorem 2.

2. Proof of the Theorems

We introduce some standard notation. Define $e(j/p) := \exp(2\pi i j/p)$, so that

$$\sum_{t=0}^{p-1} e\left(\frac{jt}{p}\right) = \begin{cases} p, & p\,|\,j, \\ 0, & (j,p)=1. \end{cases} \tag{2.1}$$

Define

$$G_p = \begin{cases} \sqrt{p}, & p \equiv 1 (\mod 4), \\ i\sqrt{p}, & p \equiv 3 (\mod 4). \end{cases} \tag{2.2}$$

Lemma 1. *Let* $\left(\frac{\cdot}{p}\right)$ *denote the Legendre symbol, modulo* p. *Then*

$$\left(\frac{z}{p}\right) = \frac{1}{G_P}\sum_{d=1}^{p-1}\left(\frac{d}{p}\right) e\left(\frac{dz}{p}\right). \tag{2.3}$$

Proof. See [1], Theorem 1.1.5 and Theorem 1.5.2. □

We will occasionally use the fact that if $\mathbb{H}$ is a subset of $\mathbb{F}_p$,

$$\sum_{d\in\mathbb{F}_p\setminus\mathbb{H}}\left(\frac{d}{p}\right) = -\sum_{d\in\mathbb{H}}\left(\frac{d}{p}\right). \tag{2.4}$$

We will also occasionally make use of some implications of the Law of Quadratic Reciprocity (see [5], page 53, for example).

Theorem 7. *Let* p *and* q *be odd primes. Then*
(a) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.
(b) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.
(c) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{((p-1)/2)((q-1)/2)}$.

We now prove Theorems 3, 4, 5 and 6,

Theorem 3. *Let* $p \geq 5$ *be a prime, and* $a,\, b \in \mathbb{F}_p$. *Then*
(i) $\sum_{t\in\mathbb{F}_p} a_{p,\,t,\,b} = -p\left(\frac{b}{p}\right)$,
(ii) $\sum_{t\in\mathbb{F}_p} a_{p,\,a,\,t} = 0$.

Proof. (i) From (1.1) and (2.3), it follows that

$$\sum_{t\in\mathbb{F}_p} a_{p,t,b} = -\sum_{x\in\mathbb{F}_p}\sum_{d=1}^{p-1}\frac{1}{G_P}\left(\frac{d}{p}\right) e\left(\frac{d(x^3+b)}{p}\right)\sum_{t\in\mathbb{F}_p} e\left(\frac{tdx}{p}\right)$$

The inner sum over t is zero unless $x=0$, in which case it equals to p. The left side therefore can be simplified to give

$$\sum_{t\in\mathbb{F}_p} a_{p,t,b} = -\sum_{d=1}^{p-1}\frac{p}{G_P}\left(\frac{d}{p}\right) e\left(\frac{db}{p}\right) = -p\left(\frac{b}{p}\right).$$

The last equality follows from (2.3).

(ii): From (1.1) and (2.3), it follows that

$$\sum_{t\in \mathbb{F}_p} a_{p,a,t} = -\sum_{x\in\mathbb{F}_p}\sum_{d=1}^{p-1}\frac{1}{G_p}\left(\frac{d}{p}\right) e\left(\frac{d(x^3+ax)}{p}\right)\sum_{t\in\mathbb{F}_p} e\left(\frac{dt}{p}\right) = 0.$$

The inner sum over t is equal to 0, by (2.1), since $1 \le d \le p-1$.

□

The result at (ii) follows also, in the case of primes $p \equiv 3 \pmod 4$, from the fact that $a_{p,\,a,\,t} = -a_{p,\,a,\,p-t}$. However, this is not the case for primes $p \equiv 1 \pmod 4$. For example,

$$\{a_{13,\,1,\,t} : 0 \le t \le 12\} = \{-6,-4,2,-1,0,5,1,1,5,0,-1,2,-4\}.$$

The results in Theorem 3 are almost certainly known, although we have not been able to find a reference.

Theorem 4. *Let $p \equiv 5 \pmod 6$ be prime and let $b \in \mathbb{F}_p^*$. Then*

$$\sum_{t=0}^{p-1} a_{p,\,t,\,b}^2 = p\left(p-1-\left(\frac{-1}{p}\right)\right).$$

Proof. From (1.1) and (2.3) it follows that

$$\sum_{t\in\mathbb{F}_p} a_{p,t,b}^2 = \frac{1}{G_p^2}\sum_{d_1,d_2=1}^{p-1}\left(\frac{d_1d_2}{p}\right)\sum_{x_1,x_2\in\mathbb{F}_p} e\left(\frac{d_1(x_1^3+b)+d_2(x_2^3+b)}{p}\right) \times\sum_{t\in\mathbb{F}_p} e\left(\frac{t(d_1x_1+d_2x_2)}{p}\right).$$

The inner sum over t is zero, unless $x_1 \equiv -d_1^{-1}d_2x_2 \pmod p$, in which case it equals p. Thus

$$\sum_{t\in\mathbb{F}_p} a_{p,t,b}^2 = \frac{p}{G_p^2}\sum_{d_1,d_2=1}^{p-1}\left(\frac{d_1d_2}{p}\right) e\left(\frac{b(d_1+d_2)}{p}\right)\sum_{x_2\in\mathbb{F}_p} e\left(\frac{d_1^{-2}d_2x_2^3(d_1^2-d_2^2)}{p}\right).$$

Since the map $x \to x^3$ is one-to-one on F_p, when $p \equiv 5 \pmod 6$, the x_2^3 in the inner sum can be replaced by x_2. Thus the inner sum is zero unless $d_2^2 - d_1^2 \equiv 0 \pmod p$, in which case it equals p. It follows that

$$\begin{aligned}\sum_{t\in\mathbb{F}_p} a_{p,t,b}^2 &= \frac{p^2}{G_p^2}\left(\sum_{d_1=1}^{p-1}\left(\frac{d_1^2}{p}\right) e\left(\frac{b(2d_1)}{p}\right) + \sum_{d_1=1}^{p-1}\left(\frac{-d_1^2}{p}\right) e\left(\frac{b(d_1-d_1)}{p}\right)\right)\\ &= \frac{p^2}{G_p^2}\left(-1+\left(\frac{-1}{p}\right)(p-1)\right) = \frac{p^2}{G_p^2}\left(\frac{-1}{p}\right)\left(p-1-\left(\frac{-1}{p}\right)\right).\end{aligned}$$

We have once again used (2.3) to compute the sums, noting that the sums above start with $d_1 = 1$. The result now follows since $p/G_p^2 \times (-1|p) = 1$ for all primes $p \ge 3$.

□

Remarks: (1) It is clear that the results will remain true if $a(t) = t$ is replaced by any function $a(t)$ which is one-to-one on F_p.
(2) It is more difficult to determine the values taken by $\sum_{t\in\mathbb{F}_p} a^2_{p,t,b}$ for primes $p \equiv 1 (\text{mod } 6)$. This is principally because the map $x \to x^3$ is not one-to-one on F_p for these primes (so that (2.1) cannot be used so easily to simplify the summation), but also because the answer depends on which coset b belongs to in $\mathbb{F}_p^*/\mathbb{F}_p^{*3}$.

Before proving the next theorem, it is necessary to recall a result about quadratic forms over finite fields. Let q be a power of an odd prime and let η denote the quadratic character on $\mathbb{F}_q^*$ (so that if $q = p$, an odd prime, then $\eta(c) = (c/p)$, the Legendre symbol). The function v is defined on $\mathbb{F}_q$ by

$$v(b) = \begin{cases} -1, & b \in \mathbb{F}_q^*, \\ q-1, & b = 0. \end{cases} \tag{2.5}$$

Suppose

$$f(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j, \qquad \text{with } a_{ij} = a_{ji},$$

is a quadratic form over $\mathbb{F}_q$, with associated matrix $A = (a_{ij})$ and let $\triangle$ denote the determinant of A (f is *non-degenerate* if $\triangle \neq 0$).

Theorem 8. *Let f be a non-degenerate quadratic form over $\mathbb{F}_q$, q odd, in an even number n of indeterminates. Then for $b \in \mathbb{F}_q$ the number of solutions of the equation $f(x_1, \ldots, x_n) = b$ in $\mathbb{F}_q^n$ is*

$$q^{n-1} + v(b)q^{(n-2)/2}\eta\left((-1)^{n/2}\triangle\right). \tag{2.6}$$

Proof. See [6], pp 282–293. □

Theorem 5. *Let $p \geq 5$ be prime and let $a \in \mathbb{F}_p^*$. Then*

$$\sum_{t=0}^{p-1} a^2_{p,\,a,\,t} = p\left(p - 1 - \left(\frac{-3}{p}\right) - \left(\frac{-3a}{p}\right)\right).$$

Proof. Once again (1.1) and (2.3) give that

$$\sum_{t\in\mathbb{F}_p} a^2_{p,\,a,\,t} = \frac{1}{G_p^2}\sum_{d_1,d_2=1}^{p-1}\left(\frac{d_1d_2}{p}\right)\sum_{x_1,x_2\in\mathbb{F}_p} e\left(\frac{d_1(x_1^3+ax_1)+d_2(x_2^3+ax_2)}{p}\right) \times \sum_{t\in\mathbb{F}_p} e\left(\frac{t\,b(d_1+d_2)}{p}\right).$$

The inner sum over t is zero, unless $d_1 \equiv -d_2 (\bmod\ p)$, in which case it equals p. Thus

$$\sum_{t\in\mathbb{F}_p} a_{p,\,a,\,t}^2 = \frac{p}{G_p^2}\left(\frac{-1}{p}\right) \sum_{x_1,\,x_2\in\mathbb{F}_p} \sum_{d_1=1}^{p-1} e\left(\frac{d_1(x_1^3 + a\,x_1 - x_2^3 - a\,x_2)}{p}\right) \tag{2.7}$$
$$= \sum_{x_1,\,x_2\in\mathbb{F}_p} \sum_{d_1=1}^{p-1} e\left(\frac{d_1(x_1 - x_2)(x_1^2 + x_1x_2 + x_2^2 + a)}{p}\right).$$

We have used the fact that $p/G_p^2 \times (-1|p) = 1$ for all primes $p \geq 3$. The inner sum over d_1 equals -1, unless one of the factors $x_1 - x_2$, $x_1^2 + x_1x_2 + x_2^2 + a$ equals 0, in which case the sum is $p - 1$. The equation $x_1 = x_2$ has p solutions and, by (2.6) with $q = p$, $n = 2$, $f(x_1, x_2) = x_1^2 + x_1x_2 + x_2^2$ and $A = \begin{pmatrix} 1 & (p+1)/2 \\ (p+1)/2 & 1 \end{pmatrix}$, the equation $x_1^2 + x_1x_2 + x_2^2 = -a$ has

$$p + (-1)\left(\frac{-1(1-(p+1)^2/4)}{p}\right) = p - \left(\frac{-3}{p}\right)$$

solutions. However, we need to be careful to avoid double counting and to examine when $x_1^2+x_1x_2+x_2^2 = -a$ has a solution with $x_1 = x_2$. The equation $3x_1^2 = -a$ will have two solutions if $\left(\frac{-3a}{p}\right) = 1$ and none if $\left(\frac{-3a}{p}\right) = -1$. Hence the number of solutions to the equation $3x_1^2 = -a$ is $\left(\frac{-3a}{p}\right) + 1$. Thus the number of solutions to $(x_1 - x_2)(x_1^2 + x_1x_2 + x_2^2 + a) = 0$ is

$$p + \left(p - \left(\frac{-3}{p}\right)\right) - \left(\left(\frac{-3a}{p}\right) + 1\right) = 2p - 1 - \left(\frac{-3}{p}\right) - \left(\frac{-3a}{p}\right).$$

Thus

$$\sum_{t\in\mathbb{F}_p} a_{p,\,a,\,t}^2 = \left(2p - 1 - \left(\frac{-3}{p}\right) - \left(\frac{-3a}{p}\right)\right)(p-1)$$
$$+ \left(p^2 - \left(2p - 1 - \left(\frac{-3}{p}\right) - \left(\frac{-3a}{p}\right)\right)\right)(-1).$$

The right side now simplifies to give the result.

□

Before proving Theorem 6, we need some preliminary lemmas.

Lemma 2. *Let $p \equiv 5$ (mod 6) be prime. Then*

$$\sum_{d,e,f=1}^{p-1} \left(\frac{ef(1+e+f)}{p}\right) \sum_{y,z\in\mathbb{F}_p} e\left(\frac{d(-(ey+fz)^3 + ey^3 + fz^3)}{p}\right) \tag{2.8}$$
$$= -p(p-1)\left(1 + \left(\frac{-1}{p}\right)\right)$$

$$+\sum_{d,e,f=1}^{p-1}\left(\frac{e+ef+f}{p}\right)\sum_{y,z\in\mathbb{F}_p} e\left(\frac{d\,fz(-f^2(y+1)^3+e^2y^3+1)}{p}\right).$$

Proof. If $z=0$, the left side of (2.8) becomes

$$\begin{aligned}
S_0 :&= \sum_{d,e,f=1}^{p-1}\left(\frac{ef(1+e+f)}{p}\right)\sum_{y\in\mathbb{F}_p} e\left(\frac{dy^3e(1-e^2)}{p}\right)\\
&= (p-1)\sum_{e,f=1}^{p-1}\left(\frac{ef(1+e+f)}{p}\right)\sum_{y\in\mathbb{F}_p} e\left(\frac{ye(1-e^2)}{p}\right)\\
&= p(p-1)\left(\sum_{f=1}^{p-1}\left(\frac{f(2+f)}{p}\right)+\sum_{f=1}^{p-1}\left(\frac{-f^2}{p}\right)\right)\\
&= p(p-1)\left(\sum_{f=1}^{p-1}\left(\frac{2f^{-1}+1}{p}\right)+\sum_{f=1}^{p-1}\left(\frac{-1}{p}\right)\right)\\
&= p(p-1)\left(-1+(p-1)\left(\frac{-1}{p}\right)\right).
\end{aligned}$$

The second equality follows since $\{y^3 : y\in\mathbb{F}_p\}=\{y : y\in\mathbb{F}_p\}$ for the primes p being considered, the third equality follows from (2.1) and the last equality follows from (2.4).

If $z\neq 0$, then the left side of (2.8) equals

(2.9)

$$S_1 := \sum_{d,e,f,z=1}^{p-1}\left(\frac{ef(1+e+f)}{p}\right)\sum_{y\in\mathbb{F}_p} e\left(\frac{d(-(ey+fz)^3+ey^3+fz^3)}{p}\right)=$$

$$\sum_{d,e,f,z=1}^{p-1}\left(\frac{ef(1+e+f)}{p}\right)\sum_{y\in\mathbb{F}_p} e\left(\frac{dz^3(-(eyz^{-1}+f)^3+e(yz^{-1})^3+f)}{p}\right).$$

Now replace y by yz and then z^3 by z (justified by the same argument as above) and finally e by ef to get this last sum equals

$$\sum_{d,e,f,z=1}^{p-1}\left(\frac{e(1+ef+f)}{p}\right)\times\sum_{y\in\mathbb{F}_p} e\left(\frac{dfz(-f^2(ey+1)^3+ey^3+1)}{p}\right).$$

We wish to extend the last sum to include $z=0$. If we set $z=0$ on the right side of the last equation (and denote the resulting sum by "r.s.") and sum over d and y we get that

$$r.s. = p(p-1)\sum_{e,f=1}^{p-1}\left(\frac{e(1+f(e+1))}{p}\right)$$

$$= p(p-1)\left(\sum_{f=1}^{p-1}\left(\frac{-1}{p}\right) + \sum_{e=1}^{p-2}\sum_{f=1}^{p-1}\left(\frac{e(1+f(e+1))}{p}\right)\right).$$

Replace f by $f(e+1)^{-1}$ in the second sum above and then

$$\begin{aligned}
r.s. &= p(p-1)\left((p-1)\left(\frac{-1}{p}\right) + \sum_{e=1}^{p-2}\sum_{f=1}^{p-1}\left(\frac{e(1+f)}{p}\right)\right) \\
&= p(p-1)\left((p-1)\left(\frac{-1}{p}\right) + \sum_{e=1}^{p-2}\left(\frac{e}{p}\right)\sum_{f=1}^{p-1}\left(\frac{1+f}{p}\right)\right) \\
&= p(p-1)\left((p-1)\left(\frac{-1}{p}\right) + \left(-\left(\frac{-1}{p}\right)\right)(-1)\right) \\
&= p^2(p-1)\left(\frac{-1}{p}\right).
\end{aligned}$$

It follows that the left side of (2.9) equals

$$\begin{aligned}
&- p^2(p-1)\left(\frac{-1}{p}\right) \\
&\quad + \sum_{d,e,f=1}^{p-1}\left(\frac{e(1+ef+f)}{p}\right)\sum_{y,z\in\mathbb{F}_p} e\left(\frac{dfz(-f^2(ey+1)^3+ey^3+1)}{p}\right),
\end{aligned}$$

and thus that the left side of (2.8) equals

(2.10)

$$\begin{aligned}
S_0 + S_1 &= -p(p-1)\left(1+\left(\frac{-1}{p}\right)\right) + \sum_{d,e,f=1}^{p-1}\left(\frac{e(1+ef+f)}{p}\right) \\
&\qquad \times \sum_{y,z\in\mathbb{F}_p} e\left(\frac{dfz(-f^2(ey+1)^3+ey^3+1)}{p}\right) \\
&= -p(p-1)\left(1+\left(\frac{-1}{p}\right)\right) + \sum_{d,e,f=1}^{p-1}\left(\frac{e+ef+f}{p}\right) \\
&\qquad \times \sum_{y,z\in\mathbb{F}_p} e\left(\frac{dfz(-f^2(y+1)^3+e^2y^3+1)}{p}\right).
\end{aligned}$$

The second equality in (2.10) follows upon replacing y by ye^{-1} and then e by e^{-1}. □

Lemma 3. *Let $p \equiv 5 \pmod 6$ be prime. Then*

(2.11)

$$S^* := \sum_{d,e,f=1}^{p-1} \left(\frac{e+ef+f}{p}\right) \sum_{y,z\in\mathbb{F}_p} e\left(\frac{dfz(-f^2(y+1)^3+e^2y^3+1)}{p}\right)$$
$$= 2p(p-1)\left(-1+(p-1)\left(\frac{-1}{p}\right)\right) - 3p(p-1)\left(\frac{-2}{p}\right) + p(p-1)S^{**},$$

where

$$S^{**} := \sum_{e,\, f=2,\; e^2\neq f^2}^{p-2} \left(\frac{(1+e)(e-f)(1+e-f)(-1+f)}{p}\right).$$

Proof. Upon changing the order of summation slightly, we get that

$$S^* = \sum_{e,f=1}^{p-1} \left(\frac{e+ef+f}{p}\right) \sum_{d=1}^{p-1} \sum_{y,z\in\mathbb{F}_p} e\left(\frac{dfz(-f^2(y+1)^3+e^2y^3+1)}{p}\right)$$

If $y=0$, the inner double sum over d and z is zero, unless $f=\pm 1$, if which case it equals $p(p-1)$ and the right side of (2.11) equals

$$p(p-1)\left(\sum_{e=1}^{p-1}\left(\frac{2e+1}{p}\right) + \sum_{e=1}^{p-1}\left(\frac{-1}{p}\right)\right) = p(p-1)\left(-1+(p-1)\left(\frac{-1}{p}\right)\right).$$

By similar reasoning, if $y=-1$, the right side of (2.11) also equals

$$p(p-1)\left(-1+(p-1)\left(\frac{-1}{p}\right)\right).$$

Thus

(2.12)

$$S^* = 2p(p-1)\left(-1+(p-1)\left(\frac{-1}{p}\right)\right)$$
$$+ \sum_{y=1}^{p-2} \sum_{e,f=1}^{p-1} \left(\frac{e+ef+f}{p}\right) \sum_{d=1}^{p-1} \sum_{z\in\mathbb{F}_p} e\left(\frac{dfz(-f^2(y+1)^3+e^2y^3+1)}{p}\right)$$
$$= 2p(p-1)\left(-1+(p-1)\left(\frac{-1}{p}\right)\right) + \sum_{y=1}^{p-2}\left(\frac{y(y+1)}{p}\right)$$
$$\times \sum_{e,f=1}^{p-1} \left(\frac{(e+f)y+e(1+f)}{p}\right) \sum_{d=1}^{p-1} \sum_{z\in\mathbb{F}_p} e\left(\frac{dfz((e^2-f^2)y+1-f^2)}{p}\right),$$

where the last equality follows upon replacing f by $f(y+1)^{-1}$ and e by ey^{-1}. The inner sum over d and z is zero unless

$$(e^2-f^2)y+1-f^2=0,$$

in which case the inner sum is $p(p-1)$. We distinguish the cases $e^2 = f^2$ and $e^2 \neq f^2$. If $e^2 = f^2$, then necessarily $e^2 = f^2 = 1$ and the sum on the right side of (2.12) becomes

(2.13)
$$p(p-1)\sum_{y=1}^{p-2}\left(\frac{y(y+1)}{p}\right)\left(\left(\frac{2(y+1)}{p}\right)+\left(\frac{0}{p}\right)+\left(\frac{-2}{p}\right)+\left(\frac{-2y}{p}\right)\right)$$
$$= -3p(p-1)\left(\frac{-2}{p}\right).$$

If $e^2 \neq f^2$ then
$$y = \frac{f^2-1}{e^2-f^2},$$
and since $y \neq 0, -1$, we exclude $f^2 = 1$ and $e^2 = 1$. After substituting for y in the sum in the final expression in (2.12), we find that
(2.14)
$$S^* = 2p(p-1)\left(-1+(p-1)\left(\frac{-1}{p}\right)\right) - 3p(p-1)\left(\frac{-2}{p}\right) + p(p-1)S^{**},$$
where
$$S^{**} := \sum_{e,\,f=2,\; e^2\neq f^2}^{p-2}\left(\frac{(1+e)(e-f)(1+e-f)(-1+f)}{p}\right). \tag{2.15}$$

□

Lemma 4. *Let $p \equiv 5$ (mod 6) be prime and let S^{**} be as defined in Lemma 3. Then*
$$S^{**} = \sum_{e=0}^{p-1}\sum_{f=0}^{p-1}\left(\frac{(1+e)(e-f)(1+e-f)(-1+f)}{p}\right)$$
$$+ 2\left(\frac{-6}{p}\right) + 3\left(\frac{-2}{p}\right) + 3\left(\frac{-1}{p}\right) + 2.$$

Proof. Clearly we can remove the restrictions $f \neq e$, $f \neq 1$ and $e \neq -1$ freely. If we set $f = -e$, we have that
$$\sum_{e,\,f=2,\; e=-f}^{p-2}\left(\frac{(1+e)(e-f)(1+e-f)(-1+f)}{p}\right) = \sum_{e=2}^{p-2}\left(\frac{-2e(1+2e)}{p}\right)$$
$$= -\left(\left(\frac{-6}{p}\right)+\left(\frac{-2}{p}\right)+\left(\frac{-1}{p}\right)\right).$$
The last equality follows from (2.4). Thus
$$S^{**} = \sum_{e,\,f=2}^{p-2}\left(\frac{(1+e)(e-f)(1+e-f)(-1+f)}{p}\right)$$

$$+\left(\frac{-6}{p}\right)+\left(\frac{-2}{p}\right)+\left(\frac{-1}{p}\right).$$

If f is set equal to 0 in the sum above we get

$$\sum_{e=2}^{p-2}\left(\frac{-e}{p}\right)=-1-\left(\frac{-1}{p}\right).$$

If f is set equal to -1 in this sum we get

$$\sum_{e=2}^{p-2}\left(\frac{-2(2+e)}{p}\right)=-\left(\left(\frac{-4}{p}\right)+\left(\frac{-2}{p}\right)+\left(\frac{-6}{p}\right)\right)$$
$$=-\left(\left(\frac{-1}{p}\right)+\left(\frac{-2}{p}\right)+\left(\frac{-6}{p}\right)\right).$$

Thus

$$S^{**}=\sum_{e=2}^{p-2}\sum_{f=0}^{p-1}\left(\frac{(1+e)(e-f)(1+e-f)(-1+f)}{p}\right)$$
$$+2\left(\left(\frac{-6}{p}\right)+\left(\frac{-2}{p}\right)+\left(\frac{-1}{p}\right)\right)+1+\left(\frac{-1}{p}\right).$$

If we set $e=0$ in this latest sum we get

$$\sum_{f=0}^{p-1}\left(\frac{-f(1-f)(-1+f)}{p}\right)=\sum_{f=0,f\neq 1}^{p-1}\left(\frac{f}{p}\right)=-1.$$

If we set $e=1$ in this sum we get

$$\sum_{f=0}^{p-1}\left(\frac{2(1-f)(2-f)(-1+f)}{p}\right)=\sum_{f=0,f\neq 1}^{p-1}\left(\frac{-2(2-f)}{p}\right)=-\left(\frac{-2}{p}\right).$$

Thus

$$S^{**}=\sum_{e=0}^{p-1}\sum_{f=0}^{p-1}\left(\frac{(1+e)(e-f)(1+e-f)(-1+f)}{p}\right)$$
$$+2\left(\frac{-6}{p}\right)+3\left(\frac{-2}{p}\right)+3\left(\frac{-1}{p}\right)+2.$$

□

Lemma 5. *Let $p\equiv 5(\mod 6)$ be prime. Then*

$$\sum_{e=0}^{p-1}\sum_{f=0}^{p-1}\left(\frac{(1+e)(e-f)(1+e-f)(-1+f)}{p}\right)=p\left(\frac{2}{p}\right)+1.$$

Proof. If f is replaced by $f+1$ and then e is replaced by $e+f$, the value of the double sum above does not change. Thus

$$\sum_{e=0}^{p-1}\sum_{f=0}^{p-1}\left(\frac{(1+e)(e-f)(1+e-f)(-1+f)}{p}\right) \tag{2.16}$$
$$=\sum_{e=0}^{p-1}\sum_{f=0}^{p-1}\left(\frac{(1+e)(e-f-1)(e-f)f}{p}\right)$$
$$=\sum_{e=0}^{p-1}\sum_{f=0}^{p-1}\left(\frac{(1+e+f)(e-1)ef}{p}\right)$$
$$=\sum_{e=0}^{p-1}\sum_{f=0}^{p-1}\left(\frac{e(e-1)}{p}\right)\sum_{f=0}^{p-1}\left(\frac{(1+e+f)f}{p}\right).$$

We evaluate the inner sum using (2.3).

$$\sum_{f=0}^{p-1}\left(\frac{(1+e+f)f}{p}\right)=\frac{1}{G_p^2}\sum_{f=0}^{p-1}\sum_{d_1,d_2=1}^{p-1}\left(\frac{d_1d_2}{p}\right)e\left(\frac{d_1f+d_2(1+e+f)}{p}\right)$$
$$=\frac{1}{G_p^2}\sum_{d_1,d_2=1}^{p-1}\left(\frac{d_1d_2}{p}\right)e\left(\frac{d_2(1+e)}{p}\right)\sum_{f=0}^{p-1}e\left(\frac{f(d_1+d_2)}{p}\right)$$
$$=\frac{p}{G_p^2}\sum_{d_2=1}^{p-1}\left(\frac{-1}{p}\right)e\left(\frac{d_2(1+e)}{p}\right)$$
$$=\frac{p}{G_p^2}\left(\frac{-1}{p}\right)\sum_{d_2=1}^{p-1}e\left(\frac{d_2(1+e)}{p}\right).$$

The next-to-last equality follows since the sum over f in the previous expression is 0, unless $d_1=-d_2$, in which case this sum is p. The sum over d_2 equals $p-1$ if $e=p-1$ and equals -1 otherwise. Hence the sum at (2.16) equals

$$\frac{p}{G_p^2}\left(\frac{-1}{p}\right)\left(\sum_{e=0}^{p-2}\left(\frac{e(e-1)}{p}\right)(-1)+(p-1)\left(\frac{2}{p}\right)\right)$$
$$=\frac{p}{G_p^2}\left(\frac{-1}{p}\right)\left(\left(\frac{2}{p}\right)+1+(p-1)\left(\frac{2}{p}\right)\right)$$
$$=\frac{p}{G_p^2}\left(\frac{-1}{p}\right)\left(p\left(\frac{2}{p}\right)+1\right)=p\left(\frac{2}{p}\right)+1,$$

the last equality following from the remark after (2.7). □

Corollary 1. *Let S^* and S^{**} be as defined in Lemma 3. Then*

$$(i) \qquad S^{**} = (p-2)\left(\frac{2}{p}\right) + 3\left(\frac{-2}{p}\right) + 3\left(\frac{-1}{p}\right) + 3,$$

$$(ii) \qquad S^{*} = p(p-1)\left(1 + (2p+1)\left(\frac{-1}{p}\right) + (p-2)\left(\frac{2}{p}\right)\right).$$

Proof. Lemmas 4 and 5 and the fact that $(-3|p) = -1$ if $p \equiv 5(\,mod\, 6)$ give (i). Lemma 3 and part (i) give (ii). □

Theorem 6. *Let $p \equiv 5$ (mod 6) be prime and let $b \in \mathbb{F}_p^*$. Then*

$$\sum_{t=0}^{p-1} a_{p,\,t,\,b}^3 = -p\left((p-2)\left(\frac{-2}{p}\right) + 2p\right)\left(\frac{b}{p}\right). \tag{2.17}$$

Proof. Let g be a generator of $\mathbb{F}_p^*$. It is a simple matter to show, using (1.1), that

$$\sum_{t=0}^{p-1} a_{p,\,t,\,b}^3 = -\sum_{t=0}^{p-1} a_{p,\,t,\,bg}^3.$$

Thus the statement at (2.17) is equivalent to the statement

$$\sum_{b=1}^{p-1}\sum_{t=0}^{p-1} a_{p,\,t,\,b}^3\left(\frac{b}{p}\right) = -p(p-1)\left((p-2)\left(\frac{-2}{p}\right) + 2p\right). \tag{2.18}$$

Let S denote the left side of (2.18). From (1.1) and (2.3) it follows that

$$\begin{aligned}
S &= -\sum_{b=1}^{p-1}\sum_{t=0}^{p-1}\sum_{x,y,z\in\mathbb{F}_p}\left(\frac{x^3+t\,x+b}{p}\right)\left(\frac{y^3+t\,y+b}{p}\right)\left(\frac{z^3+t\,z+b}{p}\right)\left(\frac{b}{p}\right)\\
&= -\frac{1}{G_p^3}\sum_{d,e,f=1}^{p-1}\left(\frac{def}{p}\right)\sum_{x,y,z,t\in\mathbb{F}_p} e\left(\frac{d(x^3+tx)+e(y^3+ty)+f(z^3+tz)}{p}\right)\\
&\qquad\qquad \times \sum_{b\in\mathbb{F}_p^*}\left(\frac{b}{p}\right) e\left(\frac{b(d+e+f)}{p}\right)\\
&= -\frac{1}{G_p^2}\sum_{d,e,f=1}^{p-1}\left(\frac{def}{p}\right)\left(\frac{d+e+f}{p}\right)\\
&\qquad\qquad \times \sum_{x,y,z,t\in\mathbb{F}_p} e\left(\frac{d(x^3+tx)+e(y^3+ty)+f(z^3+tz)}{p}\right)\\
&= -\frac{1}{G_p^2}\sum_{d,e,f=1}^{p-1}\left(\frac{def}{p}\right)\left(\frac{d+e+f}{p}\right)\sum_{x,y,z\in\mathbb{F}_p} e\left(\frac{dx^3+ey^3+fz^3}{p}\right)\\
&\qquad\qquad \times \sum_{t\in\mathbb{F}_p} e\left(\frac{t(dx+ey+fz)}{p}\right)
\end{aligned}$$

The inner sum is zero, unless $dx+ey+fz=0$ in $\mathbb{F}_p$, in which case it equals p. Upon letting $x=-d^{-1}(ey+fz)$, replacing e by de and f by fe, we get that

$$\begin{aligned}
S &= -\frac{p}{G_p^2}\sum_{d,e,f=1}^{p-1}\left(\frac{ef(1+e+f)}{p}\right)\sum_{y,z\in\mathbb{F}_p} e\left(\frac{d(-(ey+fz)^3+ey^3+fz^3)}{p}\right)\\
&= \frac{p^2(p-1)}{G_p^2}\left(1+\left(\frac{-1}{p}\right)\right)\\
&\quad -\frac{p}{G_p^2}\sum_{d,e,f=1}^{p-1}\left(\frac{e+ef+f}{p}\right)\sum_{y,z\in\mathbb{F}_p} e\left(\frac{dfz(-f^2(y+1)^3+e^2y^3+1)}{p}\right)\\
&= \frac{p^2(p-1)}{G_p^2}\left(1+\left(\frac{-1}{p}\right)\right)-\frac{p}{G_p^2}S^*\\
&= -\frac{p^2(p-1)}{G_p^2}\left(2p\left(\frac{-1}{p}\right)+(p-2)\left(\frac{2}{p}\right)\right)\\
&= -p(p-1)\left(2p+(p-2)\left(\frac{-2}{p}\right)\right),
\end{aligned}$$

which was what needed to be shown, by (2.18). The second equality above follows from Lemma 2. Above S^* is as defined in Lemma 3 and in the next-to-last equality we used Corollary 1, part (ii). In the last equality we used once again the fact that $p/G_p^2(-1|p)=1$.

□

3. Concluding Remarks

Let $p\equiv 5 \pmod 6$ be prime, $b\in\mathbb{F}_p^*$ and k be an odd positive integer. Define

$$f_k(p)=\sum_{t=0}^{p-1} a_{p,\,t,\,b}^k\left(\frac{b}{p}\right).$$

(It is not difficult to show that the right side is independent of $b\in\mathbb{F}_p^*$)

By Theorem 6

$$f_3(p)=-p\left((p-2)\left(\frac{-2}{p}\right)+2p\right).$$

We have not been able to determine $f_k(p)$ for $k\geq 5$ (We do not consider even k, since a formula for each even k can be derived from Birch's work in [2]). We conclude with a table of values of $f_k(p)$ and small primes $p\equiv 5 \pmod 6$, with the hope of encouraging others to work on this problem.

References

[1] Berndt, Bruce C.; Evans, Ronald J.; Williams, Kenneth S. *Gauss and Jacobi sums.* Canadian Mathematical Society Series of Monographs and Advanced Texts. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1998. xii+583 pp.

$p \diagdown k$	5	7	9	11
5	-275	-2315	-20195	-179195
11	-10901	-358061	-12030821	-411625181
17	-36737	-1582913	-68613377	-3016710593
23	8257	2763745	304822657	27903893665
29	-35699	-396299	184745341	35260018501
41	-654401	-88683041	-12260782721	-1716248660321

TABLE 1. $f_k(p)$ for small primes $p \equiv 5 \pmod 6$ and small odd k.

[2] Birch, B. J. *How the number of points of an elliptic curve over a fixed prime field varies.* J. London Math. Soc. **43** 1968 57–60.

[3] Blake, I. F.; Seroussi, G.; Smart, N. P. *Elliptic curves in cryptography.* Reprint of the 1999 original. London Mathematical Society Lecture Note Series, 265. Cambridge University Press, Cambridge, 2000. xvi+204 pp.

[4] Hasse, H. *Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F. K. Schmidtschen Kongruenzzetafunktionen in gewissen eliptischen Fällen.* Vorläufige Mitteilung, Nachr. Ges. Wiss. Göttingen I, Math.-phys. Kl. Fachgr. I Math. Nr. **42** (1933), 253-262

[5] Ireland, Kenneth; Rosen, Michael *A classical introduction to modern number theory.* Second edition. Graduate Texts in Mathematics, 84. Springer-Verlag, New York, 1990. xiv+389 pp.

[6] Lidl, Rudolf; Niederreiter, Harald *Finite fields.* With a foreword by P. M. Cohn. Second edition. Encyclopedia of Mathematics and its Applications, 20. Cambridge University Press, Cambridge, 1997. xiv+755 pp.

[7] Michel, Philippe *Rang moyen de familles de courbes elliptiques et lois de Sato-Tate.* Monatsh. Math. **120** (1995), no. 2, 127–136.

[8] Miller, Steven J. *One- and two-level densities for rational families of elliptic curves: evidence for the underlying group symmetries.* Compos. Math. **140** (2004), no. 4, 952–992

TRINITY COLLEGE, 300 SUMMIT STREET, HARTFORD, CT 06106-3100
E-mail address: `Saiying.He@trincoll.edu`

MATHEMATICS DEPARTMENT, TRINITY COLLEGE, 300 SUMMIT STREET, HARTFORD, CT 06106-3100
E-mail address: `james.mclaughlin@trincoll.edu`