AVERAGE VALUES OF $\pi_E^r(X)$ OVER $\mathbb{F}_p$

JONATHAN BATTISTA, JONATHAN BAYLESS, DMITRIY IVANOV, RON SCOTT

1. Introduction

Let $E(b,c) = y^2 + (1-c)xy - by = x^3 - bx^2$ be an elliptic curve where b and c are functions of the parameter $s \in \mathbb{Z}$. From [4], we know that there are certain functions $b(s)$ and $c(s)$ which give elliptic curves $E(s)$ with torsion subgroups isomorphic to $\mathbb{Z}/t\mathbb{Z}$, where t is 5, 6, 7, or 10. Now, consider these curves over the finite field $\mathbb{F}_p$. We are interested in the number of points $(x,y) \in \mathbb{F}_p^2$ such that x and y satisfy the equation of the curve $E(b,c)$. We know that the number of points on $E(b,c)$ over $\mathbb{F}_p$ is approximately $p+1$. So, we now consider the error term $a_p(E) = p + 1 - \#E(\mathbb{F}_p)$. We can bound this error term by $|a_p(E)| \le 2\sqrt{p}$. In fact, the Lang-Trotter conjecture [5] states that, for any curve E and any $r \in \mathbb{Z}$,

$$\pi_E^r(X) := \#\{p \le X : a_p(E) = r\} \sim C_{E,r}\frac{\sqrt{X}}{\log X},$$

where $C_{E,r}$ is a constant depending on E and r. As in [3], we look at the Lang-Trotter conjecture in an average sense. The main result we will prove is the following theorem.

Theorem 1.1. *Let $E(s)$ be the paramaterization of elliptic curves having a point of order $t \in \{5,6,7,10\}$. Then, if*

$$\sum_{\substack{1 \le s \le p-1 \\ a_p(E(s))=r}} 1 = C_t \cdot H(r^2 - 4p) + \mathrm{O}(1)\,,$$

is valid for some constant C_t, then the following equation holds

$$\frac{1}{\mu(N)} {\sum_{|s|\le N}}' \pi_{E(s)}^r(X) = \frac{4}{\pi} C_t \cdot K_r \cdot \frac{\sqrt{X}}{\log X} + \mathrm{O}\left(\frac{X^{3/2}}{N} + \frac{\sqrt{X}}{\log^d X}\right).$$

where $d > 0$, $\sum'$ represents the sum over non-singular curves, $\mu(N)$ represents the number of curves in the sum, and K_r is the constant defined in [1].

2. Isomorphisms of t-torsion Curves

Every elliptic curve has the form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Through a series of simple transformations outlined in [8], such a curve can be rewritten in the form $y^2 = x^3 + Ax + B$. This is called the curve's Weierstrauss normal form.

Once we have our curves in Weierstrauss normal form, we can look at the possible ways two curves can be isomorphic. Given that our point at infinity must be unique, the only valid transformations which can be made are $x = u^2x'$ and $y = u^3y'$. Substituting these into the Weierstrauss form, we see that $A = u^4A'$ and $B = u^6B'$

are the only valid relations between the coefficients of isomorphic curves in this form.

From [4], we know that t-torsion curves, where $t \in \{5, 6, 7, 10\}$, can be parameterized to give $(0, 0)$ as a point of order t:

t	Parameterization
5	$y^2 + (1-s)xy - sy = x^3 - sx^2$
6	$y^2 + (1-s)xy - (s^2+s)y = x^3 - (s^2+s)x^2$
7	$y^2 + (1-s^2+s)xy - (s^3-s^2)y = x^3 - (s^3-s^2)x^2$
10	$y^2 + \frac{1-2s-2s^2+2s^3}{s^2-3s+1}xy - \frac{s^3(2s^2-3s+1)}{(s^2-3s+1)^2}y = x^3 - \frac{s^3(2s^2-3s+1)}{(s^2-3s+1)^2}x^2$

Applying our valid transformations to these parameterizations gives a set of equations describing all possible isomorphic pairs (s, S). Unfortunately, the equations are too complicated for Maple. Attempts to use the Hasse-Weil bounds failed as the resulting curves are singular. However, we have found computational evidence which seems to point to constants for all four cases. The results for $t = 5$ are shown in Tables 1.

Table 1. 5-Torsion

Prime	Number of Classes	Average Number of Isomorphisms per Class
151	64	2.343750000
293	147	1.986394558
449	225	1.991111111
599	299	2.000000000
743	371	2.000000000
877	439	1.995444191
997	499	1.995991984

If we can establish the existence of a constant C_t for a particular t, we will have shown that all curves with t-torsion satisfy the following relationship:

$$\sum_{\substack{1 \le s \le p-1 \\ a_p(E(s)) = r}} 1 = C_t \cdot H(r^2 - 4p) + \mathrm{O}(1) \,.$$

3. Average Values of $\pi_E^r(X)$

As a first step, we define the set

$$S_f^r(X) := \{B(r) < p \le X : p \equiv r - 1 \pmod t; 4p \equiv r^2, r^2 - f^2 \pmod{4f^2}\},$$

where

$$B(r) := \max(r^2/4, 5) \text{ and } d_p(f) := \frac{r^2 - 4p}{f^2} \,.$$

Since $S_f^r(X)$ consists only of primes, we may assume that the upper bound of the set, X, is prime. Now, we prove the following proposition:

Proposition 3.1. *Given a class of elliptic curves $E(s)$ over $\mathbb{F}_p$ with the relationship*

$$\sum_{\substack{1 \le s \le p-1 \\ a_p(E(s)) = r}} 1 = C_t \cdot H(r^2 - 4p) + \mathrm{O}(1) \,,$$

the following equation holds:

$$\begin{aligned}
&\frac{1}{\mu(N)} \sum_{|s|\le N}{}' \pi^r_{E(s)}(X) \\
&= C_t \cdot \frac{4N}{\pi\mu(N)} \cdot \frac{1}{\sqrt{X}\log X} \sum_{f\le 2\sqrt{X}} \frac{1}{f} \sum_{p\in S_f^r(r-1,t,X)} L(1,\chi_d)\log p \\
&- C_t \cdot \frac{4N}{\pi\mu(N)} \int_2^X \left(\sum_{f\le 2\sqrt{y}} \frac{1}{f} \sum_{p\in S_f^r(r-1,t,y)} L(1,\chi_d)\log p \right) \frac{d}{dy}\left[\frac{1}{\sqrt{y}\log y}\right] dy \\
&+ \mathrm{O}\left(\frac{X^{3/2}}{N} + \log X\right),
\end{aligned}$$

where $L(1,\chi_d)$ is the Dirichlet L-Series $L(1,\chi_d) := \sum_{n=1}^{\infty} \frac{\chi_d(n)}{n}$, and χ_d is a character modulo $|d_p(f)|$.

Proof. Let $r \in \mathbb{Z}$ and $E(s)$ be the parameterization of an elliptic curve having a point of order $t \in \{5,6,7,10\}$. Since $a_p(E(s)) = r$, we have $p+1-r = \#E(\mathbb{F}_p)$. Also, since the group of points on $E(s)$ has a subgroup of order t, we can reduce this modulo t to give $p+1-r \equiv 0 \pmod{t}$. Thus, $p \equiv r-1 \pmod{t}$. Now, rewriting $\pi^r_{E(s)}(X)$ as a sum and changing the order of summation, we can write

$$\frac{1}{\mu(N)} \sum_{|s|\le N}{}' \pi^r_{E(s)}(X) = \frac{1}{\mu(N)} \sum_{\substack{B(r)\le p\le X \\ p\equiv r-1 \pmod{t}}} \left(\sum_{\substack{|s|\le N \\ a_p(E(s))=r}} 1 \right) + \mathrm{O}\left(\frac{X}{N\log X}\right), \tag{1}$$

where the error term comes from no longer excluding singular curves in our sum.

Using the assumed relationship for our curves, we can write

$$\sum_{\substack{1\le s\le p-1 \\ a_p(E(s))=r}} 1 = C_t \cdot H(r^2-4p) + \mathrm{O}(1), \tag{2}$$

where the $\mathrm{O}(1)$ accounts for singular curves. If instead of taking this sum over all $1 \le s \le p-1$ we take it over $|s| \le N$, we have roughly $2N/P$ times as many curves which are counted. Thus, we have

$$\begin{aligned}
\sum_{\substack{|s|\le N \\ a_p(E(s))=r}} 1 &= \Big(C_t \cdot H(r^2-4p) + \mathrm{O}(1)\Big)\left(\frac{2N}{p} + \mathrm{O}(1)\right) \\
&= C_t \cdot \frac{2N}{p} \cdot H(r^2-4p) + \mathrm{O}\left(H(r^2-4p) + \frac{2N}{p}\right). \qquad (3)
\end{aligned}$$

If we now subsitute this into equation (1), we obtain

$$
\begin{aligned}
\frac{1}{\mu(N)} \sideset{}{'}\sum_{|s|\le N} \pi^r_{E(s)}(X) \quad &= \\
\frac{C_t}{\mu(N)} \sum_{\substack{B(r)\le p\le X \\ p\equiv r-1 \pmod t}} &\left(\frac{2N}{p} H(r^2-4p) + \mathrm{O}\left(H(r^2-4p)+\frac{2N}{p}\right)\right) \\
&+ \mathrm{O}\left(\frac{X}{N\log X}\right). \qquad (4)
\end{aligned}
$$

Since $\sum_p \mathrm{O}\left(\frac{N}{p}\right)$ can be bounded by $\int_{B(r)}^X (1/y)\,dy = \log X$, we can rewrite this term as $\mathrm{O}(\log X)$. This substitution makes the right hand side

$$
\begin{aligned}
\frac{C_t}{\mu(N)} \sum_{\substack{B(r)\le p\le X \\ p\equiv r-1 \pmod t}} &\left(\frac{2N}{p} H(r^2-4p) + \mathrm{O}\left(H(r^2-4p)\right)\right) \\
&+ \mathrm{O}\left(\frac{X}{N\log X}+\log X\right). \qquad (5)
\end{aligned}
$$

Factoring out $H(r^2-4p)$ and using the equality

$$H(r^2-4p) = 2\sum_{f\le 2\sqrt{X}} \frac{h(d_p(f))}{w(d_p(f))},$$

we get

$$
\begin{aligned}
\frac{4C_t}{\mu(N)} \sum_{p\in S^r_f(r-1,t,X)} \sum_{f\le 2\sqrt{X}} &\left(\frac{h(d_p(f))}{w(d_p(f))}\left(\frac{N}{p}+\mathrm{O}(1)\right)\right) \\
&+ \mathrm{O}\left(\frac{X}{N\log X}+\log X\right). \qquad (6)
\end{aligned}
$$

After reversing the order of summation, our expression becomes

$$
\begin{aligned}
\frac{4C_t}{\mu(N)} \sum_{f\le 2\sqrt{X}} \sum_{p\in S^r_f(r-1,t,X)} &\left(\frac{h(d_p(f))}{w(d_p(f))}\left(\frac{N}{p}+\mathrm{O}(1)\right)\right) \\
&+ \mathrm{O}\left(\frac{X}{N\log X}+\log X\right). \qquad (7)
\end{aligned}
$$

From [7], we know that

$$h(d_p(f)) = \frac{w(d_p(f))\sqrt{d_p(f)}}{2\pi} L(1,\chi_d), \qquad (8)$$

where $\chi_d = \chi_{d_p(f)}$ and $d_p(f) = \left(4p - r^2\right)/f^2$. By applying this substitution and noticing that $\frac{4}{\mu(N)} \cdot \frac{\sqrt{d_p(f)}}{2\pi} L(1,\chi_d) \cdot \mathrm{O}(1)$ is $\mathrm{O}\left(\frac{1}{N} \cdot \frac{\sqrt{p}\,\log p}{f}\right)$, we have

$$\begin{aligned}
&\frac{2C_t}{\pi\mu(N)} \sum_{f \le 2\sqrt{X}} \sum_{p \in S_f^r(r-1,t,X)} \left(\frac{N\sqrt{4p-r^2}}{pf} L(1,\chi_d) \right) \\
&+ \mathrm{O}\left(\frac{1}{N} \sum_{f \le 2\sqrt{X}} \sum_{p \in S_f^r(r-1,t,X)} \left(\frac{\sqrt{p}\log p}{f} \right) \right) \\
&+ \mathrm{O}\left(\frac{X}{N \log X} + \log X \right).
\end{aligned} \tag{9}$$

The middle term can be bounded using the Brun-Titchmarsh Inequality. Since $p \le X$, we can bound $\sqrt{p}\log p$ by $\sqrt{X}\log X$, which gives

$$\frac{1}{N} \sum_{f \le 2\sqrt{X}} \sum_{p \in S_f^r(r-1,t,X)} \frac{\sqrt{p}\log p}{f} \le \frac{\sqrt{X}\log X}{N} \sum_{f \le 2\sqrt{X}} \sum_{p \in S_f^r(r-1,t,X)} \frac{1}{f}.$$

Now we can split this into two sums and pull the $1/f$ out of the inner sums, giving us

$$\frac{\sqrt{X}\log X}{N} \left(\sum_{f \le \frac{X^{1/4}}{\sqrt{t}}} \frac{1}{f} \sum_{p \in S_f^r(r-1,t,X)} 1 \quad + \sum_{\frac{X^{1/4}}{\sqrt{t}} \le f \le 2\sqrt{X}} \frac{1}{f} \sum_{p \in S_f^r(r-1,t,X)} 1 \right) \tag{10}$$

Observe that $\frac{1}{\log\left(\frac{X}{k}\right)} \le \frac{2}{\log X}$ if and only if $\log X - \log k \ge \frac{1}{2}\log X$ if and only if $\sqrt{X} \ge k$. In this case, $k = tf^2$, so the last statement is true iff $f \le \frac{X^{1/4}}{\sqrt{t}}$. Next, recall the Brun-Titchmarsh inequality [2]:

$$\pi(X,k,\ell) := \#\{p < X : p \equiv k \pmod{\ell}\} < \frac{3X}{\phi(k)\log\left(\frac{X}{k}\right)}.$$

Substituting this inequality and the Brun-Titchmarsh inequality into (10), we get

$$\begin{aligned}
&\frac{\sqrt{X}\log X}{N} \left(\sum_{f \le \frac{X^{1/4}}{\sqrt{t}}} \frac{1}{f} \sum_{p \in S_f^r(r-1,t,X)} 1 \quad + \sum_{\frac{X^{1/4}}{\sqrt{t}} \le f \le 2\sqrt{X}} \frac{1}{f} \sum_{p \in S_f^r(r-1,t,X)} 1 \right) \\
&\le \frac{\sqrt{X}\log X}{N} \left(\sum_{f \le \frac{X^{1/4}}{\sqrt{t}}} \frac{6X}{f^2\phi(f)\log X} \quad + \sum_{\frac{X^{1/4}}{\sqrt{t}} \le f \le 2\sqrt{X}} \frac{1}{f} \sum_{p \in S_f^r(r-1,t,X)} 1 \right).
\end{aligned} \tag{11}$$

For $f \ge \frac{X^{1/4}}{\sqrt{t}}$, which is equivalent to $f^2 \ge \frac{\sqrt{X}}{t}$, we have

$$\#\{n \le X : n \equiv a \pmod{[t,f^2]}\} = \frac{X}{[t,f^2]} \le \frac{X}{f^2} \le \frac{tX}{\sqrt{X}} = t\sqrt{X}.$$

Also, $\sum_{f\le \frac{X^{1/4}}{\sqrt{t}}} \frac{1}{f^2}$ is bounded by a constant because $\sum_{f\ge 0} \frac{1}{f^2}$ is a convergent series. Let $c_1 = \sum_{f\le \frac{X^{1/4}}{\sqrt{t}}} \frac{1}{f^2}$. Hence, we can bound (11) by

$$\frac{\sqrt{X}\log X}{N}\left(\frac{6c_1X}{\log X} + \sum_{\frac{X^{1/4}}{\sqrt{t}}\le f\le 2\sqrt{X}} \frac{t\sqrt{X}}{f}\right). \tag{12}$$

Now, we obviously have

$$\sum_{\frac{X^{1/4}}{\sqrt{t}}\le f\le 2\sqrt{X}} \frac{1}{f} \le \sum_{f\le 2\sqrt{X}} \frac{1}{f} \le \log X\,,$$

so we get an upper bound for (12):

$$\frac{\sqrt{X}\log X}{N}\left(\frac{6c_1X}{\log X} + t\sqrt{X}\log X\right) = \frac{6c_1X^{3/2}}{N} + \frac{tX(\log X)^2}{N} = \mathrm{O}\left(\frac{X^{3/2}}{N}\right)$$

After these substitutions and absorbing the $\mathrm{O}\left(\frac{X}{N\log X}\right)$ into $\mathrm{O}\left(X^{3/2}/N\right)$, the expression in (9) becomes

$$\begin{aligned}&\frac{2C_t}{\pi\mu(N)} \sum_{f\le 2\sqrt{X}} \sum_{p\in S_f^r(r-1,t,X)} \left(\frac{N\sqrt{4p-r^2}}{pf} L(1,\chi_d)\right)\\ &\quad + \mathrm{O}\left(\frac{x^{3/2}}{N} + \log X\right).\end{aligned} \tag{13}$$

Now, using the approximations $\sqrt{4p-r^2} = 2\sqrt{p} + \mathrm{O}\left(\frac{1}{\sqrt{p}}\right)$ and $\mu(N) = \mathrm{O}(N)$, we see (13) becomes

$$\begin{aligned}&\frac{4NC_t}{\pi\mu(N)}\left(\sum_{f\le 2\sqrt{X}} \sum_{p\in S_f^r(r-1,t,X)} \frac{L(1,\chi_d)}{\sqrt{p}f}\right)\\ &\quad + \mathrm{O}\left(\frac{1}{N}\sum_{f\le 2\sqrt{X}} \sum_{p\in S_f^r(r-1,t,X)} \frac{N\cdot L(1,\chi_d)}{p^{3/2}f}\right) + \mathrm{O}\left(\frac{X^{3/2}}{N} + \log X\right)\end{aligned} \tag{14}$$

The second term of the three above can be absorbed into $\mathrm{O}(\log X)$. To see this, notice:

$$\begin{aligned}&\mathrm{O}\left(\frac{1}{N}\sum_{f\le 2\sqrt{X}} \sum_{p\in S_f^r(r-1,t,X)} \frac{N\cdot L(1,\chi_d)}{p^{3/2}f}\right) =\\ &\quad \mathrm{O}\left(\sum_{f\le 2\sqrt{X}} \frac{1}{f} \sum_{p\in S_f^r(r-1,t,X)} \frac{L(1,\chi_d)}{p^{3/2}}\right),\end{aligned} \tag{15}$$

Switching the order of summation gives

$$\mathrm{O}\left(\sum_{p\in S_f^r(r-1,t,X)} \frac{L(1,\chi_d)}{p^{3/2}} \sum_{f\le 2\sqrt{X}} \frac{1}{f}\right). \tag{16}$$

We know the $\sum_{f\le 2\sqrt{X}} \frac{1}{f}$ term can be bounded by $\log X$ via integration. Using [6], we can bound the value of $L(1,\chi_d)$ with

$$\mathrm{O}\left(\log d_p(f)\right) = \mathrm{O}\left(\log \sqrt{4p-r^2}/f\right) < \mathrm{O}\left(\log X\right).$$

So, (16) is smaller than

$$\mathrm{O}\left(\log X \cdot \log X \cdot \sum_{p\in S_f^r(r-1,t,x)} \frac{1}{p^{3/2}}\right). \tag{17}$$

Using integration to bound the last sum, we see this expression is less than

$$\mathrm{O}\left(\log X \cdot \log X \cdot \frac{1}{\sqrt{X}}\right) < \mathrm{O}\left(\log X\right), \tag{18}$$

so the second term in (14) can be absorbed in the error term. Thus our total expression is now:

$$\frac{4NC_t}{\pi\mu(N)} \sum_{f\le 2\sqrt{X}} \sum_{p\in S_f^r(r-1,t,X)} \frac{L(1,\chi_d)}{\sqrt{p}f} + \mathrm{O}\left(\frac{X^{3/2}}{N} + \log X\right). \tag{19}$$

The $1/f$ can be factored out of the inner sum in the first term, and the expression becomes

$$\frac{4NC_t}{\pi\mu(N)} \sum_{f\le 2\sqrt{X}} \frac{1}{f} \sum_{p\in S_f^r(r-1,t,X)} \frac{L(1,\chi_d)}{\sqrt{p}} + \mathrm{O}\left(\frac{X^{3/2}}{N} + \log X\right). \tag{20}$$

Next, we will use partial summation to rewrite the main term of (20). First, index the primes in the set $S_f^r(r-1,t,X)$ as $p_1, p_2, \ldots, p_q$. Rewriting the main term of (20) with these indices gives

$$\frac{4NC_t}{\pi\mu(N)} \sum_{f\le 2\sqrt{X}} \frac{1}{f} \sum_{i=1}^{q} \frac{L(1,\chi_d)}{\sqrt{p_i}}. \tag{21}$$

Next, we recall partial summation:

$$\sum_{i=1}^{q} a_i b_i = \sum_{i=1}^{q-1} A_i\left(b_i - b_{i+1}\right) + A_q b_q, \text{ where } A_i = \sum_{k=1}^{i} a_k.$$

Applying partial summation to (21) with $a_i = L(1,\chi_d)\log p_i$ and $b_i = \frac{1}{\sqrt{p_i}\log p_i}$ gives us

$$\begin{aligned} &\frac{4NC_t}{\pi\mu(N)} \sum_{f\le 2\sqrt{X}} \frac{1}{f}\left[\sum_{i=1}^{q-1}\left(\sum_{k=1}^{i} L(1,\chi_d)\log p_k \left(\frac{1}{\sqrt{p_i}\log p_i} - \frac{1}{\sqrt{p_{i+1}}\log p_{i+1}}\right)\right)\right. \\ &\qquad\qquad \left. + \sum_{k=1}^{q} L(1,\chi_d)\log p_k \cdot \frac{1}{\sqrt{p_q}\log p_q}\right]. \end{aligned} \tag{22}$$

Since p_q and X are both the largest prime in the set $S_f^r(r-1,t,X)$, we have $p_q = X$. So, we can pull $1/\left(\sqrt{p_q}\log p_q\right) = 1/\left(\sqrt{X}\log X\right)$ out front of the last sum. Expanding the result gives

(23)
$$\begin{aligned}
&-\frac{4NC_t}{\pi\mu(N)}\sum_{f\le 2\sqrt{X}}\frac{1}{f}\sum_{i=1}^{q-1}\left(\sum_{k=1}^{i}L(1,\chi_d)\log p_k\left(\frac{1}{\sqrt{p_{i+1}}\log p_{i+1}}-\frac{1}{\sqrt{p_i}\log p_i}\right)\right)\\
&\qquad+\frac{4NC_t}{\pi\mu(N)}\cdot\frac{1}{\sqrt{X}\log X}\sum_{f\le 2\sqrt{X}}\frac{1}{f}\sum_{k=1}^{q}L(1,\chi_d)\log p_k\\
&=-\frac{4NC_t}{\pi\mu(N)}\sum_{f\le 2\sqrt{X}}\frac{1}{f}\sum_{i=1}^{q-1}\left(\sum_{k=1}^{i}L(1,\chi_d)\log p_k\left(\frac{1}{\sqrt{p_{i+1}}\log p_{i+1}}-\frac{1}{\sqrt{p_i}\log p_i}\right)\right)\\
&\qquad+\frac{4NC_t}{\pi\mu(N)}\cdot\frac{1}{\sqrt{X}\log X}\sum_{f\le 2\sqrt{X}}\frac{1}{f}\sum_{p\in S_f^r(r-1,t,X)}L(1,\chi_d)\log p\,,
\end{aligned}$$

because $\{p_k\}_{k=1}^{q}=S_f^r(r-1,t,X)$. By basic calculus, we can surely write

$$\frac{1}{\sqrt{p_{i+1}}\log p_{i+1}}-\frac{1}{\sqrt{p_i}\log p_i}=\int_{p_i}^{p_{i+1}}\frac{d}{dy}\left(\frac{1}{\sqrt{y}\log y}\right)dy\,.$$

So, we can rewrite the first term in (23) as

$$-\frac{4NC_t}{\pi\mu(N)}\sum_{f\le 2\sqrt{X}}\frac{1}{f}\sum_{i=1}^{q-1}\left(\sum_{k=1}^{i}L(1,\chi_d)\log p_k\int_{p_i}^{p_{i+1}}\frac{d}{dy}\left(\frac{1}{\sqrt{y}\log y}\right)dy\right).\tag{24}$$

Since $\sum_{k=1}^{i}L(1,\chi_d)\log p_k$ is a constant with respect to the integral, we can write it inside the integral:

$$-\frac{4NC_t}{\pi\mu(N)}\sum_{f\le 2\sqrt{X}}\frac{1}{f}\sum_{i=1}^{q-1}\int_{p_i}^{p_{i+1}}\sum_{k=1}^{i}L(1,\chi_d)\log p_k\cdot\frac{d}{dy}\left(\frac{1}{\sqrt{y}\log y}\right)dy.\tag{25}$$

Now notice that as k ranges from 1 to i, p_k ranges through all values in the set $S_f^r(r-1,t,y)$. So, we can rewrite the inner-most sum in (25) as

$$\sum_{p\in S_f^r(r-1,t,y)}L(1,\chi_d)\log p\cdot\frac{d}{dy}\left(\frac{1}{\sqrt{y}\log y}\right).$$

So, (25) becomes

$$-\frac{4NC_t}{\pi\mu(N)}\sum_{f\le 2\sqrt{X}}\frac{1}{f}\sum_{i=1}^{q-1}\int_{p_i}^{p_{i+1}}\sum_{p\in S_f^r(r-1,t,y)}L(1,\chi_d)\log p\cdot\frac{d}{dy}\left(\frac{1}{\sqrt{y}\log y}\right)dy.\tag{26}$$

Note that we are integrating over many small intervals $[p_i,p_{i+1}]$. Also note that we are adding the value of these integrals for $1\le i\le q-1$. This means we are really just integrating over the interval $[p_1,p_q]$. Also, remember that $p_q=X$. Taking all of this into account allows us to rewrite (26) as

$$-\frac{4NC_t}{\pi\mu(N)}\sum_{f\le 2\sqrt{X}}\frac{1}{f}\int_{p_1}^{X}\sum_{p\in S_f^r(r-1,t,y)}L(1,\chi_d)\log p\cdot\frac{d}{dy}\left(\frac{1}{\sqrt{y}\log y}\right)dy.\tag{27}$$

If the first prime in our set $S_f^r(r-1,t,X)$ is 2, then our integral goes from 2 to X. If the first prime in our set is not 2, then the set $S_f^r(r-1,t,y)$ is empty for $2 \le y < p_1$, and

$$\int_2^{p_1} \sum_{p\in S_f^r(r-1,t,y)} L(1,\chi_d)\log p \cdot \frac{d}{dy}\left(\frac{1}{\sqrt{y}\log y}\right) dy = 0.$$

So, we can write (27) as

$$\begin{aligned}
&-\frac{4NC_t}{\pi\mu(N)} \sum_{f\le 2\sqrt{X}} \frac{1}{f}\int_2^X \sum_{p\in S_f^r(r-1,t,y)} L(1,\chi_d)\log p\cdot \frac{d}{dy}\left(\frac{1}{\sqrt{y}\log y}\right) dy \\
&= \frac{4NC_t}{\pi\mu(N)} \int_2^X \left(\sum_{f\le 2\sqrt{y}} \frac{1}{f} \sum_{p\in S_f^r(r-1,t,y)} L(1,\chi_d)\log p\right) \frac{d}{dy}\left[\frac{1}{\sqrt{y}\log y}\right] dy.
\end{aligned} \tag{28}$$

Finally, substituting (28) into (23) gives

$$\begin{aligned}
&\frac{4NC_t}{\pi\mu(N)}\cdot\frac{1}{\sqrt{X}\log X}\sum_{f\le 2\sqrt{X}}\frac{1}{f}\sum_{p\in S_f^r(r-1,t,X)} L(1,\chi_d)\log p \\
&\quad -\frac{4NC_t}{\pi\mu(N)}\int_2^X\left(\sum_{f\le 2\sqrt{y}}\frac{1}{f}\sum_{p\in S_f^r(r-1,t,y)} L(1,\chi_d)\log p\right)\frac{d}{dy}\left[\frac{1}{\sqrt{y}\log y}\right] dy,
\end{aligned} \tag{29}$$

which, in addition to the error terms in (20), proves Proposition 3.1. □

Now, using an argument similar to that in [1], we see

Proposition 3.2. *Given an integer r and any $d>0$,*

$$\sum_{f\le 2\sqrt{X}}\frac{1}{f}\sum_{p\in S_f^r(r-1,t,X)} L(1,\chi_d)\log p = K_r X + \mathrm{O}\left(\frac{X}{\log^d X}\right),$$

where

$$K_r = \sum_{f=1}^{\infty}\frac{1}{f}\sum_{k=1}^{\infty}\frac{c_f^r(k)}{k\phi([t,kf^2])} \quad \text{and} \quad c_f^r(k) = \sum_{\substack{a \pmod{4k} \\ a\equiv 0,1 \pmod 4 \\ (r^2-af^2,4kf^2)=4 \\ 4(r-1)\equiv r^2-af^2 \pmod{(12,4kf^2)}}} \left(\frac{a}{k}\right).$$

Putting propositions 3.1 and 3.2 together yields

$$\begin{aligned}
&\frac{1}{\mu(N)}{\sum_{|s|\le N}}' \pi_{E(s)}^r(X) \\
&= C_t\cdot\frac{4N}{\pi\mu(N)}\cdot\frac{1}{\sqrt{X}\log X}\left(K_r X + \mathrm{O}\left(\frac{X}{\log^d X}\right)\right) \\
&- C_t\cdot\frac{4N}{\pi\mu(N)}\int_2^X\left(K_r y + \mathrm{O}\left(\frac{y}{\log^d y}\right)\right)\frac{d}{dy}\left[\frac{1}{\sqrt{y}\log y}\right] dy \\
&+ \mathrm{O}\left(\frac{X^{3/2}}{N} + \log X\right).
\end{aligned} \tag{30}$$

Factoring out K_r and evaluating the derivative gives

$$\begin{aligned}
&\frac{1}{\mu(N)}\sum_{|s|\le N}{}' \pi^r_{E(s)}(X)\\
&= C_t\cdot K_r\cdot\frac{4N}{\pi\mu(N)}\left(\frac{\sqrt{X}}{\log X}+\int_2^X\frac{dy}{\sqrt{y}\log^2 y}+\int_2^X\frac{dy}{2\sqrt{y}\log y}\right) \qquad (31)\\
&+\mathrm{O}\left(\frac{X^{3/2}}{N}+\frac{\sqrt{X}}{\log^d X}\right).
\end{aligned}$$

Using the fact that $\mu(N)=2N+\mathrm{O}(1)$, the equation becomes

(32)

$$\begin{aligned}
\frac{1}{\mu(N)}\sum_{|s|\le N}{}' \pi^r_{E(s)}(X) =&\frac{2}{\pi}\,C_t\cdot K_r\cdot\left(\frac{\sqrt{X}}{\log X}+\int_2^X\frac{dy}{\sqrt{y}\log^2 y}+\int_2^X\frac{dy}{2\sqrt{y}\log y}\right)\\
&+\mathrm{O}\left(\frac{X^{3/2}}{N}+\frac{\sqrt{X}}{\log^d X}\right).
\end{aligned}$$

Evaluating the first integral, we have

$$\begin{aligned}
\int_2^X\frac{dy}{\sqrt{y}\log^2 y}&=-\frac{\sqrt{X}}{\log X}-\frac{\sqrt{2}}{\log 2}+\frac{1}{2}\int_2^X\frac{dy}{\sqrt{y}\log y}\\
&=-\frac{\sqrt{X}}{\log X}+\pi_{1/2}(X)+\mathrm{O}\left(1\right).
\end{aligned}$$

where $\pi_{1/2}(X)=\int_2^X\frac{dy}{2\sqrt{y}\log y}\sim\frac{\sqrt{X}}{\log X}$ as in [3] with an error term smaller than $\mathrm{O}\left(\frac{\sqrt{X}}{\log X}\right)$. Thus,

$$\int_2^X\frac{dy}{\sqrt{y}\log^2 y}=\mathrm{O}\left(\frac{\sqrt{X}}{\log X}\right).$$

Applying this observation to (32) gives

$$\begin{aligned}
\frac{1}{\mu(N)}\sum_{|s|\le N}{}' \pi^r_{E(s)}(X) =&\frac{2}{\pi}\,C_t\cdot K_r\cdot\left(\frac{\sqrt{X}}{\log X}+\mathrm{O}\left(\frac{\sqrt{X}}{\log X}\right)+\int_2^X\frac{dy}{2\sqrt{y}\log y}\right) \qquad (33)\\
&+\mathrm{O}\left(\frac{X^{3/2}}{N}+\frac{\sqrt{X}}{\log^d X}\right).
\end{aligned}$$

Combining the $\mathrm{O}\left(\frac{\sqrt{X}}{\log X}\right)$ and $\mathrm{O}\left(\frac{\sqrt{X}}{\log^d X}\right)$ terms and substituting the asymptotic $\pi_{1/2}=\int_2^X\frac{dy}{2\sqrt{y}\log y}\sim\frac{\sqrt{X}}{\log X}$ as above, we find

$$\frac{1}{\mu(N)}\sum_{|s|\le N}{}' \pi^r_{E(s)}(X)=\frac{4}{\pi}C_t\cdot K_r\cdot\frac{\sqrt{X}}{\log X}+\mathrm{O}\left(\frac{X^{3/2}}{N}+\frac{\sqrt{X}}{\log^d X}\right). \qquad (34)$$

which is exactly the result of Theorem 1.1.

Given our conjecture that the constant C_t exists for $t\in\{5,6,7,10\}$, an immediate corollary to the theorem would be that for all curves $E(s)$ with 5,6,7, or

10-torsion, the following equation holds

$$\frac{1}{\mu(N)} \sideset{}{'}\sum_{|s|\leq N} \pi^r_{E(s)}(X) = \frac{4}{\pi} \cdot C_t \cdot K_r \cdot \frac{\sqrt{X}}{\log X} + \mathrm{O}\left(\frac{X^{3/2}}{N} + \frac{\sqrt{X}}{\log^d X} \right).$$

4. Acknowledgements

The authors would like to thank the National Science Foundation for funding the REU where this work was done. We would also like to thank Dr. Kevin James for his help with this project.

References

[1] C. David and F. Pappalardi, *Average Frobenius distributions of elliptic curves*, Internat. Math. Res. Notices (1999) 165-183.
[2] H. Halberstam and H. -E. Richert, *Sieve Methods*, Academic Press, London, 1974.
[3] K. James, *Average Frobenius distributions for elliptic curves with 3-torsion*, Preprint.
[4] D. S. Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. (3) **33** (1976), 193-237.
[5] S. Lang and H. Trotter, *Frobenius distributions in GL_2-extensions*, Lecture Notes in Math **504**, Springer-Verlag, Berlin, 1976.
[6] S. Louboutini, *Explicit upper bounds on $|L(1,\chi)|$*, C. R. Acad. Sci. Paris Sér. I Math. **323** (1996), no. 5, 443-446.
[7] P. Ribenboim, *Classical Theory of Algebraic Numbers*, Springer-Verlag, New York, 2001.
[8] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, 1994.
[9] J. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, New York, 1992.