Constructing One-Parameter Families with Forced Rank, Bounding the Average Rank of One-Parameter Families

Steven Miller*

November 16, 2001

Abstract

After reviewing sums (linear, quadratic, and cubic) of Legendre symbols, we show how to construct one-parameter families with rank r over $\mathbf{Q}(t)$. By specializing t we will often find curves of rank r or higher over $\mathbf{Q}$. We talk about excess rank, and give a very weak bound for the average rank of a family. The bound is sufficient to show that the average rank is finite. We then list some nice families. We conclude by including again the derivation of the Explicit Formula for Elliptic Curves, which relates summing a test function over zeros of the curve on one side with summing the Fourier Transform of the test function at primes on the other side.

1 Preliminaries on Quadratic Characters

1.1 Introduction

Consider the multiplicative group $\left(\mathbf{Z}/\mathrm{p}\mathbf{Z}\right)^*$ for p prime. A well known result states that the non-zero elements (mod p) are cyclic. Hence there is a generator g such that

$$\{1, g, g^2, \dots, g^{p-2}\} = \{1, 2, 3, \dots, p-1\} \tag{1.1}$$

We define the Legendre symbol $\left(\frac{x}{p}\right)$ by $\left(\frac{x}{p}\right)$ equals 0 if $x = 0$, 1 if x is equivalent to a non-zero square mod p, and -1 if x is not equivalent to a square mod p.

*E-mail: `sjmiller@math.princeton.edu`

In other words, for non-zero x, since g is a generator we can write $x = g^a$ for some a. If a is even, $\left(\frac{x}{p}\right) = 1$; if a is odd, $\left(\frac{x}{p}\right) = -1$.

Clearly there are as many squares as non-squares. There are $\frac{p-1}{2}$ of each, and then there is zero. We now calculate some simple sums of Legendre symbols. Let $\sum_{x(p)}$ denote $\sum_{x=0}^{p-1}$.

We collect several important facts whose proofs we leave to the reader.

- $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$.
- If $x \neq 0$, $\left(\frac{x^{-1}}{p}\right) = \left(\frac{x}{p}\right)$ and $\left(\frac{x^2}{p}\right) = 1$.
- $\left(\frac{x+mp}{p}\right) = \left(\frac{x}{p}\right)$.

1.2 Linear Sums

We first study $\left(\frac{f(x)}{p}\right)$, where $f(x)$ is a linear polynomial. Say $f(x) = ax + b$.

Lemma 1.1 *Let $a \neq 0$. Then $\sum_{x=0}^{p-1} \left(\frac{ax+b}{p}\right) = 0$. If $a = 0$, the sum is $p\left(\frac{b}{p}\right)$.*

Proof: We prove the first claim. As $a \neq 0$, we can change variables. Let $t = a^{-1}x$. Then we have the sum $\sum_{t(p)} \left(\frac{t+b}{p}\right)$. Changing variables again, let $u = t - b$. We now have $\sum_{u(p)} \left(\frac{u}{p}\right)$. We get $+1$ for each non-zero square and -1 from each non-square. As there are as many non-zero squares as non-squares, this sum is zero. $\Box$

1.3 Quadratic Sums

We now consider the case when $f(x)$ is a quadratic polynomial. First we'll do the case where $f(x)$ factors into two linear polynomials. I'll only do the case when each factor is monic.

Lemma 1.2

$$\sum_{x=0}^{p-1} \left(\frac{n_1 + x}{p}\right)\left(\frac{n_2 + x}{p}\right) = \begin{cases} p-1 \ if \ p \mid n_1 - n_2 \\ -1 \ otherwise \end{cases} \tag{1.2}$$

Proof: We can change variables by shifting x by $-n_2$. Let $n = n_1 - n_2$. Call this sum $S(n)$.

Assume $p|n$. Then we have $\sum_{x(p)} \left(\frac{x+n}{p}\right)\left(\frac{x}{p}\right) = \sum_{x(p)} \left(\frac{x^2}{p}\right) = p - 1$, as claimed.

Assume $(n,p)=1$. For $(a,p)=1$ (a, p relatively prime) we can change variables $x \to a^{-1}x$.

$$\begin{aligned}
S(n) &= \sum_{x=0}^{p-1} \left(\frac{n+x}{p}\right)\left(\frac{x}{p}\right) \\
&= \sum_{x=0}^{p-1} \left(\frac{n+a^{-1}x}{p}\right)\left(\frac{a^{-1}x}{p}\right) \\
&= \sum_{x=0}^{p-1} \left(\frac{a^2}{p}\right)\left(\frac{an+x}{p}\right)\left(\frac{x}{p}\right) \\
&= \sum_{x=0}^{p-1} \left(\frac{an+x}{p}\right)\left(\frac{x}{p}\right) = S(an)
\end{aligned} \tag{1.3}$$

There are $p-1$ a's that are relatively prime with p. As $S(n)=S(an)$, we may sum over a and divide by $p-1$. Initially thte a-sum will be from 1 to $p-1$. We'll add back and subtract the contribution from $a=0$.

$$\begin{aligned}
S(n) &= \frac{1}{p-1}\sum_{a=1}^{p-1}\sum_{x=0}^{p-1} \left(\frac{an+x}{p}\right)\left(\frac{x}{p}\right) \\
&= \frac{1}{p-1}\sum_{a=0}^{p-1}\sum_{x=0}^{p-1} \left(\frac{an+x}{p}\right)\left(\frac{x}{p}\right) - \frac{1}{p-1}\sum_{x=0}^{p-1}\left(\frac{x}{p}\right)^2 \\
&= \frac{1}{p-1}\sum_{x=0}^{p-1}\left(\frac{x}{p}\right)\sum_{a=0}^{p-1}\left(\frac{an+b}{p}\right) - 1 \\
&= 0-1=-1
\end{aligned} \tag{1.4}$$

This concludes the proof. □

Lemma 1.3 (Quadratic Legendre Sums)

$$\sum_{t=0}^{p-1}\left(\frac{at^2+bt+c}{p}\right) = \begin{cases} (p-1)\left(\frac{a}{p}\right) \ if \ p \mid b^2-4ac \\ -\left(\frac{a}{p}\right) \ otherwise \end{cases} \tag{1.5}$$

Proof: Assume $a \neq 0$, as otherwise it is trivial, and assume $p>2$. Let $\delta = 4^{-1}(b^2-4ac)$. Then we have

$$
\begin{aligned}
\sum_{t=0}^{p-1}\left(\frac{at^2+bt+c}{p}\right) &= \sum_{t=0}^{p-1}\left(\frac{a^{-1}}{p}\right)\left(\frac{a^2t^2+bat+ac}{p}\right) \\
&= \sum_{t=0}^{p-1}\left(\frac{a}{p}\right)\left(\frac{t^2+bt+ac}{p}\right) \\
&= \sum_{t=0}^{p-1}\left(\frac{a}{p}\right)\left(\frac{t^2+bt+4^{-1}b^2+ac-4^{-1}b^2}{p}\right) \\
&= \sum_{t=0}^{p-1}\left(\frac{a}{p}\right)\left(\frac{(t+2^{-1}b)^2-4^{-1}(b^2-4ac)}{p}\right) \\
&= \sum_{t=0}^{p-1}\left(\frac{a}{p}\right)\left(\frac{t^2-\delta}{p}\right)
\end{aligned}
\tag{1.6}
$$

In the second line we changed variables: $t \to a^{-1}t$, and in the fourth line we changed variables $t \to t - 2^{-1}b$.

If $\delta = 0$ we get $p-1$. If $\delta = \eta^2, \eta \neq 0$, then by the previous lemma we have

$$
\sum_{t=0}^{p-1}\left(\frac{t^2-\delta}{p}\right) = \sum_{t=0}^{p-1}\left(\frac{t-\eta}{p}\right)\left(\frac{t+\eta}{p}\right) = -1. \tag{1.7}
$$

We note that $\sum_{t=0}^{p-1}\left(\frac{t^2-\delta}{p}\right)$ is the same for all δ that aren't squares. Denote this sum by S, the set of squares by $\mathcal{R}$, and the non-squares by $\mathcal{N}$. Since $\sum_{\delta=0}^{p-1}\left(\frac{t^2-\delta}{p}\right) = 0$ we have

$$
\begin{aligned}
\sum_{\delta=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{t^2-\delta}{p}\right) &= \sum_{t=0}^{p-1}\left(\frac{t^2}{p}\right) + \sum_{\delta\in\mathcal{R}}\sum_{t=0}^{p-1}\left(\frac{t^2-\delta}{p}\right) + \sum_{\delta\in\mathcal{N}}\sum_{t=0}^{p-1}\left(\frac{t^2-\delta}{p}\right) \\
&= (p-1) + \frac{p-1}{2}(-1) + \frac{p-1}{2}S = 0
\end{aligned}
\tag{1.8}
$$

Hence $S = -1$, proving the lemma.

1.4 Cubic Sums

For linear and quadratic factors, we are able to exactly evaluate the Legendre sums. The situation changes dramatically for cubic and higher degree polynomials.

In generally, Hasse's Theorem is the best we can do.

Theorem 1.4 (Hasse) $\left|\sum_{x(p)} \left(\frac{x^3+ax+b}{p}\right)\right| \leq 2\sqrt{p}$.

Sometimes we are fortunate and able to cleanly evaluate these sums. For example, for any prime $p \equiv 2(3)$ the sum $\sum_{x(p)} \left(\frac{x^3+b}{p}\right) = 0$. The reason is this sum equals $\sum_{x(p)} \left(\frac{x+b}{p}\right)$, because $x \to x^3$ is an automorphism. (Hint: For such p, show the multiplicative group is cyclic, and 3 does not divide its order).

1.5 Expression for $a_E(p)$

$$\begin{aligned} a_{E_t}(p) &= p + 1 - N_p \\ &= p + 1 - \text{the number of solutions mod p, including infinity} \end{aligned} \tag{1.9}$$

Consider the curve $y^2 = x^3 + ax + b$. Mod p, if $x^3 + ax + b$ is a non-zero square, there are two y that work; if it is zero, there is one y; if it is a non-zero square, there are no y. We can ignore the point at infinity by replacing $p + 1$ with p.

Hence we see

$$\begin{aligned} N_p &= \sum_{x=0}^{p-1} \left(1 + \left(\frac{x^3 + ax + b}{p}\right)\right) \\ &= p + \sum_{x=0}^{p-1} \left(\frac{x^3 + ax + b}{p}\right). \end{aligned} \tag{1.10}$$

Therefore

Theorem 1.5 (Legendre Expansion of $a_E(p)$)

$$a_E(p) = -\sum_{x=0}^{p-1} \left(\frac{x^3 + ax + b}{p}\right). \tag{1.11}$$

2 Families of Forced Rank over $\mathbf{Q}(t)$

2.1 Introduction

We study several families investigated by Fermigier (Experimental Mathematics, Vol 5, 1996, No. 2). He considers families of Elliptic Curves $y^2 + a_1(t)xy + a_3(t)y = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t)$ over $\mathbf{Q}[t]$. By choosing the polynomials appropriately, we can force rational points onto the curve, and hence construct families of curves of rank $1, 2, 3$ and 4 (and by looking at two new families, of rank 5 and 6) over $\mathbf{Q}[t]$. By evaluating these polynomials at integers, we get families of Elliptic Curves over $\mathbf{Q}$, and a theorem of Silverman tells us that, in general, the rank of these families over $\mathbf{Q}$ is at least that of the family over $\mathbf{Q}[t]$.

For simplicity, consider a family $\mathcal{E}$ of elliptic curves in Weierstrass form: $y^2 = x^3 + A(T)x + B(T)$, $T \in \mathbf{Z}$. For every choice t of T, we get an elliptic curve. We denote the elliptic curve by E_t.

E_t is usually a non-singular (ie, nice) elliptic curve over $\mathbf{Q}$. We can talk about its Mordell-Weil group, the sign of its functional equations, etc.

We can regard $\mathcal{E}$ as an elliptic curve, not over $\mathbf{Q}$, but over $\mathbf{Q}(t)$. We can ask what its rank over $\mathbf{Q}(t)$ is. The hope is for families $\mathcal{E}$ with high rank over $\mathbf{Q}(t)$, when we replace T by t that "most" curves E_t will have high rank over $\mathbf{Q}$.

There are, of course, some obvious concerns. The curves E_t will have functional equation either even or odd. We expect half of the time they'll be even, half of the time odd.

So, if $\mathcal{E}$ has rank r, we might expect (in the limit as $t \to \infty$) half of the time E_t has rank r, and half of the time E_t has rank $r+1$. If, however, there is Excess Rank, we might expect half the time we'll have rank $r, r+2, r+4, \dots$ and the other half of the time $r+1, r+3, r+5, \dots$.

Many numerical experiments have shown that, for a large number of families of rank r, approximately 50% have even rank, and 50% odd. What is surprising is that, with a high degree of regularity, 32% are observed to have rank r, 18% rank $r+2$, and 48% rank $r+1$, 2% rank $r+3$.

The rest of this handout is primarily concerned with constructing families with high rank r over $\mathbf{Q}(t)$. By the Specialization Theorem of Silverman, all but finitely many of the "specialized" curves E_t will have rank at least r. At the end, we will show (*assuming the Generalized Riemann Hypothesis*) how to find upper bounds for ranks of families of elliptic curves.

2.2 Silverman-Rosen Theorem

Let $\mathcal{E}$ be a family of elliptic curves in Weierstrass form: $y^2 = x^3 + A(T)x + B(T)$, $T \in \mathbf{Z}$. For each t, we have the elliptic curve E_t. By Theorem 1.5 we have

$$a_{E_t}(p) = -\sum_{x=0}^{p-1} \left(\frac{x^3 + A(t)x + B(t)}{p}\right). \tag{2.1}$$

Define

$$A_{\mathcal{E}}(p) = \frac{1}{p}\sum_{t=0}^{p-1} a_{E_t}(p) \tag{2.2}$$

Silverman and Rosen (On the rank of an elliptic surface, Inv. Math., 133, 1998) prove the following:

Theorem 2.1 *Let $\mathcal{E} : y^2 = x^3 + A(T)x + B(T)$, with $A(T), B(T)$ integer polynomials of degree at most 3 and 5. Then*

$$\lim \frac{1}{X} \sum_{p \leq X} -A_{\mathcal{E}}(p) \log p = \mathit{rank}\Big(\mathcal{E}(\mathbf{Q}(T))\Big). \tag{2.3}$$

We are able, for many of the families we construct, to show $A_{\mathcal{E}}(p)$ is constant. Therefore the above and the prime number theorem allow us to conclude that this constant is the rank over $\mathbf{Q}(T)$. Recall the PNT states $\sum_{p<X} \log p = X$ plus lower order terms.

Also, Shioda (Construction of elliptic curves with high rank via the invariants of the Weyl groups, J. Math. Soc. Japan, vol 43, No. 4, 1991) gives explicit constructions for not only families of rank $2, 4, 6, 7$ and 8 over $\mathbf{Q}(T)$, but generators of the Mordell-Weil groups.

Hence we must study

$$pA_{\mathcal{E}}(p) = \sum_{t=0}^{p-1}\sum_{x=0}^{p-1} \left(\frac{f_t(x)}{p}\right). \tag{2.4}$$

If we show this sum equals rp for all p, then the family will have rank r over $\mathbf{Q}(t)$. Often we will show something slightly weaker, such as the sum equals $rp + O(1)$, where the $O(1)$ term is, for all p, universally bounded. This error would correspond to $O(\frac{1}{p})$ in $A_{\mathcal{E}}(p)$, which will not contribute.

Finally, once or twice we will show something like $A_{\mathcal{E}}(p) = r_1 p$ for half of the primes and $r_2 p$ for the other half. By Dirichlet's Theorem on Primes in Arithmetic Progression (which basically says primes are well distributed in congruence classes) this will imply the rank is $r = \frac{r_1+r_2}{2}$.

For example, let a and m ($m > 1$) be any two numbers, and consider primes of the form $nm + a$. Clearly there are no such primes if a and m have a common factor. Recall the Euler phi-function $\varphi(m)$, which gives the number of numbers in $\{1, \ldots, m-1\}$ that are relatively prime to m. Dirichlet's Theorem states, for a given m, each relatively prime a gives the same number of primes to first order, ie, $\frac{1}{\varphi(m)}$ of the primes.

NOTE: Some sections below are taken from another set of notes I've written. I may occasionally call this the "First Sum". Also, some sections have some words on the conductors of the family. These can be ignored – if anyone decides to investigate these, I'll add more later.

NOTE: The calculations below heavily require our results on linear and quadratic Legendre sums. The discussions should be entirely self-contained. I haven't explicitly written down the change of variables; hopefully that should be clear from context. Pay careful attention to the bounds – often they are from 1 to $p-1$ instead of 0 to $p-1$, and some care must be taken to add back terms.

NOTE: Often I will split up (in one line) sums into two parts, say $x = 0$ in the first part, $x \neq 0$ in the second.

2.3 Families of Rank 0

Example: $y^2 + xy = x^3 + x^2 + tx$. We rewrite this as $y^2 = x^3 + 5x^2 + 16tx = f_t(x)$. Its discriminant, Weierstrass equation and j-invariant are given by

$$\begin{aligned}
\Delta(t) &= -64t^3 + 25t^2 = t^2(25 - 64t) \\
y^2 &= x^3 - 27(-48t + 25)x - 54(360t - 125) \\
j &= \frac{-110592t^3 + 172800t^2 - 90000t + 15625}{-64t^3 + 25t^2}
\end{aligned} \tag{2.5}$$

To determine its conductor, we look at all primes $p \geq 5$ dividing $\Delta(t)$. If p also divides c_4, then the reduced curve has a cusp, and contributes p^2 to the conductor, else it has a node and contributes p. Except for $p = 5$, no prime dividing t divides c_4.

If now $p|(25-64t)$ and $p|(-48t+25)$ then $p|16t$, which implies $p|25$. So, except possibly for $p=5$, $25-64t$ and $25-48t$ have no common factors.

Therefore every reduced curve (for $p \geq 5$) has a node, and the conductor is at most of order t^2. (We do have to worry about t and $25-64t$ being square-free).

Then we have

$$\begin{aligned}
\sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\left(\frac{f_t(x)}{p}\right) &= \sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{16xt+x^3+5x^2}{p}\right) \\
&= \sum_{x\neq 0}\sum_{t=0}^{p-1}\left(\frac{16xt+x^3+5x^2}{p}\right) \\
&= \sum_{x\neq 0}\sum_{t=0}^{p-1}\left(\frac{t+x^3+5x^2}{p}\right) = 0
\end{aligned} \tag{2.6}$$

Thus this family has rank 0 over $\mathbf{Q}(t)$.

Example: $y^2+y=x^3+2x+t$. Rewriting yields $y^2=x^3+32x+64t+16$. Its discriminant, Weierstrass equation and j-invariant are given by

$$\begin{aligned}
\Delta(t) &= -432t^2-216t-539 \\
y^2 &= x^3-27(-96)x-54(-864t-216) \\
j &= \frac{-884736}{-432t^2-216t-539}.
\end{aligned} \tag{2.7}$$

As only 2 and 3 divide $c_4=-96$, for any other p dividing the discriminant the reduced curve will have a node, so again, we expect its conductor to be at most t^2.

$$\sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{f_t(x)}{p}\right) = \sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{64t+x^3+32x+16}{p}\right) = 0. \tag{2.8}$$

Thus this family has rank 0 over $\mathbf{Q}(t)$.

Let's do a more exotic example:

Example: $y^2+xy+2y=x^3+x^2+tx+1$, which on rewriting becomes $y^2=x^3+5x^2+16x+64tx+128$. Its discriminant, Weierstrass equation and j-invariant are given by

$$\begin{aligned}\Delta(t) &= -64t^3 - 167t^2 + 578t - 1297 \qquad (2.9)\\ y^2 &= x^3 - 27(-48t - 23)x - 54(360t - 1493)\\ j &= \frac{-110592t^3 - 158976t^2 - 76176t - 12167}{-64t^3 - 167t^2 + 578t - 1297}. \qquad (2.10)\end{aligned}$$

Haven't done the calculation / congruence checks, but expect the conductor to be about t^3.

$$\begin{aligned}\sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\left(\frac{f_t(x)}{p}\right) &= \sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{16xt + x^3 + 5x^2 + 16x + 128}{p}\right) \qquad (2.11)\\ &= \sum_{x\neq 0}\sum_{t=0}^{p-1}\left(\frac{t + x^3 + 5x^2 + 16x + 128}{p}\right) + p\left(\frac{128}{p}\right)\\ &= p\left(\frac{2}{p}\right) \qquad (2.12)\end{aligned}$$

Now $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, which is $+1$ for $p = 8n \pm 1$, and -1 for $p = 8n \pm 3$. By Dirichlet's Theorem for Primes in Arithmetic Progression, each of these four progressions will have (to first order) the same number of primes. Hence we expect two will contribute $+1$, and two will contribute -1, for no net contribution.

Thus this family has rank 0 over $\mathbf{Q}(t)$.

2.4 Families of Rank 1

Example: $y^2 + y = x^3 + tx$, or $y^2 = x^3 + 16tx + 16 = f_t(x)$. Its discriminant, Weierstrass equation and j-invariant are given by

$$\begin{aligned}\Delta(t) &= -64t^3 - 27 = -(4t+3)(16t^2 - 12t + 9)\\ y^2 &= x^3 - 27(-48t)x - 54(-216)\\ j &= \frac{-110592t^3}{-64t^3 - 27} \qquad (2.13)\end{aligned}$$

Except for primes dividing 48, no primes divide both c_4 and the discriminant, hence we expect the conductor to be like t^3.

$$\sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{f_t(x)}{p}\right) = \sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{16xt+x^3+16}{p}\right) \tag{2.14}$$
$$= \sum_{x\neq 0}\sum_{t=0}^{p-1}\left(\frac{t+x^3+16}{p}\right)+p\left(\frac{16}{p}\right)=p.$$

Thus this family has rank 1 over $\mathbf{Q}(t)$.

More generally, we consider the family $y^2+Axy = x^3+Bx^2+(Ct+D)x+E^2$, or $y^2 = x^3+(4B+A^2)x^2+16(Ct+D)x+64E^2 = f_t(x)$. Then for $E \neq 0$

$$\sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{f_t(x)}{p}\right) \tag{2.15}$$
$$= \sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{16Cxt+x^3+(4B+A^2)x^2+16Dx+64E^2}{p}\right)$$
$$= \sum_{x\neq 0}\sum_{t=0}^{p-1}\left(\frac{t+x^3+(4B+A^2)x^2+16Dx+64E^2}{p}\right)+p\left(\frac{64E^2}{p}\right)=p.$$

Thus this family has rank 1 over $\mathbf{Q}(t)$.

2.5 Families of Rank 2

Consider $y^2+xy = x^3+tx^2-(3+2t)x+1$, or $y^2 = (4x^2-32x)t+x^3+x^2-48x+64 = f_t(x)$. Note that $4x^2-32x$ equals zero for $x=0,8$, and both $f_t(0)$ and $f_t(8)$ are squares. Its discriminant and Weierstrass equation are given by

$$\Delta(t) = 64t^4+672t^3+1924t^2+2520t+1088 \tag{2.16}$$
$$y^2 = x^3-27(16t^2+104t+145)x-54(-64t^3-624t^2-1020t-1081).$$

Haven't done the congruence checks, but expect the conductor to be about t^4. This will reduce the range where the partial t sum does not contribute to $\sigma < \frac{1}{6}$

$$\begin{aligned}
& \sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{f_t(x)}{p}\right) && (2.17)\\
= & \sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{(4x^2-32x)t+x^3+x^2-48x+64}{p}\right)\\
= & \sum_{x\neq 0,8}\sum_{t=0}^{p-1}\left(\frac{t+x^3+x^2-48x+64}{p}\right)+\sum_{t=0}^{p-1}\left[\left(\frac{f_t(0)}{p}\right)+\left(\frac{f_t(8)}{p}\right)\right]\\
= & \ 0+2p.
\end{aligned}$$

Thus this family has rank 2 over $\mathbf{Q}(t)$

We now show how to construct many families of Elliptic Curves with the rank 2 over $\mathbf{Q}(t)$. We show below that, given a degree 2 polynomial $f(x)$ with integer roots r_1, r_2, we can find a monic degree 3 polynomial $h(x)$ such that $y^2 = f(x)t + h(x)$ has rank 2 if the roots of $f(x)$ are distinct, and 1 if the roots are the same.

Theorem 2.2 (Families of Rank 2) *Let f, h, r_1, r_2 be as in the preceding paragraph. Then we may take $h(x) = (x-B)(x-r_1)(x-r_2) + C^2$.*

Proof: Write $f(x) = a(x-r_1)(x-r_2)$. Substituting yields

$$y^2 = a(x-r_1)(x-r_2)t + (x-B)(x-r_1)(x-r_2) + C^2 = f_t(x). \qquad (2.18)$$

When $x = r_1, r_2$, $f_t(x)$ is a square. If the two roots are distinct we have

$$\begin{aligned}
& \sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{f_t(x)}{p}\right) && (2.19)\\
= & \sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{a(x-r_1)(x-r_2)t+(x-B)(x-r_1)(x-r_2)+C^2}{p}\right)\\
= & \sum_{x\neq r_1,r_2}\sum_{t=0}^{p-1}\left(\frac{t+(x-B)(x-r_1)(x-r_2)+C^2}{p}\right)+\sum_{t=0}^{p-1}\left[\left(\frac{f_t(r_1)}{p}\right)+\left(\frac{f_t(r_2)}{p}\right)\right]\\
= & \ 0+2p.
\end{aligned}$$

If the two roots are the same we get p instead.

Note our choice of f and h force two rational points to be on the curve, (r_1, C) and (r_2, C); however, we don't know if they are in the infinite part of the Mordell-Weil group, or the finite Torsion part. Moreover, we don't know if the two points are independent.

2.6 Families of Rank 3

Consider $y^2 = x^3 + 5x^2 + (4-x)(4t)^2 = f_t(x)$. Its discriminant and Weierstrass equation are given by

$$\begin{aligned} \Delta(t) &= 262144t^6 - 3141632t^4 - 512000t^2 \\ y^2 &= x^3 - 27(768t^2 + 400)x - 54(-78336t^2 - 8000). \end{aligned} \tag{2.20}$$

Again, haven't done the congruence checks, but expect the conductor to be of order t^6, which will restrict σ to be less than $\frac{1}{9}$ if we want the partial t sum to be trivial.

To investigate $\sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{f_t(x)}{p}\right)$ we use our lemma on Quadratic Legendre Sums [see Lemma 1.3]. If the coefficient in front of t^2 is not zero, then the t sum takes on two different values: $-\left(\frac{4-x}{p}\right)$ if $-4(4-x)(x^3+5x^2) \not\equiv 0(p)$, and $(p-1)\left(\frac{4-x}{p}\right)$ if $-4(4-x)(x^3+5x^2) \equiv 0(p)$. The coefficient in front of t^2 is zero only for $x=4$, and $\sum_{t=0}^{p-1}\left(\frac{144}{p}\right) = p$. Hence

$$\begin{aligned} \sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{f_t(x)}{p}\right) &= \sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{(4-x)t^2 + x^3 + 5x^2}{p}\right) \\ &= \sum_{x=4}\sum_{t=0}^{p-1}\left(\frac{144}{p}\right) + \sum_{x=0,-5}\sum_{t=0}^{p-1}\left(\frac{f_t(x)}{p}\right) + \sum_{x\neq 0,4,-5}\sum_{t=0}^{p-1}\left(\frac{f_t(x)}{p}\right) \\ &= p + (p-1)\left(\frac{4}{p}\right) + (p-1)\left(\frac{9}{p}\right) - \sum_{x\neq 0,4,-5}\left(\frac{4-x}{p}\right) \\ &= 3p + O(1) \end{aligned} \tag{2.21}$$

Thus this family has rank 3 over $\mathbf{Q}(t)$.

2.7 Families of Rank 4

Consider $y^2 = x^3 + 41x^2 + 184x + 144 - 16t^2x = f_t(x)$. Its discriminant and Weierstrass equation are given by

$$\begin{aligned} \Delta(t) &= 262144t^6 - 2158592t^4 - 81563648t^2 + 180633600 \\ y^2 &= x^3 - 27(768t^2 + 18064)x - 54(-188928t^2 - 2362688). \end{aligned} \tag{2.22}$$

Again, haven't done the congruence checks, but expect the conductor to be of order t^6, which will restrict σ to be less than $\frac{1}{9}$ if we want the partial t sum to be trivial.

To investigate $\sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{f_t(x)}{p}\right)$ we use our lemma on Quadratic Legendre Sums [see Lemma 1.3]. If the coefficient in front of t^2 is not zero, then the t sum takes on two different values: $-\left(\frac{-16x}{p}\right)$ if $4(16x)(x^3+41x^2+184x+144)\not\equiv 0(p)$, and $(p-1)\left(\frac{-16x}{p}\right)$ if $4(16x)(x^3+41x^2+184x+144)\equiv 0(p)$.

Now $x^3+41x^2+184x+144=(x+1^2)(x+2^2)(x+6^2)$, so for $x=-1,-4,-36$ the t sum contributes $p-1$. For all other x (except $x=0$) the t sum contributes $-\left(\frac{-x}{p}\right)$, which when summed over x is $O(1)$. When $x=0$ we have $\sum_{t=0}^{p-1}\left(\frac{144}{p}\right)=p$. Hence

$$\sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{f_t(x)}{p}\right)=3(p-1)+O(1)+p=4p+O(1), \tag{2.23}$$

Thus this family has rank 4 over $\mathbf{Q}(t)$.

We now give a construction that will generate families where the rank is 4. Let b,A,B,C,D be integers, and let $f(x)=x, g(x)=x(x+b), h(x)=Ax^3+Bx^2+Cx-D^2$. Consider $y^2=f(x)t^2+2g(x)t-h(x)=f_t(x)$. Then we have

Theorem 2.3 (Constructing Rank 4 Families) *With notation as above, given distinct integers r_1, r_2 and r_3 and an integer b we can find integers A, B, C and D (depending on these) such that the family f_t has First Sum contributing $4\phi(0)$.*

Note: if two of the roots are identical, we get a Rank 3 family, and so on.

Proof: The idea is as follows. $f_t(x)$ is a quadratic polynomial in t, with discriminant $D_t(x)=4(g^2(x)+f(x)h(x))$. By our lemma on Quadratic Legendre Sums we have (for $f(x)\neq 0$)

$$\sum_{t=0}^{p-1}\left(\frac{f(x)t^2+2g(x)t-h(x)}{p}\right)=\begin{cases}-\left(\frac{f(x)}{p}\right) & D_t(x)\not\equiv 0(p)\\ (p-1)\left(\frac{f(x)}{p}\right) & D_t(x)\equiv 0(p)\end{cases}. \tag{2.24}$$

Assume we can find A,B,C and D so that for some constant c, $D_t(x)=cx(x-r_1^2)(x-r_2^2)(x-r_3^2)$. As $f(x)=x$, if x is a non-zero root of $D_t(x)$, then $\left(\frac{f(x)}{p}\right)=1$. So $\sum_{t=0}^{p-1}\left(\frac{x}{p}\right)=p-1$ if $x=r_1^2,r_2^2,r_3^2$. If $x=0$, $\sum_{t=0}^{p-1}\left(\frac{f_t(0)}{p}\right)=\sum_{t=0}^{p-1}\left(\frac{D^2}{p}\right)=p$. If $x\neq 0,r_1^2,r_2^2,r_3^2$ then $\sum_{t=0}^{p-1}\left(\frac{f_t(x)}{p}\right)=-\left(\frac{x}{p}\right)$, and summing this over such x yields $O(1)$. It would be zero if we summed over all x. Since we are throwing out four terms, each term 1 in absolute value, this sum is at most 4 in absolute value. Hence it is $O(1)$.

Hence, if we can find such constants, we would have

$$\sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{f_t(x)}{p}\right) = 3(p-1)+p+O(1) = 4p+O(1). \tag{2.25}$$

We now find such A, B, C and D. Take $A = 3$.

$$\begin{aligned} D_t(x) &= 4x\Big(x(x+b)^2 + (3x^3+Bx^2+Cx-D^2)\Big) && (2.26)\\ &= 16x(x^3 + \frac{B+2b}{4}x^2 + \frac{C+b^2}{4}x - \frac{D^2}{4}) \end{aligned}$$

If we take $D_t(x) = 16x(x-r_1^2)(x-r_2^2)(x-r_3^2)$, then we can solve for B, C and D. We get $B = -4(r_1^2+r_2^2+r_3^2) - 2b$, $C = 4(r_1^2r_2^2 + r_1^2r_3^2 + r_2^2r_3^2) - b^2$, and $D^2 = 4r_1^2r_2^2r_3^2$. Taking $x = 0, r_1, r_2$, and r_3 yield four rational points on the curve.

In Weierstrass normal form we have

$$y^2 = x^3 + [2t + B(r,b)]x^2 + [3C(r,b) - 6bt - 3t^2]x + 9D^2(r,b). \tag{2.27}$$

We note that this method of construction cannot be used to yield families where the First Sum contributes $7\phi(0)$ or more, because the polynomial $D_t(x)$ is at most degree 6, and it is from roots of $D_t(x)$ that we get contributions. We can also get contributions from x where $f(x) = 0$, but for such x, if $g(x)$ doesn't vanish then we have something like $\sum_{t=0}^{p-1}\left(\frac{c_1t+c_2}{p}\right) = 0$. Hence the only contributions from $f(x) = 0$ are from x where $g(x) = 0$. But any common root of $f(x)$ and $g(x)$ is a root of $D_t(x)$, and for each common root of $f(x)$ and $g(x)$, we lose a possible contribution from $D_t(x)$. Hence this method can give at most $6\phi(0)$. (However, by looking at $y^2 = f(x)$ for f a good quartic, it might be possible to get up to $8\phi(0)$).

2.8 Families of Rank 5

We now construct a family with rank 5. To do this, we will modify our construction from the rank 4 case.

IDEA: Let

$$
\begin{aligned}
y^2 = f_t(x) &= x^2t^2 + 2g(x)t - h(x) \\
g(x) &= x^3 + ax^2 + bx + c, \;\; c \neq 0 \\
h(x) &= Ax^3 + Bx^2 + Cx + D \\
D_t(x) &= g(x)^2 + x^2 h(x).
\end{aligned} \tag{2.28}
$$

Note that $D_t(x)$ is one-fourth the discriminant of the quadratic (in t) polynomial $x^2t^2 + 2g(x)t - h(x)$, and the number of distinct, non-zero roots of $D_t(x)$ will control the First Sum.

We have to study $\sum_{x=0}^{p-1} \sum_{t=0}^{p-1} \left(\frac{f_t(x)}{p}\right)$. When $x = 0$ the t sum vanishes, as it is just $\sum_{t=0}^{p-1} \left(\frac{2ct-D}{p}\right)$. Assume now $x \neq 0$. Then by our lemma on Quadratic Legendre Sums (Lemma 1.3)

$$
\sum_{t=0}^{p-1} \left(\frac{x^2t^2 + 2g(x)t - h(x)}{p}\right) = \begin{cases} (p-1)\left(\frac{x^2}{p}\right) & if \;\; p \mid D_t(x) \\ -1\left(\frac{x^2}{p}\right) & otherwise \end{cases} \tag{2.29}
$$

Our hope is to find coefficients a, b, c, A, B, C, D so that $D_t(x)$ has six distinct, non-zero roots. Then we would have

$$
\begin{aligned}
\sum_{x=0}^{p-1} \sum_{t=0}^{p-1} \left(\frac{f_t(x)}{p}\right) &= \sum_{x=0}^{p-1} \sum_{t=0}^{p-1} \left(\frac{x^2t^2 + 2g(x)t - h(x)}{p}\right) \\
&= \sum_{x=0} \sum_{t=0}^{p-1} \left(\frac{f_t(x)}{p}\right) + \sum_{x:D_t(x)=0} \sum_{t=0}^{p-1} \left(\frac{f_t(x)}{p}\right) + \sum_{x:xD_t(x)\neq 0} \sum_{t=0}^{p-1} \left(\frac{f_t(x)}{p}\right) \\
&= 0 + 6(p-1) + (p-7)(-1) \\
&= 5p + O(1).
\end{aligned} \tag{2.30}
$$

A simple heuristic shows that we should be able to find a, b, c, A, B, C, D so that $D_t(x)$ has six distinct non-zero roots.

$$
\begin{aligned}
D_t(x) &= g(x)^2 + x^2 h(x) \\
&= (x^3 + ax^2 + bx + c)^2 + x^2(Ax^3 + Bx^2 + Cx + D) \\
&= x^6 + (A + 2a)x^5 + (B + a^2 + 2b)x^4 + (C + 2ab + 2c)x^3 \\
&\quad + (D + 2ac + b^2)x^2 + (2bc)x + c^2 \\
&=^? x^6 + R_5x^5 + R_4x^4 + R_3x^3 + R_2x^2 + R_1x + R_0 \\
&= (x + r_1)(x + r_2)(x + r_3)(x + r_4)(x + r_5)(x + r_6).
\end{aligned} \tag{2.31}
$$

We can always choose A, B, C, D so that, for any R_5, R_4, R_3, R_2 the two polynomials agree. What remains to be shown is that we can find distinct, non-zero roots $r_1, r_2, r_3, r_4, r_5, r_6$ and coefficients b, c so that we can match $D_t(x)$ with R_1, R_0.

Assume for now that we can. The resulting polynomial $f_t(x)$ will not have the coefficient of x^3 being 1; it will be $2t - A$. We convert $f_t(x)$ to $F_t(x)$, which will be in Weierstrass normal form. We do this by sending $y \to \frac{y}{2t-A}$, $x \to \frac{x}{2t-A}$, and then multiplying both sides by $(2t - A)^2$.

$$\begin{aligned} f_t(x) &= (2t - A)x^3 + x^2t^2 + (2ax^2 + 2bx + 2c)t - Bx^2 - Cx - D \\ F_t(x) &= x^3 + x^2t^2 + (2ax^2 + 2bx(2t - A) + 2c(2t - A)^2)t \\ &\quad -Bx^2 - Cx(2t - A) - D(2t - A)^2. \end{aligned} \tag{2.32}$$

Now we study the First Sum arising from $F_t(x)$, assuming that we can find coefficients so that $D_t(x)$ has six distinct non-zero roots.

$$\begin{aligned} \sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\left(\frac{F_t(x)}{p}\right) &= \sum_{2t\neq A}\sum_{x=0}^{p-1}\left(\frac{F_t(x)}{p}\right) + \sum_{2t=A}\sum_{x=0}^{p-1}\left(\frac{F_t(x)}{p}\right) \qquad (2.33) \\ & \quad 2t \neq A, \quad x \to (2t-A)x \\ & \quad as\ 2t - A \neq 0, \left(\frac{(2t-A)^2}{p}\right) = 1, pull\ out\ (2t-A)^2 \\ &= \sum_{2t\neq A}\sum_{x=0}^{p-1}\left(\frac{f_t(x)}{p}\right) + \sum_{x=0}^{p-1}\left(\frac{x^3 + (\frac{A^2}{4} + aA - B)x^2}{p}\right) \\ &= \sum_{2t\neq A}\sum_{x=0}^{p-1}\left(\frac{f_t(x)}{p}\right) + O(1) \\ &= \sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\left(\frac{f_t(x)}{p}\right) - \sum_{2t-A=0}\sum_{x=0}^{p-1}\left(\frac{f_t(x)}{p}\right) + O(1) \\ &= 5p + O(1) + O(1) - \sum_{x=0}^{p-1}\left(\frac{f_{A/2}(x)}{p}\right) \\ &= 5p + O(1) - \sum_{x=0}^{p-1}\left(\frac{x^2\frac{A^2}{4} + (ax^2 + bx + c)A - Bx^2 - Cx - D}{p}\right) \\ &= 5p + O(1) - \sum_{x=0}^{p-1}\left(\frac{(aA + \frac{A^2}{4} - B)x^2 + (bA - C)x + (cA - D)}{p}\right). \end{aligned}$$

The last sum above is negligible (i.e., is $O(1)$) if

$$D_2(x) = (bA - C)^2 - 4(aA + \frac{A^2}{4} - B)(cA - D) \not\equiv 0(p). \tag{2.34}$$

We now show that we can find a, b, c, A, B, C, D to simultaneously satisfy $D_t(x)$ has six distinct non-zero roots and $D_2(x) \neq 0$, which implies $D_2(x) \equiv 0(p)$ for at most finitely many primes.

$$\begin{aligned} \Phi(x) &= (x+4)(x+6)(x+8)(x+1)(x-6)(x-8) \\ &= x^6 + 5x^5 - 96x^4 - 500x^3 + 1904x^2 + 11520x + 9216 \\ &= x^6 + R_5x^5 + R_4x^4 + R_3x^3 + R_2x^2 + R_1x + R_0. \end{aligned} \tag{2.35}$$

This gives (on taking $a = 0$)

$$b = 60, c = 96, A = 5, B = -216, C = -692, D = -1696, \tag{2.36}$$

$$\begin{aligned} g(x) &= x^3 + 60x + 96 \\ h(x) &= 5x^3 - 216x^4 - 692x - 1696 \\ D_t(x) &= x^6 + 5x^5 - 96x^4 - 500x^3 + 1904x^2 + 11520x + 9216 \\ &= x^6 + R_5x^5 + R_4x^4 + R_3x^3 + R_2x^2 + R_1x + R_0. \end{aligned} \tag{2.37}$$

And

$$\begin{aligned} D_2(x) &= (bA - C)^2 - 4(aA + \frac{A^2}{4} - B)(cA - D) \\ &= (60 * 5 + 692)^2 - (5^2 + 4 * 216)(96 * 5 + 1696) = -950400. \end{aligned} \tag{2.38}$$

Are there 5 rational points on f_t (or F_t) for each t? Trying the six roots yields six rational points:

$$\begin{aligned} &(6, (6t + 112)),\ (8, (8t + 136)),\ (-1, (t + 35)), \\ &(-4, (4t - 52)),\ (-6, (6t - 80)),\ (-8, (8t - 112)). \end{aligned} \tag{2.39}$$

Where did our choices of $r_1, r_2, r_3, r_4, r_5, r_6$ come from? Recall we are trying to solve

$$
\begin{aligned}
D_t(x) &= x^6 + (A+2a)x^5 + (B+a^2+2b)x^4 + (C+2ab+2c)x^3 \\
&\quad + (D+2ac+b^2)x^2 + (2bc)x + c^2 \\
&= x^6 + R_5x^5 + R_4x^4 + R_3x^3 + R_2x^2 + R_1x + R_0 \\
&= (x+r_1)(x+r_2)(x+r_3)(x+r_4)(x+r_5)(x+r_6).
\end{aligned}
$$

Hence we need to find $r_1, \dots, r_6$ such that b and c are integers, where

$$
\begin{aligned}
2bc &= R_1 = r_1r_2r_3r_4r_5 + \cdots + r_2r_3r_4r_5r_6 \\
c^2 &= R_0 = r_1r_2r_3r_4r_5r_6.
\end{aligned} \tag{2.40}
$$

Consider $r_1 = r^2, r_4 = 1, r_5 = -r_2, r_6 = -r_3$. Then

$$
\begin{aligned}
c &= rr_2r_3, \quad 2bc = -2r^2r_2^2r_3 - 2r^2r_2r_3^2 + r^2r_2^2r_3^2 + r_2^2r_3^2 \qquad (2.41) \\
&\quad try\ r = 2 \\
4b &= r_2r_3 + 4r_2r_3 - 8r_3 - 8r_2.
\end{aligned} \tag{2.42}
$$

If r_2, r_3 are both even, or if one is divisible by 4, then we can find an integral b. Taking $r_2 = 6, r_3 = 8$ yields the numbers above.

We must, however, be careful. For example, taking $r_2 = 2, r_3 = 8$ yields $D_2(x) = 0$ for all x! These values would give a contribution of only $4\phi(0)$. This phenomenon may be worth looking into.

Regardless, we have proved

Theorem 2.4 (Constructing Rank 5 Families) *We can find integers a, b, c, A, B, C, D so that the family $y^2 = x^2t^2 + 2g(x)t - h(x)$, with $g(x) = x^3 + ax^2 + bx + c$ and $h(x) = Ax^3 + Bx^2 + Cx + D$ has First Sum contributing $5\phi(0)$. In particular, we may take $a = 0, b = 60, c = 96, A = 5, B = -216, C = -692, D = -1696$, obtaining*

$$
\begin{aligned}
y^2 &= x^3 - 27c_4(t)x - 54c_6(t) \\
c_4(t) &= 16t^4 + 4608t^2 - 37632t + 912576 \\
c_6(t) &= -64t^6 - 27648t^4 - 437760t^3 + 2431872t^2 \\
&\quad + 73930752t - 896845824 \\
j(t) &= 16t^{12} + \ldots - 100241750000 \\
\Delta(t) &= -41952t^9 + \ldots - 25661888000000.
\end{aligned} \tag{2.43}
$$

For a special case of the coefficients, we show that for some t, the geometric rank of E_t is at least 5. ***Due to incredible stupidity, I used a slightly different set of coefficients*** $a, b, \ldots, D$ ***for either this case, or the rank*** 6 ***case, or both. Basically, I worked some more and found smaller values for the coefficients. So the specific example I give may not be from the family above, but from a very close cousin, though it will be easy to recover which later.***

Theorem 2.5 *$y^2 = x^3 - 15823x + 767122$ has rank at least 5.*

Five points on the curve are:
$P[1] = (81, 130)$ $P[2] = (83, 160)$ $P[3] = (74, 38)$
$P[4] = (71, 40)$ $P[5] = (69, 62)$
Using a program I wrote in Mathematica (and confirming the calculation using a package from PARI), I calculated the determinant of the matrix $< P[i], P[j] >$, where $< *, * >$ is the canonical height. Actually, I used a finite approximation to the canonical height and did enough iterations that the error was less than the determinant returned. Both methods yield a determinant value of approximately 32.5, proving these points are linearly independent, hence the curve has geometric rank at least 5.

2.9 Families of Rank 6

We now construct a family of rank 6. To do this, we will modify our construction from the rank 5 case.

IDEA: Let

$$\begin{aligned} y^2 = f_t(x) &= x^3t^2 + 2g(x)t - h(x) \\ g(x) &= x^3 + ax^2 + bx + c, \ c \neq 0 \\ h(x) &= (A-1)x^3 + Bx^2 + Cx + D \\ D_t(x) &= g(x)^2 + x^3h(x). \end{aligned} \tag{2.44}$$

Note that $D_t(x)$ is one-fourth the discriminant of the quadratic (in t) polynomial $x^3t^2 + 2g(x)t - h(x)$, and the number of distinct, non-zero roots of $D_t(x)$ will control the First Sum. We write $A - 1$ as the coefficient, and not A, as this way the coefficient of x^6 in $D_t(x)$ is A, and not $A + 1$.

We have to study $\sum_{x=0}^{p-1} \sum_{t=0}^{p-1} \left(\frac{f_t(x)}{p}\right)$. When $x = 0$ the t sum vanishes if $c \neq 0$, as it is just $\sum_{t=0}^{p-1} \left(\frac{2ct-D}{p}\right)$. Assume now $x \neq 0$. Then by our lemma on Quadratic Legendre Sums

$$\sum_{t=0}^{p-1} \left(\frac{x^3t^2 + 2g(x)t - h(x)}{p}\right) = \begin{cases} (p-1)\left(\frac{x^3}{p}\right) \ if \ p \mid D_t(x) \\ -1\left(\frac{x^3}{p}\right) \ \ otherwise \end{cases} \tag{2.45}$$

Our hope is to find coefficients a, b, c, A, B, C, D so that $D_t(x)$ has six distinct, non-zero roots. We are now in better shape then the rank 5 case, as there we had $\left(\frac{x^2}{p}\right)$. Summing this over x such that $xD_t(x) \neq 0$ lost us a p in the double sum. But here, summing $\left(\frac{x^3}{p}\right)$ will be $O(1)$. The only change is that, in the rank 5 case, our roots $r_1, \dots, r_6$ didn't have to be squares, as their contribution was $(p-1)\left(\frac{x^2}{p}\right)$; now, however, they must be, as we have $(p-1)\left(\frac{x^3}{p}\right)$.

Assume we can find such coefficients. Then

$$\begin{aligned}
\sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{f_t(x)}{p}\right) &= \sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{x^3t^2 + 2g(x)t - h(x)}{p}\right) &\quad (2.46)\\
= & \sum_{x=0}\sum_{t=0}^{p-1}\left(\frac{f_t(x)}{p}\right) + \sum_{x:D_t(x)=0}\sum_{t=0}^{p-1}\left(\frac{f_t(x)}{p}\right) + \sum_{x:xD_t(x)\neq 0}\sum_{t=0}^{p-1}\left(\frac{f_t(x)}{p}\right)\\
= & \ 0 + 6(p-1) + \sum_{x:xD_t(x)\neq 0}\left(\frac{x^3}{p}\right)\\
= & \ 6p + O(1).
\end{aligned}$$

For $1 \leq i \leq 6$, let $r_i = -\rho_i^2$. Then we are trying to find $a, \dots, D$ such that $D_t(x)$ has six distinct, non-zero perfect square roots, or

$$\begin{aligned}
D_t(x) &= g(x)^2 + x^3h(x) &\quad (2.47)\\
&= (x^3 + ax^2 + bx + c)^2 + x^3((A-1)x^3 + Bx^2 + Cx + D)\\
&= Ax^6 + (B + 2a)x^5 + (C + a^2 + 2b)x^4 + (D + 2ab + 2c)x^3\\
&\quad + (2ac + b^2)x^2 + (2bc)x + c^2\\
&= A\Big(x^6 + \frac{B+2a}{A}x^5 + \frac{C + a^2 + 2b}{A}x^4 + \frac{D + 2ab + 2c}{A}x^3\\
&\quad + \frac{2ac + b^2}{A}x^2 + \frac{2bc}{A}x + \frac{c^2}{A}\Big)\\
&= A(x^6 + R_5x^5 + R_4x^4 + R_3x^3 + R_2x^2 + R_1x + R_0)\\
&= A(x + r_1)(x + r_2)(x + r_3)(x + r_4)(x + r_5)(x + r_6) = A\Phi(x).
\end{aligned}$$

Because of the freedom to chose B, C, D there is no problem matching coefficients for the x^5, x^4, x^3 terms. We must simultaneously solve

$$\begin{aligned} 2ac + b^2 &= R_2 A \\ 2bc &= R_1 A \\ c^2 &= R_0 A. \end{aligned} \tag{2.48}$$

We can always send $A \to Aw^2$. This rescales b and c by w, and instead of $2ac + b^2 = R_2 A$ we have $2ac + b^2 w = R_2 A w$. Taking $w = 2c$ simplifies our work to solving $a + b^2 = R_2 A$, which we can always do. We now choose an A to make solving the other two equations simple.

Take $A = 4R_0$. Then $c^2 = 4R_0^2$, or $c = 2R_0$. Substituting into $2bc = R_1 A$ yields $b = R_1$. We now send $A \to Aw^2 = (4R_0) * (2c)^2 = 64R_0^3$. Thus we obtain:

$$\begin{array}{rclcrcl} c^2 & = & 64R_0^4 & \to & c & = & 8R_0^2 \\ 2bc & = & 64R_0^3 R_1 & \to & b & = & 4R_0 R_1 \\ 2ac + b^2 & = & 64R_0^3 R_2 & \to & a & = & 4R_0 R_2 - R_1^2. \end{array} \tag{2.49}$$

EXAMPLE: Let's take $r_i = -\rho_i^2 = -i^2$. Then

$$\begin{aligned} A\Phi(x) &= A(x-1)(x-4)(x-9)(x-16)(x-25)(x-36) \\ &= A\Big(x^6 - 91x^5 + 3003x^4 - 44473x^3 \\ &\quad +296296x^2 - 773136x + 518400\Big) \\ &= A\Big(x^6 + \frac{B+2a}{A}x^5 + \frac{C+a^2+2b}{A}x^4 + \frac{D+2ab+2c}{A}x^3 \\ &\quad + \frac{2ac+b^2}{A}x^2 + \frac{2bc}{A}x + \frac{c^2}{A}\Big) \\ &= A(x^6 + R_5 x^5 + R_4 x^4 + R_3 x^3 + R_2 x^2 + R_1 x + R_0). \end{aligned} \tag{2.50}$$

We find, for these choices of roots, that

$$R_0 = 518400, R_1 = -773136, R_2 = 296296. \tag{2.51}$$

Hence, solving for A, b, c, a yields

$$\begin{array}{rclcl} A & = & 64R_0^3 & = & 8916100448256000000 \\ c & = & 8R_0^2 & = & 2149908480000 \\ b & = & 4R_0 R_1 & = & -1603174809600 \\ a & = & 4R_0 R_2 - R_1^2 & = & 16660111104. \end{array} \tag{2.52}$$

We now solve for B, C, D, getting

$$\begin{array}{rclcl} B & = & R_5 A - 2a & = & -811365140824616222208 \\ C & = & R_4 A - a^2 - 2b & = & 26497490347321493520384 \\ D & = & R_3 A - 2ab - 2c & = & -343107594345448813363200. \end{array} \tag{2.53}$$

Note: using Mathematica as a check, the above choices of $a, \dots, D$ do yield $D_t(x) = A(x-1)(x-4)(x-9)(x-16)(x-25)(x-36)$.

We convert $f_t(x)$ to $F_t(x)$, which will be in Weierstrass normal form. We do this by sending $y \to \frac{y}{t^2+2t-A+1}$, $x \to \frac{x}{t^2+2t-A+1}$, and then multiplying both sides by $(t^2+2t-A+1)^2$. For future reference, we note that

$$\begin{aligned} t^2 + 2t - A + 1 &= (t-t_1)(t-t_2) \\ &= (t - 2985983999)(t - 2985984001). \end{aligned} \tag{2.54}$$

$$\begin{aligned} f_t(x) &= t^2x^3 + (2x^3 + 2ax^2 + 2bx + 2c)t - (A-1)x^3 - Bx^2 - Cx - D \\ &= (t^2+2t-A+1)x^3 + (2at-B)x^2 + (2bt-C)x + (2ct-D) \\ F_t(x) &= x^3 + (2at-B)x^2 + (2bt-C)(t^2+2t-A+1)x \\ &\quad +(2ct-D)(t^2+2t-A+1)^2. \end{aligned} \tag{2.55}$$

Now we study the First Sum arising from $F_t(x)$.

$$\begin{aligned} \sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\left(\frac{F_t(x)}{p}\right) &= \sum_{t\neq t_1,t_2}\sum_{x=0}^{p-1}\left(\frac{F_t(x)}{p}\right) + \sum_{t=t_1,t_2}\sum_{x=0}^{p-1}\left(\frac{F_t(x)}{p}\right) \\ &\quad t \neq t_1, t_2, \quad x \to (t^2+2t-A+1)x \\ &\quad as\ (t^2+2t-A+1) \neq 0, \left(\frac{(t^2+2t-A+1)^2}{p}\right) = 1, \\ &\quad pull\ out\ (t^2+2t-A+1)^2 \\ &= \sum_{t\neq t_1,t_2}\sum_{x=0}^{p-1}\left(\frac{f_t(x)}{p}\right) + \sum_{t=t_1,t_2}\sum_{x=0}^{p-1}\left(\frac{x^3+(2at-B)x^2}{p}\right) \\ &= \sum_{t\neq t_1,t_2}\sum_{x=0}^{p-1}\left(\frac{f_t(x)}{p}\right) + O(1) \\ &= \sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\left(\frac{f_t(x)}{p}\right) - \sum_{t=t_1,t_2}\sum_{x=0}^{p-1}\left(\frac{f_t(x)}{p}\right) + O(1) \end{aligned} \tag{2.56}$$

$$
\begin{aligned}
&= 6p + O(1) + O(1) + \sum_{t=t_1,t_2} \sum_{x=0}^{p-1} \left(\frac{f_t(x)}{p}\right) \\
&= 6p + O(1) + \sum_{t=t_1,t_2} \sum_{x=0}^{p-1} \left(\frac{(2at-B)x^2 + (2bt-C)x + (2ct-D)}{p}\right).
\end{aligned}
$$

The last sum above is negligible (i.e., is $O(1)$) if

$$D(t) = (2bt - C)^2 - 4(2at - B)(2ct - D) \not\equiv 0(p). \tag{2.57}$$

Calculating yields

$$
\begin{aligned}
D(t_1) &= 4291243480243836561123092143580209905401856 \qquad (2.58) \\
D(t_2) &= 4291243816662452751895093255391719515488256.
\end{aligned}
$$

Hence (except for finitely many primes) the sum is $6p + O(1)$ as desired, and we have proved

Theorem 2.6 (Constructing Rank 6 Families) *We can find integers a, b, c, A, B, C, D so that the family $y^2 = x^3t^2 + 2g(x)t - h(x)$, with $g(x) = x^3 + ax^2 + bx + c$ and $h(x) = (A-1)x^3 + Bx^2 + Cx + D$ has First Sum contributing $6\phi(0)$. In particular, with the choices of a thru D above we have:*

$$
\begin{aligned}
y^2 &= x^3 - 27c_4(t)x - 54c_6(t) \\
c_4(t) &= 153904781721600t^3 + 128964333230708919474585 6t^2 \\
&\quad - 5071147536616949257314153796730 88t \\
&\quad - 807191439118196649640049638547084784697344 \\
c_6(t) &= -3715041853440000t^5 + \dots \\
j(t) &= 534877027461504000000t^9 + \dots \\
\Delta(t) &= -79869999842655731712000000000t^{10} + \dots. \qquad (2.59)
\end{aligned}
$$

For a special case of the coefficients, we show that for some t, the geometric rank of E_t is at least 6. ***Due to incredible stupidity, I used a slightly different set of coefficients*** $a, b, \dots, D$ ***for either this case, or the rank*** 6 ***case, or both. Basically, I worked some more and found smaller values for the coefficients. So the specific example I give may not be from the family above, but from a very close cousin, though it will be easy to recover which later.***

Theorem 2.7 *$y^2 = x^3 + Ax + B$ has rank at least 6, where*

$$\begin{aligned} A &= 112318704018571720597 2 \\ B &= 5078689385911793763978603137 2848 \end{aligned}$$

Six points on the curve are:

$$\begin{aligned} P[1] &= (67585071288, 20866449849961716) \\ P[2] &= (60673071396, 18500949214922664) \\ P[3] &= (49153071576, 14991664661755236) \\ P[4] &= (33025071828, 11131001682078096) \\ P[5] &= (12289072152, 8151425152633980) \\ P[6] &= (-13054927452, 5822267813027064) \end{aligned}$$

Using a program I wrote in Mathematica (and confirming the calculation using a package from PARI), I calculated the determinant of the matrix $< P[i], P[j] >$, where $< *, * >$ is the canonical height. Actually, I used a finite approximation to the canonical height and did enough iterations that the error was less than the determinant returned. Both methods yield a determinant value of approximately $880,000$, proving these points are linearly independent, hence the curve has geometric rank at least 6.

2.10 Families of Rank 6

We give another construction for a family of rank 6. To do this, we will modify our construction from the rank 5 and 6 cases.

IDEA: Let

$$\begin{aligned} y^2 = f_t(x) &= x^4t^2 + 2g(x)t - h(x) \\ g(x) &= x^4 + ax^3 + bx^2 + cx + d, \ d \neq 0 \\ h(x) &= -x^4 + Ax^3 + Bx^2 + Cx + D \\ D_t(x) &= g(x)^2 + x^4h(x). \end{aligned} \tag{2.60}$$

The idea is similar to before. We try and find choices of the free coefficients such that $D_t(x) = \prod_1^8(\alpha^2 x - \rho_i)$, with each root non-zero. For $x = 0$, we have $\sum_t \left(\frac{2dt-D}{p}\right)$, which vanishes. By Lemma 1.3, for x a root of D_t we have a contribution of $(p-1)\left(\frac{x^4}{p}\right) = (p-1)\left(\frac{\rho_i^4}{p}\right) = p-1$; for all other x a contribution of $-\left(\frac{x^4}{p}\right) = -1$. Hence summing over x and t yields $7(p-1) + \sum_{x\neq\rho_i,0} -1 = 6p+1$. We've chosen the coefficients of the x^4 term to be $t^2 + 2t + 1 = (t+1)^2$. We will later show this allows us to change coordinates over $\mathbf{Q}$ and obtain an elliptic curve.

So, all we need to do is choose the coefficients so we have 7 distinct roots. It is easy to see this can always be done, as

$$\begin{aligned} D_t(x) &= (2a+A)x^7 + (a^2+2b+B)x^6 + (2c+2ab+C)x^5 \\ &\quad + (b^2+2ac+2d+D)x^4 + (2bc+2ad)x^3 \\ &\quad + (2bd+c^2)x^2 + (2cd)x + d^2 \\ &= \prod_{i=1}^{7}(\alpha^2 x - \rho_i) \\ &= \sum_{k=0}^{7} x^k (-1)^{k+1} \alpha^{2k} R_k. \end{aligned} \tag{2.61}$$

If $\prod_{i=1}^{7} \rho_i = -\Box$, then we can solve for d. Matching the x^7, x^6, x^5 and x^4 coefficients is always possible (because of A, B, C, D). We put in the α^2 to facilitate solving for integral a, b, c, d.

Taking $\alpha = 2d$ yields

$$\begin{aligned} d^2 &= -R_0 \\ 2cd &= (2d)^2 R_1 \\ 2bd + c^2 &= -(2d)^4 R_2 \\ 2bc + 2ad &= (2d)^6 R_3. \end{aligned} \tag{2.62}$$

Solving yields c then b then a are integers divisible by $2d$. Taking $\rho_i \in \{1, -1, 2, -2, 3, -3, 4\}$ and $\alpha = 2d = 24$ yields

$$\begin{aligned} d &= 12, \ c = -864, \ b = -2740608, \ a = 192844800 \\ D &= -1013478801432, \ C = 169376669763264 \\ B &= -183270506625785088 \\ A &= 21035720122782898176. \end{aligned} \tag{2.63}$$

Hence we can find integer coefficients such that

$$y^2 = (t+1)^2 x^4 + \dots \tag{2.64}$$

We quote the following theorem (Mordell, Diophantine Equations, 1968, pg 77; also see Nagao, Construction of High-Rank Elliptic Curves, Kobe J. Math, 1994, 11, 212):

Theorem 2.8 *Let* $a_4, a_3, a_2, a_1, a_0 \in \mathbf{Q}, a_4 \neq 0$. *Then* E *and* E' *are isomorphic over* $\mathbf{Q}(\sqrt{a_4})$, *where*

$$\begin{aligned} E &= a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \\ E' &= x^3 + a_2x^2 + (a_3a_1 - 4a_4a_0)x + (a_3^2a_0 + a_4a_1^2 - aa_4a_2a_0) \end{aligned}$$

Let $a = \sqrt{a_4}$. *Then the isomorphism is given by*

$$(x, y) \to (-2ay + 2a^2x^2 + a_3x, 4a^2xy + a_3y - 4a^3x^3 - 3aa_3x^2 - 2aa_2x - aa_1).$$

Hence, for the family we've constructed above (explicitly forcing the coefficient of x^4 to be a perfect square), we see we again obtain a cubic with First Sum contributing 6.

2.11 Families of Rank $7, 8$

We can modify the previous construction

$$\begin{aligned} y^2 &= x^3t^2 + 2g(x)t - h(x) \\ g(x) &= x^4 + ax^3 + bx^2 + cx + d, \ d \neq 0 \\ h(x) &= Ax^4 + Bx^3 + Cx^2 + Dx + E \end{aligned} \tag{2.65}$$

to obtain what should be higher rank families. Choosing appropriate quartics for $g(x), h(x)$ such that $D_t(x) = g^2(x) + x^3h(x)$ has eight distinct non-zero perfect square roots should yield a contribution of $8\phi(0)$. As the coefficient of t^2 is x^3, we won't lose $\phi(0)$ from summing over non-roots of $D_t(x)$. By specializing to certain $t = \alpha s^2 + \beta s + \gamma$ for some constants, we can arrange it so $y^2 = k^2(s)x^4 + \cdots$, and by the previous arguments obtain a cubic. Unfortunately, we can no longer explicitly evaluate the First Sum (because of the replacement $t \to \alpha s^2 + \beta s + \gamma$), so for this to be applicable we would need another method to determine its rank over $\mathbf{Q}(T)$, even though we can construct eight points on it for all s.

$$\begin{aligned} D_t(x) &= x^8 + (2a + A)x^7 + (a^2 + 2b + B)x^6 + (2c + 2ab + C)x^5 \\ &\quad + (b^2 + 2ac + 2d + D)x^4 + (2bc + 2ad + E)x^3 \\ &\quad + (2bd + c^2)x^2 + (2cd)x + d^2 \\ &= \prod_{i=1}^{8}(x - \alpha^2\rho_i^2) \\ &= \sum_{k=0}^{8} x^k(-1)^k\alpha^{16-2k}R_k. \end{aligned} \tag{2.66}$$

Matching coefficients for x^4, x^5, x^6 and x^7 is possible because of A, B, C, D.

$$\begin{aligned} d^2 &= \alpha^{16} R_0 \\ 2cd &= -\alpha^{14} R_1 \\ 2bd + c^2 &= \alpha^{12} R_2. \end{aligned} \tag{2.67}$$

Let $R_0 = r_0^2$. Then we find

$$\begin{aligned} d &= \alpha^8 r_0 \\ c &= -\frac{\alpha^6 R_1}{2r_0} \\ b &= \frac{\alpha^4 R_2}{2r_0} - \frac{\alpha^4 R_1^2}{8r_0^3}. \end{aligned} \tag{2.68}$$

Taking $\alpha = 2r_0$ yields d, b, c integral. (Note this is not always the minimal α; for example, if R_1 and R_2 are even, one may take $\alpha = r_0$).

If we take two of the roots to be the same, we should get a contribution of $7\phi(0)$.

3 Average Rank for Families

We will be brief here, as these bounds are poor. In the Appendix I've included again the handout on the Explicit Formula for an elliptic curve.

Let $\phi(x)$ be an even Schwartz function whose Fourier Transform (also a Schwartz function) is compactly supported, say in the interval $(-\sigma, \sigma)$.

The Explicit Formula relates summing ϕ over the zeros of the elliptic curve to summing $\hat{\phi}$ at the primes, assuming the Generalized Riemann Hypothesis is true (all non-trivial zeros have real part $\frac{1}{2}$ or 1, depending on how you normalize). By Theorem A.116 we have

$$\begin{aligned}
\sum \phi\Big(\gamma_E \frac{\log N_E}{2\pi}\Big) &= \hat{\phi}(0) + \phi(0) \\
&- 2\sum_p \frac{\log p}{\log N_E}\frac{1}{p}\hat{\phi}(\frac{\log p}{\log N_E})a_E(p) \\
&- 2\sum_p \frac{\log p}{\log N_E}\frac{1}{p^2}\hat{\phi}(2\frac{\log p}{\log N_E})a_E^2(p) + \frac{\log\log N_E}{\log N_E}
\end{aligned} \tag{3.69}$$

were γ_E runs through the imaginary parts of zeros of the elliptic curve (assuming GRH) and N_E is the conductor.

We need a more useful version of the Explicit Formula. The problem is the conductor will depend on $E = E_t$. We will want to sum the above over $t \in [N, 2N]$. Unfortunately, we cannot pull the sum over t past the conductor, as the conductor varies with the curve.

For example, from the previous section, we often know how to evaluate $\sum_{t(p)} a_{E_t}(p)$. This is often rp. If now we want $t \in [N, 2N]$, notice that $a_{E_t}(p) = a_{E_{t+mp}}(p)$ for any m. The reason is our family will be something like $y^2 = x^3 + A(T)x + B(T)$, and $a_{E_t}(p)$ is determined by looking at solutions mod p. If you replace t by $t + mp$ in the polynomials $A(T)$, $B(T)$, you get the same answer mod p.

Thus, summing t from N to $2N$ is equivalent to $\frac{N}{p}$ complete sums of t mod p, with a leftover (or incomplete) sum of at most p terms, each term (by Hasse) is at most $2\sqrt{p}$.

We can modify our derivation of the Explicit Formula and derive the following:

$$\sum \phi\Big(\gamma_E \frac{\log M}{2\pi}\Big) = \frac{\log N_E}{\log M}\hat{\phi}(0) + \phi(0)$$

$$
\begin{aligned}
&- \quad 2\sum_p \frac{\log p}{\log M}\frac{1}{p}\hat{\phi}\Big(\frac{\log p}{\log M}\Big)a_E(p) \\
&- \quad 2\sum_p \frac{\log p}{\log M}\frac{1}{p^2}\hat{\phi}\Big(2\frac{\log p}{\log M}\Big)a_E^2(p) + \frac{\log\log M}{\log M}
\end{aligned} \tag{3.70}
$$

Quick Proof: Instead of scaling by the conductor N_E in the derivation, scale by $\log M$.

We will choose $\log M = \frac{1}{N}\sum_{t=N}^{2N} \log N_{E_t}$. Hence $\log M$ is the average of the conductor's logarithms.

The above is now beautifully designed for summing over t. We get

$$
\begin{aligned}
\frac{1}{N}\sum_{t=N}^{2N}\sum \phi\Big(\gamma_E\frac{\log M}{2\pi}\Big) &= \frac{1}{N}\sum_{t=N}^{2N}\frac{\log N_E}{\log M}\hat{\phi}(0) + \frac{1}{N}\sum_{t=N}^{2N}\phi(0) \\
&- \quad 2\sum_p \frac{\log p}{\log M}\frac{1}{p}\hat{\phi}\Big(\frac{\log p}{\log M}\Big)\frac{1}{N}\sum_{t=N}^{2N} a_E(p) \\
&- \quad 2\sum_p \frac{\log p}{\log M}\frac{1}{p^2}\hat{\phi}\Big(2\frac{\log p}{\log M}\Big)\frac{1}{N}\sum_{t=N}^{2N} a_E^2(p) \\
&+ \quad \frac{1}{N}\sum_{t=N}^{2N}\frac{\log\log N_E}{\log N_E}
\end{aligned} \tag{3.71}
$$

From our choice of $\log M$, we have

$$
\begin{aligned}
\frac{1}{N}\sum_{t=N}^{2N}\sum \phi\Big(\gamma_E\frac{\log M}{2\pi}\Big) &= \hat{\phi}(0) + \phi(0) \\
&- \quad 2\sum_p \frac{\log p}{\log M}\frac{1}{p}\hat{\phi}\Big(\frac{\log p}{\log M}\Big)\frac{1}{N}\sum_{t=N}^{2N} a_E(p) \\
&- \quad 2\sum_p \frac{\log p}{\log M}\frac{1}{p^2}\hat{\phi}\Big(2\frac{\log p}{\log M}\Big)\frac{1}{N}\sum_{t=N}^{2N} a_E^2(p) \\
&+ \quad \frac{1}{N}\sum_{t=N}^{2N}\frac{\log\log M}{\log M}
\end{aligned} \tag{3.72}
$$

For large N, the error term will be like $\frac{\log\log N}{\log N}$, hence negligible. Some care is needed to show this.

For many families, we will be able to show $\frac{1}{N}\sum_{t=N}^{2N} a_E^2(p) = p + O(1)$, and hence by Theorem A.5, this term will contribute $-\frac{1}{2}\phi(0)$. Unfortunately, in general the best we can do is note that this sum is negative, so (ignoring the error)

$$\begin{aligned}\frac{1}{N}\sum_{t=N}^{2N}\sum \phi\Big(\gamma_E\frac{\log M}{2\pi}\Big) \quad &\leq \quad \hat{\phi}(0) + \phi(0) \\ &\qquad -2\sum_p \frac{\log p}{\log M}\frac{1}{p}\hat{\phi}\Big(\frac{\log p}{\log M}\Big)\frac{1}{N}\sum_{t=N}^{2N} a_E(p).\end{aligned} \tag{3.73}$$

Unfortunately, $a_{E_t}(p)$ can be both positive and negative, so we cannot just drop this term. We don't want to use Hasse to replace it by $2\sqrt{p}$, as this would result in a very large bound.

Since our function $\hat{\phi}$ is supported in $(-\sigma, \sigma)$, this means $\hat{\phi}(x) = 0$ if $|x| > \sigma$. As $x = \frac{\log p}{\log M}$, this means $p < M^\sigma$. Using Hasse would yield something like $\sum_p^{M^\sigma} p^{-\frac{1}{2}}$ which is like $M^{\frac{1}{2}\sigma}$. With some work, we can show for many families that M is like N to a power. Regardless, we see this term is growing enormously!

So, instead of using Hasse, we instead sum over t and gain cancellation there. Let's say we can show $-\sum_{t(p)} a_{E_t}(p) = rp + O(1)$. Then we would have

$$\begin{aligned}\frac{1}{N}\sum_{t=N}^{2N} -a_{E_t}(p) \quad &= \quad \frac{1}{N}\frac{N}{p}rp + O\Big(\frac{1}{N}\frac{N}{p}\Big) + O\Big(\frac{1}{N}p\cdot 2\sqrt{p}\Big) \\ &= \quad r + O\Big(\frac{1}{p} + \frac{p^{1.5}}{N}\Big)\end{aligned} \tag{3.74}$$

where the last term follows from our having an incomplete t-sum of at most p terms, each term at most $2\sqrt{p}$. If σ is very small, then we shall see the error terms are negligible.

By Theorem A.5, the r term gives a contribution of $r\phi(0)$. We now estimate the two error terms.

We first do the $\frac{1}{p}$ error. For error calculations like this, we use $\ll$ to indicate it is less than some constant which does not depend on any of the quantities involved. We will replace $\hat{\phi}(x)$ by its maximum value, which we then incorporate into $\ll$.

This yields

$$\begin{aligned} S_1 &\ll 2\sum_p^{M^\sigma} \frac{\log p}{\log M}\frac{1}{p}\hat{\phi}\Big(\frac{\log p}{\log M}\Big)\frac{1}{p} \\ &\ll \frac{1}{\log M}\sum_p^{M^\sigma}\frac{\log p}{p^2} \\ &\ll \frac{1}{\log M}, \end{aligned} \tag{3.75}$$

as $\sum_p \frac{\log p}{p^2}$ is finite.

We now handle the second error term, the $\frac{p^{1.5}}{N}$ term.

$$\begin{aligned} S_2 &\ll 2\sum_p^{M^\sigma} \frac{\log p}{\log M}\frac{1}{p}\hat{\phi}\Big(\frac{\log p}{\log M}\Big)\frac{p^{1.5}}{N} \\ &\ll \sum_p^{M^\sigma}\frac{p^{1.5}}{pN} \\ &\ll \sum_p^{M^\sigma}\frac{p^{\frac{1}{2}}}{N} \\ &\ll \frac{1}{N}\sum_n^{M^\sigma} n^{\frac{1}{2}} \\ &\ll \frac{1}{N}M^{\frac{3\sigma}{2}} \end{aligned} \tag{3.76}$$

We need to know how M is related to N. A poor bound is to look at the discriminant $\Delta(t)$. Clearly $M \leq \max_t N_t$. The largest (up to factors of 2 or 3, which won't matter of a logarithm scale) that N_t can be is $\Delta(t)^2$. Up to multiplicative constants, if $\Delta(t)$ is a polynomial of degree d, then $M \leq N^{2d}$.

Thus $\frac{1}{N}M^{\frac{3\sigma}{2}} \leq N^{3d\sigma-1}$, and this term will have negligible contribution for $\sigma < \frac{1}{3d}$.

Thus

Theorem 3.1 *For $\sigma < \frac{1}{3d}$, ignoring the error terms which do not contribute as $N \to \infty$, we have*

$$\begin{aligned}\frac{1}{N}\sum_{t=N}^{2N}\sum \phi\Big(\gamma_E \frac{\log M}{2\pi}\Big) &\leq \hat{\phi}(0) + \phi(0) + r\phi(0) \\ &\leq \hat{\phi}(0) + (r+1)\phi(0). \end{aligned} \tag{3.77}$$

3.1 Average Rank of the above Families

Let

$$\begin{aligned}\hat{\phi}(y) &= \begin{cases} \frac{1}{2}(\frac{1}{2}\sigma - \frac{1}{2}|y|) & |y| \leq \sigma \\ 0 & |y| > \sigma \end{cases} \\ \phi(x) &= \frac{\sin^2 2\pi(\frac{1}{2}\sigma)x}{(2\pi x)^2}. \end{aligned} \tag{3.78}$$

(Another Fourier Transform pair we could use is $\hat{\phi}(y) = \frac{1}{2}(\sigma - |y|), |y| \leq \sigma$ and $\phi(x) = \frac{1-\cos(2\pi\sigma x)}{(2\pi x)^2}$.)

The reason for such a choice is ϕ is a positive function. On the LHS of Theorem 3.1, we can drop all the zeros except the ones at the critical point. Depending on our normalizaton, these are either the zeros at $s = \frac{1}{2}$ or $s = 1$. Let's choose the normalization $s = 1$, so, assuming the GRH, the zeros for the curve E_t are $\rho_{E_t} = 1 + i\gamma_{E_t}$. So, we drop all zeros γ_{E_t} but $\gamma_{E_t} = 0$.

Then $\phi(0) = (\frac{1}{2}\sigma)^2$ and $\hat{\phi}(0) = \int_{-\infty}^{\infty}\phi(x)dx = \frac{\sigma}{4}$. As $\phi(x) \geq 0$, we obtain an upper bound for the average rank of our family of Elliptic Curves:

$$\begin{aligned}\frac{1}{N}\sum_{t=N}^{2N}\sum_{\rho_{E_t}=1+i\gamma_{E_t}} \phi\Big(t\frac{\log M}{2\pi}\Big) &\leq \hat{\phi}(0) + (r+1)\phi(0) \\ \frac{1}{N}\sum_{t=N}^{2N}\sum_{\gamma_{E_t}=0} \phi\Big(0\frac{\log M}{2\pi}\Big) &\leq \frac{\sigma}{4} + (r+1)\phi(0) \\ \frac{1}{N}\sum_{t=N}^{2N}\sum_{\gamma_{E_t}=0} \phi(0) &\leq \phi(0)\frac{1}{\sigma} + (r+1)\phi(0) \\ \frac{1}{N}\sum_{t=N}^{2N}\sum_{\gamma_{E_t}=0} 1 &\leq \frac{1}{\sigma} + (r+1). \end{aligned} \tag{3.79}$$

The larger we can take σ, the better the bound on the average rank. The LHS above is the average rank of the family, which we'll denote by AvRank($\mathcal{E}$).

We've shown we may take $\sigma < \frac{1}{3d}$. Therefore, the best we get is plugging in $\frac{1}{3d}$ and we find

Theorem 3.2 (Bounding AvRank($\mathcal{E}$) of a One-Parameter Family $\mathcal{E}$) *Assume the discriminant $\Delta(t)$ is a polynomial of degree d, and the degrees of the polynomials $A(T)$ and $B(T)$ aren't too large (being less than 3 and 5 respectively works). Then we can show the error terms are negligible if we choose functions supported in $(-\sigma,\sigma)$, $\sigma < \frac{1}{3d}$. Choosing our test function $\hat{\phi}$ wisely yields*

$$\begin{aligned} AvRank(\mathcal{E}) &\leq \frac{1}{\sigma} + (r+1) \\ &\leq 3d + r + 1. \end{aligned} \tag{3.80}$$

Thus the average rank of the family is finite.

Using a more delicate analysis and smoothing, Brumer and Heath-Brown have shown that for the family of all elliptic curves (which is *not* a one-parameter family) there is no contribution for $\sigma < \frac{4}{7}$, which implies the average rank is bounded by 2.25.

For a large number of one-parameter families, assuming some additional hypotheses (which are true for $A(T)$, $B(T)$ polynomials of small degree and conjectured to be true for any choice), Silverman (The average rank of an algebraic family of elliptic curves, Journal fr die reine und angewandte Mathematik, 1998) has shown the average rank is basically bounded by $d_{\text{cond}} + r + \frac{1}{2}$. Here d_{cond} is the degree of the conductor of $\mathcal{E}$ over $\mathbf{Q}(t)$.

4 Nice Families

Earlier we've given many constructions for families with rank; however, while we are able to evaluate all the sums we need for this problem with these families, there are other problems where these families do not yield tractable sums.

Below I'll list some families that have many of their related sums explicitly calculable.

4.1 Rank 0 Families

$y^2 = x^3 + 2^4(-3)^3(9t+1)^2$, $9t+1$ is square-free. Each curve has even functional equation; however, $j(t)$ is constant for this family.

$y^2 = x^3 \pm 4(4t+2)x$, $4t+2$ is square-free. If the sign is positive, the curve has odd functional equation; negative and it has even functional equation. Again, $j(t)$ is constant for this family.

$y^2 = x^3 + (t+1)x^2 + tx$, $t(t-1)$ is square-free. It is expected that half of the time the sign is even, half odd. $j(t)$ is not constant.

$y^2 = x^3 + x + t$, $27t^2 + 4$ square-free, $j(t)$ not constant.

$y^2 = x^3 + x^2 + 2t + 1$, $(2t+1)(54t+31)$ square-free, $j(t)$ not constant.

$y^2 = x^3 + tx^2 - (t+3)x + 1$, $t^2 + 3t + 9$ square-free. Every curve has odd functional equation, and $j(t)$ is not constant.

4.2 Rank 1 Families

$y^2 = x^3 + tx^2 + 1$, $4t^3 + 27$ is square-free, $j(t)$ is not constant.

4.3 Rank 2 Families

$y^2 = x^3 - t^2x + t^2$, $t(4t^2 - 27)$ is square-free, $j(t)$ is not constant.

$y^2 = x^3 - t^2x + t^4$, $t(27t^2 - 4)$ is square-free, $j(t)$ is not constant.

A The Explicit Formula

A.1 Summation Lemmas

We collect below certain basic integrals / sums that we will need.

Lemma A.1 (Abel's Summation Formula - Integral Version) *Let* $h(x)$ *be a continuously differentiable function. Let* $A(x) = \sum_{n \leq x} a_n$. *Then*

$$\sum_{n \leq x} a_n h(n) = A(x)h(x) - \int_1^x A(u)h'(u)du \tag{A.81}$$

Lemma A.2 (Partial Summation)

$$\sum_M^N a_n b_n = A_N b_N - A_{M-1} b_M + \sum_M^{N-1} A_n (b_n - b_{n+1}) \tag{A.82}$$

A.2 Preliminaries

Our studies will lead to investigating

$$\sum \phi(\gamma_E \frac{\log c_E}{2\pi}).$$

We first prove the explicit formula for $\sum \phi(\gamma_E)$, for replacing ϕ by ϕ_r, where $r = \frac{\log c_E}{2\pi}$, we obtain the desired formula. We record for later the relationship between $\hat{\phi}$ and $\hat{\phi}_r$, where $\hat{\phi}_r(\xi) = \hat{\phi}(r\xi)$.

Lemma A.3 *Let* $\hat{\phi}(\xi) = \int_{\mathbf{R}} \phi(x) e^{-2\pi i x \xi} dx$. *Then* $\hat{\phi}_r(\xi) = \frac{1}{r}\hat{\phi}(\xi/r)$.

The proof is immediate from the definition of the Fourier Transform.

Lemma A.4 (Sum of $\hat{\phi}$ over primes)

$$\frac{1}{\log N} \sum_{p \equiv 1(m)} \frac{\log p}{p} \hat{\phi}(a \frac{\log p}{\log N}) = \frac{1}{2a\varphi(m)} \phi(0) + O(\frac{1}{\log N}). \tag{A.83}$$

Unfortunate notation, but denote the Euler Phi-function by φ. If m is a prime, $\varphi(m) = m - 1$; in general, $\varphi(m)$ is the number of numbers from 1 to m that are relatively prime with m. We will use ϕ and $\hat{\phi}$ to denote a generic test function and its Fourier Transform. We will take $\hat{\phi}$ to be an even Schwartz function, often with compact support.

By RH (or GRH if $m \neq 1$) and partial summation we have

$$\sum_{\substack{p\le x\\ p\equiv 1(m)}} \log p = \frac{x}{\varphi(m)} + O(x^{\frac{1}{2}}\log^2(mx))$$

$$\sum_{\substack{p\le x\\ p\equiv 1(m)}} \frac{\log p}{p} = \frac{\log x}{\varphi(m)} + O(1). \tag{A.84}$$

For notational convenience, let $M = \varphi(m)$. Using partial summation on the p sum gives

$$\begin{aligned}
\sum_{p\equiv 1(m)} \frac{\log p}{p}\hat{\phi}(a\frac{\log p}{\log N}) &= -\int_0^\infty \Big(\frac{\log x}{M} + O(1)\Big)\frac{d}{dx}\hat{\phi}(a\frac{\log x}{\log N}) \\
&= \int_0^\infty \frac{1}{Mx}\hat{\phi}(a\frac{\log x}{\log N}) + O\Big(\frac{1}{x\log N}\Big|\hat{\phi}(a\frac{\log x}{\log N})\Big|\Big) \\
&= \frac{\log N}{a}\int_0^\infty \frac{1}{M}\hat{\phi}(u) + O\Big(\frac{1}{\log N}\Big|\hat{\phi}(u)\Big|\Big)du \\
&= \frac{\log N}{a}\frac{1}{2}\int_{-\infty}^\infty \frac{1}{M}\hat{\phi}(u) + O\Big(\frac{1}{\log N}\Big|\hat{\phi}(u)\Big|\Big)du \\
&= \frac{\log N}{2aM}\phi(0) + O(1).
\end{aligned} \tag{A.85}$$

Dividing by $\log N$ yields the lemma.

In particular, setting $m = 1$ and $a = 1, 2$ yields

Theorem A.5

$$\frac{1}{\log N}\sum_p \frac{\log p}{p}\hat{\phi}(\frac{\log p}{\log N}) = \frac{1}{2}\phi(0) + O(\frac{1}{\log N})$$

$$\frac{1}{\log N}\sum_p \frac{\log p}{p}\hat{\phi}(2\frac{\log p}{\log N}) = \frac{1}{4}\phi(0) + O(\frac{1}{\log N}). \tag{A.86}$$

Let E be a modular elliptic curve (arising from a newform f on $\Gamma_0(N)$) whose zeros satisfy the GRH, namely $\rho_E = 1 + i\gamma_E$. To simplify notation, we drop the subscript E below. Then to E we can attach an L-function $L(s,E) = L(s)$. Define $\Lambda(s)$ by

$$\Lambda(s) = (2\pi)^{-s}N^{s/2}\Gamma(s)L(s).$$

Then we have

$$\Lambda(s) = \epsilon\Lambda(2-s), \tag{A.87}$$

where $\epsilon = \epsilon_f = \pm 1$. The logarithmic derivative is

$$\frac{\Lambda'(s)}{\Lambda(s)} = \frac{1}{2}\log\frac{N}{4\pi^2} + \frac{\Gamma'(s)}{\Gamma(s)} + \frac{L'(s)}{L(s)} = -\frac{\Lambda'(2-s)}{\Lambda(2-s)} \tag{A.88}$$

We express $\frac{L'(s)}{L(s)}$ in a form convenient for deriving the explicit formula. For each prime p, let E_p be the number of points on the reduced elliptic curve E (including infinity), and let $t_p = 1 + p - E_p$. Then it is well known (see, for example, AEC, page 240) that

$$L(s) = \prod_{p|\triangle}(1 - t_p p^{-s})^{-1} \prod_{p\ \dagger\ \triangle}(1 - t_p p^{-s} + p^{1-2s})^{-1} \tag{A.89}$$

$$L(s) = \sum \lambda(n)n^{-s},\ \lambda(p) = t_p, \tag{A.90}$$

where if $p|\triangle$, then $t_p = -1, 0$, or 1. Hence we obtain

$$\frac{L'(s)}{L(s)} = -\sum_{p|\triangle}\frac{d}{ds}\log(1 - t_p p^{-s}) - \sum_{p\ \dagger\ \triangle}\frac{d}{ds}\log(1 - t_p^{-s} + p^{1-2s}). \tag{A.91}$$

Straightforward calculations show the first term equals

$$-\sum_{p|\triangle}\sum_{k=1}^{\infty}\frac{(\log p)t_p^k}{(p^k)^s}. \tag{A.92}$$

To handle the second term in the sum, we let $u = p^{-s}$ and factor

$$1 - t_p p^{-s} + p^{1-2s} = pu^2 - t_p u + 1 = (1 - \alpha_p u)(1 - \beta_p u), \tag{A.93}$$

where

$$\alpha_p + \beta_p = t_p, \quad \alpha_p\beta_p = p. \tag{A.94}$$

We see the second term in $\frac{L'(s)}{L(s)}$ is

$$\sum_{p\ \dagger\ \triangle}\sum_{k=1}^{\infty}\frac{(\log p)(\alpha_p^k + \beta_p^k)}{(p^k)^s}. \tag{A.95}$$

Combining yields

$$\frac{L'(s)}{L(s)} = -\sum_{p|\triangle}\sum_{k=1}^{\infty}\frac{(\log p)t_p^k}{(p^k)^s} - \sum_{p\ \dagger\ \triangle}\sum_{k=1}^{\infty}\frac{(\log p)(\alpha_p^k + \beta_p^k)}{(p^k)^s}. \tag{A.96}$$

A.3 The Explicit Formula

The following derivation is a modification of that in Zeros of Principle L-Functions (Rudnick and Sarnak, Duke Journal of Mathematics, 1996). See their proposition 2.1, pages 277-278.

Let $\phi \in \mathcal{S}(\mathbf{R})$ be an even function whose Fourier Transform has compact support. By the GRH, the non-trivial zeros of the L-function associated to our elliptic curve satisfy

$$\rho = 1 + i\gamma, \quad \gamma \in \mathbf{R}.$$

Note that for $Re(s) = 1$, $\frac{s-1}{i} \in \mathbf{R}$, and hence $\phi(\frac{s-1}{i})$ exists and is well defined. We are thus led to define

$$H(s) = \phi(\frac{s-1}{i}). \tag{A.97}$$

Initially, $H(s)$ is defined only for $Re(s) = 1$. Using the Inverse Fourier Transform we see

$$\phi(x) = \int_{\mathbf{R}} \hat{\phi}(\xi) e^{2\pi i x \xi} d\xi. \tag{A.98}$$

Therefore

$$\phi(x + iy) = \int_{\mathbf{R}} \hat{\phi}(\xi) e^{2\pi i (x+iy)\xi} d\xi, \tag{A.99}$$

and as ϕ has compact support, we see we can extend ϕ, and hence $H(s)$ is well defined, and

$$H(x + iy) = \int_{\mathbf{R}} \left[\hat{\phi}(\xi) e^{2\pi (x-1)\xi}\right] e^{2\pi i y \xi} d\xi. \tag{A.100}$$

Thus $H(x + iy)$ is the Fourier Transform of a function in $\mathcal{S}(\mathbf{R})$, and hence is rapidly decreasing in $Im(s) = y$.

So both $H(s)$ and $\Lambda(s)$ are nice entire functions. Consider

$$\mathcal{I} = \frac{1}{2\pi i} \int_{Re(s) = 2\frac{1}{2}} \frac{\Lambda'(s)}{\Lambda(s)} H(s) ds. \tag{A.101}$$

We shift contours from $Re(s) = 2\frac{1}{2}$ to $-\frac{1}{2}$. This picks up zeros/poles of $\Lambda(s)$. Two factors of $\Lambda(s)$ contribute potential zeros/poles, the L term and the Γ term. The only pole of the Γ-function in this range is at $s = 0$; however, as $\Lambda(2) \neq 0$, there is a zero of the L-function that cancels. Hence the only surviving zeros/poles are from the zeros of the L function in the critical strip, and the residue is just $H(1 + i\gamma) = \phi(\gamma)$. Therefore

$$\mathcal{I} = \sum \phi(\gamma) + \frac{1}{2\pi i}\int_{Re(s)=-\frac{1}{2}} \frac{\Lambda'(s)}{\Lambda(s)} H(s)ds. \tag{A.102}$$

By (A.88), we have $\frac{\Lambda'(s)}{\Lambda(s)} = -\frac{\Lambda'(2-s)}{\Lambda(2-s)}$, so substituting this above and changing s to $2-s$ we obtain

$$\mathcal{I} = \sum \phi(\gamma) - \frac{1}{2\pi i}\int_{Re(s)=2\frac{1}{2}} \frac{\Lambda'(s)}{\Lambda(s)} H(2-s)ds. \tag{A.103}$$

Bringing $\sum \phi(\gamma)$ over to the LHS and recalling the definition of $\mathcal{I}$ yields

$$\sum \phi(\gamma) = \frac{1}{2\pi i}\int_{Re(s)=2\frac{1}{2}} \frac{\Lambda'(s)}{\Lambda(s)} \Big[H(s) + H(2-s)\Big]ds. \tag{A.104}$$

We can shift the contour above to $Re(s) = 1$, as we are assuming there are no zeros of the L-function off the critical line. We do so, and note that for $s = 1+iy$, $H(2-s) = H(s) = \phi(y)$, as we are assuming ϕ even. Using (A.88) for $\frac{\Lambda'(s)}{\Lambda(s)}$ gives (for $s = 1+iy, ds = idy$)

$$\begin{aligned}\sum \phi(\gamma) &= \frac{1}{2\pi}\int_{\mathbf{R}} \Big[\log(\frac{N}{4\pi^2}) + 2\frac{\Gamma'(1+iy)}{\Gamma(1+iy)}\Big]\phi(y)dy \\ &+ \frac{1}{2\pi i}\int_{\mathbf{R}} \frac{L'(1+iy)}{L(1+iy)} 2\phi(y)ds. \end{aligned}\tag{A.105}$$

We use (A.96) to substitute for $\frac{L'(1+iy)}{L(1+iy)}$; by Hasse's theorem $|t_p| < 2p^{\frac{1}{2}}$. We shift this piece back to $Re(s) = 2\frac{1}{2}$. By the DCT we can interchange the summations and integration. We then shift back to $Re(s) = 1$. As

$$\begin{aligned}\int_{\mathbf{R}} (\frac{1}{p^k})^{1+iy}\phi(y)dy &= \int_{\mathbf{R}} \frac{1}{p^k}\phi(y)e^{-ik\log(p)y}dy \\ &= \frac{1}{p^k}\hat{\phi}(\frac{k\log(p)}{2\pi}), \end{aligned}\tag{A.106}$$

we obtain the explicit formula:

$$\sum \phi(\gamma) = \frac{1}{2\pi}\int_{\mathbf{R}} \Big[\log(\frac{N}{4\pi^2}) + 2\frac{\Gamma'(1+iy)}{\Gamma(1+iy)}\Big]\phi(y)dy$$

$$- \quad \frac{1}{2\pi} \sum_{p|\triangle} \sum_{k=1}^{\infty} \frac{2\log(p) t_p^k}{p^k} \hat{\phi}(\frac{1}{2\pi} k \log(p))$$

$$- \quad \frac{1}{2\pi} \sum_{p \dagger \triangle} \sum_{k=1}^{\infty} \frac{2\log(p)(\alpha_p^k + \beta_p^k)}{p^k} \hat{\phi}(\frac{1}{2\pi} k \log(p)) \quad \text{(A.107)}$$

A.4 Tractable Explicit Formula

In the previous section, we derived the explicit formula for the sum over the zeros of an elliptic curve (assuming the GRH, of course). Below we will show that many of the terms are $O(\frac{1}{\log N})$.

First, we replace $\phi(x)$ by $\phi_r(x)$, $r = \frac{1}{2\pi}\log N$. A straightforward calculation shows that

$$\frac{1}{2\pi} \int_{\mathbf{R}} \left[\log(\frac{N}{4\pi^2}) + 2\frac{\Gamma'(1+iy)}{\Gamma(1+iy)} \right] \phi(y) dy \to \int_{\mathbf{R}} \phi(y) dy + O(\frac{1}{\log N}). \quad \text{(A.108)}$$

To prove the above, use (see Alfohrs, Complex Analysis)

$$\frac{\Gamma'(z)}{\Gamma(z)} = C + \log z - \frac{1}{2z} - \int_0^{\infty} \frac{2u}{u^2+z^2} \frac{du}{e^{2\pi u} - 1}, \quad Re(z) > 0. \quad \text{(A.109)}$$

Hence we find

$$\begin{aligned} \sum \phi(\gamma \frac{\log N}{2\pi}) &= \int_{\mathbf{R}} \phi(y) dy && \text{(A.110)} \\ &- 2 \sum_{p|\triangle} \sum_{k=1}^{\infty} \frac{\log p}{\log N} \frac{t_p^k}{p^k} \hat{\phi}(k \frac{\log p}{\log N}) \\ &- 2 \sum_{p \dagger \triangle} \sum_{k=1}^{\infty} \frac{\log p}{\log N} \frac{\alpha_p^k + \beta_p^k}{p^k} \hat{\phi}(k \frac{\log p}{\log N}) + O(\frac{1}{\log N}). \end{aligned}$$

As $|\alpha_p|, |\beta_p| < p^{\frac{1}{2}}$ and $|t_p| \le 2p^{\frac{1}{2}}$, we can bound the $k \ge 3$ terms above by $||\phi||_\infty \frac{1}{\log N}$. For $p \dagger \triangle$, $\alpha_p + \beta_p = t_p$ and $\alpha_p \beta_p = p$. Hence $\alpha_p^2 + \beta_p^2 = t_p^2 - 2p$, and it is sufficient to study

$$\begin{aligned} \sum \phi(\gamma \frac{\log N}{2\pi}) &= \int_{\mathbf{R}} \phi(y) dy \\ &- 2 \sum_{p} \sum_{k=1}^{2} \frac{\log p}{\log N} \frac{t_p^k}{p^k} \hat{\phi}(k \frac{\log p}{\log N}) \\ &- 2 \sum_{p \dagger \triangle} \frac{\log p}{\log N} \frac{-2p}{p^2} \hat{\phi}(2 \frac{\log p}{\log N}) + O(\frac{1}{\log N}). \text{(A.111)} \end{aligned}$$

Lemma A.6 $\frac{1}{\log N}\sum_{p|\triangle}\frac{\log p}{p}\hat{\phi}(a\frac{\log p}{\log N}) = O(\frac{\log\log N}{\log N})$.

In the above, $\triangle$ is the discriminant of the elliptic curve, and N is its conductor. Further, the conductor and the discriminant have the same prime factors, so we may replace $\triangle$ by N.

$\frac{\log p}{p}$ is a decreasing function, so in the sum, the sum is largest when we have many small prime factors of N; in fact, the sum is greatest when N is the product of the first n primes. So

$$N = 2\cdot\ 3\cdots\ p_n\ \geq\ 2^n\ \to\ n\ \leq\ \frac{\log N}{\log 2}. \tag{A.112}$$

As $\sum_{p=2}^{X}\frac{\log p}{p} = \log X + O(1)$ (Davenport, Multiplicative Number Theory, page 57) we have

$$\begin{aligned}\frac{1}{\log N}\sum_{p|N}\frac{\log p}{p}\hat{\phi}(a\frac{\log p}{\log N}) &\ll \frac{1}{\log N}\sum_{p=2}^{\frac{\log N}{a\log 2}}\frac{\log p}{p} \\ &= \frac{1}{\log N}\left[\log(\frac{\log N}{a\log 2}) + O(1)\right] \\ &= O(\frac{\log\log N}{\log N}),\end{aligned} \tag{A.113}$$

yielding the lemma.

Therefore, the cost of expanding $\sum_{p\ \dagger\ \triangle}\frac{\log p}{\log N}\frac{-2p}{p^2}\hat{\phi}(2\frac{\log p}{\log N})$ to a sum over all primes can be safely absorbed in our error. Therefore we now study

$$\begin{aligned}\sum\phi(\gamma\frac{\log N}{2\pi}) &= \int_{\mathbf{R}}\phi(y)dy \\ &- 2\sum_p\sum_{k=1}^{2}\frac{\log p}{\log N}\frac{t_p^k}{p^k}\hat{\phi}(k\frac{\log p}{\log N}) \\ &- 2\sum_p\frac{\log p}{\log N}\frac{-2p}{p^2}\hat{\phi}(2\frac{\log p}{\log N}) + O(\frac{1}{\log N}).\end{aligned} \tag{A.114}$$

The last sum, by Lemma A.4, is just $4\frac{1}{4}\phi(0) = \phi(0)$. Thus we can write the explicit formula as:

$$\sum\phi(\gamma\frac{\log N}{2\pi}) = \int_{\mathbf{R}}\phi(y)dy + \phi(0)$$

$$
\begin{aligned}
&- \quad 2\sum_p \frac{\log p}{\log N}\frac{t_p}{p}\hat{\phi}(\frac{\log p}{\log N}) \\
&- \quad 2\sum_p \frac{\log p}{\log N}\frac{t_p^2}{p^2}\hat{\phi}(2\frac{\log p}{\log N}) \;+\; O(\frac{\log\log N}{\log N}) \qquad \text{(A.115)}
\end{aligned}
$$

We make one final simplification. $t_p = 1 + p - E_p$, where E_p is the number of points (including infinity) on the curve reduced mod p. Let us say $y^2 = f(x)$. Then $E_p = 1 + \sum_{x=0}^{p-1}\Big(1 + (\frac{f(x)}{p})\Big)$. Hence $t_p = -\sum_{x=0}^{p-1}(\frac{f(x)}{p})$, and we have

Theorem A.7 (The Explicit Formula)

$$
\begin{aligned}
\sum \phi(\gamma\frac{\log N}{2\pi}) \quad &= \quad \int_{\mathbf{R}} \phi(y)dy + \phi(0) \\
&- \quad 2\sum_p \frac{\log p}{\log N}\frac{t_p}{p}\hat{\phi}(\frac{\log p}{\log N}) \\
&- \quad 2\sum_p \frac{\log p}{\log N}\frac{t_p^2}{p^2}\hat{\phi}(2\frac{\log p}{\log N}) + O(\frac{\log\log N}{\log N}) \\
&= \quad \hat{\phi}(y) + \phi(0) \\
&+ \quad 2\sum_p \frac{\log p}{\log N}\frac{1}{p}\hat{\phi}(\frac{\log p}{\log N})\sum_{x=0}^{p-1}\left(\frac{f(x)}{p}\right) \\
&- \quad 2\sum_p \frac{\log p}{\log N}\frac{1}{p^2}\hat{\phi}(2\frac{\log p}{\log N})\Big(\sum_{x=0}^{p-1}\left(\frac{f(x)}{p}\right)\Big)^2 + O(\frac{\log\log N}{\log N})
\end{aligned}
\qquad \text{(A.116)}
$$