1- and 2-Level Densities for Families of Elliptic Curves: Evidence for the Underlying Group Symmetries

Steven J. Miller

A Dissertation
Presented to the Faculty
of Princeton University
in Candidacy for the Degree
of Doctor of Philosophy

Recommended for Acceptance
By the Department of
Mathematics

June 2002

Abstract

Following Rubinstein [Ru], Iwaniec-Luo-Sarnak [ILS], and Katz-Sarnak [KS1], [KS2], we use the 1- and 2-level densities to study the distribution of low lying zeros for families of elliptic curves.

For any automorphic cupsidal L-function, the n-level correlations of the high zeros (for test functions of suitable support) equal the GUE's. While the classical compact groups have identical n-level correlations over all the eigenvalues of a typical matrix, they have distinguishable n-level densities for their eigenvalues near 1.

To any geometric family, the philosophy of Katz and Sarnak ([KS1], [KS2]) states the n-level density depends only on a symmetry group attached to the family. For typical elliptic curve families they predict orthogonal symmetries. One can further analyze the distributions depending on the signs of the functional equations. As our families of elliptic curves are self-dual, we expect the densities to be controlled by the distribution of signs (all even: SO(even); all odd: SO(odd); equidistributed: O).

Previous 1-level density investigations of elliptic curve families were for test functions supported in $(-1, 1)$, where the orthogonal groups' densities are identical. The orthogonal groups have distinguishable (from each other and the other classical compact groups) 2-level densities for functions of arbitrarily small support.

Consider a rational elliptic surface of rank r over $\mathbb{Q}(t)$. Assume GRH (and ABC or the Square-Free Sieve conjecture if $\Delta(t)$ has an irreducible factor of degree ≥ 4). The Birch and Swinnerton-Dyer conjecture and Silverman's Specialization Theorem imply for t large, each curve has r zeros at the critical point. We prove removing these zeros' contributions yield modified densities depending only on the distribution of signs. For all even, odd, and equidistributed, we obtain SO(even), SO(odd) and O as predicted. We verify this for several families of known constant sign.

Let $M(t)$ be the product of the irreducible polynomials dividing $\Delta(t)$ but not $c_4(t)$. Helfgott [Hel] has shown, assuming standard conjectures, $j(t)$ and $M(t)$ non-constant imply the signs are equidistributed. Thus, for rational elliptic surfaces, the 2-level density provides conditional evidence that the underlying group (in general) is O and not SO(even) or SO(odd). Nevertheless, for small support, we unconditionally verify Katz and Sarnak's conjecture for the 1-level density of a rational elliptic surface and the 2-level density for some families of constant sign.

Finally, we use the 2-level density to obtain better upper bounds on the percent of curves in a family of rank r with rank $r + 2$ or higher, and we explore potential lower order corrections to the densities for several families.

Acknowledgements

As long as this thesis is, the acknowledgement section should be longer.

I would first like to thank my family, especially my parents, brother Jeff and wife Liz, and the Goldbergs, my friends (AcDec, BCYC, Constructors, GMB, GCHC, GCU, HA, IFCBC, Microform, the Milfees, the Missouri Club, Quaker Bridge, Section 31, the Singing Mimes, and the Superfly to name a few), and my suitemates (especially Eric Adelizzi, Michael Buchanan, Eduardo Dueñez, and Luke Yoon).

I have been extremely fortunate in having terrific advisors. I'd like to thank Professors Frank Firk, Henryk Iwaniec, and Peter Sarnak for their patience, wisdom, experience, and the privilege of working with them.

I'm grateful to my colleagues at Yale and Princeton for numerous hours of enlightening discussions and support, especially Professors Aldo Antonelli, Roger Howe, Peter Jones, Serge Lang, Ravi Ramakrishna, George Seligman, and Greg Zuckerman at Yale, Professors John Conway, Jordan Ellenberg, Charlie Fefferman, Nick Katz, Simon Kochen, Joe Kohn, Wenzhi Luo, Eli Stein, and Andrew Wiles at Princeton, and my study partners Jared Anderson, Eduardo Dueñez, Harald Helfgott, David Nadler, Alex Peng, Atul Pokharel, Scott Rickert, Serkan Savasoglu, and Rami Shakarchi

I am also grateful to the undergraduate math majors of Princeton, who, for the two years I helped run the Junior Research Seminar, were a terrific audience and wonderful fellow investigators.

Special thanks to Stephen D. Miller, for going out and making a name for me in Number Theory.

Finally, I would like to thank the support staff of the Math Department for all their help and friendship, and Mr. Twisty for showing me how to bend the rules.

To Liz

for her constant love and support, which made a difficult task possible

Contents

Part I

Introduction

1 Summary of Thesis Results

1.1 Historical Background

In attempting to describe the energy levels of heavy nuclei ([Wig1], [Wig2], [Po], [BFFMPW]), researchers were confronted with daunting calculations for a many bodied system with extremely complicated interaction forces. Unable to explicitly calculate the energy eigenstates, physicists developed Random Matrix Theory to predict general properties of the system.

Let $\mathbf{H}$ represent the Hamiltonian of the system and ψ_E the energy eigenstate with energy E; hence $\mathbf{H}\psi_E = E\psi_E$. The hope was that the Hamiltonian of a many bodied nucleus (such as Uranium, with over 200 protons and neutrons) could be well modeled by a random matrix. Physical symmetries (for example, time reversal symmetry) would constrain the possible operators $\mathbf{H}$ (Hermitian, real-symmetric, etc.). Similar to ensembles from Statistical Mechanics, one assigns probability measures to matrices from various groups. By explicitly calculating properties associated to an individual matrix and integrating over the group, one can often use the group average to make good predictions about the expected behavior of statistics from a generic, randomly chosen element.

There are striking similarities to statistics associated to energy levels in physics and statistics associated to zeros of L-functions in Number Theory. The non-trivial zeros of an L-function correspond to the energy levels; instead of shooting high energy neutrons at the nucleus (to determine the energy levels), we instead hit the zeros with Schwartz test functions. In physics, we are only able to bombard our nucleus with neutrons whose energy level is restricted in some range; in Number Theory, with present analytic technology, this corresponds to only being able to evaluate sums of Schwartz test functions at the zeros when the functions have compact support in some fixed range.

The first L-function encountered is the Riemann-Zeta function (see, for example, [Da]):

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \Big(1 - p^{-s}\Big)^{-1}, \quad \mathrm{Re}(s) > 1. \tag{1.1}$$

While initially defined only for $\mathrm{Re}(s) > 1$, $\zeta(s)$ can be meromorphically continued to the entire complex plane, and satisfies a functional equation:

$$\xi(s) = \Gamma\Big(\frac{s}{2}\Big)\pi^{-\frac{s}{2}}\zeta(s) = \xi(1-s). \tag{1.2}$$

Due to the functional equation, it is enough to understand the behavior of $\zeta(s)$ for $\text{Re}(s) \geq \frac{1}{2}$. Because of the Gamma factor, $\zeta(s)$ trivially vanishes for s a negative even integer. The Riemann Hypothesis (RH) states all the (non-trivial) zeros have $\text{Re}(s) = \frac{1}{2}$. We call $0 \leq \text{Re}(s) \leq 1$ the critical strip, $\text{Re}(s) = \frac{1}{2}$ the critical line, and $s = \frac{1}{2}$ the critical point.

More generally, we may consider automorphic L-functions (see, for example, [Iw])

$$L(s,f) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_p L_p(p^{-s},f)^{-1}, \quad \text{Re}(s) > s_0. \tag{1.3}$$

In this thesis we study elliptic curves (see [Kn] or [Si1]). Let E be the elliptic curve $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ with discriminant Δ. For each prime p, consider the reduced curve E_p: $(a_i)_p = a_i \bmod p$. Let N_p be the number of incongruent solutions (x,y) to E_p mod p (including the point at infinity), and define $a_p = p + 1 - N_p$. We form the L-function

$$L(s,E) \quad = \quad \prod_{p|\Delta} \frac{1}{1 - a_p p^{-s}} \prod_{p \nmid \Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}. \tag{1.4}$$

By the Modularity Theorem for Elliptic Curves ([Wi], [TW], [BCDT]) $L(s,E)$ is analytic, has a functional equation (s into $2-s$), and is equal to $L(s,f)$ for a weight two, level N cuspidal newform, where N is the conductor of the elliptic curve. By sending $s \to s + \frac{1}{2}$, the functional equation is now s into $1-s$, and again the critical strip is $0 \leq \text{Re}(s) \leq 1$. The Generalized Riemann Hypothesis (GRH) asserts that all (non-trivial) zeros have $\text{Re}(s) = \frac{1}{2}$.

1.2 n-Level Correlations

In an impressive set of computations, starting with the $10^{20\text{th}}$ zero of $\zeta(s)$, Odlyzko (see [Od1], [Od2]) studied the normalized spacings between adjacent zeros and found remarkable agreement with Random Matrix Theory. Specifically, consider the set of $N \times N$ random Hermitian matrices with entries chosen from the Gaussian distribution (the GUE). As $N \to \infty$, the limiting distribution of spacings between adjacent eigenvalues is indistinguishable from what Odlyzko observed!

Additionally, one can study the n-level correlations. Let $\{\alpha_j\}_{j=1}^{N}$ be an increasing sequence of numbers. In practice, we will take these to be either zeros of an L-function or eigenvalues of a matrix. For a compact box $B \subset \mathbb{R}^{n-1}$ we define the n-level correlation by

$$\frac{\#\Big\{(\alpha_{j_1}-\alpha_{j_2},\dots,\alpha_{j_{n-1}}-\alpha_{j_n}) \in B, j_i \in \{1,\dots,N\}, j_i = j_k \text{ iff } i = k\Big\}}{N} \tag{1.5}$$

Instead of using a box, one can look at a smoothed version with a test function f on $\mathbb{R}^n$. See Rudnick-Sarnak [RS] for more details. For test functions whose Fourier Transform has small support, Montgomery [Mon] proved the 2- and Hejhal [Hej] proved the 3-level correlations for the zeros of $\zeta(s)$ are the same as that of the GUE, and Rudnick-Sarnak [RS] proved the n-level correlations for all automorphic cuspidal L-functions are the same as the GUE.

The universality that Rudnick and Sarnak observed is somewhat surprising, but explainable as follows: the correlations are controlled by the second moments of the a_p's, and while there are many possible limiting distributions for the a_p's, they all have the same second moment.

Unfortunately, many different systems will have the same n-level correlations. Consider the classical compact groups: U(N), SU(N), $USp(2N)$, SO(even) and SO(odd). Fix a group, and choose a generic matrix element. Calculating the n-level correlations of its eigenvalues, integrating over the group, and taking the limit as $N \to \infty$, Katz and Sarnak prove the resulting answer is universal, independent of the particular group chosen. In particular, we cannot use the n-level correlations to distinguish GUE behavior, U(N), from the other classical compact groups.

This brings up the intriguing possibility of investigating a statistic more sensitive to the underlying symmetry or structure than the n-level correlations. Following Iwaniec-Luo-Sarnak and Rubinstein, we introduce the concept of a family and n-level density for low lying zeros, and find a statistic which will depend on finer properties of the family.

1.3 Families and n-Level Density

Let $L(s,f)$ be the L-function associated to f. If we were to directly study the distribution of its zeros, there are two natural ways to proceed. First, we may take ever larger sets of zeros, normalize each by its average spacing, and then look at related statistics. Second, we may attempt to study the behavior of the low lying zeros (ie, those zeros near the critical point, $s = \frac{1}{2}$).

The first method leads to the n-level correlations, which are insensitive to the behavior of the low lying zeros. For example, fix a compact box $B \subset \mathbb{R}^{n-1}$ and a positive integer k. Consider the contributions to the n-level correlation from any k zeros. Since the box is compact, provided the zeros tend to infinity, only finitely many will give us an n-tuple in the box if we force one of the zeros to be from the any k zeros. Letting N tend to infinity, we see there is no net contribution from these zeros. Note it is crucial that we take n distinct zeros in the definition of the n-level correlation. Thus, we may remove finitely many zeros without changing this statistic.

In many instances, the behavior of $L(\frac{1}{2}, f)$ encodes critical information about the function. For example, for L-functions of elliptic curves, the order of vanishing of $L(s, E)$ at $s = \frac{1}{2}$ is conjecturally equal to the geometric rank of the Mordell-Weil group (Birch and Swinnerton-Dyer conjecture; known to be true when the function vanishes to at most first order: see [CW], [Ko]). The point $s = \frac{1}{2}$ is clearly special, as it is the center of the critical strip, and leads to the fascinating possibility that there could be a difference in spacing statistics for zeros near $\frac{1}{2}$ than zeros higher up; as we've remarked, if we look at large batches of zeros, this information will be drowned out. If we force the Mordell-Weil group to be large, we expect many zeros exactly at $s = \frac{1}{2}$, and this might influence the behavior of the neighboring zeros. Hence we are led to study the distribution of the first few, or low lying, zeros.

By (often time consuming) computation, we can calculate the zeros of $L(s, f)$. Once found, we can try to interpret the results in terms of natural quantities associated to the function: how many zeros are there at $s = \frac{1}{2}$? How do the heights of the zeros above the critical point compare to the coefficients and special quantities of our function?

Similar to choosing an $N \times N$ matrix at random and calculating its eigenvalues, we only get one string of values. If, however, we can find a large number of functions similar to our original one, then we may calculate the zeros of each, and see how they vary from function to function.

This leads us to the concept of *family*. Roughly, a family will be a collection of geometric objects and their associated L-functions, where the geometric objects have similar properties. (In nuclear physics, this corresponds to amalgamating energy resonance data from different elements with similar invariants).

Iwaniec, Luo and Sarnak [ILS] considered (among other examples) all cuspidal newforms of a given level and weight. Rubinstein [Ru] considers twists by fundamental discriminants $D \in [N, 2N]$ of a fixed modular form.

In this thesis, we study the family of all elliptic curves and one-parameter families of elliptic curves. Thus, in our case the notion of family is the standard one from geometry: we have a collection of curves over a base, and the geometry is much clearer in our examples than in [ILS] and [Ru].

Explicitly, we will consider the family of all elliptic curves,

$$\mathcal{F} : y^2 = x^3 + ax + b,\ a \in [-N^2, N^2],\ b \in [-N^3, N^3], \tag{1.6}$$

and one-parameter families

$$\begin{aligned} \mathcal{F} : y^2 + a_1(t)xy + a_3(t)y &= x^3 + a_2(t)x^2 + a_4(t)x + a_6(t) \\ & \quad a_i(t) \in \mathbb{Z}[t],\ t \in [N, 2N]. \end{aligned} \tag{1.7}$$

Let $f(x)$ be an even Schwartz function whose Fourier Transform is supported in a neighborhood of the origin. We assume f is of the form $\prod_{i=1}^n f_i(x_i)$, although at the expense of more complicated notation we may drop this assumption.

We define the n-level density by

$$D_{n,\mathcal{F}}(f) = \frac{1}{|\mathcal{F}|} \sum_{E \in \mathcal{F}} \sum_{\substack{j_1, \dots, j_n \\ j_i \neq \pm j_k}} f_1\Big(\frac{\log N_E}{2\pi}\gamma_E^{(j_1)}\Big) \cdots f_n\Big(\frac{\log N_E}{2\pi}\gamma_E^{(j_n)}\Big), \tag{1.8}$$

where $\gamma_E^{(j_i)}$ runs through the non-trivial zeros of the curve E, and N_E is its conductor. We rescale the zeros by $\log N_E$ as this is the order of the number of zeros with imaginary part less than a large absolute constant. See [ILS].

We use the Explicit Formula (Theorem A.29) to relate sums of test functions over zeros to sums over primes of $a_E(p)$ and $a_E^2(p)$.

$$\begin{aligned} \sum_{\gamma_E^{(j)}} G\Big(\frac{\log N_E}{2\pi}\gamma_E^{(j)}\Big) &= \widehat{G}(0) + G(0) - 2\sum_p \frac{\log p}{\log N_E}\frac{1}{p}\widehat{G}\Big(\frac{\log p}{\log N_E}\Big)a_E(p) \\ & \quad -2\sum_p \frac{\log p}{\log N_E}\frac{1}{p^2}\widehat{G}\Big(\frac{2\log p}{\log N_E}\Big)a_E^2(p) + O(\frac{\log\log N_E}{\log N_E}). \end{aligned} \tag{1.9}$$

Simple combinatorics removes the $j_i = \pm j_k$ terms, and we obtain $D_{n,\mathcal{F}}(f)$. For $\widehat{F}$ of small support, for many families and $n \leq 2$, we show as $|\mathcal{F}| \to \infty$,

$$D_{n,\mathcal{F}}(f) \to \int \cdots \int f_1(x_1) \cdots f_n(x_n) W_{n,\mathcal{G}}(x_1, \cdots, x_n) dx_1 \cdots dx_n, \tag{1.10}$$

where $\mathcal{G} = \mathcal{G}(\mathcal{F})$ is the symmetry group associated to the family. For families of elliptic curves, geometric considerations ([KS1], [KS2]) lead one to expect orthogonal symmetries.

Which of the three orthogonal groups arises is controlled by the distribution of signs of the functional equation: we expect $\mathcal{G}$ to be SO(even) if every curve is even, SO(odd) if every curve is odd, and O if we have equidistribution in sign.

Katz and Sarnak [KS1] determined the $N \to \infty$ limits:

$\mathcal{G}$	$W_{n,\mathcal{G}}$
U(N), $\text{U}_k(N)$	$\det\Big(K_0(x_j,x_k)\Big)_{1\le j,k\le n}$
USp(N)	$\det\Big(K_{-1}(x_j,x_k)\Big)_{1\le j,k\le n}$
SO(even)	$\det\Big(K_1(x_j,x_k)\Big)_{1\le j,k\le n}$
SO(odd)	$\det\Big(K_{-1}(x_j,x_k)\Big)_{1\le j,k\le n} + \sum_{\nu=1}^{n}\delta(x_\nu)\det\Big(K_{-1}(x_j,x_k)\Big)_{1\le j,k\ne\nu\le n}$

where

$$K_\epsilon(x,y) = \frac{\sin\Big(\pi(x-y)\Big)}{\pi(x-y)} + \epsilon\frac{\sin\Big(\pi(x+y)\Big)}{\pi(x+y)}. \tag{1.11}$$

1.4 Expression for $D_{1,\mathcal{F}}(f)$

Using the Explicit Formula to relate sums of a function f against zeros of an L-function to sums of its Fourier Transform against primes, we evaluate not $\int f(x)W_{n,\mathcal{G}}(x)dx$ but $\int \widehat{f}(u)\widehat{W_{n,\mathcal{G}}}(u)du$. Denoting SO(even) (SO(odd)) by O^+ (O^-), the Fourier Transforms for the 1-level densities are

$$\begin{aligned}
\widehat{W_{1,\text{O}^+}}(u) &= \delta_0(u) + \frac{1}{2}\eta(u) \\
\widehat{W_{1,O}}(u) &= \delta_0(u) + \frac{1}{2} \\
\widehat{W_{1,\text{O}^-}}(u) &= \delta_0(u) - \frac{1}{2}\eta(u) + 1 \\
\widehat{W_{1,Sp}}(u) &= \delta_0(u) - \frac{1}{2}\eta(u) \\
\widehat{W_{1,U}}(u) &= \delta_0(u).
\end{aligned} \tag{1.12}$$

where $\eta(u)$ is 1, $\frac{1}{2}$, and 0 for $|u|$ less than 1, 1, and greater than 1, and δ_0 is the standard Dirac Delta functional. Note that the first three densities agree for $|u| < 1$ and split (ie, become distinguishable) for $|y| \geq 1$, but are all distinguishable from U for any support. Hence, unlike the n-level correlations over all zeros, the 1-level density is already sufficient to observe non-GUE and non-symplectic behavior.

It is difficult to evaluate the relevant sums over zeros (which become sums over primes by the Explicit Formula) for test functions with large support. Brumer and Heath-Brown ([Br], [BHB5]) have done the family of all elliptic curves with support less than $\frac{2}{3}$; twists of a given curve have been done for support less than 1. Implicit in the work of Silverman [Si3] is an analysis of the 1-level density for many one-parameter families of elliptic curves, but with very small support.

Unfortunately, none of these are sufficient to determine which is the underlying symmetry group. Further, previous investigations have rescaled each curve's zeros by the average of the logarithms of the conductors. This simplifies the calculations; however, the normalization is no longer natural for each curve. In this thesis we perform both calculations (normalizing each curve's zeros by the correct local quantity $\log N_E$, and by the average log-conductor $\log M = \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} \log N_E$).

1.5 Expression for $D_{2,\mathcal{F}}(f)$

Theorem 1.1 (2-Level Densities for the Classical Compact Groups) *Let $c(\mathcal{G}) = 0$, $\frac{1}{2}$ or 1 for $\mathcal{G} = \mathrm{SO(even)}$, O, and $\mathrm{SO(odd)}$. For $\mathcal{G}$ one of these three groups we have*

$$\begin{aligned}\int\int \widehat{f_1}(u_1)\widehat{f_2}(u_2)\widehat{W_{2,\mathcal{G}}}(u)du_1du_2 \quad &= \quad \Big[\widehat{f_1}(0)+\frac{1}{2}f_1(0)\Big]\Big[\widehat{f_2}(0)+\frac{1}{2}f_2(0)\Big]2\int |u|\widehat{f_1}(u)\widehat{f_2}(u)du \\ &\quad - 2\widehat{f_1f_2}(0) - f_1(0)f_2(0) + \ c(\mathcal{G})f_1(0)f_2(0).\end{aligned}$$

For $\mathcal{G} = U$ we have

$$\int\int \widehat{f_1}(u_1)\widehat{f_2}(u_2)\widehat{W_{2,U}}(u)du_1du_2 \quad = \quad \widehat{f_1}(0)\widehat{f_2}(0) + \int |u|\widehat{f_1}(u)\widehat{f_2}(u)du - \widehat{f_1f_2}(0),$$

and for $\mathcal{G} = Sp$, we have

$$\begin{aligned}\int\int \widehat{f_1}(u_1)\widehat{f_2}(u_2)\widehat{W_{2,\mathcal{G}}}(u)du_1du_2 \quad &= \quad \Big[\widehat{f_1}(0)+\frac{1}{2}f_1(0)\Big]\Big[\widehat{f_2}(0)+\frac{1}{2}f_2(0)\Big] \\ &\quad + 2\int |u|\widehat{f_1}(u)\widehat{f_2}(u)du - 2\widehat{f_1f_2}(0) - f_1(0)f_2(0) \\ &\quad - f_1(0)\widehat{f_2}(0) - \widehat{f_1}(0)f_2(0) + 2f_1(0)f_2(0).\end{aligned}$$

These densities are all distinguishable for functions with arbitrarily small support.

Assume the family has rank r over $\mathbb{Q}(t)$. By the Birch and Swinnerton-Dyer conjecture, Silverman's Specialization Theorem [Si2] implies $\exists t_0$ such that $\forall t \geq t_0$, the rank of E_t is at least r. We call these the *family zeros.*

As, in the limit, each curve's L-function has r zeros at the critical point, we isolate the contribution of these zeros from the 2-level density. After performing the necessary combinatorics, we are left with two pieces: the contribution from the family zeros, and the contribution from the remaining zeros.

The contribution to the 2-level density from the r family zeros is

$$r\widehat{f_1}(0)f_2(0) + rf_1(0)\widehat{f_2}(0) + (r^2 - r)f_1(0)f_2(0). \tag{1.13}$$

Let $D^{(r)}_{n,\mathcal{F}}(f)$ be the n-level density for the non-family zeros; ie, what is left after removing the trivial contributions from the r family zeros.

The utility of the 2-level density is that, even for functions with arbitrarily small support, the three likely candidate orthogonal symmetries *are* distinguishable, and in a very satisfying way. The three candidates differ by a factor which encodes the distribution of sign in the family, and all differ from the GUE's 2-level density.

While the 1-level density is sufficient to distinguish the various symmetry groups, it can only do so for large support (support at least 1). For some families, this is not a problem (see [ILS]); however, for elliptic curves, the polynomial growth of the conductor in a family makes even moderate support unreachable at present. This is why we concentrate on 2 and higher level densities.

1.6 Results

To calculate the 1-level density, we do not need to know any information about the sign of the functional equations. For the 2-level density, all we need is the percent of curves with even and odd functional equation. For the higher level densities, we need more than the percentage of odd / even; we need to know which curves are odd and which are even. For the family of all elliptic curves, or any family where we expect equidistribution in sign, this becomes a daunting challenge; however, the 2-level density *is* sufficient to distinguish the three groups.

Following Iwaniec-Luo-Sarnak [ILS] and Rubinstein [Ru], we calculated the 1- and 2-level densities for families of elliptic curves. The main result is Theorem 7.9.

We first fix notation. Let $D(t)$ be the product of the irreducible polynomial factors of $\Delta(t)$. Let $C(t)$ be the conductor of the curve E_t. Let B be the largest square which divides $D(t)$ for all t. Pass to a subsequence $ct + t_0$, and call $t \in [N, 2N]$ good if $D(ct + t_0)$ is square-free, except for primes $p|B$, where the power of such $p|D(t)$ is independent of t.

Then

Rational Surfaces Density Theorem: *Consider a one-parameter family of elliptic curves of rank r over $\mathbb{Q}(t)$ that is a rational surface. Assume GRH, $j(t)$ non-constant, and the ABC or Square-Free Sieve conjecture if $\Delta(t)$ has an irreducible polynomial factor of degree at least 4.*

Possibly after passing to a subsequence, for t good, $C(t)$ is a polynomial of degree m. Let f_i be an even Schwartz function of small but non-zero support σ_i ($\sigma_1 < \min(\frac{1}{2}, \frac{2}{3m})$ for the 1-level density, $\sigma_1 + \sigma_2 < \frac{1}{3m}$ for the 2-level density). Assume the Birch and Swinnerton-Dyer conjecture for interpretation purposes. The densities of the non-family zeros are

$$\begin{aligned}
D_{1,\mathcal{F}}^{(r)}(f_1) &= \widehat{f_1}(0) + \frac{1}{2}f_1(0) \\
D_{2,\mathcal{F}}^{(r)}(f) &= \prod_{i=1}^{2}\left[\widehat{f_i}(0) + \frac{1}{2}f_i(0)\right] + 2\int_{-\infty}^{\infty}|u|\widehat{f_1}(u)\widehat{f_2}(u)du \\
&\quad -2\widehat{f_1f_2}(0) - f_1(0)f_2(0) + (f_1f_2)(0)N(\mathcal{F},-1), \qquad (1.14)
\end{aligned}$$

where $N(\mathcal{F},-1)$ is the percent of curves with odd sign. The 1-level density of the non-family zeros, for small support, agrees with SO(even)*, O, and* SO(odd)*. The 2-level density of the non-family zeros, for small support, agrees with* SO(even)*, O, and* SO(odd) *depending on whether the signs are all even, equidistributed in the limit, or all odd. Thus, as our families have orthogonal symmetries, the densities of the non-family zeros agree with Katz and Sarnak's predictions, at least for small support.*

We study several families of constant sign, and show the density is as expected. Thus, for these constant sign families, the 2-level density reflects the predicted symmetry, which is invisible through the 1-level density because of support considerations.

Similar to the universality Rudnick and Sarnak [RS] found in studying n-level correlations of L-functions, our universality follows from the sums of $a_t^2(p)$ in our families (the second moments). For non-constant $j(t)$, this follows from a Sato-Tate law proved by Michel [Mi] (Theorem 2.4); however, for many of our families we show this by direct calculation. While Michel's result is sufficient to prove the observed universality (modulo the distribution of signs), his evaluation of the second moment for the family has a large error term, which is not surprising as his result holds for all families. For many families, we are able to explicitly determine the lower order corrections to the second moment. While these terms (in the limit) do not contribute to the n-level density, for many families considered there is a positive contribution of size $\frac{1}{\log N}$ to the densities.

1.7 Outline of the Proof of the Rational Surfaces Density Theorem

Using standard methods as well as a new construction, we construct families of elliptic curves of rank r over $\mathbb{Q}(t)$. For a prime p and a curve $E_t \in \mathcal{E}$, let

$$\begin{aligned} a_t(p) &= \sum_{x=0}^{p-1} \left(\frac{f_{E_t}(x)}{p} \right) = O(\sqrt{p}) \\ A_{\mathcal{E}}(p) &= \frac{1}{p} \sum_{t=0}^{p-1} a_{E_t}(p) = O(1). \end{aligned} \tag{1.15}$$

The first statement is just Hasse's Theorem; the second follows from Deligne [De]. Rosen and Silverman [RSi] prove

Theorem 1.2 (Rosen-Silverman) *For an elliptic surface (a one-parameter family), assume Tate's conjecture. Then*

$$\lim_{X \to \infty} \frac{1}{X} \sum_{p \le X} -A_{\mathcal{E}}(p) \log p = \text{rank } \mathcal{E}(\mathbb{Q}(t)) \tag{1.16}$$

Most of our examples are rational surfaces, where Tate's conjecture is known. Let

$$A_{r,\mathcal{F}}(p) = \sum_{t(p)} a_t^r(p). \tag{1.17}$$

Note $A_{1,\mathcal{F}}(p) = pA_{\mathcal{E}}(p)$. Knowledge of $A_{1,\mathcal{F}}(p)$ and $A_{2,\mathcal{F}}(p)$ is all we need to determine $D_{2,\mathcal{F}}(f)$ for surfaces where Tate's conjecture is known (modulo, of course, GRH, the distribution of sign of the functional equations, and being able to get a good handle on how the conductors vary with t. The last is the difficult part of the proof).

For any one parameter family, if $p_1, \dots, p_n$ are distinct primes (Lemma 2.5),

$$\sum_{t(p_1 \cdots p_n)} a_{t_1}^{r_1}(p_1) \cdots a_{t_n}^{r_n}(p_n) = A_{r_1,\mathcal{F}}(p_1) \cdots A_{r_n,\mathcal{F}}(p_n). \tag{1.18}$$

We substitute the above into the Explicit Formula. There is no net contribution if any of the r_i's is greater than 2. If Tate's conjecture is true, we can interpret sums of $A_{1,\mathcal{F}}(p)$ in terms of the rank over $\mathbb{Q}(t)$. See Lemma B.9.

We are left with determining $A_{2,\mathcal{F}}(p)$, performing the necessary combinatorial arguments, handling the conductors, and determining the distribution of signs. By clever choice and delicate character sums, we can often evaluate $A_{2,\mathcal{F}}(p)$ directly without recourse to higher theorems, although Michel's result (Theorem 2.4) is often, though not always, applicable.

Equation 1.18 can be generalized to apply to the family of all elliptic curves; unfortunately, the method of proof used is specific to elliptic curves, and crucially uses the fact that $a_{t+mp}(p) = a_t(p)$.

To handle the conductors, we show that by passing to a subsequence, and then sieving an auxiliary polynomial to being square-free (see Theorem 4.3), the conductors are given by a monotone integer polynomial. As the construction works for any family with deg $\Delta(t) \leq 12$, modulo the distribution of signs, we are able to determine the 1- and 2-level densities for a sub-family of any rational one-parameter family.

The main difficulty in the proof is the t-dependence in the conductors. It required very delicate arguments to handle it. For comparison purposes, we give a simple proof of the corresponding results for the rescaled densities.

In their investigations of 1-level densities for weight k cuspidal newforms of level N, Iwaniec, Luo and Sarnak evaluate $\frac{1}{|\mathcal{F}|}\sum_{f\in\mathcal{F}} a_f(m)a_f(n)$ by application of the Petersson Formula; for us, Equation 1.18 is our best analogue (for small support) to the Petersson Formula.

1.8 Applications

To date, there are two main applications of investigating higher (n ¿ 1) level densities. First, it provides evidence that the underlying group symmetries really are SO(even), O and SO(odd), and which group depends only on the distribution of signs. For supports reachable by present methods, the 1-level density is unable to distinguish the three candidates; the 2-level density can, and does not necessitate knowing *which* curves in a family are odd; all that is needed is the percent. Of course, for most families it is only conjectured that there is equidistribution in sign. Nevertheless, there are a few special constant sign families which provide the first examples of a family of elliptic curves where we can definitively say which of the three candidates works; moreover, the expected candidate is the observed one.

Second, we obtain improved estimates of the percent of curves with high rank above the family rank. Unfortunately, the arguments are not useful for rank slightly above the family rank, and are therefore useless (unless we can greatly increase the support) in resolving the Excess Rank phenomenon observed by Fermigier [Fe2] and others. Consider a family of elliptic curves $\mathcal{E}$ of rank r over $\mathbb{Q}(t)$. By Silverman's Specialization Theorem [Si2], for t sufficiently large, the rank of E_t over $\mathbb{Q}$ is at least r. If we assume equidistribution of sign, we might expect half the curves to have rank r and half rank $r+1$. For many families (though all with constant $A_{\mathcal{E}}(p)$), Fermigier observed approximately 32% had rank r, 18% rank $r+2$, and 48% rank $r+1$, 2% rank $r+3$. The Excess Rank question is: will the 18% persist for large values of N?

Briefly, assume equidistribution of sign. Then $D_{1,\mathcal{F}}(f) = \widehat{f_1}(0) + \frac{1}{2}f_1(0) + rf_1(0)$. To estimate the percent with rank at least $r+R$, P_R, we get $Rf(0)P_R \leq \widehat{f_1}(0) + \frac{1}{2}f_1(0)$, $R > 1$. Note the family rank r has been cancelled from both sides.

By using the 2-level density, however, we get *squares* of the rank on the left hand side. (Sometimes it's better to use, not the 2-level density, but a close cousin where we don't require the sums to be over distinct zeros). Unfortunately, the support is smaller. Assume we can calculate the 1-level density for functions of support $< \sigma$. Let $f(x_1,x_2) = \prod_i f_i(x_i)$, $\text{supp}(f_i) = \sigma_i$. While we expect to be able to calculate $D_{2,\mathcal{F}}(f)$ for $\sigma_1 + \sigma_2 \leq \sigma$, our method of proof yields the weaker $\sigma_1 + \sigma_2 \leq \frac{\sigma}{2}$; however, once R is large, the 2-level density yields better results.

Additionally, some of the families have interesting potential lower order density terms. A detailed analysis of the correction to the second moment of the $a_t(p)$'s (and $a_E(p)$ for the family of all elliptic curves) sheds some light on the Excess Rank phenomenon.

The correction term to the second moment, as remarked before, results in a potential contribution to the 1-level density. We can only say potential as the error terms propagating through our proofs are of size $\frac{1}{\log N}$ and $\frac{\log\log N}{\log N}$! A significantly more delicate analysis is needed; however, assuming reasonable cancellation, these corrections do indicate the possibility of lower order terms in the densities.

In estimating the number of curves of a given rank, this leads to slightly higher theoretical bounds for small N, though of course, in the limit, the bounds converge to what we get by ignoring the corrections. The existence of these lower order corrections opens up the exciting possibility of detecting fine structure distinguishing families of elliptic curves which, at first glance, seem to have the same underlying group symmetry.

1.9 Notation

We follow standard notation. All elliptic curves are over $\mathbb{Q}$. We consider one-parameter families $E_t : y^2 + a_1(t)xy + a_3(t)y = x^3 + a_2(t)x + a_4(t) + a_6(t)$, $a_i(t)$ an integer polynomial.

By ([TW], [Wi] and [BCDT]), all elliptic curves are modular. Hence we may freely use $L(s, E)$ and its functional equation.

Definition 1.3 (n-Level Density) *$D_{n,\mathcal{F}}(f)$ is the n-level density of the family $\mathcal{F}$ with test function $f(x) = \prod_i f_i(x)$. Each curve's zeros are rescaled by the logarithm of its conductor. In the explicit formula we sum over all n-tuples $(j_1, \dots, j_n)$ with $j_i \neq \pm j_k$.*

A related quantity often encountered is

Definition 1.4 *$D^*_{n,\mathcal{F}}(f)$ is the n-level density without the combinatorics; ie, the sums are over all n-tuples of zeros.*

Rescaling each curves' zeros by the logarithm of its conductor gives the correct local scaling; it is, however, significantly harder to handle these sums. We often study a related quantity:

Definition 1.5 (Modified n-Level Density) *$D'_{n,\mathcal{F}}(f)$ differs from the n-level density by rescaling each curve's zeros by the average log-conductor, $\log M = \frac{1}{|\mathcal{F}|} \sum_{E \in \mathcal{F}} \log N_E$, instead of by $\log N_E$.*

Finally (under certain assumptions), our families often have r family zeros at the critical point. Removing the contributions from these zeros yields

Definition 1.6 *$D^{(r)}_{n,\mathcal{F}}(f)$ is the n-level density with the contribution from r critical point zeros removed.*

1.10 Assumptions

We assume the following at various points in the thesis:

Generalized Riemann Hypothesis (for Elliptic Curves) *Let $L(s, E)$ be the (normalized) L-function of the elliptic curve E. Then the non-trivial zeros of $L(s, E)$ satisfy $\text{Re}(s) = \frac{1}{2}$.*

Occasionally we assume the Riemann Hypothesis for the Riemann Zeta-function and Dirichlet L-functions.

Birch and Swinnerton-Dyer Conjecture [BSD1], [BSD2] *Let E be an elliptic curve of geometric rank r over $\mathbb{Q}$ (the Mordell-Weil group is $\mathbb{Z}^r \oplus T$, T is the subset of torsion points).*

Then the analytic rank (the order of vanishing of the L-function at the critical point) is also r.

We assume the above only for interpretation purposes.

Tate's Conjecture for Elliptic Surfaces [Ta] *Let $\mathcal{E}/\mathbb{Q}$ be an elliptic surface and $L_2(\mathcal{E}, s)$ be the L-series attached to $H^2_{\acute{e}t}(\mathcal{E}/\overline{\mathbb{Q}}, \mathbb{Q}_l)$. Then $L_2(\mathcal{E}, s)$ has a meromorphic continuation to $\boldsymbol{C}$ and satisfies $-\mathrm{ord}_{s=2}L_2(\mathcal{E}, s) = \mathrm{rank}\ NS(\mathcal{E}/\mathbb{Q})$, where $NS(\mathcal{E}/\mathbb{Q})$ is the $\mathbb{Q}$-rational part of the Néron-Severi group of $\mathcal{E}$. Further, $L_2(\mathcal{E}, s)$ does not vanish on the line $Re(s) = 2$.*

Most of the one-parameter families we investigate are rational surfaces, where Tate's conjecture is known. See, for example, [RSi].

ABC Conjecture *Fix $\epsilon > 0$. For coprime positive integers a, b and c with $c = a + b$ and $N(a, b, c) = \prod_{p|abc} p$, $c \ll_\epsilon N(a, b, c)^{1+\epsilon}$.*

The full strength of ABC is never needed in the arguments below; rather, we need a consequence of ABC, the Square-Free Sieve (see [Gr]):

Square-Free Sieve Conjecture *Fix an irreducible polynomial $f(t)$ of degree at least 4. As $N \to \infty$, the number of $t \in [N, 2N]$ with $D(t)$ divisible by p^2 for some $p > \log N$ is $o(N)$.*

For irreducible polynomials of degree at most 3, the above is known, complete with a better error than $o(N)$. See [Ho], chapter 4.

We use the Square-Free Sieve for the following: let $D(t)$ be the product of the irreducible polynomial factors of $\Delta(t)$. If no square divides $D(t)$ for all t, for $D(t)$ square-free we can often compute the conductors $C(t)$ exactly, obtaining $C(t)$ is an integral polynomial. By inclusion / exclusion, we can handle the sieving by factors $d < \log N$; we need the Square-Free Sieve to bound the number of $t \in [N, 2N]$ with $D(t)$ divisibly by p^2 for some $p > \log N$. (If $\forall t$, a square B divides $D(t)$, instead of sieving to $D(t)$ square-free we sieve to $D(t)$ square-free save for primes $p|B$, where the power of $p|D(t)$ is independent of t). We call such t (or $D(t)$) good.

The Sign Conjecture for Elliptic Curves states, in the limit, half of all curves have even functional equation and half have odd. Of course, this may depend on the method of parametrization. We often only need a restricted version, namely

Restricted Sign Conjecture (for the Family $\mathcal{F}$) *Consider a 1-parameter family $\mathcal{F}$ of elliptic curves. As $N \to \infty$, the signs of the curves E_t are equidistributed for $t \in [N, 2N]$.*

The Restriced Sign conjecture sometimes fails. First, there are families with constant $j(t)$ where all curves have the same sign. Additionally, Rizzo [Ri] shows that for the family

$$E_t : y^2 = x^3 + tx^2 - (t+3)x + 1, \quad j(t) = 256(t^2 + 3t + 9), \tag{1.19}$$

for every $t \in \mathbb{Z}$, E_t has odd functional equation. This example is due to Washington [Wa]. Further, Rizzo proves for the family

$$E_t : y^2 = x^3 + \frac{t}{4}x^2 - \frac{36t^2}{t-1728}x - \frac{t^3}{t-1728}, \quad j(t) = t, \tag{1.20}$$

as t ranges over $\mathbb{Z}$, in the limit 50.1859% have even functional equation and 49.8141% have odd functional equation.

Failure of the Restricted Sign conjecture by all curves in a family having the same sign is easily manageable; in fact, it is only in such cases that we are able to explicitly determine all n-level densities. Failure such as Rizzo's second example, with a split other than $100\% - 0\%$ or $50\% - 50\%$, leads to a non-equal mixing of SO(even) and SO(odd).

Helfgott [Hel] has recently related the Restricted Sign conjecture to the Square-Free Sieve conjecture and standard conjectures on sums of Moebius:

Polynomial Moebius *Let $f(t)$ be an irreducible polynomial such that no fixed square divides $f(t)$ for all t. Then $\sum_{t=N}^{2N} \mu(f(t)) = o(N)$.*

The Polynomial Moebius conjecture is known for linear $f(t)$.

Helfgott shows the Square-Free Sieve and Polynomial Moebius imply the Restricted Sign conjecture for many families. More precisely, let $M(t)$ be the product of the irreducible polynomials dividing $\Delta(t)$ and not $c_4(t)$.

Theorem 1.7 (Equidistribution of Sign in a Family) *Let $\mathcal{F}$ be a one-parameter family with coefficients integer polynomials in $t \in [N, 2N]$. If $j(t)$ and $M(t)$ are non-constant, then the signs of E_t, $t \in [N, 2N]$, are equidistributed as $N \to \infty$. Further, if we restrict to good t, $t \in [N, 2N]$*

such that $D(t)$ is good (usually square-free), the signs are still equidistributed in the limit.

In Appendix F we numerically investigate the conjectured equidistribution of sign for a representative family with $j(t)$ and $M(t)$ non-constant. It is a pleasure to thank Atul Pokharel for providing the graphs.

1.11 Organization of the Thesis

We first enumerate several useful results for calculating the 1- and 2-level densities. We calculate these densities for the classical compact groups, and a useful expansion for the densities for families of elliptic curves. We prove our result on sub-families of rational one-parameter elliptic surfaces.

Next, we calculate the densities for several families of elliptic curves of constant sign, followed by many examples with conjectured equidistribution of signs.

We then use the 2-level density to obtain improved bounds on the percent of elliptic curves with high rank above the rank of the family over $\mathbb{Q}(t)$.

We show for many families of elliptic curves there is a strong possibility that there is a lower order correction term to the densities. As the term is of size $\frac{1}{\log N}$, to show it really is present requires a significantly more detailed analysis of all previous error terms, which are $O(\frac{\log\log N}{\log N})$.

Finally, we sketch the complications that arise in studying the 3- and higher level densities in non-constant sign families, and provide numerous appendices for calculations used in the thesis.

2 Summation Preliminaries

2.1 Partial Summation

Lemma 2.1 (Partial Summation: Discrete Version)

$$\sum_{M}^{N} a_n b_n = A_N b_N - A_{M-1} b_M + \sum_{M}^{N-1} A_n (b_n - b_{n+1}) \tag{2.1}$$

Lemma 2.2 (Abel's Summation Formula - Integral Version) *Let $h(x)$ be a continuously differentiable function. Let $A(x) = \sum_{n \leq x} a_n$. Then*

$$\sum_{n \leq x} a_n h(n) = A(x)h(x) - \int_1^x A(u) h'(u) du \tag{2.2}$$

See, for example, [Rud], page 70.

2.2 Useful Expansion of $a_E(p)$

We have the following expansion of $\left(\frac{x}{p}\right)$:

$$\left(\frac{x}{p}\right) = G_p^{-1} \sum_{c=1}^{p} \left(\frac{c}{p}\right) \mathbf{e}\left(\frac{cx}{p}\right), \tag{2.3}$$

where $G_p = \sum_{a(p)} \left(\frac{a}{p}\right) \mathbf{e}\left(\frac{a}{p}\right)$, which equals $\sqrt{p}$ for $p \equiv 1(4)$ and $i\sqrt{p}$ for $p \equiv 3(4)$. See, for example, [BEW].

For the curve $y^2 = f_E(x)$, $a_E(p) = -\sum_{x(p)} \left(\frac{f_E(x)}{p}\right)$. We expand the x-sum by using Gauss sums, namely

$$a_E(p) = G_p^{-1} \sum_{x(p)} \sum_{c=1}^{p} \left(\frac{c}{p}\right) \mathbf{e}\left(\frac{c f_E(x)}{p}\right). \tag{2.4}$$

2.3 First Order Sums: Rosen-Silverman Theorem

Consider a one-parameter family

$$\mathcal{E} : y^2 + a_1(t)xy + a_3(t)y = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t). \tag{2.5}$$

Let $a_t(p) = p + 1 - N_p$, where N_p is the number of solutions mod p (including ∞). Define

$$A_{\mathcal{E}}(p) = \frac{1}{p} \sum_{t(p)} a_t(p). \tag{2.6}$$

$A_{\mathcal{E}}(p)$ is bounded independent of p ([De]). Rosen and Silverman [RSi] have proved a conjecture of Nagao [Na3]:

Theorem 2.3 (Rosen-Silverman) *For an elliptic surface (a one-parameter family), assume Tate's conjecture. Then*

$$\lim_{X \to \infty} \frac{1}{X} \sum_{p \le X} -A_{\mathcal{E}}(p) \log p = \text{rank } \mathcal{E}(\mathbb{Q}(t)) \tag{2.7}$$

Tate's conjecture is known for rational surfaces (see [RSi]). An elliptic surface $y^2 = x^3 + A(t)x + B(t)$ is rational iff one of the following is true: (1) $0 < \max\{3\text{deg}A, 2\text{deg}B\} < 12$; (2) $3\text{deg}A = 2\text{deg}B = 12$ and $\text{ord}_{t=0} t^{12}\Delta(t^{-1}) = 0$. See [RSi], pages $46 - 47$ for more details.

2.4 Second Order Sums: Michel's Theorem

Theorem 2.4 (Michel [Mi]) *Consider a one-parameter family with non-constant $j(t)$. Then*

$$\sum_{t(p)} a_t^2(p) = p^2 + O(p^{\frac{3}{2}}). \tag{2.8}$$

We calculate the error term for many families, as this information will be useful in observing potential lower order correction terms to the densities, as well as obtaining better support for the densities. We often show the sum is $p^2 - m_{\mathcal{F}} p + O(1)$, $m_{\mathcal{F}} > 0$.

2.5 Sums of $a_t^{r_1}(p_1) \cdots a_t^{r_n}(p_n)$

Define

$$A_{r,\mathcal{F}}(p) = \sum_{t(p)} a_t^r(p). \tag{2.9}$$

Lemma 2.5 *Let $p_1, \dots, p_n$ be distinct primes and $r_i \geq 1$. Then*

$$\sum_{t(p_1 \cdots p_n)} \prod_{i=1}^{n} a_t^{r_i}(p_i) \quad = \quad \prod_{i=1}^{n} A_{r_i,\mathcal{F}}(p_i). \tag{2.10}$$

Proof: We proceed by induction; $n = 1$ is clear. Let $P = \prod_{i=1}^{n-1} p_i$, $I = \{0, 1, \dots, Pp_n - 1\}$, $I_n = \{0, 1, \dots, p_n - 1\}$, and $J_{n-1} = \{0, 1, \dots, P - 1\}$. We claim

$$\begin{aligned} I \quad &= \quad \bigsqcup_{t_n \in I_n} \Big(t_n + p_n J_{n-1} \Big) \\ & \quad\quad t_n + p_n J_{n-1} = \{t_n, t_n + p_n, \dots, t_n + p_n(P-1)\}. \end{aligned} \tag{2.11}$$

The union is clearly of disjoint sets. Assume $t_n + ap_n = t_n' + a'p_n$. Then $t_n - t_n' \equiv 0(p_n)$. This forces $t_n = t_n'$, which forces $a = a'$. As there are $p_n \cdot P$ elements, we have all of I.

Thus t running through I is the same as $t_n + p_n t'$, $t_n \in I_n$ and $t' \in J_{n-1}$. We chose this decomposition because

$$\forall m: \quad a_{t_n + mp_n}^{r_n}(p_n) \quad = \quad a_{t_n}^{r_n}(p_n). \tag{2.12}$$

Therefore

$$\begin{aligned} \sum_{t(Pp_n)} \prod_{i=1}^{n} a_t^{r_i}(p_i) \quad &= \quad \sum_{t_n \in I_n} \sum_{t' \in J_{n-1}} \prod_{i=1}^{n} a_{t_n + p_n t'}^{r_i}(p_i) \\ &= \quad \sum_{t_n \in I_n} \sum_{t' \in J_{n-1}} a_{t_n + p_n t'}^{r_n}(p_n) \prod_{i=1}^{n-1} a_{t_n + p_n t'}^{r_i}(p_i) \\ &= \quad \sum_{t_n \in I_n} \sum_{t' \in J_{n-1}} a_{t_n}^{r_n}(p_n) \prod_{i=1}^{n-1} a_{t_n + p_n t'}^{r_i}(p_i) \\ &= \quad \sum_{t_n \in I_n} a_{t_n}^{r_n}(p_n) \sum_{t' \in J_{n-1}} \prod_{i=1}^{n-1} a_{t_n + p_n t'}^{r_i}(p_i). \end{aligned} \tag{2.13}$$

As the primes are distinct, for any t_n, as t' runs through J_{n-1}, $t_n + p_n t'$ mod P also runs through all values of J_{n-1} once. Proof: assume two different t' yield the same value mod P. As p_n is invertible mod P (*this is where we use the primes are distinct*), this forces the two choices of t' to be the same. Thus

$$\sum_{t(Pp_n)} \prod_{i=1}^{n} a_t^{r_i}(p_i) \quad = \quad \sum_{t_n \in I_n} a_{t_n}^{r_n}(p_n) \sum_{t' \in J_{n-1}} \prod_{i=1}^{n-1} a_{t'}^{r_i}(p_i)$$

$$\begin{aligned} &= \sum_{t_n \in I_n} a_{t_n}^{r_n}(p_n) \prod_{i=1}^{n-1} A_{r_i,\mathcal{F}}(p_i) \\ &= A_{r_n,\mathcal{F}}(p_n) \prod_{i=1}^{n-1} A_{r_i,\mathcal{F}}(p_i) \end{aligned} \tag{2.14}$$

By induction, we are done. Note this theorem crucially depends on Equation 2.12. As we can write the coefficients of our modular forms as character sums over t, caring only about the values mod p, we have $a_{t+mp}(p) = a_t(p)$. Lemma 2.5 is our best analogue to the Petersson formula, which is used in [ILS] to obtain large support for the density functions.

2.6 Sums of $a_{a,b}^{r_1}(p_1) \cdots a_{a,b}^{r_n}(p_n)$

Consider the family of all elliptic curves: $y^2 = x^3 + ax + b$. We calculate the sums we will need in investigating the modified n-level densities. Define

$$A_{r,\mathcal{F}}(p) = \sum_{a(p)} \sum_{b(p)} a_{a,b}^r(p). \tag{2.15}$$

Lemma 2.6 *Let $p_1, \dots, p_n$ be distinct primes and $r_i \geq 1$. Then*

$$\sum_{a,b(p_1 \cdots p_n)} \prod_{i=1}^{n} a_{a,b}^{r_i}(p_i) \quad = \quad \prod_{i=1}^{n} A_{r_i,\mathcal{F}}(p_i). \tag{2.16}$$

Proof: We proceed by induction; $n = 1$ is clear. Let $P = \prod_{i=1}^{n-1} p_i$, $I = \{0, 1, \dots, Pp_n - 1\}$, $I_n = \{0, 1, \dots, p_n - 1\}$, and $J_{n-1} = \{0, 1, \dots, P - 1\}$.

As in the proof of Lemma 2.5, we have

$$\begin{aligned} I \quad &= \quad \bigsqcup_{b_n \in I_n} \Big(b_n + p_n J_{n-1}\Big) \\ & \qquad b_n + p_n J_{n-1} = \{b_n, b_n + p_n, \dots, b_n + p_n(P-1)\}, \end{aligned} \tag{2.17}$$

Thus b running through I is the same as $b_n + p_n b'$, $b_n \in I_n$ and $b' \in J_{n-1}$, and similarly for a and a_n. We chose this decomposition because

$$\forall l, m: \quad a_{a_n + lp_n, b_n + mp_n}^{r_n}(p_n) \quad = \quad a_{a_n,b_n}^{r_n}(p_n). \tag{2.18}$$

Therefore

$$\begin{aligned}
\sum_{a,b(Pp_n)} \prod_{i=1}^{n} a_{a,b}^{r_i}(p_i) &= \sum_{a_n,b_n \in I_n} \sum_{a',b' \in J_{n-1}} \prod_{i=1}^{n} a_{a_n+p_n a', b_n+p_n b'}^{r_i}(p_i) \\
&= \sum_{a_n,b_n \in I_n} \sum_{a',b' \in J_{n-1}} a_{a_n+p_n a', b_n+p_n b'}^{r_n}(p_n) \prod_{i=1}^{n-1} a_{a_n+p_n a', b_n+p_n b'}^{r_n}(p_i) \\
&= \sum_{a_n,b_n \in I_n} \sum_{a',b' \in J_{n-1}} a_{a_n,b_n}^{r_n}(p_n) \prod_{i=1}^{n-1} a_{a_n+p_n a', b_n+p_n b'}^{r_n}(p_i) \\
&= \sum_{a_n,b_n \in I_n} a_{a_n,b_n}^{r_n}(p_n) \sum_{a',b' \in J_{n-1}} \prod_{i=1}^{n-1} a_{a_n+p_n a', b_n+p_n b'}^{r_n}(p_i). \qquad (2.19)
\end{aligned}$$

As the primes are distinct, for any b_n, as b' runs through J_{n-1}, $b_n + p_n b'$ mod P also runs through all values of J_{n-1} once, and similarly for a_n and a'. Thus

$$\begin{aligned}
S &= \sum_{a_n,b_n \in I_n} a_{t_n}^{r_n}(p_n) \sum_{a',b' \in J_{n-1}} \prod_{i=1}^{n-1} a_{a',b'}^{r_i}(p_i) \\
&= \sum_{a_n,b_n \in I_n} a_{t_n}^{r_n}(p_n) \prod_{i=1}^{n-1} A_{r_i,\mathcal{F}}(p_i) \\
&= A_{r_n,\mathcal{F}}(p_n) \prod_{i=1}^{n-1} A_{r_i,\mathcal{F}}(p_i) \qquad (2.20)
\end{aligned}$$

Note this theorem crucially depends on Equation 2.18. As we can write the coefficients of our modular forms as character sums over a and b, caring only about the values mod p, we have $a_{a+lp,b+mp}(p) = a_{a,b}(p)$. □

This is *the* essential theorem for simplifying the calculations needed for the density investigations.

3 Sieving Families of Elliptic Curves

3.1 Introduction

Given a one-parameter family of elliptic curves E_t, we need to control the conductors $C(t)$ to determine the 1- and 2-level densities. Let the curves have discriminants $\Delta(t)$, and let $D(t)$ be the product of the irreducible polynomial factors of $\Delta(t)$.

$D(t)$ may always be divisible a fixed square: $\forall t$, $4|t(t+1)(t+2)(t+3)$. Let B be the largest square dividing $D(t)$ for all t. We prove in Theorem 4.3 that for a rational elliptic surface, by passing to a subsequence $\tau = c_1 t + c_0$, for $\frac{D(\tau)}{B}$ square-free, $C(t)$ is given by an integer polynomial in τ. Call such t (or $D(t)$) good.

Thus, we can determine the conductors by restricting to t good. In order to evaluate the sums of $\prod_i a_t^{r_i}(p_i)$, it is necessary to restrict t to arithmetic progressions; however, restricting to t good ($\frac{D(\tau)}{B}$ square-free) does not yield t in arithmetic progressions.

We overcome this difficulty by doing a partial sieve with good bounds on overcounting. For notational convenience, we consider the case where $B = 1$ below, and indicate how to modify for general B.

Let $S(t)$ be some quantity associated to our family which we desire to sum over $\mathcal{T}_1$, where

$$\begin{aligned} \mathcal{T}_1 &= \Big\{t \in [N, 2N] : \ D(t) \text{ is square-free}\Big\} \\ \mathcal{T}_2 &= \Big\{t \in [N, 2N] : \ d^2 \nmid D(t) \text{ for } 2 \le d \le \log^l N\Big\}. \end{aligned} \tag{3.1}$$

Clearly $\mathcal{T}_1 \subset \mathcal{T}_2$. We will show that $\mathcal{T}_2$ may be written as a union of arithmetic progressions, and $|\mathcal{T}_2 - \mathcal{T}_1| = o(N)$.

The main obstruction is estimating the number of $t \in [N, 2N]$ such that $D(t)$ is divisible by the square of a prime $p \ge \log^l N$. If $k = \deg D(t)$, we have

$$\begin{aligned} \sum_{\substack{D(t)\ square-free \\ t \in [N,2N]}} S(t) &= \sum_{d=1}^{N^{k/2}} \mu(d) \sum_{\substack{D(t)\equiv 0(d^2) \\ t\in[N,2N]}} S(t) \\ &= \sum_{d=1}^{\log^l N} \mu(d) \sum_{\substack{D(t)\equiv 0(d^2) \\ t\in[N,2N]}} S(t) + \sum_{d \ge \log^l N}^{N^{k/2}} \mu(d) \sum_{\substack{D(t)\equiv 0(d^2) \\ t\in[N,2N]}} S(t). \end{aligned} \tag{3.2}$$

For $k > 3$, the second piece is too difficult to estimate – there are too many d terms (d runs to $N^{k/2}$). If all the irreducible factors of $D(t)$ are of degree at most 3, the second piece is small. For factors of degree at most 2, this follows immediately, while for factors of degree 3 it follows from Hooley ([Ho]). For larger degrees, we need the ABC conjecture (or one of its consequences, the Square-Free Sieve conjecture).

3.2 Incongruent Solutions of Polynomials

We paraphrase several standard results about solutions of polynomial equations mod m. See, for example, [Nag].

Lemma 3.1 *Let $D(t)$ be a polynomial of degree k, and let p be a prime not dividing the coefficient of x^k. Then $D(t) \equiv 0$ mod p has at most k incongruent solutions.*

Lemma 3.2 *Let $D(t)$ be an integral polynomial and let $D(t) \equiv 0$ mod $p_i^{\alpha_i}$ have ν_i incongruent solutions. If the primes are distinct, there are $\prod_{i=1}^r \nu_i$ incongruent solutions of $D(t) \equiv 0$ mod $\prod_{i=1}^r p_i^{\alpha_i}$.*

Proof: Chinese Remainder Theorem. We use the above when each $\alpha_i = 2$.

Lemma 3.3 *Suppose the discriminant of a primitive integral polynomial $D(t)$ is not divisible by a prime p. Then the number of incongruent solutions of $D(t) \equiv 0$ mod p is the same as the number of incongruent solutions of $D(t) \equiv 0$ mod p^α.*

We use the above for $\alpha = 2$. Recall an integral polynomial is primitive if the greatest common divisor of its coefficients is 1.

Let $D(t)$ be a primitive, integral polynomial of degree k with discriminant δ: $D(t) = a_k t^k + \cdots + a_0$.

Definition 3.4 *Let $\nu(d)$ be the number of incongruent solutions of $D(t) \equiv 0$ mod d^2.*

Lemma 3.5 *For d square-free, $\nu(d) \ll d^\epsilon$.*

Let $d = \prod_{i=1}^r p_i$. By Lemma 3.1, for each $p_i \nmid a_k$, there are at most k incongruent solutions of $D(t) \equiv 0$ mod p_i. By Lemma 3.3, for each prime p_i with $(p_i, a_k\delta) = 1$, the number of incongruent solutions to $D(t) \equiv 0$ mod p_i^2 equals the number of incongruent solutions of $D(t) \equiv 0$ mod p_i. Hence, $\nu(p_i) \leq k$ if $p_i \nmid a_k\delta$. For $p_i | a_k\delta$, there are at most p_i^2 incongruent solutions to $D(t) \equiv 0$ mod p_i^2. By Lemma 3.2,

$$\nu(d) = \prod_{i=1}^r \nu(p_i). \tag{3.3}$$

Let $C = \prod_{p_i | a_k \delta} p_i^2$ and let $\tau(d)$ denote the number of divisors of d. For d the product of r distinct primes, $\tau(d) = 2^r$ or $r = \frac{\log \tau(d)}{\log 2}$. For square-free d,

$$\begin{aligned} \nu(d) &= \prod_{i=1}^{r} \nu(p_i) \le \prod_{\substack{i=1 \\ p_i | a_k \delta}}^{r} p_i^2 \cdot \prod_{\substack{i=1 \\ p_i \nmid a_k \delta}}^{r} k \\ &\le Ck^r \le Ck^{\frac{\log \tau(d)}{\log 2}} = C\Big(\tau(d)\Big)^{\frac{\log k}{\log 2}}. \end{aligned} \tag{3.4}$$

As $\tau(d) \ll d^\epsilon$ ([HW], Theorem 315, page 260), for square-free d, $\nu(d) \ll d^\epsilon$.

3.3 Common Prime Divisors of Polynomials

Lemma 3.6 *Let $f(t)$ and $g(t)$ be two integer polynomials with no non-constant factors over $\mathbb{Z}[t]$. Then $\exists c$ (independent of t) such that if p divides both $f(t)$ and $g(t)$, then $p|c$. In particular, $f(t)$ and $g(t)$ have no common large prime divisors.*

Proof: we proceed by induction. We may assume deg $f(t) \geq$ deg $g(t)$. If $f(t)$ or $g(t)$ is constant the claim is immediate. If $f(t) = f_1 t + f_0$ and $g(t) = g_1 t + g_0$, then $p|(f(t), g(t))$ implies $p|g_1 f(t) - f_1 g(t) = g_1 f_0 - f_1 g_0 = c$.

Assume deg $f \geq 2$. If $g(t)$ is constant, take $c = g(t)$. Thus we may assume deg $g \geq 1$. Clearly we may assume f and g have no common factors over $\mathbb{Z}$. Assume for some t, $p|(f(t), g(t))$.

By Euclid's Algorithm, $\exists a_1$, $B_1(t)$ such that $f_1(t) = a_1 f(t) - B_1(t) g(t)$ is of lower degree than both $f(t)$ and $g(t)$. If $f_1(t) = 0$, then $a_1 f(t) = B_1(t) g(t)$. As deg $g(t) \geq 1$, $f(t)$ and $g(t)$ have a common non-constant factor over $\mathbb{Z}[t]$, a contradiction. Thus $f_1(t) \neq 0$, and since $p|g(t)$ and $p|f(t)$, $p|f_1(t)$.

Assume $h(t) \in \mathbb{Z}[t]$ divides both $f_1(t)$ and $g(t)$. Then $h(t)|a_1 f(t) = f_1(t) + B_1(t) g(t)$. As $f(t)$ and $g(t)$ have no common non-constant factor over $\mathbb{Z}[t]$, $h(t)$ is constant. Therefore $f_1(t)$ and $g(t)$ satisfy the same conditions $f(t)$ and $g(t)$ satisfied, and deg $f_1(t) +$ deg $g(t) <$ deg $g(t) +$ deg $f(t)$.

If $f_1(t)$ is constant, we are done: take $c = f_1(t)$. If $f_1(t)$ is non-constant, we apply the above construction to the pair $g(t)$ and $f_1(t)$ and obtain $g_1(t)$. Continuing in this manner, eventually either $f_i(t)$ or $g_i(t)$ is constant; as the initial degrees are finite, the process terminates.

Thus, we find $\exists c$ such that if $\exists t$ such that $p|(f(t), g(t))$ then $p|c$. If the two polynomials had a common integral factor, we could incorporate its prime divisors into c. □

3.4 Estimating $\mathcal{T}_2$

$$\sum_{t\in\mathcal{T}_2} S(t) \quad = \quad \sum_{d=1}^{\log^l N} \mu(d) \sum_{\substack{D(t)\equiv 0(d^2)\\ t\in[N,2N]}} S(t). \tag{3.5}$$

There are $\frac{N}{d^2}\nu(d) + O(\nu(d))$ solutions to $D(t) \equiv 0 \bmod d^2$ for $t \in [N, 2N]$. By Lemma 3.5, $\nu(d) \ll d^\epsilon$ for square-free d. Taking $S(t) = 1$ yields

$$\begin{aligned}
|\mathcal{T}_2| &= \sum_{d=1}^{\log^l N} \mu(d) \sum_{\substack{D(t)\equiv 0(d^2)\\ t\in[N,2N]}} 1 \\
&= \sum_{d=1}^{\log^l N} \mu(d) \left[\frac{N}{d^2}\nu(d) + O(\nu(d))\right] \\
&= N \sum_{d=1}^{\log^l N} \frac{\mu(d)\nu(d)}{d^2} + O(\log^{l(1+\epsilon)} N).
\end{aligned} \tag{3.6}$$

As $\nu(d) \ll d^\epsilon$ for square-free d,

$$\begin{aligned}
\Big| \prod_{p<\log^l N} \Big(1 - \frac{\nu(p)}{p^2}\Big) - \sum_{d=1}^{\log^l N} \frac{\mu(d)\nu(d)}{d^2} \Big| &\ll \sum_{d=\log^l N}^{\infty} \frac{d^\epsilon}{d^2} \\
&\ll \frac{1}{\log^{l(1-\epsilon)} N}.
\end{aligned} \tag{3.7}$$

Therefore

$$\begin{aligned}
|\mathcal{T}_2| &= N \prod_{p<\log^l N} \Big(1 - \frac{\nu(p)}{p^2}\Big) + O\Big(\frac{N}{\log^{l(1-\epsilon)} N}\Big) + O(\log^{l(1-\epsilon)} N) \\
&= N \prod_{p<\log^l N} \Big(1 - \frac{\nu(p)}{p^2}\Big) + O\Big(\frac{N}{\log^{l(1-\epsilon)} N}\Big).
\end{aligned} \tag{3.8}$$

We may take the product over all primes with negligible cost as

$$1 - \prod_{p\geq\log^l N} \Big(1 - \frac{\nu(p)}{p^2}\Big) \ll \sum_{n\geq\log^l N} \frac{n^\epsilon}{n^2} \ll \frac{1}{\log^{l(1-\epsilon)} N}. \tag{3.9}$$

Thus

$$\prod_{p<\log^l N} \Big(1 - \frac{\nu(p)}{p^2}\Big) = \prod_p \Big(1 - \frac{\nu(p)}{p^2}\Big) + O\Big(\frac{1}{\log^{l(1-\epsilon)} N}\Big). \tag{3.10}$$

We have shown

Lemma 3.7 *Let $\mathcal{T}_2$ be the set of $t \in [N, 2N]$ such that $d^2 \nmid D(t)$ for $2 \leq d \leq \log^l N$.*

$$|\mathcal{T}_2| = N \prod_p \Big(1 - \frac{\nu(p)}{p^2}\Big) + O\Big(\frac{N}{\log^{l(1-\epsilon)} N}\Big). \tag{3.11}$$

3.5 Estimating $\mathcal{T}_1$

Assuming the ABC conjecture, Granville ([Gr], Theorem 1) proves the number of $t \in [N, 2N]$ such that $D(t)$ is square-free is

$$|\mathcal{T}_1| = N \prod_p \Big(1 - \frac{\nu(p)}{p^2}\Big) + o(N). \tag{3.12}$$

Note that if the degree of $D(t)$ is at most 3, the ABC conjecture is not needed (for example, see Hooley [Ho]). We do find the family has a positive percent of t giving $D(t)$ square-free (as we are assuming no square divides $D(t)$ for all t, no $\nu(p) = p^2$, hence the product can be bounded away from 0). Up to a lower order term, we get the right amount by looking at primes $\leq \log^l N$.

3.6 Evaluation of $|\mathcal{T}_2 - \mathcal{T}_1|$ and Applications

Recall $\mathcal{T}_1$ is the set of $t \in [N, 2N]$ with $D(t)$ square-free. Clearly, the set $\mathcal{T}_2$ of t with $D(t)$ not divisible by d^2 for $2 \leq d \leq \log^l N$ contains $\mathcal{T}_1$. Thus, we need to estimate $\mathcal{T}_2 - \mathcal{T}_1$. Recall

$$\begin{aligned} |\mathcal{T}_1| &= N \prod_{p \leq \log^l N} \Big(1 - \frac{\nu(p)}{p^2}\Big) + O\Big(\frac{N}{\log^l N}\Big) \\ |\mathcal{T}_2| &= N \prod_{p \leq \log^l N} \Big(1 - \frac{\nu(p)}{p^2}\Big) + o(N). \end{aligned} \tag{3.13}$$

Therefore $|\mathcal{T}_2 - \mathcal{T}_1| = o(N)$ since $\mathcal{T}_1 \subset \mathcal{T}_2$; ie, we overcount only a very small number of t. Let $\mathcal{T} = \mathcal{T}_2 - \mathcal{T}_1$. We have proved

$$\begin{aligned}\sum_{\substack{t\in[N,2N]\\ D(t)\ square-free}} S(t) &= \sum_{t\in\mathcal{T}_1} S(t)\\ &= \sum_{t\in\mathcal{T}_2} S(t) + O\Big(\sum_{t\in\mathcal{T}} S(t)\Big)\\ &= \sum_{d=1}^{\log^l N} \mu(d) \sum_{\substack{D(t)\equiv 0(d^2)\\ t\in[N,2N]}} S(t) + O\Big(\sum_{t\in\mathcal{T}} S(t)\Big).\end{aligned} \tag{3.14}$$

If we can control $\sum_{t=N}^{2N} S^2(t)$ well (for example, showing it is of size N), then we can handle summing over $\mathcal{T}_1$. We use arithmetic progressions to handle the piece with $d \le \log^l N$, and Cauchy-Schwartz to handle $t \in \mathcal{T}$.

$$\sum_{t\in\mathcal{T}} S(t) \ \ll\ \Big(\sum_{t\in\mathcal{T}} S^2(t)\Big)^{\frac{1}{2}}\Big(\sum_{t\in\mathcal{T}} 1\Big)^{\frac{1}{2}} \ \ll\ \Big(\sum_{t\in[N,2N]} S^2(t)\Big)^{\frac{1}{2}} o\Big(\sqrt{N}\Big). \tag{3.15}$$

If we can show $\sum_{t=N}^{2N} S^2(t) = O(N)$, then the error term is negligible as $N \to \infty$.

3.7 Sieving Polynomials of Degree at most 2

3.7.1 Polynomials of Degree 1

Let $D(t) = a_1 t + a_0$, $a_1 > 0$

$$\begin{aligned}\sum_{\substack{D(t)\ square-free\\ t\in[N,2N]}} 1 &= \sum_{d=1}^{2\sqrt{a_1 N}} \mu(d) \sum_{\substack{D(t)\equiv 0(d^2)\\ t\in[N,2N]}} 1\\ &= \sum_{d=1}^{\log^l N} \mu(d) \sum_{\substack{D(t)\equiv 0(d^2)\\ t\in[N,2N]}} 1 + \sum_{d=\log^l N}^{2\sqrt{a_1 N}} \mu(d) \sum_{\substack{D(t)\equiv 0(d^2)\\ t\in[N,2N]}} 1\\ &= \sum_{d=1}^{\log^l N} \mu(d) \sum_{\substack{D(t)\equiv 0(d^2)\\ t\in[N,2N]}} 1 + \sum_{d=\log^l N}^{2\sqrt{a_1 N}} \frac{N}{d^2}\nu(d) + O(d^\epsilon)\\ &= \sum_{d=1}^{\log^l N} \mu(d) \sum_{\substack{D(t)\equiv 0(d^2)\\ t\in[N,2N]}} 1 + N \sum_{d=\log^l N}^{\infty} \frac{d^\epsilon}{d^2} + \sum_{d=\log^l N}^{2\sqrt{a_1 N}} d^\epsilon\end{aligned}$$

$$
\begin{aligned}
&= \sum_{d=1}^{\log^l N} \mu(d) \sum_{\substack{D(t)\equiv 0(d^2)\\ t\in[N,2N]}} 1 + O\Big(\frac{N}{\log^{l(1-\epsilon)} N}\Big) + O\Big(N^{\frac{1}{2}(1+\epsilon)}\Big) \\
&= \sum_{d=1}^{\log^l N} \mu(d) \sum_{\substack{D(t)\equiv 0(d^2)\\ t\in[N,2N]}} 1 + O\Big(\frac{N}{\log^{l(1-\epsilon)} N}\Big). \qquad (3.16)
\end{aligned}
$$

The above argument works as d goes to at most a multiple of $\sqrt{N}$. Thus the $O(\nu(d))$ error is manageable.

3.7.2 Polynomials of Degree 2

Let $D(t) = a_2t^2 + a_1t + a_0$. If $p^2|D(t)$ for $t \in [N, 2N]$, then $p \ll N$. Let

$$
\mathcal{T}_3 \quad = \quad \Big\{t \in [N, 2N] :\ \exists p \in [\log^l N, cN] \text{ such that } p^2|D(t)\Big\}. \qquad (3.17)
$$

By Lemma 3.3, the number of incongruent roots of $D(t) \equiv 0 \bmod p^2$ equals the number of incongruent roots of $D(t) \equiv 0 \bmod p$; for p large, this is at most 2.

$$
\begin{aligned}
\sum_{t\in\mathcal{T}_3} 1 \quad &\ll \quad \sum_{p=\log^l N}^{cN} \#\{t \in [N, 2N] :\ D(t) \equiv 0(p^2)\} \\
&\ll \quad \sum_{p=\log^l N}^{cN} \Big(\frac{N}{p^2}2 + 2\Big) \\
&\ll \quad N \sum_{n=\log^l N}^{cN} \frac{1}{n^2} + O\Big(\pi(cN)\Big) \\
&\ll \quad O\Big(\frac{1}{\log^l N} + \frac{N}{\log N}\Big) = o(N). \qquad (3.18)
\end{aligned}
$$

Thus, the earlier construction of sets $\mathcal{T}_1$ and $\mathcal{T}_2$ will work. We needed to estimate the number of $t \in [N, 2N]$ with $D(t)$ divisible by the square of a large prime, which is accomplished by showing $|\mathcal{T}_3| = o(N)$. This proof fails for degree 3 or more because of the factor $\pi(cN^{k/2})$, which is manageable only for $k \leq 2$.

3.8 Conditions Implying $|\mathcal{F}| = c_{\mathcal{F}} N + o(N)$

Assume no square divides $D(t)$ for all t. We have seen that the number of $t \in [N, 2N]$ with $D(t)$ not divisible by d^2, $d \leq \log^l N$, is $\prod_p \left(1 - \frac{\nu(p)}{p^2}\right) + o(N)$. Let $D(t) = \prod_i D_i^{r_i}(t)$, $D_i(t)$ irreducible. By multiple applications of Lemma 3.6, $\exists c$ such that $\forall t$, there is no prime $p > c$ which divides two of the $D_i(t)$. Thus, if $D(t)$ is divisible by p^2 for a large prime, one of the factors is divisible by p^2. As there are finitely many factors, it is sufficient to bound by $o(N)$ the number of $t \in [N, 2N]$ with $p^2 | D(t)$ for a large prime for irreducible $D(t)$.

For polynomials of degree at most 2, the claim follows immediately from crude sieving; for polynomials of degree 3 it follows from Hooley ([Ho]). For polynomials of degree 4 or more, Granville ([Gr]) showed this to be a consequence of the ABC conjecture.

Let $|\mathcal{F}|$ equal the number of $t \in [N, 2N]$ with $D(t)$ square-free. Let $c_{\mathcal{F}} = \prod_{p \leq \log^l N} \left(1 - \frac{\nu(p)}{p^2}\right)$. We have seen extending the product to all primes costs $O(\frac{1}{\log^{l(1-\epsilon)} N})$. Thus, we need only bound $c_{\mathcal{F}}$ away from zero.

Let $D(t) = a_k t^k + \cdots a_0$ with discriminant δ. For $p \nmid a_k \delta$, $\nu(p) \leq k$ by Lemmas 3.1 and 3.3.

Let $\mathcal{P}$ be the set of primes dividing $a_k \delta$ and all primes at most $\sqrt{k}$. The contribution from $p \notin \mathcal{P}$ is bounded away from 0:

$$\begin{aligned}
P_0 &= \prod_{p \notin \mathcal{P}} \left(1 - \frac{\nu(p)}{p^2}\right) \\
\log P_0 &= \sum_{p \notin \mathcal{P}} \log \left(1 - \frac{\nu(p)}{p^2}\right) \\
&= -\sum_{p \notin \mathcal{P}} \sum_{n=1}^{\infty} \frac{1}{n} \left(\frac{\nu(p)}{p^2}\right)^n \\
&\geq -\sum_{p \notin \mathcal{P}} \frac{\nu(p)/p^2}{1 - \frac{k}{k+1}} \\
&\geq -k(k+1) \sum_{p \notin \mathcal{P}} \frac{1}{p^2} \geq -\frac{\pi^2}{6} k(k+1) \\
P_0 &\geq e^{-\pi^2 k(k+1)}. \qquad (3.19)
\end{aligned}$$

Therefore, if $\nu(p) < p^2$ for $p | a_k \delta$ and $p \leq \sqrt{k}$, then $c_{\mathcal{F}} > 0$.

If $D(t)$ is divisible by a square for all t, not surprisingly the above arguments fail (as $D(t)$ is never square-free). Let P be the largest power of primes such that $\forall t$, $P^2 | D(t)$. By changing variables $\tau \to P^m t + t_0$, for m sufficiently large, $D(\tau)$ is divisible by fixed powers of $p | P$, depending only on $D(t_0)$. Thus, instead of sieving to $D(t)$ square-free, we sieve to $D(\tau)$ square-free except for primes dividing P.

Let δ_τ denote the new discriminant. As the discriminant is a product over the differences of the roots, t_0 does not change the discriminant, and P^m rescales by a power of P. Thus, $\delta_\tau = P^M\delta$. Further, the new leading coefficient is $P^{mk}a_k$. Thus, for $p \nmid P$, our previous arguments are still applicable, and we are no longer sieving over $p|P$. We have therefore shown

Theorem 3.8 (Conditions on $D(t)$ implying $|\mathcal{F}| = c_{\mathcal{F}}N + o(N)$) *Assume no square divides $D(t)$ for all t. Let $\mathcal{P}$ be the set of primes dividing $a_k\delta$ and all primes at most $\sqrt{k}$. If $\forall p \in \mathcal{P}$, $\nu(p) \leq p^2 - 1$, then $|\mathcal{F}| = c_{\mathcal{F}}N + o(N)$, $c_{\mathcal{F}} > 0$. If $\forall t$, $B^2|D(t)$ or if for some prime $p \in \mathcal{P}$, $\nu(p) = p^2$, let P be the product of all primes in $\mathcal{P}$ or dividing B. By changing variables to $\tau = P^m t + t_0$ for m large and sieving to $D(\tau)$ square-free except for $p|P$ (where $\forall t$, the power of $p|P$ dividing $D(t)$ is constant), we again obtain $|\mathcal{F}| = c_{\mathcal{F}}N + o(N)$, $c_{\mathcal{F}} > 0$. In this case, $c_{\mathcal{F}}$ no longer includes factors from $p|P$.*

If all irreducible factors of $D(t)$ have degree at most 3, these results are unconditional; if there is an irreducible factor with degree at least 4 these results are conditional, and a consequence of the ABC or Square-Free Sieve conjecture.

Further, let $\mathcal{T} = \{t \in [N, 2N] : \exists d > \log^l N \text{ with } d^2|D(t)\}$. Then $\mathcal{T} = o(N)$.

4 Handling the Conductors $C(t)$

4.1 Introduction

For many families of elliptic curves, we show by sieving to a subsequence of t we obtain a sub-family where for a positive percent of t, the conductors are a monotone polynomial in t. In particular, we prove this for all rational surfaces.

Tate's Algorithm (see [Cr], pages 49 – 52) allows us to calculate the conductor $C(t)$ for an elliptic curve E_t over $\mathbb{Q}$:

$$C(t) = \prod_{p|\Delta(t)} p^{f_p(t)}, \tag{4.1}$$

where for $p > 3$, if the curve is minimal for p then $f_p(t) = 0$ if $p \nmid \Delta(t)$, 1 if $p|\Delta(t)$ and $p \nmid c_4(t)$, and 2 if $p|\Delta(t)$ and $p|c_4(t)$. From [Si1] (Remark 1.1, page 172), if $p > 3$ and $p^{12} \nmid \Delta(t)$, then the equation is minimal at p.

We need $C(t)$ to be monotone for a sub-family to bound some error terms used to calculate the 1- and 2-level densities (Theorem 7.9). Clearly, $f_p(t)$ depends on t, as for a given p, $p|\Delta(t)$ for only certain t.

Let $\Delta(t) = d\Delta_1(t)\Delta_2(t)$, where $\Big(\Delta_2(t), c_4(t)\Big) = 1$ and $\Delta_1(t)$ is the product of powers of irreducible polynomials dividing $\Delta(t)$ and $c_4(t)$. By possibly changing d, we may take $\Delta_i(t)$ primitive. Let $D_i(t)$ be the product of all irreducible non-constant polynomials dividing $\Delta_i(t)$. Let $c_4(t) = c\gamma_1(t)\gamma_2(t)$. Then (up to an explicitly calculable list of primes), $C(t) = D_1^2(t)D_2(t)$ if $\Delta(t)$ has no irreducible polynomial factor occurring at least 12 times. Hence, while $f_p(t)$ may vary, the product of $p^{f_p(t)}$, except for a finite set of primes, is well behaved.

Possibly after passing to a sub-family, for the potential bad primes, $f_p(t) = f_p$. Let

$$\begin{aligned} \mathcal{P}_0 &= \{p : p \leq \deg \Delta(t)\} \ \cup \ \{p : p|cd\} \\ P_0 &= \prod_{p \in \mathcal{P}_0} p. \end{aligned} \tag{4.2}$$

The idea is that while for such p, $f_p(t)$ may vary, by changing variables from t to $P_0^m t + t_1$ for some enormous m, for $p \in \mathcal{P}_0$, $f_p(P_0^m t + t_1) = f_p(t_1)$. Thus, for this subsequence, $f_p(t)$ is constant.

We need two preliminary results. First, given a finite set of primes $\mathcal{P}_0$, we may find an m and a

t_1 such that for those primes, $f_p(P_0^m t+t_1)$ is constant. Second, Lemma 3.6: given two polynomials with no non-constant factors over $\mathbb{Q}$, there is a finite set of primes $\mathcal{P}_2$ such that if $\exists t$ such that $\exists p$ dividing both polynomials, then $p \in \mathcal{P}_2$.

4.2 $C(t)$

4.2.1 Notation

For the elliptic curve $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$,

$$\begin{aligned}
b_2 &= a_1^2 + 2^2a_2\\
b_4 &= a_1a_3 + 2a_4\\
b_6 &= a_3^2 + 2^2a_6\\
b_8 &= a_1^2a_6 - a_1a_3a_4 + 2^2a_2a_6 + a_2a_3^2 - a_4^2\\
c_4 &= b_2^2 - 2^3\cdot 3b_4\\
c_6 &= -b_2^3 + 2^2\cdot 3^2b_2b_4 - 2^3\cdot 3^3b_6\\
\Delta &= -b_2^2b_8 - 2^3b_4^3 - 3^3b_6^2 + 3^2b_2b_4b_6.
\end{aligned} \tag{4.3}$$

Note b_i, c_i and Δ are integer polynomials in the a_i's. Let $T(r,s,h,u)$ denote the coordinate transformation

$$\begin{aligned}
ua_1' &= a_1 + 2s\\
ua_2' &= a_2 - sa_1 + 3r - s^2\\
ua_3' &= a_3 + ra_1 + 2h\\
ua_4' &= a_4 - sa_3 + 2ra_2 - (h+rs)a_1 + 3r^2 - 2sh\\
ua_6' &= a + 6 + ra_4 + r^2a_2 + r^3 - ha_3 - h^2 - rha_1.
\end{aligned} \tag{4.4}$$

Note Cremona uses t where we use h; as we are considering one-parameter families E_t, we have changed notation.

4.2.2 $f_p(t)$, $p \in \mathcal{P}_0$

Consider the original family of elliptic curves

$$E_t: \; y^2 + a_1(t)xy + a_3(t)y = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t). \tag{4.5}$$

Assume $\Delta(t)$ is not identically zero. Thus, $\exists t_1 > 0$ such that $\forall t \geq t_1$, $\Delta(t) \neq 0$. While we may choose any $t \geq t_1$, for definiteness take t_1.

Apply Tate's Algorithm to E_{t_1}. If the initial equation was non-minimal for p, we change coordinates by $T(0,0,0,p)$ and restart the algorithm. We may have to apply the algorithm and restart several times, but after finitely many passes through, the algorithm terminates.

Assume we restarted $L_{t_1}(p) - 1$ times; thus for p we pass through Tate's Algorithm $L_{t_1}(p)$ times. As t_1 is fixed, we eventually obtain $f_p(t_1)$ for each $p \in \mathcal{P}_0$. Thus, for each such prime, after possibly many coordinate changes, one of the following conditions held: $p \nmid \Delta$, $p \nmid c_4$, $p^2 \nmid a_6$, $p^3 \nmid b_8$, $p^3 \nmid b_6$, $p \nmid w(a_2, a_4, a_6)$, $p \nmid xa_3^2(a_3) + 4xa_6(a_6)$, $p \nmid xa_4^2(a_4) - 4xa_2(a_2)xa_6(a_6)$, $p^4 \nmid a_4$, $p^6 \nmid a_6$, and every function is polynomial in the a_i's.

Thus, after possibly many coordinate changes $T(r,s,h,u)$, some polynomial with integer coefficients of the a_i's is not divisible by either p, p^2, p^3, p^4 or p^6.

Consider $\tau = P_0^m t + t_1$. The idea is, by choosing m enormous, $f_p(\tau) = f_p(t_1)$ for $p \in \mathcal{P}_0$.

This is because in Tate's Algorithm, we only need the values modulo a power of p. We have

$$\begin{aligned} a_i(\tau) &= a_i(P_0^m t + t_1) \\ &= P_0^m t \widehat{a}_i(P_0^m t) + a_i(t_1) \\ &= \widetilde{a}_i(t) + a_i(t_1). \end{aligned} \tag{4.6}$$

In applying Tate's Algorithm, we need $a_i(\tau)$ modulo powers of p. If m is sufficiently large, we can ignore $\widetilde{a}_i(t)$ in all equivalence checks, as for the powers of p we investigate, $\widetilde{a}_i(t) \equiv 0$. Let

$$\begin{aligned} n_t(p) &= \mathrm{ord}\Big(p, \Delta(t)\Big) \\ n &= \max_{p \in \mathcal{P}_0} n_{t_1}(p) \end{aligned}$$

$$L \quad = \quad \max_{p \in \mathcal{P}_0} L_{t_1}(p). \tag{4.7}$$

We prove $f_p(\tau) = f_p(t_1)$ for large m. How large must m be? Excluding lines $42 - 65$, on each pass through Tate's Algorithm we sometimes divide our coefficients by powers of p: up to p^2 on lines 26 and 30, up to p^3 on line 34, up to p^4 on line 69, and p^{12} on line 80.

Over-estimating, we divide by at most $p^{2\cdot 2+1\cdot 3+1\cdot 4+1\cdot 12} = p^{23}$.

For lines $42 - 65$, we have a loop which can be executed at most $n+4$ times. We constantly divide by increasing powers of p; the largest power is the last time through the loop, which is at most $p^{2(n+6)}$. As we pass through this loop at most $n+4$ times, we divide by at most $p^{2n^2+20n+48}$.

Thus, on each pass we have divisions by at most $p^{2n^2+20n+48+23}$. As we loop through the main part of Tate's Algorithm at most L times, we have divisions by at most $p^{(2n^2+20n+71)L}$.

Thus, if $m > (2n^2 + 20n + 71)L$, then $\forall t$, none of the $\widetilde{a}_i(t) = P_0^m t\widehat{a}_i(t)$ terms will affect any congruence. If m were smaller, when we divide by powers of p, the P_0^m terms could give a contribution that is not congruent to zero mod the relevant power of p. By taking m enormous, this cannot happen.

Significantly smaller choices of m work: many of the divisions (for example, from lines $42-65$) arise only once: if we enter those lines, we determine $f_p(\tau)$ and do not need to restart. Thus, we could have taken $m > 2n^2 + 20n + 48 + 23L$. As improvements of this nature will still lead to an $m > 1$, we stay with the easier bound. When working with a specific family, we will compute better (but not necessarily optimal) m.

4.3 Rational Surfaces I

4.3.1 Preliminaries

Recall an elliptic surface $y^2 = x^3 + A(t)x + B(t)$ is rational iff one of the following is true: (1) $0 < \max\{3\text{deg } A(t), 2\text{deg } B(t)\} < 12$; (2) $3\text{deg } A(t) = 2\text{deg } B(t) = 12$ and $\text{ord}_{t=0} t^{12}\Delta(t^{-1}) = 0$. See [RSi], pages $46 - 47$ for more details.

Assume we are in case (1). No non-constant polynomial of degree 11 or more divides $\Delta(t)$; however, a twelfth or higher power of a prime might divide $\Delta(t)$. Let $k = \text{deg } \Delta(t)$, and write

$$\begin{aligned} \Delta(t) &= d\Delta_1(t)\Delta_2(t) \\ c_4(t) &= c\gamma_1(t)\gamma_2(t) \end{aligned}$$

$$\begin{aligned}\mathcal{P}_0 &= \{p : p \leq \deg \Delta(t)\} \ \cup \ \{p : p | cd\} \\ P_0 &= \prod_{p \in \mathcal{P}_0} p. \qquad (4.8)\end{aligned}$$

where $\Delta_1(t)$ through $\gamma_2(t)$ are primitive polynomials, $\Delta_1(t)$ and $\gamma_1(t)$ are divisible by the same non-constant irreducible polynomials, $\Delta_2(t)$ and $c_4(t)$ are not both divisible by any non-constant polynomial, and d and c are the largest integers dividing $\Delta(t)$ and $c_4(t)$.

Let $D_i(t)$ be the product of all non-constant irreducible polynomials dividing $\Delta_i(t)$, and similarly for $c_i(t)$. Let $D(t) = D_1(t)D_2(t) = \alpha_\kappa t^\kappa + \cdots + \alpha_0$, $c(t) = c_1(t)c_2(t)$. Note it is possible $D(t)$ is of degree less than k.

Apply Lemma 3.6 to $c(t)$ and $D_2(t)$. Thus $\exists c'$ such that if $\exists t$ where p divides both polynomials, then $p|c'$. Let $\mathcal{P}_2$ be the prime divisors of c' not in $\mathcal{P}_0$ and let $\mathcal{P}_1$ be the prime divisors of $\alpha_\kappa \cdot \text{Discriminant}(D(t))$ not in $\mathcal{P}_0$. Define

$$\begin{aligned}\mathcal{P} &= \bigcup_{i=1}^{2} \mathcal{P}_i \\ P &= \prod_{p \in \mathcal{P}} p. \qquad (4.9)\end{aligned}$$

Note every prime in $\mathcal{P}$ is greater than k and not in $\mathcal{P}_0$.

As the product of primitive polynomials is primitive, $D(t)$ is primitive. Thus for any prime, either $D(t)$ mod p is a constant not divisible by p, or a non-constant polynomial of degree at most k. In the second case, as there are at most k roots to $D(t) \equiv 0$ mod p, we find that given a $p > k$, $\exists t_p$ such that $D(t_p) \not\equiv 0$ mod p. By the Chinese Remainder Theorem, $\exists t_0 \equiv t_p$ mod p for all $p \in \mathcal{P}$.

4.3.2 Calculating the Conductor

$\forall p \in \mathcal{P}$, $D(Pt + t_0) \equiv D(t_0) \not\equiv 0$ mod p. As $\mathcal{P}$ and $\mathcal{P}_0$ are disjoint, this implies that $D(Pt + t_0)$ is minimal for all $p \in \mathcal{P}$, as $\mathcal{P}_0$ contains the factors of d. Moreover, $f_p(Pt + t_0) = 0$ for $p \in \mathcal{P}$.

By changing variables again, from t to $P_0^m t + t_1$, we can determine the powers of $p \in \mathcal{P}_0$ in the conductor. Combining the two changes, we send t to $\tau = P(P_0^m t + t_1) + t_0$.

Originally we had $\Delta(t) = d\Delta_1(t)\Delta_2(t)$. Now we have $\Delta(\tau) = d\Delta_1(\tau)\Delta_2(\tau)$. It is possible that $D_1(\tau)D_2(\tau)$ is no longer primitive; however, if there is a common prime divisor p, p divides $\alpha_\kappa(P \cdot P_0^m)^\kappa$, implying $p \in \mathcal{P}_0 \sqcup \mathcal{P}$.

We sieve to $D(\tau)$ square-free for $p \notin \mathcal{P}_0 \sqcup \mathcal{P}$. As $\mathcal{P}_0 \sqcup \mathcal{P}$ contains all primes less than k, as well as the prime divisors of P_0, P, α_κ and Discriminant$(\Delta(t))$, we can perform the sieving. Note the discriminants of $\Delta(t)$ and $\Delta(\tau)$ differ by a power of $P \cdot P_0^m$. Thus, away from these primes, $D(\tau) \equiv 0 \bmod p^2$ has at most $k < p^2$ roots, and we may sieve to a positive percent of t. The sieving is unconditional if each irreducible factor of $D(\tau)$ is of degree at most 3.

$D(\tau)$ is divisible by fixed powers of primes in $\mathcal{P}_0$ and never divisible by primes in $\mathcal{P}$. Thus $\exists c_1$, c_2 with factors in $\mathcal{P}_0$ such that $D'(\tau) = \frac{D_1(\tau)}{c_1}\frac{D_2(\tau)}{c_2}$ is not divisible by any $p \in \mathcal{P}_0 \sqcup \mathcal{P}$. In the sequel we sieve to $D'(\tau)$ square-free; for $p \notin \mathcal{P}_0 \sqcup \mathcal{P}$, this is the same as $D(\tau)$ not divisible by p^2.

We need to determine $f_p(\tau)$ for $p \in \mathcal{P}_0$, $p \in \mathcal{P}$, and $p \notin \mathcal{P}_0 \sqcup \mathcal{P}$.

By our previous arguments, if m is sufficiently large, $f_p(\tau) = f_p(t_1)$ for $p \in \mathcal{P}_0$.

If $p \in \mathcal{P}$, $p \notin \mathcal{P}_0$. Then mod p, $\Delta(\tau) = \Delta\Big(P(P_0 t + t_1) + t_0\Big) \equiv \Delta(t_0) \not\equiv 0$. Thus, for these p, $f_p(\tau) = 0$.

Assume $p \notin \mathcal{P}_0 \sqcup \mathcal{P}$. The leading term of $dD(\tau)$ is $d\alpha_\kappa(P \cdot P_0^m)^\kappa$. By construction, p does not divide the leading coefficient of $\Delta(\tau)$, as $\mathcal{P}_0 \sqcup \mathcal{P}$ contains the prime divisors of d, α_k, P and P_0. If we sieve to $\Delta(\tau)$ square-free for $p \notin \mathcal{P}_0 \sqcup \mathcal{P}$ (ie, $D'(\tau)$ square-free), then as the degree of $\Delta(\tau)$ is at most 10, the curve is minimal for such p. Thus, $f_p(\tau)$ is 1 if $p|D_2(\tau)$ and 2 if $p|D_1(\tau)$.

Thus, we have shown

Theorem 4.1 *All quantities as above, for $D'(\tau)$ square-free, the conductors are*

$$C(\tau) = \prod_{p \in \mathcal{P}_0} p^{f_p} \cdot \left(\frac{|D_1(\tau)|}{c_1}\right)^2 \frac{|D_2(\tau)|}{c_2} \tag{4.10}$$

For sufficiently large τ, $C(\tau)$ is a monotone increasing polynomial (we may drop the absolute values), and a positive percent of τ yield $D'(\tau)$ square-free.

4.4 Rational Surfaces II

We consider what could go wrong in our proof if we are in case (2), where 3deg $A(t) =$ 2deg $B(t) = 12$ and $\text{ord}_{t=0} t^{12}\Delta(t^{-1}) = 0$.

Thus, $\Delta(t)$ is a degree twelve polynomial, and we need to worry about minimality issues. As before, we have

$$\Delta(t) \quad = \quad -2^4\Big(2^2A^3(t) + 3^3B^2(t)\Big)$$

$$\begin{aligned}\Delta(t) &= d\Delta_1(t)\Delta_2(t) \\ c_4(t) &= c\gamma_1(t)\gamma_2(t) \\ \mathcal{P}_0 &= \{p : p \leq \deg\, \Delta(t)\} \ \cup\ \{p : p|cd\} \\ P_0 &= \prod_{p \in \mathcal{P}_0} p. \end{aligned} \tag{4.11}$$

4.4.1 $D(t)$ not divisible by a twelfth power

Assume at first that no twelfth power of an irreducible non-constant polynomial divides $\Delta(t)$.

By changing variables as in the previous case, we find $f_p(\tau) = f_p$ for $p \in \mathcal{P}_0$ and $f_p(\tau) = 0$ for $p \in \mathcal{P}$. Thus, we need only determine $f_p(\tau)$ for $p \notin \mathcal{P}_0 \sqcup \mathcal{P}$; for $D'(\tau)$ square-free and p large, the curve is minimal at p, and we argue similarly as before.

4.4.2 $(\alpha t + \beta)^{12} | D(t)$, $(\alpha t + \beta) \nmid c_4(t)$

Assume now a twelfth power of an irreducible polynomial divides $\Delta(t)$. As $\Delta(t)$ is degree 12, we write this as $\alpha t + \beta$. As $(\alpha t + \beta) \nmid c_4(t)$, Tate's algorithm gives $f_p = 1$: we calculate the order of p in $\Delta(\tau)$ on line 3, and this is greater than zero; by lines $3 - 18$ we change variables by $T(r, 0, h, 1)$, which does not change $c_4(\tau)$; lines $19 - 21$ imply $f_p(\tau) = 1$ as $p \nmid c_4(\tau)$.

4.4.3 $(\alpha t + \beta)^{12} | D(t)$, $(\alpha t + \beta) | c_4(t)$

As $\Delta(t) = -64A^3(t) - 432B^2(t)$, $(\alpha t + \beta) | B(t)$. By comparing degrees, either $\alpha t + \beta$ divides $A(t)$ four times and $B(t)$ six times or $A(t)$ twice and $B(t)$ thrice.

In the first case, $(\alpha t + \beta)^4 || A(t)$ and $(\alpha t + \beta)^6 || B(t)$; thus we may change variables by $y \to (\alpha t + \beta)^3 y$, $x \to (\alpha t + \beta)^2 x$, and we obtain a constant family. Thus, this case is not a rational surface.

In the second case, $(\alpha t + \beta)^2 || A(t)$ and $(\alpha t + \beta)^3 || B(t)$. Let $A(t) = (\alpha t + \beta)^2 A_1(t)$ and $B(t) = (\alpha t + \beta)^3 B_1(t)$, with $(\alpha t + \beta) \nmid A_1(t) B_1(t)$. Further, as this is to be a rational surface, deg $A_1(t) = 2$ and deg $B_1(t) = 3$.

It is sufficient to show there do not exist rational constants such that $(\alpha t + \beta)^6 | c_a^2 A_1^3(t) + c_b^3 B_1^2(t)$ for any such $A_1(t)$, $B_1(t)$. By a rational change of variables $t \to \frac{t-\beta}{\alpha}$, it is sufficient to consider the case $\alpha t + \beta = t$. By multiplying the coefficients of $A_1(t)$ and $B_1(t)$ by rationals, it is sufficient to show $t^6 \nmid B_1^2(t) - A_1^3(t)$. The non-existence follows immediately from

Lemma 4.2 *Assume $t \nmid A_1(t) B_1(t)$, with $A_1(t) = a_2 t^2 + a_1 t + a_0$, $B_1(t) = b_3 t^3 + b_2 t^2 + b_1 t + b_0$, and a_2, a_0, b_3,b_0 non-zero. Then there are no choices of rational a_i, b_j such that $t^6 | B_1^2(t) - A_1^3(t)$.*

Expanding $B_1^2(t) - A_1^3(t)$ yields $h_6t^6 + \cdots + h_0$, where

$$\begin{aligned}
h_6 &= b_3^2 - a_2^3 \\
h_5 &= 2b_3b_2 - 3a_2^2a_1 \\
h_4 &= 2b_3b_1 + b_2^2 - 3a_2^2a_0 - 3a_2a_1^2 \\
h_3 &= 2b_3b_0 + 2b_2b_1 - 6a_2a_1a_0 - a_1^3 \\
h_2 &= 2b_2b_0 + b_1^2 - 3a_2a_0^2 - 3a_1^2a_0 \\
h_1 &= 2b_1b_0 - 3a_1a_0^2 \\
h_0 &= b_0^2 - a_0^3. \qquad (4.12)
\end{aligned}$$

We want $h_0 = \cdots = h_5 = 0$, $h_6 \neq 0$. From $h_0 = 0$ we obtain $b_0 = c_0^3$ and $a_0 = c_0^2$. From $h_1 = 0$ we get $2b_1 = 3a_1c_0$. From $h_2 = 0$, $8b_2c_0 = 12a_2c_0^2 + 3a_1^2$.

From h_3, h_4 and h_5 equal zero we get

$$\begin{aligned}
0 &= 16b_3c_0^3 - 12a_2a_1c_0^2 + a_1^3 \\
0 &= 64b_3a_1c_0^3 - 16a_2^2c_0^4 - 40a_2a_1^2c_0^2 + 3a_1^4 \\
0 &= 4b_3a_2c_0^2 + b_3a_1^2 - 4a_2^2a_1c_0 \qquad (4.13)
\end{aligned}$$

We have three equations for b_3 in terms of c_0, a_1 and a_2. $c_0 \neq 0$ as $a_0b_0 \neq 0$; further, $a_2b_3 \neq 0$. If $a_1 = 0$ then $b_3 = a_2 = 0$, and the degrees of $A_1(t)$ and $B_1(t)$ are too small. Hence $c_0a_1a_2 \neq 0$.

Thus we may write $a_1 = c_1c_0$ ($c_1 \neq 0$), $a_2 = c_2$, and $b_3 = c_3c_2$ ($c_3 \neq 0$). Substituting and removing powers of c_0 (and c_2 in the third equation) yield

$$\begin{aligned}
0 &= 16c_3c_2 - 12c_2c_1 + c_1^3 \\
0 &= 64c_3c_2c_1 - 16c_2^2 - 40c_2c_1^2 + 3c_1^4 \\
0 &= 4c_3c_2 + c_3c_1^2 - 4c_2c_1. \qquad (4.14)
\end{aligned}$$

Multiplying the first equation by $-3c_1$ and adding it to the second equation (and then cancelling a c_2) gives

$$\begin{aligned} 0 &= 16c_3c_2 - 12c_2c_1 + c_1^3 \\ 0 &= 16c_3c_2 - 4c_1^2 - 16c_2 \\ 0 &= 4c_3c_2 + c_3c_1^2 - 4c_1 \end{aligned} \tag{4.15}$$

Algebraic manipulations (second minus first; first minus four times third, divide by c_1; third) give

$$\begin{aligned} 0 &= 12c_2c_1 - c_1^3 - 4c_1^2 - 16c_2 \\ 0 &= 16 - 4c_3c_1 - 12c_2 + c_1^2 \\ 0 &= 4c_3c_2 + c_3c_1^2 - 4c_1 \end{aligned} \tag{4.16}$$

The first equation yields

$$c_2 = \frac{1}{4}\frac{c_1^2(c_1+4)}{3c_1-4}. \tag{4.17}$$

Note $c_1 \neq 0, -4$, as these values yield $c_2 = 0$.

$16c_3c_2 - 4c_1^2 - 16c_2 = 0$. Dividing by 4 yields $4c_2(c_3 - 1) = c_1^2$. Substituting for $c_2 = c_2(c_1)$ gives $c_3(c_1) = \frac{4c_1}{c1+4}$. Substituting for $c_2(c_1)$ and $c_3(c_1)$ into $4c_3c_2 + c_3c_1^2 - 4c_1 = 0$ yields $4c_1(4c_1^3 - 3c_1^2 - 8c_1 + 16)$. By the rational root test, there are no non-zero solutions with c_1 rational. □

4.5 Generalizations

The previous arguments are applicable to any family where deg $\Delta(t) \leq 12$ (which can include some non-rational families).

It is straightforward to generalize these arguments for all families; as all our examples are either rational surfaces or have deg $\Delta(t) \leq 12$, we will not state these generalizations.

4.6 Summary

We summarize our sieving and conductor results:

Theorem 4.3 (Conductors and Cardinalities for Families) *For a one-parameter family with deg* $\Delta(t) \leq 12$*, which includes all rational families, by sieving a subsequence we obtain a family with conductors given by a monotone polynomial; further, by Theorem 3.8, possibly after changing variables to* $\tau = P^m t + t_0$*, a positive percent of* $t \in [N, N]$ *are square-free except for primes* $p|P$*, where the power of such* p *dividing* $D(\tau)$ *is independent of* t*. If all the irreducible factors of* $\Delta(t)$ *are degree* 3 *or less, the sieving is unconditional; for degree* 4 *and higher, the sieving is a consequence of the ABC or Square-Free Sieve conjecture.*

Part II

Density Preliminaries

5 1- and 2-Level Density Kernels for the Classical Compact Groups

By [KS1], the m-level densities for the classical compact groups are

$$\begin{aligned}
W_{m,\epsilon}(x) &= \mathbf{det}\Big(K_\epsilon(x_i,x_j)\Big)_{i,j\leq m} \\
W_{m,\mathrm{O}^+}(x) &= \mathbf{det}(K_1(x_i,x_j))_{i,j\leq m} \\
W_{m,\mathrm{O}^-}(x) &= \mathbf{det}(K_{-1}(x_i,x_j))_{i,j\leq m} + \sum_{k=1}^{m}\delta(x_k)\mathbf{det}(K_{-1}(x_i,x_j))_{i,j\neq k} \\
&= (W_{m,\mathrm{O}^-})_1(x) + (W_{m,\mathrm{O}^-})_2(x) \\
W_{m,O}(x) &= \frac{1}{2}W_{m,\mathrm{O}^+}(x) + \frac{1}{2}W_{m,\mathrm{O}^-}(x) \\
W_{m,U}(x) &= \mathbf{det}(K_0(x_i,x_j))_{i,j\leq m} \\
W_{m,Sp}(x) &= \mathbf{det}(K_{-1}(x_i,x_j))_{i,j\leq m} \qquad (5.1)
\end{aligned}$$

where $K(y) = \frac{\sin\pi y}{\pi y}$, $K_\epsilon(x,y) = K(x-y) + \epsilon K(x+y)$ for $\epsilon = 0, \pm 1$, O^+ denotes the group SO(even) and O^- the group SO(odd).

5.1 Needed Fourier Transforms

Let δ be the Dirac Delta functional: $\int f(x)\delta(x) = f(0)$. Let $I(x) = \chi_{[-1,1]}(x)$ be the characteristic function of the unit interval.

Lemma 5.1 $\widehat{1} = \delta$

PROOF: This is proved in the theory of distributions. Formally, using duality, one can argue $\int f \cdot 1 = \widehat{f}(0) = \int \widehat{f} \cdot \delta$.

Lemma 5.2 $\widehat{\chi_{[-\frac{1}{2},\frac{1}{2}]}}\ (u) = K(u)$

PROOF:

$$\begin{aligned}
\int_{-\infty}^{\infty} \chi_{[-\frac{1}{2},\frac{1}{2}]}(x) e^{2\pi i x u} dx &= \int_{-\frac{1}{2}}^{\frac{1}{2}} \Big[\cos(2\pi x u) + i\sin(2\pi x u)\Big] dx \\
&= \int_{-\frac{1}{2}}^{\frac{1}{2}} \cos(2\pi x u) dx \\
&= \frac{\sin \pi u}{\pi u} \qquad (5.2)
\end{aligned}$$

Lemma 5.3 $\widehat{K(2x)}(u) = \frac{1}{2}I(u)$.

PROOF:

$$\begin{aligned}
\widehat{K(2x)}(u) &= \int_{-\infty}^{\infty} K(2x)e^{2\pi ixu}dx \\
&= \int_{-\infty}^{\infty} K(2x)e^{2\pi i2x(\frac{1}{2}u)}\frac{2dx}{2} \\
&= \frac{1}{2}\int_{-\infty}^{\infty} K(t)e^{2\pi it(\frac{1}{2}u)}dt \\
&= \frac{1}{2}\chi_{[-\frac{1}{2},\frac{1}{2}]}(\frac{1}{2}u) = \frac{1}{2}I(u). \qquad (5.3)
\end{aligned}$$

Lemma 5.4 $\widehat{K^2}(u) = 1 - |u|,\ |u| \leq 1$.

PROOF: We use duality for even functions: $\int f(x)g(x)dx = \int \widehat{f}(y)\widehat{g}(y)dy$. See [La2], pages $242 - 243$. Let $K_u(t) = K(t)e^{2\pi iut}$. Then $\widehat{K_u}(y) = \widehat{K}(y+u)$, and recall $\widehat{K}(y) = \chi_{[-\frac{1}{2},\frac{1}{2}]}(y)$. As K is even, the arguments below are justified.

$$\begin{aligned}
\int_{-\infty}^{\infty} K^2(t)e^{2\pi iut}dt &= \int_{-\infty}^{\infty} \Big(K(t)\Big)\Big(K(t)e^{2\pi iut}\Big)dt \\
&= \int_{-\infty}^{\infty} K(t)K_u(t)dt \\
&= \int_{-\infty}^{\infty} \chi_{[-\frac{1}{2},\frac{1}{2}]}(y)\chi_{[-\frac{1}{2},\frac{1}{2}]}(y+u)dy \qquad (5.4)
\end{aligned}$$

$\chi_{[-\frac{1}{2},\frac{1}{2}]}(y)\chi_{[-\frac{1}{2},\frac{1}{2}]}(y+u)$ is one on the intersection of $\{-\frac{1}{2} \leq y \leq \frac{1}{2}\}$ and $\{-\frac{1}{2} \leq y+u \leq \frac{1}{2}\}$ and zero elsewhere. If $|u| > 1$, $\chi_{[-\frac{1}{2},\frac{1}{2}]}(y)\chi_{[-\frac{1}{2},\frac{1}{2}]}(y+u) = 0$, and the integral vanishes. If $u \in [0,1]$, the intersection is $-\frac{1}{2} \leq y \leq \frac{1}{2} - u$, and integrating over y gives $1-u$. If $u \in [-1,0]$, it is one on the intersection of $\{-\frac{1}{2} \leq y \leq \frac{1}{2}\}$ and $\{-\frac{1}{2} \leq y - |u| \leq \frac{1}{2}\}$. We get $-\frac{1}{2} + |u| \leq y \leq \frac{1}{2}$, and integrating over y gives $1 - |u|$. Therefore the Fourier Transform of K^2 is $1-|u|$, $|u| \leq 1$.

5.2 1-Level Densities

For $|u_1| \leq 1$, $\frac{1}{2}I(u_1) = -\frac{1}{2}I(u_1) + 1$.

$$\begin{aligned}
W_{1,\mathrm{O}^+}(x_1) &= \mathbf{det}\Big(K_1(x_i,x_j)\Big)_{i,j\leq 1} \\
&= K_1(x_1,x_1) = 1 + K(2x_1)
\end{aligned}$$

$$\begin{aligned} &= 1(x_1) + K(2x_1) \\ \widehat{W_{1,\mathrm{O}^+}}(u_1) &= \delta(u_1) + \frac{1}{2}I(u_1). \end{aligned} \tag{5.5}$$

$$\begin{aligned} W_{1,\mathrm{O}^-}(x_1) &= \mathbf{det}\Big(K_{-1}(x_i,x_j)\Big)_{i,j\leq 1} \\ &\quad + \sum_{k=1}^{1} \delta(x_k)\mathbf{det}\Big(K_{-1}(x_i,x_j)\Big)_{i,j\neq 1} \\ &= K_{-1}(x_1,x_1) + \delta(x_1) \\ &= 1 - K(2x_1) + \delta(x_1) \\ &= 1(x_1) - K(2x_1) + \delta(x_1) \\ \widehat{W_{1,\mathrm{O}^-}}(u_1) &= \delta(u_1) - \frac{1}{2}I(u_1) + 1(u_1). \end{aligned} \tag{5.6}$$

$$\begin{aligned} W_{1,Sp}(x_1) &= \mathbf{det}\Big(K_{-1}(x_i,x_j)\Big) \\ &= K_{-1}(x_1,x_1) \\ &= 1(x_1) - K(2x_1) \\ \widehat{W_{1,Sp}}(u_1) &= \delta(u_1) - \frac{1}{2}I(u_1). \end{aligned} \tag{5.7}$$

$$\begin{aligned} W_{1,U}(x_1) &= \mathbf{det}\Big(K_0(x_i,x_j)\Big) \\ &= K_0(x_1,x_1) = 1(x_1) \\ \widehat{W_{1,U}}(u_1) &= \delta(u_1). \end{aligned} \tag{5.8}$$

We have shown

Theorem 5.5 (1-Level Densities)

$$\begin{aligned} \widehat{W_{1,\mathrm{O}^+}}(u) &= \delta(u) + \frac{1}{2}I(u) \\ \widehat{W_{1,O}}(u) &= \delta(u) + \frac{1}{2} \\ \widehat{W_{1,\mathrm{O}^-}}(u) &= \delta(u) - \frac{1}{2}I(u) + 1 \end{aligned}$$

$$\begin{aligned}\widehat{W_{1,Sp}}(u) &= \delta(u) - \frac{1}{2}I(u) \\ \widehat{W_{1,U}}(u) &= \delta(u). \end{aligned} \tag{5.9}$$

For functions whose Fourier Transforms are supported in $[-1,1]$*, the three orthogonal densities are indistinguishable, though they are distinguishable from* U *and* Sp*. To detect differences between the orthogonal groups using the* 1*-level density, one needs to work with functions whose Fourier Transforms are supported beyond* $[-1,1]$*.*

5.3 Preliminaries for the 2-Level Densities

$$\begin{aligned} W_{2,\epsilon}(x) &= \mathbf{det}\Big(K_\epsilon(x_i,x_j)\Big)_{i,j\le 2} \\ &= K_\epsilon(x_1,x_1)K_\epsilon(x_2,x_2) - K_\epsilon(x_1,x_2)K_\epsilon(x_2,x_1) \\ &= \Big[1+\epsilon K(2x_1)\Big]\Big[1+\epsilon K(2x_2)\Big] - \\ &\quad \Big[K(x_1-x_2)+\epsilon K(x_1+x_2)\Big]\Big[K(x_2-x_1)+\epsilon K(x_1+x_2)\Big] \\ &= W_{2,\epsilon,a}(x) - W_{2,\epsilon,b}(x). \end{aligned} \tag{5.10}$$

We now calculate $\widehat{W_{2,\epsilon,a}}(u)$.

$$\begin{aligned} W_{2,\epsilon,a}(x) &= \Big[1+\epsilon K(2x_1)\Big]\Big[1+\epsilon K(2x_2)\Big] \\ &= 1+\epsilon K(2x_1)+\epsilon K(2x_2)+\epsilon^2 K(2x_1)K(2x_2) \\ &= 1(x_1)1(x_2)+\epsilon K(2x_1)1(x_2)+\epsilon 1(x_1)K(2x_2)+\epsilon^2 K(2x_1)K(2x_2) \\ \widehat{W_{2,\epsilon,a}}(u) &= \widehat{1(x_1)}\widehat{1(x_2)}+\epsilon\widehat{K(2x_1)}\widehat{1(x_2)}+\epsilon\widehat{1(x_1)}\widehat{K(2x_2)}+\widehat{K(2x_1)}\widehat{K(2x_2)} \\ &= \delta(u_1)\delta(u_2)+\frac{\epsilon}{2}\chi_{[-\frac{1}{2},\frac{1}{2}]}(\frac{u_1}{2})\delta(u_2)+\frac{\epsilon}{2}\delta(u_1)\chi_{[-\frac{1}{2},\frac{1}{2}]}(\frac{u_1}{2}) \\ &\quad +\chi_{[-\frac{1}{2},\frac{1}{2}]}(\frac{u_1}{2})\chi_{[-\frac{1}{2},\frac{1}{2}]}(\frac{u_2}{2}) \\ &= \delta(u_1)\delta(u_2)+\frac{\epsilon}{2}I(u_1)\delta(u_2)+\frac{\epsilon}{2}\delta(u_1)I(u_2)+\frac{\epsilon^2}{4}I(u_1)I(u_2) \\ &\quad \text{where } \ I(u)=\chi_{[-\frac{1}{2},\frac{1}{2}]}(\frac{u}{2})=\chi_{[-1,1]}(u) \end{aligned} \tag{5.11}$$

It is straightforward to calculate the Fourier Transforms of the above, as each function is even and of the form $g_1(x_1)g_2(x_2)$. We also use the fact that $\widehat{g(2x)}=\frac{1}{2}\widehat{g}(\frac{x}{2})$.

We now calculate $\widehat{W_{2,\epsilon,b}}(u)$. Note that K is even, so $K(x_i - x_j) = K(x_j - x_i)$.

$$\begin{aligned} W_{2,\epsilon,b}(x) &= \Big[K(x_1 - x_2) + \epsilon K(x_1 + x_2)\Big]\Big[K(x_2 - x_1) + \epsilon K(x_1 + x_2)\Big] \\ &= K^2(x_1 - x_2) + \epsilon^2 K^2(x_1 + x_2) + 2\epsilon K(x_1 - x_2)K(x_1 + x_2) \\ \widehat{W_{2,\epsilon,b}}(u) &= \widehat{T_-}(u_1, u_2) + \epsilon^2 \widehat{T_+}(u_1, u_2) + 2\epsilon \widehat{T_3}(u_1, u_2) \qquad (5.12) \end{aligned}$$

Let $\eta = \pm 1$. Then

$$\widehat{T_\pm}(u_1, u_2) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} K^2(x_1 + \eta x_2) e^{2\pi i (u_1,u_2)\cdot(x_1,x_2)} dx_1 dx_2. \qquad (5.13)$$

Change variables: $t_1 = x_1 + \eta x_2, t_2 = x_2$. Then $x_1 = t_1 - \eta t_2, x_2 = t_2$, and the Jacobian is $+1$. Hence $dx_1 dx_2 = dt_1 dt_2$, and $(u_1, u_2) \cdot (x_1, x_2) = u_1 t_1 + (-\eta u_1 + u_2)t_2$. Hence

$$\begin{aligned} \widehat{T_\pm}(u_1, u_2) &= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} K^2(t_1) e^{2\pi i (u_1 t_1 + (-\eta u_1 + u_2)t_2)} dt_1 dt_2 \\ &= \int_{-\infty}^{\infty} K^2(t_1) e^{2\pi i u_1 t_1} dt_1 \int_{-\infty}^{\infty} 1(t_2) e^{2\pi i (-\eta u_1 + u_2)t_2} dt_2 \\ &= \int_{-\infty}^{\infty} K^2(t_1) e^{2\pi i u_1 t_1} dt_1 \cdot \delta(-\eta u_1 + u_2) \qquad (5.14) \end{aligned}$$

We have previously shown the Fourier Transform of $K^2(x_1)$ is $1 - |u_1|$, $|u_1| \le 1$. We therefore find

$$T_\pm(u_1, u_2) \quad = \quad \delta(-\eta u_1 + u_2)\Big(1 - |u_1|\Big). \qquad (5.15)$$

We calculate $\widehat{T_3}(u_1, u_2)$, the Fourier Transform of $K(x_1 - x_2)K(x_1 + x_2)$. Change variables: $t_1 = x_1 - x_2$, $t_2 = x_1 + x_2$. Therefore $x_1 = \frac{1}{2}t_1 + \frac{1}{2}t_2$, $x_2 = -\frac{1}{2}t_1 + \frac{1}{2}t_2$. The Jacobian is the absolute value of the determinant of the transformation, which is $\frac{1}{2}$. In the exponential we have $u_1 x_1 + u_2 x_2$, which becomes $\frac{1}{2}(u_1 - u_2)t_1 + \frac{1}{2}(u_1 + u_2)t_2$.

$$\widehat{T_3}(u_1, u_2) \quad = \quad \int\int K(x_1 - x_2)K(x_1 + x_2) e^{2\pi i (u_1 x_1 + u_2 x_2)} dx_1 dx_2$$

$$\begin{aligned}
&= \int\int K(t_1)K(t_2)e^{2\pi i(\frac{1}{2}(u_1-u_2)t_1+\frac{1}{2}(u_1+u_2)t_2)}\frac{dt_1dt_2}{2} \\
&= \frac{1}{2}\int K(t_1)e^{2\pi i\frac{1}{2}(u_1-u_2)t_1}dt_1\int K(t_2)e^{2\pi i\frac{1}{2}(u_1+u_2)t_2}dt_2 \\
&= \frac{1}{2}\chi_{[-\frac{1}{2},\frac{1}{2}]}(\frac{u_1-u_2}{2})\chi_{[-\frac{1}{2},\frac{1}{2}]}(\frac{u_1+u_2}{2}) \\
&= \frac{1}{2}I(u_1-u_2)I(u_1+u_2), \qquad (5.16)
\end{aligned}$$

where I is the characteristic function of $[-1,1]$. If $|u_1|+|u_2|>1$, the above vanishes; I is symmetric, and either u_1-u_2 or u_1+u_2 is $\pm(|u_1|+|u_2|)$. If $|u_1|+|u_2|\leq 1$, the above is 1. Hence

$$\widehat{T_3}(u_1,u_2)=\frac{1}{2}, \quad |u_1|+|u_2|\leq 1 \qquad (5.17)$$

Collecting the pieces we obtain (for $|u_1|+|u_2|\leq 1$)

$$\begin{aligned}
\widehat{W_{2,\epsilon}}(u) &= \widehat{T_-}(u_1,u_2)+\epsilon^2\widehat{T_+}(u_1,u_2)+2\epsilon\widehat{T_3}(u_1,u_2) \\
&= \delta(-u_1+u_2)\Big(1-|u_1|\Big)+\epsilon^2\delta(u_1+u_2)\Big(1-|u_1|\Big)+\epsilon. \qquad (5.18)
\end{aligned}$$

We have proved

Lemma 5.6 (Expansion for $\widehat{W_{2,\epsilon}}(u)$) *Let $K(y)=\frac{\sin\pi y}{\pi y}$, $K_\epsilon(x,y)=K(x-y)+\epsilon K(x+y)$, $\epsilon=\pm1$, and $W_{2,\epsilon}(x)=\boldsymbol{det}(K_\epsilon(x_i,x_j))$. For $|u_1|+|u_2|\leq 1$ we have*

$$\begin{aligned}
\widehat{W_{2,\epsilon}}(u) &= \widehat{W_{2,\epsilon,a}}(u)-\widehat{W_{2,\epsilon,b}}(u) \\
&= \delta(u_1)\delta(u_2)+\frac{\epsilon}{2}I(u_1)\delta(u_2)+\frac{\epsilon}{2}\delta(u_1)I(u_2)+\frac{\epsilon^2}{4}I(u_1)I(u_2)+ \\
&\quad \delta(-u_1+u_2)\Big(|u_1|-1\Big)+\epsilon^2\delta(u_1+u_2)\Big(|u_1|-1\Big)-\epsilon \qquad (5.19)
\end{aligned}$$

By duality, $\int\int f_1(x_1)f_2(x_2)W_{2,\epsilon}(x)dx_1dx_2 = \int\int\widehat{f_1}(u_1)\widehat{f_2}(u_2)\widehat{W_{2,\epsilon}}(u)du_1du_2$. Note (since f_i is even)

$$\int\int\widehat{f_1}(u_1)\widehat{f_2}(u_2)\delta(\pm u_1+u_2)\Big(|u_1|-1\Big)du_1du_2=\int(|u|-1)\widehat{f_1}(u)\widehat{f_2}(u)du. \qquad (5.20)$$

We simplify $\int \widehat{f_1}(u)\widehat{f_2}(u)du$. By duality (for even functions)

$$\begin{aligned}
\int \widehat{f_1}(u)\widehat{f_2}(u)du &= \int f_1(x)f_2(x)dx \\
&= \int (f_1f_2)(x)dx \\
&= \widehat{f_1f_2}(0). \qquad (5.21)
\end{aligned}$$

Therefore, for even functions of the form $f_1(x_1)f_2(x_2)$ whose Fourier Transforms are supported in $|u_1|+|u_2| \leq 1$,

Lemma 5.7

$$\begin{aligned}
\int\int f_1(x_1)f_2(x_2)W_{2,\epsilon}(x)dx &= \widehat{f_1}(0)\widehat{f_2}(0) + \frac{\epsilon}{2}f_1(0)\widehat{f_2}(0) + \frac{\epsilon}{2}\widehat{f_1}(0)f_2(0) + \frac{\epsilon^2}{4}f_1(0)f_2(0) \\
&\quad + (1+\epsilon^2)\int(|u|-1)\widehat{f_1}(u)\widehat{f_2}(u)du - \epsilon f_1(0)f_2(0) \\
&= \Big[\widehat{f_1}(0)+\frac{\epsilon}{2}f_1(0)\Big]\Big[\widehat{f_2}(0)+\frac{\epsilon}{2}f_2(0)\Big] + \\
&\quad (1+\epsilon^2)\int |u|\widehat{f_1}(u)\widehat{f_2}(u)du \\
&\quad -(1+\epsilon^2)\widehat{f_1f_2}(0) - \epsilon f_1(0)f_2(0). \qquad (5.22)
\end{aligned}$$

5.4 2-Level Densities

We calculate the pieces needed to evaluate the densities (Equation 5.1). We calculate $\sum_{k=1}^{2}\delta(x_k)\mathbf{det}(K_{-1}(x_i,x_j))_{i,j\neq k}$; we've already calculated $W_{2,\epsilon}(x) = \mathbf{det}(K_\epsilon(x_i,x_j))$.

$$\begin{aligned}
(W_{2,\mathrm{O}^-})_2(x) &= \sum_{k=1}^{2}\delta(x_k)\mathbf{det}(K_{-1}(x_i,x_j))_{i,j\neq k} \\
&= \delta(x_1)K_{-1}(x_2,x_2) + \delta(x_2)K_1(x_1,x_1) \\
&= \delta(x_1)\Big(1-K(2x_2)\Big) + \delta(x_2)\Big(1-K(2x_1)\Big) \\
&= \delta(x_1)+\delta(x_2)-\delta(x_1)K(2x_2)-\delta(x_2)K(2x_1) \\
&= \delta(x_1)1(x_2)+1(x_1)\delta(x_2)-\delta(x_1)K(2x_2)-K(2x_1)\delta(x_2) \\
(\widehat{W_{2,\mathrm{O}^-}})_2(u) &= 1(u_1)\delta(u_2)+\delta(u_1)1(u_2)-\frac{1}{2}1(u_1)I(u_2)-\frac{1}{2}I(u_1)1(u_2).
\end{aligned}$$

$$(5.23)$$

We determine the effect of $(\widehat{W_{2,\mathrm{O}^-}})_2(u)$ on $\widehat{f_1}(u_1)\widehat{f_2}(u_2)$ when $|u_1|+|u_2|<1$.

$$\begin{aligned}\int\int \widehat{f_1}(u_1)\widehat{f_2}(u_2)(\widehat{W_{2,\mathrm{O}^-}})_2(u) &= \int\int \widehat{f_1}(u_1)\widehat{f_2}(u_2)1(u_1)\delta(u_2) + \int\int \widehat{f_1}(u_1)\widehat{f_2}(u_2)\delta(u_1)1(u_2)\\ &\quad -\frac{1}{2}\int\int \widehat{f_1}(u_1)\widehat{f_2}(u_2)1(u_1)I(u_2)\\ &\quad -\frac{1}{2}\int\int \widehat{f_1}(u_1)\widehat{f_2}(u_2)I(u_1)1(u_2)\\ &= f_1(0)\widehat{f_2}(0)+\widehat{f_1}(0)f_2(0)-\frac{1}{2}f_1(0)f_2(0)-\frac{1}{2}f_1(0)f_2(0)\\ &= f_1(0)\widehat{f_2}(0)+\widehat{f_1}(0)f_2(0)-f_1(0)f_2(0). \qquad (5.24)\end{aligned}$$

Theorem 5.8 ($\mathcal{G}=$ SO(even), O, or SO(odd)) *Let $c(\mathcal{G})=0, \frac{1}{2}, 1$ for $\mathcal{G}=$ SO(even), O, SO(odd). For even functions supported in $|u_1|+|u_2|<1$*

$$\begin{aligned}\int\int \widehat{f_1}(u_1)\widehat{f_2}(u_2)\widehat{W_{2,\mathcal{G}}}(u)du_1du_2 &= \left[\widehat{f_1}(0)+\frac{1}{2}f_1(0)\right]\left[\widehat{f_2}(0)+\frac{1}{2}f_2(0)\right]\\ &\quad + 2\int |u|\widehat{f_1}(u)\widehat{f_2}(u)du - 2\widehat{f_1f_2}(0)-f_1(0)f_2(0)\\ &\quad + c(\mathcal{G})f_1(0)f_2(0). \qquad (5.25)\end{aligned}$$

*For arbitrarily small support, the three 2-level densities differ. One increases by a factor of $\frac{1}{2}f_1(0)f_2(0)$ moving from $\widehat{W_{2,\mathrm{O}^+}}$ to $\widehat{W_{2,O}}$ to $\widehat{W_{2,\mathrm{O}^-}}$. Therefore, the 2-level density, for test functions with arbitrarily small support, **is** sensitive enough to distinguish SO(even), O, and SO(odd).*

Define $\widehat{W_{2,\mathcal{D}}}$ as the common density component for the three orthogonal groups. Then

$$\begin{aligned}\int\int \widehat{f_1}(u_1)\widehat{f_2}(u_2)\widehat{W_{2,\mathcal{G}}}(u)du_1du_2 &= \int\int \widehat{f_1}(u_1)\widehat{f_2}(u_2)\widehat{W_{2,\mathcal{D}}}(u)du_1du_2\\ &\quad + c(\mathcal{G})f_1(0)f_2(0). \qquad (5.26)\end{aligned}$$

To determine the density for Sp, we use Lemma 5.7 with $\epsilon=-1$. Rewriting the result in a similar form as the orthogonal densities yields

Theorem 5.9 ($\mathcal{G}=Sp$)

$$\begin{aligned}\int\int \widehat{f_1}(u_1)\widehat{f_2}(u_2)\widehat{W_{2,Sp}}(u)du_1du_2 &= \left[\widehat{f_1}(0)+\frac{1}{2}f_1(0)\right]\left[\widehat{f_2}(0)+\frac{1}{2}f_2(0)\right]\\ &\quad + 2\int |u|\widehat{f_1}(u)\widehat{f_2}(u)du - 2\widehat{f_1f_2}(0)-f_1(0)f_2(0)\\ &\quad -f_1(0)\widehat{f_2}(0)-\widehat{f_1}(0)f_2(0)+2f_1(0)f_2(0). \qquad (5.27)\end{aligned}$$

To calculate $W_{2,U}(x)$, we need to take the determinant of

$$\begin{pmatrix} 1 & \frac{\sin\pi(x_1-x_2)}{\pi(x_1-x_2)} \\ \frac{\sin\pi(x_1-x_2)}{\pi(x_1-x_2)} & 1 \end{pmatrix} \tag{5.28}$$

Thus we need the Fourier Transform of $1-\left(\frac{\sin\pi(x_1-x_2)}{\pi(x_1-x_2)}\right)^2$. We find

Theorem 5.10 **(**$\mathcal{G}=U$**)**

$$\widehat{W_{2,U}}(u) = \delta(u_1,u_2) - \delta(u_1+u_2)\Big(1-|u_1|\Big). \tag{5.29}$$

Thus

$$\int\int \widehat{f_1}(u_1)\widehat{f_2}(u_2)\widehat{W_{2,U}}du_1du_2 \quad = \quad \widehat{f_1}(0)\widehat{f_2}(0) + \int|u|\widehat{f_1}(u)\widehat{f_2}(u)du - \widehat{f_1f_2}(0). \tag{5.30}$$

Thus, for test functions with arbitrarily small support, the 2-level densities for the classical compact groups are mutually distinguishable.

6 1- and 2-Level Densities for Families of Elliptic Curves

For $i = 1$ and 2, let f_i be an even Schwartz function whose Fourier Transform is supported in $(-\sigma_i, \sigma_i)$ and $f(x_1, x_2) = f_1(x_1)f_2(x_2)$. $\widehat{f}(u_1, u_2) = \widehat{f_1}(u_1)\widehat{f_2}(u_2)$. We recall the Explicit Formula (Theorem A.29) for an elliptic curve E with conductor N_E, which relates sums over zeros to sums over primes:

$$\begin{aligned}
\sum_{\gamma_E^{(j)}} G\Big(\gamma_E^{(j)} \frac{\log N_E}{2\pi}\Big) &= \widehat{G}(0) + G(0) - 2\sum_p \frac{\log p}{\log N_E}\frac{1}{p}\widehat{G}\Big(\frac{\log p}{\log N_E}\Big)a_E(p) \\
&\quad -2\sum_p \frac{\log p}{\log N_E}\frac{1}{p^2}\widehat{G}\Big(\frac{2\log p}{\log N_E}\Big)a_E^2(p) \\
&\quad +O\Big(\frac{\log\log N_E}{\log N_E}\Big). \qquad (6.1)
\end{aligned}$$

6.1 1-Level Density: $D_{1,\mathcal{F}}(f)$

$$\begin{aligned}
D_{1,\mathcal{F}}(f) &= \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\sum_{\gamma_E^{(j)}} f_1\Big(\gamma_E^{(j)}\frac{\log N_E}{2\pi}\Big) \\
&= \widehat{f_1}(0) + f_1(0) - 2\sum_p \frac{1}{p}\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\frac{\log p}{\log N_E}\widehat{f_1}\Big(\frac{\log p}{\log N_E}\Big)a_E(p) \\
&\quad -2\sum_p \frac{1}{p^2}\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\frac{\log p}{\log N_E}\widehat{f_1}\Big(\frac{2\log p}{\log N_E}\Big)a_E^2(p) \\
&\quad +O\Big(\frac{\log\log N_E}{\log N_E}\Big). \qquad (6.2)
\end{aligned}$$

By Rosen-Silverman ([RS], see Lemma B.9), for rational elliptic surfaces the first sum would be $rf_1(0) + o(1)$, where r is the rank of the elliptic curve over $\mathbb{Q}(t)$, if the conductors were constant. For families with non-constant $j(t)$, if the conductors were constant Michel's Theorem (Theorem 2.4) and Corollary B.3 would show the second sum contributes $-\frac{1}{2}f_1(0) + O(\frac{1}{\log N})$. This is similar to the universality Rudnick and Sarnak [RS] found. The difficult part of our proof is handling the conductor dependence.

As the 1-level density calculations are sub-calculations which arise in the 2-level investigations, we postpone their proofs for now.

6.2 2-Level Density: $D_{2,\mathcal{F}}(f)$ and $D^*_{2,\mathcal{F}}(f)$

Recall the 2-level density $D_{2,\mathcal{F}}(f)$ is the sum over all indices j_1, j_2 with $j_1 \neq \pm j_2$.

Definition 6.1 *$D^*_{2,\mathcal{F}}(f)$ differs from the 2-level density $D_{2,\mathcal{F}}(f)$ in that j_1 may equal $\pm j_2$.*

We first calculate $D^*_{2,\mathcal{F}}(f)$, and then subtract off the contribution from $j_1 = \pm j_2$. Assuming GRH, we may write the zeros as $1 + i\gamma^{(j)}$, with $\gamma^{(j)} = -\gamma^{(-j)}$.

$$\begin{aligned}
D^*_{2,\mathcal{F}}(f) &= \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\sum_{j_1}\sum_{j_2} f_1(L\gamma_E^{(j_1)})f_2(L\gamma_E^{(j_2)}) \\
&= \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\prod_{i=1}^{2}\Bigg[\widehat{f_i}(0) + f_i(0) - 2\sum_{p_i}\frac{\log p_i}{\log N_E}\frac{1}{p_i}\widehat{f_i}\Big(\frac{\log p_i}{\log N_E}\Big)a_E(p_i) \\
&\qquad -2\sum_{p_i}\frac{\log p_i}{\log N_E}\frac{1}{p_i^2}\widehat{f_i}\Big(2\frac{\log p_i}{\log N_E}\Big)a_E^2(p_i) + O\Big(\frac{\log\log N_E}{\log N_E}\Big)\Bigg] \\
&= \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\prod_{i=1}^{2}\Bigg[\widehat{f_i}(0) + f_i(0) + S_{i,1} + S_{i,2}\Bigg] \qquad (6.3)
\end{aligned}$$

We use Theorem E.1 to drop the error terms, as they do not contribute in the limit as $|\mathcal{F}| \to \infty$. The astute reader will notice Theorem E.1 requires us to know the 1-level density, and we have postponed that calculation; however, in the process of calculating the 2-level density we will determine the needed sums for the 1-level density (without using Theorem E.1 to evaluate them). Thus, there is no harm in removing the error terms

There are five types of sums we need to investigate: $\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{i,1}$, $\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{i,2}$, $\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{1,1}S_{2,1}$, $\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{1,2}S_{2,2}$, and $\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{i,1}S_{j,2}$ $(i \neq j)$. In $S_{\alpha,\beta}$, the α refers to which prime (p_1 or p_2), and β the power of $a_E(p_\alpha)$ (1 or 2). The first and the second are what we need to calculate the one-level densities. We find

Lemma 6.2

$$\begin{aligned}
D^*_{2,\mathcal{F}}(f) &= \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\prod_{i=1}^{2}\Bigg[\widehat{f_i}(0) + f_i(0) + S_{i,1} + S_{i,2}\Bigg] \\
&= \prod_{i=1}^{2}\Bigg[\widehat{f_i}(0) + f_i(0)\Bigg] + \\
&\quad \Bigg[\widehat{f_1}(0) + f_1(0)\Bigg]\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{2,1} + \Bigg[\widehat{f_2}(0) + f_2(0)\Bigg]\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{1,1} + \\
&\quad \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{1,1}S_{2,1} +
\end{aligned}$$

$$\left[\widehat{f_1}(0)+f_1(0)\right]\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}S_{2,2}+\left[\widehat{f_2}(0)+f_2(0)\right]\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}S_{1,2}+$$
$$\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}S_{1,1}S_{2,2}+\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}S_{1,2}S_{2,1}+\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}S_{1,2}S_{2,2}. \tag{6.4}$$

6.2.1 $j_1 = \pm j_2$

Let $\rho = 1 + i\gamma_E^{(j)}$ be a zero. For a curve with even functional equation, we may label the zeros by

$$\cdots \leq \gamma_E^{(-2)} \leq \gamma_E^{(-1)} \leq 0 \leq \gamma_E^{(1)} \leq \gamma_E^{(2)} \leq \cdots, \gamma_E^{(-k)} = -\gamma_E^{(k)}, \tag{6.5}$$

while for a curve with odd functional equation we label the zeros by

$$\cdots \leq \gamma_E^{(-1)} \leq 0 \leq \gamma_E^{(0)} = 0 \leq \gamma_E^{(1)} \leq \cdots, \gamma_E^{(-k)} = -\gamma_E^{(k)}. \tag{6.6}$$

We isolate from $D^*_{2,\mathcal{F}}(f)$ the contribution from $j_1 = j_2$. By the Explicit Formula, Theorem A.29, these terms contribute

$$\begin{aligned}
D^*_{2,\mathcal{F},=}(f) &= \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\sum_j (f_1f_2)\Big(\frac{\log N_E}{2\pi}\gamma_E^{(j)}\Big) \\
&= \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\Bigg[\widehat{f_1f_2}(0)+(f_1f_2)(0)-2\sum_p\frac{\log p}{\log N_E}\frac{1}{p}\widehat{f_1f_2}\Big(\frac{\log p}{\log N_E}\Big)a_E(p) \\
&\quad -2\sum_p\frac{\log p}{\log N_E}\frac{1}{p^2}\widehat{f_1f_2}\Big(\frac{2\log p}{\log N_E}\Big)a_E^2(p)+O\Big(\frac{\log\log N_E}{\log N_E}\Big)\Bigg] \\
&= D_{1,\mathcal{F}}(f_1f_2).
\end{aligned} \tag{6.7}$$

We want to exclude $j_1 = \pm j_2$, and not just $j_1 = j_2$. If an elliptic curve has even functional equation, j_i ranges over all non-zero integers, and $\gamma_E^{(-j)} = -\gamma_E^{(j)}, j \neq -j$. Since our functions are even, the sum over all pairs (j_1, j_2) with $j_1 = \pm j_2$ is twice the sum over all pairs (j, j).

If an elliptic curve has odd functional equation, j_i ranges over all integers. The curve vanishes to odd order at the critical point $s = 1$. Except for one zero (labeled $\gamma_E^{(0)}$), for every non-zero j, $\gamma_E^{(-j)} = -\gamma_E^{(j)}$, and $j \neq -j$. Here the sum over all pairs (j_1, j_2) with $j_1 = \pm j_2$ is not twice the sum over all pairs (j, j).

Consider for simplicity a curve with odd functional equation and three zeros, labeled by $j = -1, 0$ and 1. Summing over $(j_1 = j_2)$ gives three pairs: $(-1,-1), (0,0), (1,1)$. Twice this sum is equivalent to summing over the following six pairs: $(-1,-1), (-1,1), (0,0), (0,0), (1,-1), \ (1,1)$. The sum over $j_1 = \pm j_2$ gives five pairs: $(-1,-1), (-1,1), (0,0), (1,-1), (1,1)$. The sum over $(j_1, j_2), j_1 = \pm j_2$ differs from twice the sum over (j, j) by counting $(0,0)$ once, not twice.

For odd functional equation, twice the sum over pairs (j, j) minus the contribution from the pair $(0,0)$ equals the sum over all pairs (j_1, j_2), $j_1 = \pm j_2$.

Let $\epsilon_E = \pm 1$ be the sign of the functional equation for E. We have shown

Lemma 6.3

$$\sum_{j_1 = \pm j_2} (f_1 f_2)\Big(\frac{\log N_E}{2\pi}\gamma_E^{(j_1)}\Big) \quad = \quad 2\sum_j (f_1 f_2)\Big(\frac{\log N_E}{2\pi}\gamma_E^{(j)}\Big) - \frac{1-\epsilon_E}{2}(f_1 f_2)(0). \tag{6.8}$$

Summing over all $E \in \mathcal{F}$ yields

Lemma 6.4

$$\begin{aligned} D^*_{2,\mathcal{F},\pm}(f) &= \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\sum_{j_1=\pm j_2}(f_1 f_2)\Big(\frac{\log N_E}{2\pi}\gamma_E^{(j_1)}\Big) \\ &= 2D^*_{2,\mathcal{F},=}(f) - \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\frac{1-\epsilon_E}{2}(f_1 f_2)(0) \\ &= 2D_{1,\mathcal{F}}(f_1 f_2) - (f_1 f_2)(0)\frac{1}{|\mathcal{F}|}\sum_{\substack{E\in\mathcal{F} \\ \epsilon_E=-1}} 1. \end{aligned} \tag{6.9}$$

6.2.2 2-Level Density Expansion

Recall the 2-level density $D_{2,\mathcal{F}}(f)$ equals $D^*_{2,\mathcal{F}}(f) - D^*_{2,\mathcal{F},\pm}(f)$.

Definition 6.5 $N(\mathcal{F}, -1) = \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\frac{1-\epsilon_E}{2}$*, ie, the percent of curves with odd sign.*

We have shown

Lemma 6.6 (2-Level Density Expansion)

$$\begin{aligned} D_{2,\mathcal{F}}(f) &= D^*_{2,\mathcal{F}}(f) - 2D_{1,\mathcal{F}}(f_1 f_2) + (f_1 f_2)(0)N(\mathcal{F}, -1) \\ &= \prod_{i=1}^{2}\Big[\widehat{f_i}(0) + f_i(0)\Big] \end{aligned}$$

$$
\begin{aligned}
&+ \Big[\widehat{f_1}(0)+f_1(0)\Big]\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{2,1} + \Big[\widehat{f_2}(0)+f_2(0)\Big]\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{1,1}\\
&+ \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{1,1}S_{2,1}\\
&+ \Big[\widehat{f_1}(0)+f_1(0)\Big]\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{2,2} + \Big[\widehat{f_2}(0)+f_2(0)\Big]\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{1,2}\\
&+ \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{1,1}S_{2,2} + \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{1,2}S_{2,1} + \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{1,2}S_{2,2}\\
&- 2D_{1,\mathcal{F}}(f_1f_2) + (f_1f_2)(0)N(\mathcal{F},-1) + O\Big(\frac{\log\log N}{\log N}\Big). \qquad (6.10)
\end{aligned}
$$

To evaluate the above, we only need to know the percent of curves with odd sign; we do not need to know which *curves are even or odd. This is very different from the* 3 *and higher level densities, where we will have to execute sums over the subset of curves with odd sign.*

6.3 Useful Expansion for the 1- and 2-Level Densities for One Parameter Families

Let $\mathcal{E}$ denote a one-parameter family of elliptic curves, $t \in [N, 2N]$, over $\mathbb{Q}(t)$, and $\mathcal{F}$ denote a sub-family of $\mathcal{E}$. In the applications, $\mathcal{F}$ will be obtained by sieving to $D(t)$ good, where $D(t)$ is the product of the irreducible polynomial factors of $\Delta(t)$.

6.3.1 Needed Prime Sums

Lemma 6.7 (Prime Sums) *Let $C(N)$ be a power of N. By Lemmas B.2, B.3 and B.4,*

1. $\sum_p \frac{\log p}{\log C(N)}\frac{1}{p}\widehat{f_1}\Big(\frac{\log p}{\log C(N)}\Big) = \frac{1}{2}f_1(0) + O\Big(\frac{1}{\log N}\Big)$
2. $\sum_p \frac{\log p}{\log C(N)}\frac{1}{p}\widehat{f_1}\Big(2\frac{\log p}{\log C(N)}\Big) = \frac{1}{4}f_1(0) + O\Big(\frac{1}{\log N}\Big)$
3. $\sum_p \frac{\log^2 p}{\log^2 C(N)}\frac{1}{p}\widehat{f_1}\widehat{f_2}\Big(\frac{\log p}{\log C(N)}\Big) = \frac{1}{2}\int_{-\infty}^{\infty}|u|\widehat{f_1}(u)\widehat{f_2}(u)du + O\Big(\frac{1}{\log N}\Big)$

If instead we are summing over primes congruent to a mod m, we use Lemma B.1 and B.5 and the right-hand sides are modified by $\frac{1}{\varphi(m)}$.

6.3.2 Expansions of Sums

We use the expansion from Lemma 6.6. Recall

$$S_{i,j} \quad = \quad -2\sum_{p_i} \frac{\log p_i}{\log C(t)} \frac{1}{p_i^j} \widehat{f}_i\Big(2^{j-1}\frac{\log p_i}{\log C(t)}\Big) a_t^j(p_i). \tag{6.11}$$

In $S_{i,j}$, i refers to the prime (p_1, p_2) and j refers to the power of $a_t(p)$ $(a_t(p), a_t^2(p))$. The 1-level density $D_{1,\mathcal{F}}(f_1)$ is

$$D_{1,\mathcal{F}}(f) \quad = \quad \widehat{f}_1(0) + f_1(0) + \frac{1}{|\mathcal{F}|}\sum_{t\in\mathcal{F}} S_{1,1} + \frac{1}{|\mathcal{F}|}\sum_{t\in\mathcal{F}} S_{1,2} + O\Big(\frac{\log\log N_E}{\log N_E}\Big). \tag{6.12}$$

To determine the 1- and 2-level densities, there are eight sums over $t \in \mathcal{F}$ to evaluate:

1. $\frac{1}{|\mathcal{F}|}\sum_{t\in\mathcal{F}} S_{1,1}$ and $\frac{1}{|\mathcal{F}|}\sum_{t\in\mathcal{F}} S_{2,1}$

2. $\frac{1}{|\mathcal{F}|}\sum_{t\in\mathcal{F}} S_{1,2}$ and $\frac{1}{|\mathcal{F}|}\sum_{t\in\mathcal{F}} S_{2,2}$

3. $\frac{1}{|\mathcal{F}|}\sum_{t\in\mathcal{F}} S_{1,1}S_{2,2}$ and $\frac{1}{|\mathcal{F}|}\sum_{t\in\mathcal{F}} S_{2,1}S_{1,2}$

4. $\frac{1}{|\mathcal{F}|}\sum_{t\in\mathcal{F}} S_{1,1}S_{2,1}$

5. $\frac{1}{|\mathcal{F}|}\sum_{t\in\mathcal{F}} S_{1,2}S_{2,2}$.

We have written the sums in pairs where the two sums are handled similarly. Substituting the definitions leads to five types of sums:

1. $-2\sum_p \frac{1}{p}\frac{1}{|\mathcal{F}|}\sum_{t\in\mathcal{F}} \frac{\log p}{\log C(t)} \widehat{f}_1\Big(\frac{\log p}{\log C(t)}\Big) a_t(p)$

2. $-2\sum_p \frac{1}{p^2}\frac{1}{|\mathcal{F}|}\sum_{t\in\mathcal{F}} \frac{\log p}{\log C(t)} \widehat{f}_1\Big(2\frac{\log p}{\log C(t)}\Big) a_t^2(p)$

3. $4\sum_{p_1}\sum_{p_2} \frac{1}{p_1 p_2^2}\frac{1}{|\mathcal{F}|}\sum_{t\in\mathcal{F}} \frac{\log p_1}{\log C(t)}\frac{\log p_2}{\log C(t)} \widehat{f}_1\Big(\frac{\log p}{\log C(t)}\Big)\widehat{f}_2\Big(2\frac{\log p}{\log C(t)}\Big) a_t(p_1)a_t^2(p_2)$

4. $4\sum_{p_1}\sum_{p_2} \frac{1}{p_1 p_2}\frac{1}{|\mathcal{F}|}\sum_{t\in\mathcal{F}} \frac{\log p_1}{\log C(t)}\frac{\log p_2}{\log C(t)} \widehat{f}_1\Big(\frac{\log p}{\log C(t)}\Big)\widehat{f}_2\Big(\frac{\log p}{\log C(t)}\Big) a_t(p_1)a_t(p_2)$

5. $4\sum_{p_1}\sum_{p_2} \frac{1}{p_1^2 p_2^2}\frac{1}{|\mathcal{F}|}\sum_{t\in\mathcal{F}} \frac{\log p_1}{\log C(t)}\frac{\log p_2}{\log C(t)} \widehat{f}_1\Big(2\frac{\log p}{\log C(t)}\Big)\widehat{f}_2\Big(2\frac{\log p}{\log C(t)}\Big) a_t^2(p_1)a_t^2(p_2)$

In the above sums, we use Lemma B.8 to restrict to primes greater than $\log^l N$, $l < 2$. Label the five sums $\frac{1}{|\mathcal{F}|}\sum_{t\in\mathcal{F}} S(t;p)$ by $T_k(p)$ and $T_k(p_1, p_2)$. Trivially by Hasse some of the above do not contribute.

In the third sum, if $p_1 = p_2 = p$, we get $\ll \frac{1}{\log N}\sum_p \frac{p^{\frac{3}{2}}\log p}{p^3} = O(\frac{1}{\log N})$. In the second sum, we get $\ll \frac{1}{\log N}\sum_p \frac{p\log p}{p^2} = O(1)$. In the fifth sum, if $p_1 = p_2 = p$ we get $\ll \frac{1}{\log N}\sum_p \frac{p^2\log p}{p^4}$ $= O(\frac{1}{\log N})$.

Thus, we only study the third and fifth sums when $p_1 \neq p_2$. The fourth sum has the potential to contribute when $p_1 = p_2$. Hence we break it into two cases: $p_1 \neq p_2$ and $p_1 = p_2$.

6.3.3 Conditions on the Family to Evaluate the Sums

Conditions on the Family $\mathcal{F}$ (6.13)

Let $T_k(p)$ and $T_k(p_1,p_2)$ $(= \frac{1}{|\mathcal{F}|}\sum_{t\in\mathcal{F}} S(t;p)$) equal

1. $\frac{\log p}{\log C(N)}\widehat{f}_1\Big(\frac{\log p}{\log C(N)}\Big)\Bigg[-r + O\Big(p^{-\alpha} + \frac{p^\beta}{|\mathcal{F}|} + \frac{1}{\log^\gamma N}\Big)\Bigg]$

2. $\frac{\log p}{\log C(N)}\widehat{f}_1\Big(2\frac{\log p}{\log C(N)}\Big)\Bigg[p + O\Big(p^{1-\alpha} + \frac{p^\beta}{|\mathcal{F}|} + \frac{p}{\log^\gamma N}\Big)\Bigg]$

3. $\frac{\log p_1}{\log C(N)}\frac{\log p_2}{\log C(N)}\widehat{f}_1\Big(\frac{\log p_1}{\log C(N)}\Big)\widehat{f}_2\Big(2\frac{\log p_2}{\log C(N)}\Big)\Bigg[-rp_2 + O\Big(p_1^{-\alpha_1}p_2^{1-\alpha_2} + \frac{p_1^{\beta_1}p_2^{\beta_2}}{|\mathcal{F}|} + \frac{p_2}{\log^\gamma N}\Big)\Bigg]$

4. (a) $\frac{\log p_1}{\log C(N)}\frac{\log p_2}{\log C(N)}\widehat{f}_1\Big(\frac{\log p_1}{\log C(N)}\Big)\widehat{f}_2\Big(\frac{\log p_2}{\log C(N)}\Big)\Bigg[r^2 + O\Big(p_1^{1-\alpha_1}p_2^{1-\alpha_2} + \frac{p_1^{\beta_1}p_2^{\beta_2}}{|\mathcal{F}|} + \frac{1}{\log^\gamma N}\Big)\Bigg]$ if $p_1 \neq p_2$

   (b) $\frac{\log^2 p}{\log^2 C(N)}\widehat{f}_1\widehat{f}_2\Big(\frac{\log p}{\log C(N)}\Big)\Bigg[p + O\Big(p^{1-\alpha} + \frac{p^\beta}{|\mathcal{F}|} + \frac{p}{\log^\gamma N}\Big)\Bigg]$ if $p_1 = p_2 = p$

5. $\frac{\log p_1}{\log C(N)}\frac{\log p_2}{\log C(N)}\widehat{f}_1\Big(2\frac{\log p_1}{\log C(N)}\Big)\widehat{f}_1\Big(2\frac{\log p_2}{\log C(N)}\Big)\Bigg[p_1p_2 + O\Big(p_1^{1-\alpha_1}p_2^{1-\alpha_2} + \frac{p_1^{\beta_1}p_2^{\beta_2}}{|\mathcal{F}|} + \frac{p_1p_2}{\log^\gamma N}\Big)\Bigg]$

where $\alpha, \beta, \gamma > 0$, $\alpha_i, \beta_i \geq 0$ and whenever two α_i or β_i occur, at least one is positive.

By Lemma 6.7 we can evaluate the eight $S_{i,j}$ sums for a family satisfying Conditions 6.13:

Lemma 6.8 ($S_{i,j}$ Sums) *If the family satisfies Conditions 6.13, then (up to lower order terms which do not contribute for small support),*

1. $\frac{1}{|\mathcal{F}|}\sum_{t\in\mathcal{F}} S_{i,1} = rf_i(0)$

2. $\frac{1}{|\mathcal{F}|}\sum_{t\in\mathcal{F}} S_{i,2} = -\frac{1}{2}f_i(0)$

3. $\frac{1}{|\mathcal{F}|}\sum_{t\in\mathcal{F}} S_{1,1}S_{2,2} + S_{2,1}S_{1,2} = -\frac{1}{2}rf_1(0)f_2(0) + -\frac{1}{2}rf_1(0)f_2(0)$

4. $\frac{1}{|\mathcal{F}|}\sum_{t\in\mathcal{F}} S_{1,1}S_{2,1} = r^2 f_1(0)f_2(0) + 2\int_{-\infty}^{\infty}|u|\widehat{f_1}(u)\widehat{f_2}(u)du$

5. $\frac{1}{|\mathcal{F}|}\sum_{t\in\mathcal{F}} S_{1,2}S_{2,2} = \frac{1}{4}f_1(0)f_2(0)$

6.3.4 1- and 2-Level Densities, Assuming Certain Conditions on the Family

Substituting Lemma 6.8 into the 1- and 2-level density expansions we obtain

Lemma 6.9 (1- and 2-Level Densities) *Assume $|\mathcal{F}|$ is a positive multiple of N and $\mathcal{F}$ satisfies conditions 6.13. Up to lower order correction terms (which vanish as $|\mathcal{F}| \to \infty$), for even Schwartz functions with small support,*

$$D_{1,\mathcal{F}}(f) = \widehat{f_1}(0) + \frac{1}{2}f_1(0) + rf_1(0) \tag{6.14}$$

and

$$\begin{aligned} D_{2,\mathcal{F}}(f) &= \prod_{i=1}^{2}\left[\widehat{f_i}(0) + \frac{1}{2}f_i(0)\right] + 2\int_{-\infty}^{\infty}|u|\widehat{f_1}(u)\widehat{f_2}(u)du \\ &\quad -2\widehat{f_1f_2}(0) - f_1(0)f_2(0) + (f_1f_2)(0)N(\mathcal{F},-1) \\ &\quad +(r^2-r)f_1(0)f_2(0) + r\widehat{f_1}(0)f_2(0) + rf_1(0)\widehat{f_2}(0). \end{aligned} \tag{6.15}$$

If we have a one-parameter family, let $D_{1,\mathcal{F}}^{(r)}(f_1)$ and $D_{2,\mathcal{F}}^{(r)}(f_1)$ be the 1- and 2-level densities from the non-family zeros (ie, the contributions from the r family zeros have been removed). Then

$$D_{1,\mathcal{F}}^{(r)}(f_1) = \widehat{f_1}(0) + \frac{1}{2}f_1(0) \tag{6.16}$$

and

$$\begin{aligned} D_{2,\mathcal{F}}^{(r)}(f_1) &= \prod_{i=1}^{2}\left[\widehat{f_i}(0) + \frac{1}{2}f_i(0)\right] + 2\int_{-\infty}^{\infty}|u|\widehat{f_1}(u)\widehat{f_2}(u)du \\ &\quad -2\widehat{f_1f_2}(0) - f_1(0)f_2(0) + (f_1f_2)(0)N(\mathcal{F},-1). \end{aligned} \tag{6.17}$$

Thus, removing the contribution from the r family zeros, the 2-level density of the remaining zeros is SO(even) *if all curves are even, O if half are even and half odd, and* SO(odd) *if all are odd.*

Proof: The 1-level density is immediate from substitution. Substituting for the eight $S_{i,j}$ sums for $D_{2,\mathcal{F}}(f)$ yields (up to lower order terms which don't contribute for small support)

$$\begin{aligned}
D_{2,\mathcal{F}}(f) &= = \prod_{i=1}^{2}\left[\widehat{f}_i(0)+f_i(0)\right] \\
&\quad + \left[\widehat{f_1}(0)+f_1(0)\right] r f_2(0) + \left[\widehat{f_2}(0)+f_2(0)\right] r f_1(0) \\
&\quad + r^2 f_1(0)f_2(0) + 2\int_{-\infty}^{\infty}|u|\widehat{f_1}(u)\widehat{f_2}(u)du \\
&\quad + \left[\widehat{f_1}(0)+f_1(0)\right]\Big(-\frac{1}{2}f_2(0)\Big) + \left[\widehat{f_2}(0)+f_2(0)\right]\Big(-\frac{1}{2}f_1(0)\Big) \\
&\quad - \frac{1}{2}rf_1(0)f_2(0) - \frac{1}{2}rf_1(0)f_2(0) + \frac{1}{4}f_1(0)f_2(0) \\
&\quad - 2D_{1,\mathcal{F}}(f_1f_2) + (f_1f_2)(0)N(\mathcal{F},-1) + O\Big(\frac{\log\log N}{\log N}\Big) \\
&= \prod_{i=1}^{2}\left[\widehat{f}_i(0)+\frac{1}{2}f_i(0)\right] + 2\int_{-\infty}^{\infty}|u|\widehat{f_1}(u)\widehat{f_2}(u)du \\
&\quad + 2rf_1(0)f_2(0) + r\widehat{f_1}(0)f_2(0) + rf_1(0)\widehat{f_2}(0) - rf_1(0)f_2(0) + r^2 f_1(0)f_2(0) \\
&\quad - 2D_{1,\mathcal{F}}(f_1f_2) + (f_1f_2)(0)N(\mathcal{F},-1). \qquad (6.18)
\end{aligned}$$

Substituting

$$D_{1,\mathcal{F}}(f_1f_2) = \widehat{f_1f_2}(0) + \frac{1}{2}f_1(0)f_2(0) + rf_1(0)f_2(0) \qquad (6.19)$$

yields

$$\begin{aligned}
D_{2,\mathcal{F}}(f) &= \prod_{i=1}^{2}\left[\widehat{f}_i(0)+\frac{1}{2}f_i(0)\right] + 2\int_{-\infty}^{\infty}|u|\widehat{f_1}(u)\widehat{f_2}(u)du \\
&\quad + rf_1(0)f_2(0) + r\widehat{f_1}(0)f_2(0) + rf_1(0)\widehat{f_2}(0) + r^2 f_1(0)f_2(0) \\
&\quad - 2\widehat{f_1f_2}(0) - f_1(0)f_2(0) - 2rf_1(0)f_2(0) + (f_1f_2)(0)N(\mathcal{F},-1) \\
&= \prod_{i=1}^{2}\left[\widehat{f}_i(0)+\frac{1}{2}f_i(0)\right] + 2\int_{-\infty}^{\infty}|u|\widehat{f_1}(u)\widehat{f_2}(u)du \\
&\quad - 2\widehat{f_1f_2}(0) - f_1(0)f_2(0) + (f_1f_2)(0)N(\mathcal{F},-1) \\
&\quad + (r^2-r)f_1(0)f_2(0) + r\widehat{f_1}(0)f_2(0) + rf_1(0)\widehat{f_2}(0). \qquad (6.20)
\end{aligned}$$

If the family has rank r over $\mathbb{Q}(t)$, there is a natural interpretation of these terms. By the Birch and Swinnerton-Dyer conjecture (used only for interpretation purposes) and Silverman's

Specialization Theorem, for all t sufficiently large, each curve's L-function has at least r zeros at the critical point. We isolate the contributions from the r family zeros.

Let $L_t = \frac{\log C(t)}{2\pi}$. Recall the 1-level density is $D_{1,\mathcal{F}}(f) = \widehat{f}(0) + \frac{1}{2}f(0) + rf(0)$. Let j_i range over all zeros of a curve, and j_i' range over all but the r family zeros.

$$\begin{aligned}
D_{2,\mathcal{F}}(f) &= \frac{1}{|\mathcal{F}|}\sum_{t\in\mathcal{F}}\sum_{j_1}\sum_{j_2} f_1(L\gamma_E^{(j_1)})f_2(L_t\gamma_E^{(j_2)}) \\
&\quad - 2D_{1,\mathcal{F}}(f_1f_2) + (f_1f_2)(0)N(\mathcal{F},-1) \\
&= \frac{1}{|\mathcal{F}|}\sum_{t\in\mathcal{F}}\Big(rf_1(0) + \sum_{j_1'} f_1(L_t\gamma_E^{(j_1')})\Big)\Big(rf_2(0) + \sum_{j_2'} f_2(L_t\gamma_E^{(j_2')})\Big) \\
&\quad - 2D_{1,\mathcal{F}}(f_1f_2) + (f_1f_2)(0)N(\mathcal{F},-1) \\
&= \frac{1}{|\mathcal{F}|}\sum_{t\in\mathcal{F}}\sum_{j_1'}\sum_{j_2'} f_1(L_t\gamma_E^{(j_1')})f_2(L_t\gamma_E^{(j_2')}) \\
&\quad +rf_1(0)D_{1,\mathcal{F}}(f_2) + D_{1,\mathcal{F}}(f_1)rf_2(0) - r^2f_1(0)f_2(0) \\
&\quad -2D_{1,\mathcal{F}}(f_1f_2) + (f_1f_2)(0)N(\mathcal{F},-1) \\
&= \frac{1}{|\mathcal{F}|}\sum_{t\in\mathcal{F}}\sum_{j_1'}\sum_{j_2'} f_1(L_t\gamma_E^{(j_1')})f_2(L_t\gamma_E^{(j_2')}) + (f_1f_2)(0)N(\mathcal{F},-1) \\
&\quad +rf_1(0)\Big(\widehat{f_2}(0) + (r+\frac{1}{2})f_2(0)\Big) + \Big(\widehat{f_1}(0) + (r+\frac{1}{2})f_1(0)\Big)rf_2(0) \\
&\quad -r^2f_1(0)f_2(0) - 2\Big(\widehat{f_1f_2}(0) + \frac{1}{2}f_1(0)f_2(0) + rf_1(0)f_2(0)\Big) \\
&= \Bigg[\frac{1}{|\mathcal{F}|}\sum_{t\in\mathcal{F}}\sum_{j_1'}\sum_{j_2'} f_1(L_t\gamma_E^{(j_1')})f_2(L_t\gamma_E^{(j_2')}) \\
&\quad -2\Big(\widehat{f_1f_2}(0) + \frac{1}{2}f_1(0)f_2(0)\Big) + (f_1f_2)(0)N(\mathcal{F},-1)\Bigg] \\
&\quad +rf_1(0)\widehat{f_2}(0) + r\widehat{f_1}(0)f_2(0) + (r^2-r)f_1(0)f_2(0) \\
&= D_{2,\mathcal{F}}^{(r)}(f_1) + rf_1(0)\widehat{f_2}(0) + r\widehat{f_1}(0)f_2(0) + (r^2-r)f_1(0)f_2(0). \qquad (6.21)
\end{aligned}$$

We isolate

Lemma 6.10 *The contribution from r critical point zeros is*

$$rf_1(0)\widehat{f_2}(0) + r\widehat{f_1}(0)f_2(0) + (r^2-r)f_1(0)f_2(0). \qquad (6.22)$$

7 Sieving One Parameter Families to Calculate 1- and 2-Level Densities

7.1 Introduction

Let $\mathcal{E}$ be a one-parameter family of elliptic curves E_t with discriminants $\Delta(t)$ and conductors $C(t)$. For many families, we can evaluate the conductors exactly if we sieve to a subfamily $\mathcal{F}$ defined as the $t \in [N, 2N]$ with $D(t)$ good, where $D(t)$ is the product of the irreducible polynomial factors of $\Delta(t)$. Usually good will mean square-free, although occasionally it will mean square-free except for a fixed set of primes, and for these special primes, the power of $p|D(t)$ is independent of t.

Let our family $\mathcal{F}$ be the set of good $t \in [N, 2N]$ where the conductors are given by a monotone polynomial in t. We use this polynomial for the conductors at non-good t; this is permissible as these curves are not in our family, and do not originally appear in our sums.

For each d, let

$$E(d) = \{t \in [N, 2N] : d^2|D(t)\}. \tag{7.1}$$

Let $S(t)$ be some quantity associated to the elliptic curve E_t. For example, $S(t) = \frac{\log p}{\log C(t)}$ $F(\frac{\log p}{\log C(t)})a_t(p)$. Let $D(t) = a_k t^k + \cdots + a_0$, $a_k \geq 1$. Then

$$\sum_{\substack{t=N \\ D(t)\ good}}^{2N} S(t) = \sum_{d=1}^{(2a_k N)^{\frac{k}{2}}} \mu(d) \sum_{t \in E(d)} S(t). \tag{7.2}$$

In particular, setting $S(t) = 1$ yields the cardinality of the family:

$$|\mathcal{F}| = \sum_{\substack{t=N \\ D(t)\ good}}^{2N} 1. \tag{7.3}$$

In all the families we investigate, $|\mathcal{F}| = c_{\mathcal{F}} N + o(N)$, $c_{\mathcal{F}} > 0$.

Let $t_1(d), \dots, t_{\nu(d)}(d)$ be the incongruent roots of $D(t) \equiv 0 \bmod d^2$. The presence of $\mu(d)$ allows us to restrict to d square-free. For small d, we may take the $t_i(d) \in [N, N + d^2]$. For such d,

$$\sum_{t \in E(d)} S(t) = \sum_{i=1}^{\nu(d)} \sum_{t'=0}^{[N/d^2]} S\Big(t_i(d) + t'd^2\Big) \ + \ O\Big(\nu(d)||S||_\infty\Big). \tag{7.4}$$

The error piece is from boundary effects for the last value of t'. $E(d)$ restricts us to $t \in [N, 2N]$; as each $t_i(d) \geq N$, and at most one is exactly N, it is possible in summing to $t' = [N/d^2]$ we've added an extra term.

7.1.1 Assumptions for Sieving

We evaluate the sums under the following assumptions:

1. For square-free $D(t)$, the conductors $C(t)$ are given by a monotone polynomial in t.
2. A positive percent of $t \in [N, 2N]$ have $D(t)$ square-free; ie, $|\mathcal{F}| = c_{\mathcal{F}} N + o(N)$.

We constantly use Lemma 3.5, $\nu(d) \ll d^\epsilon$ for square-free d, as well as

$$\sum_{\substack{t=N \\ D(t) \ good}}^{2N} 1 \ = \ \sum_{d=1}^{\log^l N} \mu(d) \sum_{\substack{t=N \\ D(t) \equiv 0(d^2)}}^{2N} 1 \ + \ o(N) = c_{\mathcal{F}} N + o(N), \ c_{\mathcal{F}} > 0. \tag{7.5}$$

7.1.2 Sums to Sieve

We have five types of sums $c \sum_p \frac{1}{|\mathcal{F}|} \sum_{t \in \mathcal{F}} S(t;p)$ to evaluate:

1. $-2 \sum_p \frac{1}{p} \frac{1}{|\mathcal{F}|} \sum_{t \in \mathcal{F}} \frac{\log p}{\log C(t)} \widehat{f_1}\Big(\frac{\log p}{\log C(t)}\Big) a_t(p)$
2. $-2 \sum_p \frac{1}{p^2} \frac{1}{|\mathcal{F}|} \sum_{t \in \mathcal{F}} \frac{\log p}{\log C(t)} \widehat{f_1}\Big(2\frac{\log p}{\log C(t)}\Big) a_t^2(p)$
3. $4 \sum_{p_1} \sum_{p_2} \frac{1}{p_1 p_2^2} \frac{1}{|\mathcal{F}|} \sum_{t \in \mathcal{F}} \frac{\log p_1}{\log C(t)} \frac{\log p_2}{\log C(t)} \widehat{f_1}\Big(\frac{\log p}{\log C(t)}\Big) \widehat{f_2}\Big(2\frac{\log p}{\log C(t)}\Big) a_t(p_1) a_t^2(p_2)$
4. $4 \sum_{p_1} \sum_{p_2} \frac{1}{p_1 p_2} \frac{1}{|\mathcal{F}|} \sum_{t \in \mathcal{F}} \frac{\log p_1}{\log C(t)} \frac{\log p_2}{\log C(t)} \widehat{f_1}\Big(\frac{\log p}{\log C(t)}\Big) \widehat{f_2}\Big(\frac{\log p}{\log C(t)}\Big) a_t(p_1) a_t(p_2)$
5. $4 \sum_{p_1} \sum_{p_2} \frac{1}{p_1^2 p_2^2} \frac{1}{|\mathcal{F}|} \sum_{t \in \mathcal{F}} \frac{\log p_1}{\log C(t)} \frac{\log p_2}{\log C(t)} \widehat{f_1}\Big(2\frac{\log p}{\log C(t)}\Big) \widehat{f_2}\Big(2\frac{\log p}{\log C(t)}\Big) a_t^2(p_1) a_t^2(p_2)$

We evaluate the sums over $t \in \mathcal{F}$ below and then execute the summation over the prime(s). $\widehat{f_i}$ is supported in $[-\sigma_i, \sigma_i]$. There are no contributions (for σ_i sufficiently small) in the prime sum(s) for sufficiently small error terms.

We want to show the family satisfies Conditions 6.13. Thus, we need to show the five sums are

$$\text{Five Sums of } \frac{1}{|\mathcal{F}|}\sum_{t\in\mathcal{F}} S(t;p) \tag{7.6}$$

1. $\frac{\log p}{\log C(N)}\widehat{f}_1\Big(\frac{\log p}{\log C(N)}\Big)\Bigg[-r+O\Big(p^{-\alpha}+\frac{p^\beta}{|\mathcal{F}|}+\frac{1}{\log^\gamma N}\Big)\Bigg]$

2. $\frac{\log p}{\log C(N)}\widehat{f}_1\Big(2\frac{\log p}{\log C(N)}\Big)\Bigg[p+O\Big(p^{1-\alpha}+\frac{p^\beta}{|\mathcal{F}|}+\frac{p}{\log^\gamma N}\Big)\Bigg]$

3. $\frac{\log p_1}{\log C(N)}\frac{\log p_2}{\log C(N)}\widehat{f}_1\Big(\frac{\log p_1}{\log C(N)}\Big)\widehat{f}_2\Big(2\frac{\log p_2}{\log C(N)}\Big)\Bigg[-rp_2+O\Big(p_1^{-\alpha_1}p_2^{1-\alpha_2}+\frac{p_1^{\beta_1}p_2^{\beta_2}}{|\mathcal{F}|}+\frac{p_2}{\log^\gamma N}\Big)\Bigg]$

4. (a) $\frac{\log p_1}{\log C(N)}\frac{\log p_2}{\log C(N)}\widehat{f}_1\Big(\frac{\log p_1}{\log C(N)}\Big)\widehat{f}_2\Big(\frac{\log p_2}{\log C(N)}\Big)\Bigg[r^2+O\Big(p_1^{1-\alpha_1}p_2^{1-\alpha_2}+\frac{p_1^{\beta_1}p_2^{\beta_2}}{|\mathcal{F}|}+\frac{1}{\log^\gamma N}\Big)\Bigg]$ if $p_1\neq p_2$

   (b) $\frac{\log^2 p}{\log^2 C(N)}\widehat{f}_1\widehat{f}_2\Big(\frac{\log p}{\log C(N)}\Big)\Bigg[p+O\Big(p^{1-\alpha}+\frac{p^\beta}{|\mathcal{F}|}+\frac{p}{\log^\gamma N}\Big)\Bigg]$ if $p_1=p_2=p$

5. $\frac{\log p_1}{\log C(N)}\frac{\log p_2}{\log C(N)}\widehat{f}_1\Big(2\frac{\log p_1}{\log C(N)}\Big)\widehat{f}_1\Big(2\frac{\log p_2}{\log C(N)}\Big)\Bigg[p_1p_2+O\Big(p_1^{1-\alpha_1}p_2^{1-\alpha_2}+\frac{p_1^{\beta_1}p_2^{\beta_2}}{|\mathcal{F}|}+\frac{p_1p_2}{\log^\gamma N}\Big)\Bigg]$

where $\alpha,\beta,\gamma>0$, $\alpha_i,\beta_i\geq 0$ and whenever two α_i or β_i occur, at least one is positive.

7.1.3 Definition of Terms for Sieving

Recall $A_{r,\mathcal{F}}(p)=\sum_{t(p)}a_t^r(p)$. For distinct primes, by Lemma 2.5

$$\sum_{t(p_1\cdots p_n)}\prod_{j=1}^n a_t^{r_i}(p_j) \quad = \quad \prod_{j=1}^n A_{r_i,\mathcal{F}}(p_i). \tag{7.7}$$

By Lemma B.8, we may assume all of our primes (in the expansion from the Explicit Formula in the n-level densities) are at least $\log^l N$, $l\in[1,2)$. $S(t)$ will equal $\widetilde{a}_P(t)G_P(t)$, where for distinct primes p_1 and p_2

$$\begin{aligned}\widetilde{a}_P(t) &= a_t^{r_1}(p_1)a_t^{r_2}(p_2)\\ G_P(t) &= \prod_{\substack{j=1\\ r_j\neq 0}}^2 \frac{\log p_j}{\log C(t)}f_j\Big(2^{r_j-1}\frac{\log p_j}{\log C(t)}\Big)\\ (r_1,r_2) &\in \Big\{(1,0),(0,1),(2,0),(1,1),(0,2),(1,2),(2,1),(2,2)\Big\}.\end{aligned} \tag{7.8}$$

Thus $\widetilde{a}_P(t)G_P(t)$ is merely a convenient way of encoding the eight sums we need to examine for the 1 and 2-level densities.

Actually, this is slightly off. We have to study

$$\prod_{\substack{j=1 \\ r_j \neq 0}}^{2} \frac{1}{p_j^{r_j}} \frac{\log p_j}{\log C(t)} g_j\Big(2^{r_j-1}\frac{\log p_j}{\log C(t)}\Big) a_t^{r_j}(p_j). \tag{7.9}$$

We won't incorporate the $\frac{1}{p_j^{r_j}}$ factors in G_P; we state them for guidance purposes. If both r_j's are non-zero and the two primes are equal, we obtain

$$\frac{1}{p^{r_1+r_2}}\Big(\frac{\log p}{\log C(t)}\Big)^2 \times \cdots \times a_t^{r_1+r_2}(p). \tag{7.10}$$

For example, if $r_1 = r_2 = 1$ we would get $(\frac{\log p}{\log C(t)})^2 \times \cdots \times a_t^2(p)$. Thus, the definition of G_P needs to be slightly modified. We want to deal with distinct primes p_1 and p_2. There will be no contribution for equal primes if $r_1 + r_2 \geq 3$; simply bound each $a_t(p)$ by Hasse. There is a contribution if $r_1 = r_2 = 1$. By modifying the definition of G_P we may regard it as a case where $r = (2, 0)$; however, we will now have the factor $(\frac{\log p}{\log C(t)})^2$, and instead of $f_1(\cdots)$ we will have $f_1 f_2(\cdots)$. Note we evaluate the test functions at $\frac{\log p}{\log C(t)}$ and not $2\frac{\log p}{\log C(t)}$. Thus, we have

$$G_P(t) \quad = \quad \prod_{\substack{j=1 \\ r_j \neq 0}}^{2} \Big(\frac{\log p_j}{\log C(t)}\Big)^{\kappa(r)} g_j\Big(2^{r_j-\kappa(r)}\frac{\log p_j}{\log C(t)}\Big), \tag{7.11}$$

where $\kappa(r)$ is 2 if $r = (2, 0)$ and this arises from $p_1 = p_2 = p$ and $\kappa(r) = 1$ otherwise; $g_j = f_j$ unless $r = (2, 0)$ arising from $p_1 = p_2 = p$, in which case $g_1 = f_1 f_2$.

We may now assume the primes are distinct. Define

$$\begin{aligned} P &= \prod_{\substack{j=1 \\ r_j \neq 0}}^{2} p_j \\ r &= (r_1, r_2),\ r_j \in \{0, 1, 2\} \\ S_c(r, P) &= \sum_{t(P)} \widetilde{a}_P(t) = \sum_{t(P)} a_t^{r_1}(p_1) a_t^{r_2}(p_2) \\ &= A_{r_1,\mathcal{F}}(p_1) A_{r_2,\mathcal{F}}(p_2), \end{aligned} \tag{7.12}$$

where for convenience we set $A_0(p) = 1$. We often have incomplete sums of $\widetilde{a}_P(t)$ mod P. Let $S_I(r, P)$ denote a generic incomplete sum. Then by Hasse,

$$\begin{aligned} S_I(r, P) &\leq P \cdot 2^{r_1} \sqrt{p_1^{r_1}} \cdot 2^{r_2} \sqrt{p_2^{r_2}} \\ &= 2^{r_1+r_2} p_1^{1+\frac{r_1}{2}} \cdot p_2^{1+\frac{r_2}{2}} \\ &= 2^r P^{1+\frac{r}{2}}, \end{aligned} \tag{7.13}$$

where the last expression is a convenient abuse of notation:

$$\begin{aligned} 2^r &= 2^{r_1+r_2} \\ P^r &= p_1^{r_1} \cdot p_2^{r_2}. \end{aligned} \tag{7.14}$$

For a fixed i and d, we evaluate the arguments at $t = t_i(d) + t'd^2$. Let

$$\begin{aligned} \widetilde{a}_{d,i,P}(t') &= \widetilde{a}_P\Big(t_i(d) + t'd^2\Big) \\ G_{d,i,P}(t') &= G_P\Big(t_i(d) + t'd^2\Big). \end{aligned} \tag{7.15}$$

7.1.4 Ranges and Contributions of Sums over Primes

Each prime sum is to (approximately) $C(N)^{\frac{\sigma_j}{2^{r_j-\kappa(r)}}} \approx N^{\frac{m\sigma_j}{2^{r_j-\kappa(r)}}}$, as $C(t)$ is a degree m polynomial. We assume $\sigma_j < \frac{1}{2}$ as we do not worry about $p^2 > N$. This is harmless, as handling the error terms forces the support to be significantly less than $\frac{1}{2}$.

Lemma 7.1 (Contributions from Sums over Primes) *For $r_j = 1$, summing $\frac{p^{\frac{1}{2}}}{|\mathcal{F}|}$ does not contribute for $\sigma_j < \frac{2}{3m}$. For $r_j = 2$, summing $\frac{1}{|\mathcal{F}|}$ does not contribute for $\sigma_j < \frac{2}{m}$ for $\kappa(r) = 1$ and $\frac{1}{m}$ for $k(r) = 2$. As we often have two sums, dividing the above supports by 2 ensures all errors are manageable: write $\frac{1}{|\mathcal{F}|}$ as $\frac{1}{\sqrt{|\mathcal{F}|}} \frac{1}{\sqrt{|\mathcal{F}|}}$.*

7.1.5 Expected Result

In many of the families we investigate, we have

$$\begin{aligned} A_{1,\mathcal{F}}(p) &= -rp + O(1) \\ A_{2,\mathcal{F}}(p) &= p^2 + O(p^{\frac{3}{2}}). \end{aligned} \tag{7.16}$$

For some families $\exists m$ such that $\varphi(m) = 2$ and the main term of $A_{2,\mathcal{F}}(p)$ is zero for primes congruent to m_1 mod m and $2p^2$ for primes congruent to m_2 mod m. By using Dirichlet's Theorem for Primes in Arithmetic Progressions, these can be handled similarly. In the arguments below we assume $A_{2,\mathcal{F}}(p) = p^2 + O(p^{\frac{3}{2}})$.

For a general rational surface, $A_{1,\mathcal{F}}(p)$ is not approximately constant. A careful book-keeping of the arguments below show that constancy of the main term is not needed. Rather, we only need to be able to handle sums such as

$$\sum_p \frac{\log p}{\log X} f\Big(\frac{\log p}{\log X}\Big) \frac{A_{1,\mathcal{F}}(p)}{p^2}. \tag{7.17}$$

By Rosen and Silverman (see Lemma B.9), for surfaces where Tate's conjecture is known, we may replace $A_{1,\mathcal{F}}(p)$ in the above sum with the rank of the family over $\mathbb{Q}(t)$. For notational simplicity, in the proof below we assume $A_{1,\mathcal{F}}(p) = -rp + O(1)$, and content ourselves with noting a similar proof works in general.

$A_{r_j}(p_j) = c_j \cdot p_j^{r_j}$ plus lower order terms not contributing for any support. Hence $S_c(r,P) = c_1 c_2 p_1^{r_1} p_2^{r_2} = c_1 c_2 P^r$ plus lower terms. We hit $S(r,P)$ with $\frac{\log p_j}{\log C(t)} \frac{1}{p_j^{r_j}}$ for each non-zero r_j. Thus, we have approximately $\frac{1}{p_1^{r_1} p_2^{r_2}} = \frac{1}{P^r}$.

A sum like $\sum_{p_j} \frac{\log p_j}{\log C(t)} \frac{1}{p_j} g(\frac{\log p_j}{\log C(t)})$ contributes; if we had an additional $\frac{1}{\log N}$ there would be no net contribution.

We see above things are setting up to just contribute. For each pair (d,i) we expect (if we can manage the conductors) to have approximately $\frac{N/d^2}{P}$ complete sums of $S_c(r,P) = c_1 c_2 P^r$. Hitting this with $\frac{1}{P^r}$ and then executing the sums over the primes gives exactly $\frac{1}{P}$. Thus, we expect terms of the size P^r to contribute, and $\frac{P^r}{\log N}$ to not contribute.

We rewrite Conditions 6.13 in a more tractable form, using $A_{1,\mathcal{F}}(p)$, $A_{2,\mathcal{F}}(p)$ and $S_c(r,P)$. Assume the family satisfies Equation 7.16 (or the related equation if $a_t(p)$ vanishes for half the primes). Then

1. $P = p$, $\widetilde{a}_P(t) = a_t(p)$: $\frac{S_c(r,P)}{P} = \frac{-rp+O(1)}{p} = -r + O(\frac{1}{p})$

2. $P = p$, $\widetilde{a}_P(t) = a_t^2(p)$: $\frac{S_c(r,P)}{P} = \frac{p^2+O(p^{\frac{3}{2}})}{p} = p + O(\sqrt{p})$

3. $P = p_1p_2$, $\widetilde{a}_P(t) = a_t(p_1)a_t^2(p_2)$: $\frac{S_c(r,P)}{P} = \frac{-rp_1p_2^2+O(p_1p_2^{\frac{3}{2}})}{p_1p_2} = -rp_2 + O(\sqrt{p_2})$

4. $P = p_1p_2$, $\widetilde{a}_P(t) = a_t(p_1)a_t(p_2)$:

   (a) $\frac{S_c(r,P)}{P} = \frac{r^2p_1p_2+O(p_1+p_2)}{p_1p_2} = r^2 + O(\sqrt{p_1} + \sqrt{p_2})$ if $p_1 \neq p_2$

   (b) $\frac{S_c(r,P)}{P} = \frac{p^2+O(p^{\frac{3}{2}})}{p} = p + O(\sqrt{p})$ if $p_1 = p_2 = p$

5. $P = p_1p_2$, $\widetilde{a}_P(t) = a_t^2(p_1)a_t^2(p_2)$: $\frac{S_c(r,P)}{P} = \frac{p_1^2p_2^2+O(p_1^{\frac{3}{2}}p_2^{\frac{3}{2}})}{p_1p_2} = p_1p_2 + O(\sqrt{p_1p_2})$

We have proved

Lemma 7.2 (Conditions to Evaluate the Five Types of Sums) *Assume the family satisfies Equation 7.16. If, up to lower order terms, the five sums (Equation 7.6) are $G_P(N)\frac{S_c(r,P)}{P}$, then the family satisfies Conditions 6.13.*

7.2 Taylor Expansion of $G_{d,i,P}(t')$

Fix i and d. We calculate the first order Taylor Expansion of $G_{d,i,P}(t')$. $G_{d,i,P}$ involves t' only through expressions like $\frac{\log p_j}{\log C(t)}$, where $t = t_i(d) + t'd^2$. Let $C(t) = h_mt^m + \cdots$.

The derivative of $G_{d,i,P}$ in t' will involve nice functions times factors like

$$\begin{aligned}
\frac{d}{dt'}\frac{\log p_j}{\log C(t)} &= -\frac{\log p_j}{\log^2 C(t)}\frac{d}{dt'}\log C(t_i(d)+t'd^2) \\
&= -\frac{\log p_j}{\log^2 C(t)}\frac{1}{C(t)}\frac{d}{dt'}C(t_i(d)+t'd^2) \\
&= -\frac{\log p_j}{\log^2 C(t)}\frac{mh_mt^{m-1}d^2+\cdots}{h_mt^{m-1}\cdot(t_i(d)+t'd^2)+\cdots} \\
&\leq \left(\frac{10m}{|h_m|}\max_{0\leq k\leq m-1}|m-k|\cdot|h_{m-k}|\right)\frac{\log p_j}{\log^2 C(t)}\frac{d^2}{t_i(d)+t'd^2}, \qquad (7.18)
\end{aligned}$$

provided N is sufficiently large (we need N large in order to explicitly write down the universal constant in the last line).

As $p_j \leq C(t)^\sigma$, where σ is related to the support of G, $\frac{\log p_j}{\log C(t)} \leq \sigma$. We therefore find that

Lemma 7.3 (Taylor Expansion of $G_{d,i,P}$)

$$G_{d,i,P}(t') = G_{d,i,P}(0) + O\Big(\frac{1}{\log N}\Big). \qquad (7.19)$$

The constant above does not depend on p_j, d or i.

It is essential that our constant is independent of the primes, d and i, as we sum over i and d to get $S(r,P)$, and then we sum $S(r,P)$ over primes.

By the Mean Value Theorem $\exists \xi \in [0,t']$, corresponding to $t_\xi = t_i(d) + \xi d^2 \in [N, 2N + d^2] \subset [N, 2.1N]$, such that

$$G_{d,i,P}(t') = G_{d,i,P}(0) + \frac{d}{dt'} G_{d,i,P}\Big|_{t'=\xi} \Big(t' - 0\Big). \tag{7.20}$$

How do primes enter the Taylor Expansion? First, we have factors $\frac{\log p_j}{\log C(t)}$, which can be universally bounded from the support of G. Second, we evaluate G and its derivative at $2^{r_j - \kappa(r)} \frac{\log p_j}{\log C(t_\xi)}$. We may universally bound these by nice functions of $||G||_\infty$ and $||G'||_\infty$, where by G' we mean any of the derivatives of factors of G. Recall $G_{d,i,P}(t') = G^{(1)}_{d,i,P}(t') G^{(2)}_{d,i,P}(t')$, where if an $r_j = 0$ take the corresponding $G^{(j)}_{d,i,P}(t') \equiv 1$. When we take derivatives with respect to t', we get the first term times the derivative of the second plus the derivative of the first times the second. We see it is sufficient to universally bound functions like $\frac{d}{dt'} g(\frac{\log p}{\log C(t)})$.

$\log C(t_\xi) \approx \log C(N)$. Evaluating the derivative at ξ, by Equation 7.18 we have something bounded by $\frac{1}{\log C(t_\xi)} \frac{d^2}{t_i(d)+\xi d^2}$. We then multiply by $t'-0$. Thus we are bounded by $\frac{1}{\log C(N)} \frac{t' d^2}{t_i(d)+\xi d^2}$. As $t_i(d) \geq N$ and $t' d^2 \leq N$, the bound is at most $\frac{1}{\log C(N)}$.

Lemma 7.4 (Further Taylor Expansion of $G_{d,i,P}$)

$$G_{d,i,P}(t') \quad = \quad G_P(N) + O\Big(\frac{1}{\log N}\Big). \tag{7.21}$$

The constant above does not depend on p_j, d or i.

The proof is similar to the previous lemma. $G_{d,i,P}(0) = G_P\Big(t_i(d)\Big)$, $t_i(d) \in [N, N + d^2]$. Thus, to replace $G_{d,i,P}(0)$ with $G_P(N)$ involves Taylor Expanding $G_P(t)$ around $t = N$. □

This allows us to replace all the conductors of curves with $D(t)$ good with the value from $t = N$ with small error. This is very convenient, as $G_P(N)$ has no t', i or d-dependence. Consequently, we will be able to move it past all summations except over primes, which will allow us to take advantage of cancellations in t-sums of the $a_t(p)$'s.

7.3 Removing the $\nu(d)||S||_\infty$ Term for $d < \log^l N$

$$\sum_{t\in E(d)} S(t) = \sum_{i=1}^{\nu(d)} \sum_{t'=0}^{[N/d^2]} S\Big(t_i(d) + t'd^2\Big) \ + \ O\Big(\nu(d)||S||_\infty\Big). \tag{7.22}$$

We show the $O\Big(\nu(d)||S||_\infty\Big)$ piece does not contribute for $d < \log^l N$. Using Hasse to trivially bound $||S||_\infty$ gives $2^r P^r$. We hit this with $\frac{1}{P^r}$ and sum over the primes, which will be at most $O(N^\sigma)$. We now sum over $d < \log^l N$, getting

$$\ll \quad N^\sigma \sum_{d=1}^{\log^l N} \nu(d) \ll N^\sigma \sum_{d=1}^{\log^l N} d^\epsilon \ll N^\sigma \log^{l(1+\epsilon)} N. \tag{7.23}$$

We then divide by the cardinality of the family, which is assumed to be a multiple of N. There is no contribution for $\sigma_1 + \sigma_2 < 1$.

7.4 Sieving Preliminaries

Let B be the largest square which divides $D(t)$ for all t. Recall by t good we mean $D(t)$ is square-free except for primes dividing B, and for $p|B$, the power of $p|D(t)$ is independent of t. By Theorem 3.8, possibly after passing to a subsequence, we can approximate t good by

$$\sum_{\substack{t\in[N,2N] \\ t \ good}} S(t) \quad = \quad \sum_{\substack{d=1 \\ (d,B)=1}}^{\log^l N} \mu(d) \sum_{\substack{t\in[N,2N] \\ D(t)\equiv 0(d^2)}} S(t) + O\Big(\sum_{t\in\mathcal{T}} S(t)\Big), \tag{7.24}$$

where the set of good t is $c_{\mathcal{F}}N + o(N)$, $c_{\mathcal{F}} > 0$, $\mathcal{T}$ is the set of $t \in [N, 2N]$ such that $D(t)$ is divisible by the square of a prime $p > \log^l N$ and $|\mathcal{T}| = o(N)$.

7.5 Contributions from $d < \log^l N$

We would like to use Lemma 7.4 to replace $G_{d,i,P}(t')$ with $G_P(N)$ plus a manageable error. While this is fine for pairs such as $r = (2, 0)$ or $r = (2, 2)$, this fails for pairs such as $r = (1, 0)$. In this case, we need to evaluate $\sum_p \frac{1}{p} S(r, p)$. If we replace $\widetilde{a}_p(t)$ with $|a_t(p)| \leq 2\sqrt{p}$, we get

$$\ll \frac{1}{|\mathcal{F}|}\frac{1}{p}N\sqrt{p}, \tag{7.25}$$

which is disastrous when we sum over p. The reason we must trivially bound $\widetilde{a}_P(t)$ is the Taylor Expansion. We evaluate the derivative at $\xi(t') = \xi(p_j, i, d; t')$. The dependence of the other parameters prevents us from obtaining complete sums (mod P) and using that cancellation for control.

Thus, we cannot just replace $G_{d,i,P}(t')$ with $G_P(N)$. The Taylor Expansion *will* be useful in handling many of the terms, but it is not sufficient by itself. We need to keep the cancellation from summing $\widetilde{a}_P(t)$.

We use Partial Summation (Lemma 2.1) twice. Note we may always replace a $G_{d,i,P}(t')$ with a $G_P(N)$ at a cost of $\frac{1}{\log N}$.

Let $\widetilde{A}_P(u) = \sum_{t'=0}^{u} \widetilde{a}_P(t')$. As $(p_i, d) = 1$ (*this is why we are assuming* $d \leq \log^l N$ *and* $p_i \geq \log^l N$), every time t' increases by P we have a complete sum of the $\widetilde{a}_P$'s. Thus,

$$\begin{aligned}
\widetilde{A}_P(u) &= \left[\frac{u}{P}\right] S_c(r,P) + O\Big(P^{1+\frac{r}{2}}\Big) \\
&= \frac{u}{P} S_c(r,P) + O\Big(P^R\Big) \\
& \quad R = 1 + \frac{r}{2},\ P^R = \prod_{\substack{j=1 \\ r_j \neq 0}}^{2} p_j^{1+\frac{r_j}{2}}.
\end{aligned} \tag{7.26}$$

In the above, the first error term is from our bound for the incomplete sum of at most P terms, each term bounded by $\sqrt{p_1^{r_1} p_2^{r_2}} = P^{\frac{r}{2}}$. Dropping the greatest integer brackets costs at most $S_c(r,P) = O(P^r)$. $P^r = p_1^{r_1} p_2^{r_2}$, and $P^{1+\frac{r}{2}} = p_1^{1+\frac{r_1}{2}} p_2^{1+\frac{r_2}{2}}$. As $r_j \in \{0,1,2\}$, $r_j \leq 1 + \frac{r_j}{2}$. Thus, we may incorporate the error from removing the greatest integer brackets into the $O(P^R)$ term.

$$\begin{aligned}
S(d,i,r,P) &= \sum_{t'=0}^{[N/d^2]} \widetilde{a}_{d,i,P}(t') G_{d,i,P}(t') \\
&= \left(\frac{[N/d^2]}{P} S_c(r,P) + O\Big(P^R\Big)\right) G_{d,i,P}([N/d^2]) \\
& \quad - \sum_{u=0}^{[N/d^2]-1} \left(\frac{u}{P} S_c(r,P) + O\Big(P^R\Big)\right)\Big(G_{d,i,P}(u) - G_{d,i,P}(u+1)\Big)
\end{aligned}$$

$$S(r,P) \quad = \quad \sum_{d=1}^{\log^l N} \mu(d) \sum_{i=1}^{\nu(d)} S(d,i,r,P) = \sum_{w=1}^{4} \sum_{d=1}^{\log^l N} \mu(d) \sum_{i=1}^{\nu(d)} S_w(d,i,r,P). \tag{7.27}$$

7.5.1 First Sum: $\frac{[N/d^2]}{P} S_c(r,P) G_{d,i,P}([N/d^2])$

Summing over i and d yields

$$\begin{aligned}
S_1(r,P) &= \sum_{d=1}^{\log^l N} \mu(d) \sum_{i=1}^{\nu(d)} \frac{[N/d^2]}{P} S_c(r,P) G_{d,i,P}([N/d^2]) \\
&= \frac{S_c(r,P)}{P} \sum_{d=1}^{\log^l N} \mu(d) \sum_{i=1}^{\nu(d)} \left[\frac{N}{d^2}\right] \left(G_P(N) + O\Big(\frac{1}{\log N}\Big)\right) \\
&= \frac{S_c(r,P) G_P(N)}{P} \sum_{d=1}^{\log^l N} \mu(d) \sum_{i=1}^{\nu(d)} \sum_{t'=0}^{[N/d^2]} \left(1 + O\Big(\frac{1}{\log N}\Big)\right) \\
&= \frac{S_c(r,P) G_P(N)}{P} \sum_{d=1}^{\log^l N} \mu(d) \Bigg(O(\nu(d)) + \sum_{\substack{t=N \\ D(t)\equiv 0(d^2)}}^{2N} 1 \Bigg) \left(1 + O\Big(\frac{1}{\log N}\Big)\right) \\
&= \frac{S_c(r,P) G_P(N)}{P} |\mathcal{F}| + \frac{S_c(r,P)}{P} \cdot o(N).
\end{aligned} \tag{7.28}$$

In the last line, the error term follows from Equation 7.5 (which gives the d, t-sums are $|\mathcal{F}| + o(N)$) and Lemma 3.5 (which gives $\nu(d) \ll d^\epsilon$). Dividing by $|\mathcal{F}| = c_{\mathcal{F}} N + o(N)$, the error term will not contribute when we sum over primes, leaving us with $\frac{S_c(r,P) G_P(N)}{P}$.

7.5.2 Second Sum: $O(P^R) G_{d,i,P}([N/d^2])$

Summing over i and d yields

$$\begin{aligned}
S_2(r,P) &\ll \sum_{d=1}^{\log^l N} |\mu(d)| \sum_{i=1}^{\nu(d)} P^R |G_{d,i,P}([N/d^2])| \\
&\ll P^R \sum_{d=1}^{\log^l N} |\mu(d)| \sum_{i=1}^{\nu(d)} ||G||_\infty \\
&\ll P^R \sum_{d=1}^{\log^l N} |\mu(d)| \sum_{i=1}^{\nu(d)} 1.
\end{aligned} \tag{7.29}$$

As $\nu(d) \ll d^\epsilon$, we obtain

$$S_2(r,P) \ \ll \ P^R \log^{l(1+\epsilon)} N \leq P^R \log^{2l} N \ = \ P^{1+\frac{r}{2}} \log^{2l} N. \tag{7.30}$$

We divide by $|\mathcal{F}| = c_{\mathcal{F}} N + o(N)$, hit it with $\frac{1}{P^r}$ and then sum over the primes. By Lemma 7.1, for small support ($\sigma = \sigma_1 + \sigma_2 < \frac{2}{3m}$) there is no contribution.

7.5.3 Third Sum: $\sum_{u=0}^{[N/d^2]-1} \frac{u}{P} S_c(r,P)\Big(G_{d,i,P}(u) - G_{d,i,P}(u+1)\Big)$

We apply Partial Summation, where $a_u = G_{d,i,P}(u) - G_{d,i,P}(u+1)$ and $b_u = \frac{u}{P} S_c(r,P)$. Thus

$$\begin{aligned} S_3(d,i,r,P) \ &= \ \left(G_{d,i,P}(0) - G_{d,i,P}\Big([N/d^2]\Big)\right) \frac{[N/d^2]-1}{P} S_c(r,P) \\ &\quad - \sum_{u=0}^{[N/d^2]-2} \Big(G_{d,i,P}(0) - G_{d,i,P}(u+1)\Big) \frac{1}{P} S_c(r,P). \end{aligned} \tag{7.31}$$

Using the Taylor Expansion, we gain a $\frac{1}{\log N}$ in the first term, making it of size $\frac{S_c(r,P)}{P} \frac{[N/d^2]}{\log N} \ll \frac{S_c(r,P)}{P} \frac{|\mathcal{F}|}{d^2 \log N}$.

For the second term, we have $< [N/d^2]$ summands, each $\ll \frac{1}{\log N} \frac{S_c(r,P)}{P}$. We again obtain a term of size $\frac{S_c(r,P)}{P} \frac{|\mathcal{F}|}{d^2 \log N}$.

We sum over i and d.

$$\begin{aligned} S_3(r,P) \ &\ll \ \sum_{d=1}^{\log^l N} |\mu(d)| \sum_{i=1}^{\nu(d)} \frac{S_c(r,P)}{P} \frac{|\mathcal{F}|}{d^2 \log N} \\ &\ll \ \frac{S_c(r,P)}{P} \frac{|\mathcal{F}|}{\log N} \sum_{d=1}^{\log^l N} \sum_{i=1}^{\nu(d)} \frac{1}{d^2} \\ &\ll \ \frac{S_c(r,P)}{P} \frac{|\mathcal{F}|}{\log N} \sum_{d=1}^{\log^l N} \frac{\nu(d)}{d^2}. \end{aligned} \tag{7.32}$$

As $\nu(d) \ll d^\epsilon$, $S_3(r,P) \ll \frac{S_c(r,P)}{P} \frac{|\mathcal{F}|}{\log N}$

7.5.4 Fourth Sum: $\sum_{u=0}^{[N/d^2]-1} O(P^R)\Big(G_{d,i,P}(u) - G_{d,i,P}(u+1)\Big)$

Using the Taylor Expansion for $G_{d,i,P}(u) - G_{d,i,P}(u+1)$ is not sufficient. This would give $\frac{NP^R}{d^2 \log N}$. Summing over i and d is manageable, and would give us $O(P^R \frac{|\mathcal{F}|}{\log N})$. Dividing by the cardinality of the family gives $O(\frac{P^R}{\log N})$.

The problem is in summing over the primes, as we no longer have $\frac{1}{|\mathcal{F}|}$. We multiply by $\frac{1}{P^r}$. We recall the definitions of r and R and unwind the above.

Consider the case $r = (1,0)$. Then $P = p_1 = p$, $R = 1 + \frac{r_1}{2} = \frac{3}{2}$, and $\frac{1}{P^r} = \frac{1}{p}$. We have

$$\sum_{p=\log^l N}^{N^{m\sigma}} \frac{1}{p} \frac{p^{\frac{3}{2}}}{\log N} \gg N^{m\sigma}. \tag{7.33}$$

As $N \to \infty$, this term blows up. We need significantly better cancellation in

$$S_4(r,P) \quad = \quad \sum_{d=1}^{\log^l N} \mu(d) \sum_{i=1}^{\nu(d)} \sum_{u=0}^{[N/d^2]-1} O(P^R)\Big(G_{d,i,P}(u) - G_{d,i,P}(u+1)\Big). \tag{7.34}$$

Taking absolute values, and using the maximum of the $O(P^R)$ terms gives

$$S_4(r,P) \quad \ll \quad P^R \sum_{d=1}^{\log^l N} \sum_{i=1}^{\nu(d)} \sum_{u=0}^{[N/d^2]-1} \Big|G_{d,i,P}(u) - G_{d,i,P}(u+1)\Big|. \tag{7.35}$$

The constant is independent of P. Taking the maximum of the P^R term involves the maximum of either the incomplete sum or one complete sum. Using Hasse, the constant is at most $2^{r_1+r_2}$. Thus, the constant in Equation 7.35 does not depend on P.

If exactly one of the r_j's is non-zero, then

$$G_{d,i,P}(u) - G_{d,i,P}(u+1) = g\Big(\frac{\log p}{\log C(t_i(d) + ud^2)}\Big) - g\Big(\frac{\log p}{\log C(t_i(d) + (u+1)d^2)}\Big) \tag{7.36}$$

for some Schwartz function g of compact support.

If both of the r_j's are non-zero, we may write $G_{d,i,P}(u)$ as the product of two functions, say g_1 and g_2. Thus

$$G_{d,i,P}(u) = \prod_{j=1}^{2} g_j\Big(\frac{\log p_j}{\log C(t_i(d)+ud^2)}\Big) \tag{7.37}$$

Recall

$$\begin{aligned} |a_1a_2 - b_1b_2| &= |a_1a_2 - b_1a_2 + b_1a_2 - b_1b_2| \\ &\leq |a_1a_2 - b_1a_2| + |b_1a_2 - b_1b_2| \\ &= |a_2|\cdot|a_1 - b_1| + |b_1|\cdot|a_2 - b_2| \end{aligned} \tag{7.38}$$

We apply the above to our function $G_{d,i,P}(u) = g_1(d,i,p_1;u)g_2(d,i,p_2;u)$. Each $g_j(d,i,p_j;u)$ can be bounded independently of d, i, p_j and u, as each g_j is a Schwartz function defined in terms of the n-level density test functions. Let $B = \max_j ||g_j||_\infty + 1$. Then

$$\begin{aligned} S_4(d,i,r,P)(u) &= G_{d,i,P}(u) - G_{d,i,P}(u+1) \\ &= \prod_{\substack{j=1 \\ r_j\neq 0}}^{2} g_j\Big(\frac{\log p_i}{\log C(t_i(d)+ud^2)}\Big) - \prod_{\substack{j=1 \\ r_j\neq 0}}^{2} g_j\Big(\frac{\log p_j}{\log C(t_i(d)+(u+1)d^2)}\Big) \\ &\leq \sum_{\substack{j=1 \\ r_j\neq 0}}^{2} B\cdot\left|g_j\Big(\frac{\log p_j}{\log C(t_i(d)+ud^2)}\Big) - g_j\Big(\frac{\log p_j}{\log C(t_i(d)+(u+1)d^2)}\Big)\right|. \end{aligned} \tag{7.39}$$

We sum the above over u, i and d.

$$\begin{aligned} S_4(r,P) &\leq 2^r P^R \sum_{d=1}^{\log^l N} |\mu(d)| \sum_{i=1}^{\nu(d)} \sum_{u=0}^{[N/d^2]-1} S_4(d,i,r,P)(u) \\ &\leq 2^r P^R \sum_{d=1}^{\log^l N} \sum_{i=1}^{\nu(d)} \sum_{\substack{j=1 \\ r_j\neq 0}}^{2} B \sum_{u=0}^{[N/d^2]-1} \left|g_j\Big(\frac{\log p_j}{\log C(t_{i,d}(u))}\Big) - g_j\Big(\frac{\log p_j}{\log C(t_{i,d}(u+1))}\Big)\right| \\ t_{i,d}(u) &= t_i(d) + ud^2 \end{aligned} \tag{7.40}$$

As each g_j is a Schwartz function, they are of bounded variation ([Fo], page 97, Example 3.25c). We show the u-sums are bounded independent of p_j, i, d, and N.

We may add

$$\left|g_j(0) - g_j\Big(\frac{\log p_j}{\log C(t_i(d))}\Big)\right| + \left|g_j\Big(\frac{\log p_j}{\log C(t_i(d) + [N/d^2]d^2)}\Big) - g_j(1000\sigma)\right|. \tag{7.41}$$

Let $x_u(d,i,p_j) = \frac{p_j}{\log N_{t_i(d)+ud^2}}$. *As the conductors are monotone increasing,* $x_u(d,i,p_j) > x_{u+1}(d,i,p_j)$. Thus, we have a partition of $[0, 1000\sigma]$, and we may now apply theorems on bounded variation to bound the u-sum independent of p_j, i, d and N, obtaining $\ll 1000\sigma$.

Note we are regarding the above as an exercise in the bounded variation of $g(x)$ on $[0,\sigma]$. If we were to regard this as a problem in the bounded variation of $g_{j;p_j,d,i}$ we would have u ranging over at least $\Big[0, [N/d^2]\Big]$. Even though we would gain a $\frac{1}{\log N}$ from the derivatives, the bounded variation bound depends on the size of the interval, which here is of length $[N/d^2]$. We return to the problems we faced in the beginning, where the Taylor Expansion was insufficient.

We note several points. We do not need the full strength of bounded variation; it is sufficient that each g_j has continuous, bounded first derivative on $[0, 1000\sigma]$. By the Mean Value Theorem, the u-sum is $\ll ||g_j'||_\infty \cdot |1000\sigma - 0|$. We show this in the next subsection.

It is essential that we apply theorems on bounded variation (or the Mean Value Theorem) to a one-dimensional function. If, however, we want to remove the dependence on the primes, and both r_j's are non-zero, we must deal with evaluating functions at both $\frac{\log p_1}{\log N_{t(u)}}$ and $\frac{\log p_2}{\log N_{t(u)}}$. We would have to replace this pair with $x_u(d,i,p_j)$ and $x_{u+1}(d,i,p_j)$; it is much simpler to add terms and remain in the one-dimensional case.

Thus, the u and the j-sums are universally bounded. We are left with $\ll P^R$. Summing over i and d gives $\ll P^R \log^{l(1+\epsilon)} N$. We multiply by $\frac{1}{P^r}$ and sum over the primes. The prime sums give $N^{h(\sigma)}$; dividing by the cardinality of the family (a multiple of N), we find there is no contribution for small support.

Note: *if our conductors are not monotone, we cannot apply theorems on bounded variation. The problem is we could transverse* $[0, 1000\sigma]$ *(or a large subset of it) many times. It is essential that the u-sums are evaluated at a monotone sequence. This is why* S_4 *is the most difficult of the error pieces, and why we needed to obtain polynomial expressions for the conductors for good* t.

7.5.5 The Mean Value Theorem and Bounded Variation

Lemma 7.5 ([Fo], Example 3.25*c*) *If* F *is differentiable on* $\mathbb{R}$ *and* F' *is bounded, then* F *is of bounded variation on* $[a,b]$, $-\infty < a < b < \infty$.

Proof: Let $a \le x_0 < x_1 \cdots < x_{M-1} < x_M \le b$. Then

$$\begin{aligned} S &= \sum_{n=0}^{M-1} \Big| F(x_n) - F(x_{n+1}) \Big| \\ &= \sum_{n=0}^{M-1} \Big| F'(\xi_n) \cdot (x_n - x_{n+1}) \Big|, \ \xi_n \in [x_n, x_{n+1}] \\ &\le \sum_{n=0}^{M-1} ||F'||_\infty |x_n - x_{n+1}| = ||F'||_\infty \cdot |x_M - x_0|. \end{aligned} \tag{7.42}$$

Note that the variation is bounded by $||F'||_\infty \cdot |b-a|$.

7.5.6 Summary of Contributions for $d < \log^l N$

Lemma 7.6 (Contributions for $d < \log^l N$) *Based on our Sieving Assumptions for the family (for good $D(t)$ the conductors are given by a monotone polynomial in t, a positive percent of $t \in [N, 2N]$ give $D(t)$ good), the main term contribution from $d < \log^l N$ is $\frac{S_c(r,P)}{P} G_P(N)|\mathcal{F}|$. The error terms are either of size $\frac{S_c(r,P)}{P} o(|\mathcal{F}|)$, which won't contribute when we sum over primes, or are such that their sum over primes will not contribute.*

7.6 Contributions from $t \in \mathcal{T}$

7.6.1 Preliminaries

We are left with estimating the contributions from the troublesome set

$$\mathcal{T} \ = \ \Big\{ t \in [N, 2N] : \exists d > \log^l N \text{ with } d^2 | D(t) \Big\} \tag{7.43}$$

We have shown in Theorem 3.8 that $|\mathcal{T}| = o(N)$. By Cauchy-Schwartz

$$\Big| \sum_{t \in \mathcal{T}} S(t) \Big| \ \le \ \Big(\sum_{t \in \mathcal{T}} S^2(t) \Big)^{\frac{1}{2}} \Big(\sum_{t \in \mathcal{T}} 1 \Big)^{\frac{1}{2}} \ \le \ \Big(\sum_{t=N}^{2N} S^2(t) \Big)^{\frac{1}{2}} o\Big(\sqrt{N}\Big). \tag{7.44}$$

We then sum over the primes, and need to show the sum over t is $O(N)$. As it stands, however, this is not sufficient to control the error. Quick sketch: assume $S(t) = a_t(p) g(\frac{\log p}{\log C(t)})$. Ignoring the t-dependence in the conductors, we have

$$\begin{aligned}\sum_{t=N}^{2N} S(t) &\approx g^2\Big(\frac{\log p}{\log C(N)}\Big)\frac{N}{p}\sum_{t(p)} a_t^2(p) \\ &\approx g^2\Big(\frac{\log p}{\log C(N)}\Big)\frac{N}{p}p^2 = O(Np). \qquad (7.45)\end{aligned}$$

Taking the square-root, we hit it with $\frac{1}{p}$ and sum over $p \leq N^\sigma$, which is not $O(\sqrt{N})$.

$S(t)$ is the product of at most two terms involving factors such as $a_t^{r_j}(p_j)$. We hit this with factors $p_j^{-r_j}$ and sum over p. Thus, instead of $S(t)$ consider $S_1(t)S_2(t)$, where $S_j(t)$ incorporates the sum over primes to the j^{th} power and all relevant factors.

$$\begin{aligned}S &= \sum_{t=N}^{2N}\Bigg[\prod_{\substack{j=1\\ r_j\neq 0}}^{2}\sum_{p_j\geq \log^l N} p_j^{-r_j} g_j\Big(\frac{\log p_j}{\log C(t)}\Big)a_t^{r_j}(p_j)\Bigg]^2 \\ &= \sum_{t=N}^{2N}\prod_{w=1}^{2}\prod_{\substack{j=1\\ r_j\neq 0}}^{2}\sum_{p_{j_w}\geq \log^l N} p_{j_w}^{-r_{j_w}} g_{j_w}\Big(\frac{\log p_{j_w}}{\log C(t)}\Big)a_t^{r_{j_w}}(p_{j_w}). \qquad (7.46)\end{aligned}$$

We proceed similarly as in the $d \leq \log^l N$ case, except now there are no d and i, and we have potentially four factors instead of one or two. On expanding, we combine terms where we have the same prime occurring multiple times. Thus, there are five types of sums: four distinct primes (four factors), three distinct primes (three factors), ..., all primes the same (one factor). We do the worst case, when there are four factors; the other cases are handled similarly.

7.6.2 A Specific Case: Four Distinct Primes

Assume we have four distinct primes. Relabeling, we have $p^{-r_i}a_t^{r_i}(p_i)$ for $i = 1$ to 4. Let $P = \prod_{i=1}^4 p_i$. Interchange the t-summation with the p_i-summations. As before, we apply partial summation to $\sum_{t=N}^{2N}\prod_{i=1}^4 a_t^{r_i}(p_i)\ \cdot g_i(p_i,t)p^{-r_i}\ = \sum_{t=N}^{2N} a(P,t)\cdot b(P,t)$, the only change being the addition of the factors $\prod_i p^{-r_i}$. Now $A(u) = \sum_{t=N}^{u} a(P,t) = \frac{u-N}{P}S_c(P)\ +O(\prod_{i=1}^4 p_i^{1+\frac{r_i}{2}})$, $S_c(P) = \prod_{i=1}^4 A_{r_i,\mathcal{F}}(p_i)$ by Lemma 2.5. Let $P^R = \prod_{i=1}^4 p_i^{1+\frac{r_i}{2}}$; the error in the partial summation is $O(P^R)$.

As in Equation 7.27 we have

$$S = \prod_{i=1}^{4}\sum_{p_i}\sum_{t=N}^{2N} a_t^{r_i}(p_i)\cdot p^{-r_i}G(P,t)$$

$$\begin{aligned} = \quad & \prod_{i=1}^{4}\sum_{p_i}\Big(\frac{N}{P}S_c(r,P)+O(P^R)\Big)p_i^{-r_i}G(P,2N) \\ & -\prod_{i=1}^{4}\sum_{p_i}\sum_{u=N}^{2N-1}\Big(\frac{u-N}{P}S_c(r,P)+O(P^R)\Big)p_i^{-r_i}\Big(G(P,u)-G(P,u+1)\Big). \qquad (7.47)\end{aligned}$$

For $r \geq 2$ by Hasse $A_{r,\mathcal{F}}(p) \leq 2^r p^{1+\frac{r}{2}}$. For $r = 1$ for a rational surface, $A_{1,\mathcal{F}}(p) \ll p$. Hence $\forall r$, $A_{r,\mathcal{F}}(p) \ll p^r$.

$$\prod_{i=1}^{4}\frac{S_c(P)}{p_i}p_i^{-r_i} \ \ll\ \prod_{i=1}^{4}\frac{A_{r_i,\mathcal{F}}(p_i)}{p_i^{1+r_i}} \ \ll\ \prod_{i=1}^{4}\frac{p_i^{r_i}}{p_i^{1+r_i}} \ =\ \prod_{i=1}^{4}\frac{1}{p_i}. \qquad (7.48)$$

We can immediately handle the first sum. Inserting absolute values yields something like

$$\prod_{i=1}^{4}\sum_{p_i}\frac{\log p_i}{\log C(2N)}\Big|g_i\Big(\frac{\log p_i}{\log C(2N)}\Big)\Big|\frac{1}{p_i} \quad \ll \quad \prod_{i=1}^{4}O(1) \qquad (7.49)$$

where the last result (the sums over the primes) follows from Corollary B.2.

Pulling out the prime factors and using partial summation again, the third sum is handled similarly.

The second and fourth pieces are more difficult, and result in significantly decreased support. We analyze this loss later. For now, we need only note that the second sum is $\prod_i \sum_{p_i} p_i^{r_i/2}$. For test functions of small support, this sum is $o(N)$.

There is a slight obstruction in applying the same argument to the fourth sum, namely, that $G(P,u)$ could be the product of four factors. Similar to the identity $|a_1a_2 - b_1b_2| \leq |a_1| \cdot |a_1 - b_1|$ $+|b_1| \cdot |a_2 - b_2|$, we have

$$\begin{aligned} |a_1a_2a_3a_4 - b_1b_2b_3b_4| \quad \leq & \quad |a_2a_3a_4| \cdot |a_1 - b_1| + |b_1a_3a_4| \cdot |a_2 - b_2| \\ & + |b_1b_2a_4| \cdot |a_3 - b_3| + |b_1b_2b_3| \cdot |a_4 - b_4| \\ \leq & \quad \prod_{j=1}^{4}\Big(|a_j| + |b_j| + 1\Big)\sum_{i=1}^{4}|a_i - b_i| \qquad (7.50)\end{aligned}$$

The rest of the proof in this case is identical to the fourth sum in the $d \leq \log^l N$ case.

Note: as we have always inserted absolute values before summing over primes, it is permissible to extend from the primes are distinct to all possible 4-tuples.

7.6.3 Handling the Other Cases

The other cases (especially cases where some primes are equal) are handled similarly. The only real change is if we have less than four factors, and this only affects the Fourth Sum. For example, if we have three factors instead of 4, set $a_4 = b_4 = 1$ in Equation 7.50.

7.7 Determining the Admissible Supports of the Test Functions

The largest errors arise from $r_i = 1$ terms, and these arise from using Hasse to trivially estimate partial sums, bounding partial sums of $a_t(p)$ by $p^{3/2}$. Let $C(t)$ be a polynomial of degree m for good t. We assume all supports are at most $\frac{1}{2}$ (as otherwise p^2 could exceed N, changing some of our arguments above). In the 1-level densities, we encounter errors like

$$\sum_{p=\log^l N}^{N^{\sigma m}} \frac{1}{p} \frac{\log p}{\log N^m} g\Big(\frac{\log p}{\log N^m}\Big) p^{\frac{3}{2}} \ll \sum_{p=\log^l N}^{N^{\sigma m}} p^{\frac{1}{2}} \ll N^{\frac{3\sigma m}{2}} \tag{7.51}$$

We divide by a multiple of $|\mathcal{F}| = N$. The errors are manageable for $\sigma < \min\left(\frac{2}{3m}, \frac{1}{2}\right)$.

In the 2-level density, the worst case (not including the Cauchy-Schwartz arguments to handle the overcounting of almost square-free numbers) was when we had two $r_i = 1$ terms. We have two functions of support σ_1 and σ_2, and we obtain

$$\prod_{i=1}^{2} \sum_{p_i=\log^l N}^{N^{\sigma_i m}} \frac{1}{p} \frac{\log p_i}{\log N^m} g\Big(\frac{\log p_i}{\log N^m}\Big) p_i^{\frac{3}{2}} \ll \prod_{i=1}^{2} \sum_{p_i=\log^l N}^{N^{\sigma m}} p_i^{\frac{1}{2}} \ll N^{\frac{3(\sigma_1+\sigma_2)m}{2}} \tag{7.52}$$

We divide by a multiple of N, the cardinality of the family, and see the errors are manageable for $\sigma_1 + \sigma_2 < \min\left(\frac{2}{3m}, \frac{1}{2}\right)$. Thus, if we take $\sigma_1 = \sigma_2$, we see the support of each test function is half that from the 1-level density.

In applying Cauchy-Schwartz, we decrease even further the allowable support. The worst case is where we have four distinct primes with $r_i = 1$. We sum as before, and obtain $N^{3(\sigma_1+\sigma_2)k}$ (there is no factor of 2 as two of the primes are associated to test functions with support σ_1 and two to σ_2). We take the square-root, and this must be $O(\sqrt{N})$. Thus, we now find $\sigma_1 + \sigma_2 < \frac{1}{2}\frac{2}{3m}$. Setting $\sigma_1 = \sigma_2$ yields the support is one-quarter that of the 1-level density.

Note: instead of using Cauchy-Schwartz, we can use Lemma B.6, provided we can prove $|\mathcal{T}| = o\Big(\frac{N}{\log^2 N}\Big)$. Unfortunately, even in the case where the degree of the irreducible factors of $\Delta(t)$ is

2 or 3, we do not have such a bound; assuming the ABC conjecture only gives $|\mathcal{T}| = o(N)$. The problem is the number of primes in $[\log^l N, N]$ is of size $\frac{N}{\log N}$.

7.8 1- and 2-Level Densities

Assume the original family has rank r over $\mathbb{Q}(t)$. The Birch and Swinnerton-Dyer conjecture and Silverman's Specialization Theorem imply, for all t sufficiently large, each curve's L-function has r family zeros at the critical point.

The Birch and Swinnterton-Dyer conjecture is only used for interpretation purposes. The results we find below are derived independently of this conjecture; however, assuming this allows us to interpret some of the n-level density terms as contributions from expected family zeros.

Definition 7.7 (Non-Family Density) *Let $D^{(r)}_{n,\mathcal{F}}(f)$ be the n-level density from the non-family zeros (ie, the trivial contributions from the r family zeros have been removed).*

Theorem 7.8 ($D_{n,\mathcal{F}}(f)$ and $D^{(r)}_{n,\mathcal{F}}(f)$, $n = 1$ or 2) *For any one-parameter family of rank r over $\mathbb{Q}(t)$ satisfying*

1. *For good t(relative to $D(t)$), the conductors $C(t)$ are a monotone polynomial in t.*
2. *Up to $o(N)$, the good $t \in [N, 2N]$ are obtainable by sieving up to $d = \log^l N$; further, the number of such t is $|\mathcal{F}| = c_{\mathcal{F}} N + o(N)$, $c_{\mathcal{F}} > 0$.*
3. *$A_{1,\mathcal{F}}(p) = -rp + O(1)$, $A_{2,\mathcal{F}}(p) = p^2 + O(p^{\frac{3}{2}})$ (or $\exists m$ such that $(m_i, m) = 1$, $p \equiv m_i(m)$ implies $A_{2,\mathcal{F}}(p) = c_i p^2 + O(p^{\frac{3}{2}})$, $\frac{1}{\varphi(m)} \sum_{(m_i,m)=1} c_i = 1$ and similarly for $A_{1,\mathcal{F}}(p)$).*

Then for f_i even Schwartz functions of small but non-zero support σ_i,

$$\begin{aligned} D_{1,\mathcal{F}}(f) &= \widehat{f_1}(0) + \frac{1}{2} f_1(0) + r f_1(0) \\ D^{(r)}_{1,\mathcal{F}}(f_1) &= \widehat{f_1}(0) + \frac{1}{2} f_1(0) \end{aligned} \tag{7.53}$$

and

$$\begin{aligned} D_{2,\mathcal{F}}(f) &= \prod_{i=1}^{2} \left[\widehat{f_i}(0) + \frac{1}{2} f_i(0) \right] + 2 \int_{-\infty}^{\infty} |u| \widehat{f_1}(u) \widehat{f_2}(u) du \\ &\quad -2\widehat{f_1 f_2}(0) - f_1(0) f_2(0) + (f_1 f_2)(0) N(\mathcal{F}, -1) \\ &\quad +(r^2 - r) f_1(0) f_2(0) + r \widehat{f_1}(0) f_2(0) + r f_1(0) \widehat{f_2}(0) \end{aligned}$$

$$\begin{aligned} D_{2,\mathcal{F}}^{(r)}(f_1) &= \prod_{i=1}^{2}\left[\widehat{f_i}(0)+\frac{1}{2}f_i(0)\right]+2\int_{-\infty}^{\infty}|u|\widehat{f_1}(u)\widehat{f_2}(u)du \\ &\quad -2\widehat{f_1f_2}(0)-f_1(0)f_2(0)+(f_1f_2)(0)N(\mathcal{F},-1). \qquad (7.54)\end{aligned}$$

Removing the contribution from the r family zeros, for small support the 2-level density of the remaining zeros agrees with SO(even)*,* O *or* SO(odd) *if the signs are all even, equidistributed, or all odd. If Tate's conjecture is true for the surface, we may interpret r as the rank of $\mathcal{E}$ over $\mathbb{Q}(t)$.*

Let m = deg $C(t)$. For the 1-level density, $\sigma < \min(\frac{1}{2},\frac{2}{3m})$. For the 2-level density, $\sigma_1+\sigma_2 < \frac{1}{3m}$. For families where $\Delta(t)$ has no irreducible factors of degree 4 or more, the sieving is unconditional, otherwise the results are conditional on ABC or the Square-Free Sieve conjecture.

Proof: When we sieve we obtain $\frac{S_c(r,P)G_P(N)}{P}$ plus lower order terms. By Theorem 7.2, the family satisfies Conditions 6.13. Thus Lemma 6.9 is applicable. □

As remarked, we do not need to assume $A_{1,\mathcal{F}}(p) = -rp+O(1)$. A more cumbersome proof (using Lemma B.9) handles $A_{1,\mathcal{F}}(p)$ for surfaces where Tate's conjecture is known.

To apply Theorem 7.8, we need to compute three types of quantities:

1. The conductors are monotone polynomials for $D(t)$ good. By changing $t \to ct+t_0$, Tate's Algorithm will yield $C(t)$ is a monotone integer polynomial for $D(t)$ good.

2. A positive percent of $D(t)$ are good. Let δ_D be the discriminant of $D(t)$ and $\mathcal{P} = \{p : p|a_k\delta_D\} \cup \{p : p \le \sqrt{k}\}$. If $\forall p \in \mathcal{P}$, $\nu(p) \le p^2-1$, by Theorem 3.8 a positive percent of t give $D(t)$ square-free.

3. $A_{1,\mathcal{F}}(p)$ and $A_{2,\mathcal{F}}(p)$. If Tate's conjecture is true, Rosen-Silverman (Theorem 2.3) gives $A_{1,\mathcal{F}}(p)$; if $j(t)$ is non-constant, Michel's Theorem (Theorem 2.4) gives $A_{2,\mathcal{F}}(p)$.

For rational surfaces, by possibly passing to a subsequence, the above conditions are satisfied. Let $\mathcal{P}$ be the set of primes dividing $a_k\delta$ and all primes at most $\sqrt{k}$. If $\forall p \in \mathcal{P}$, $\nu(p) \le p^2-1$, by Theorem 3.8 $|\mathcal{F}| = c_{\mathcal{F}}N+o(N)$, $c_{\mathcal{F}} > 0$. If not, by Theorem 4.3, by sieving a subsequence, Conditions 1 and 2 are satisfied for any family where deg $\Delta(t) \le 12$, which includes all rational surfaces. For rational surfaces, Rosen and Silverman handle the first half of Condition 3, and for non-constant $j(t)$, Michel's Theorem handles the second. Note, for N_0 sufficiently large, any polynomial is monotone for $t \ge N_0$.

Thus by the above (Theorem 2.3, Theorem 2.4 and Lemma B.9 to handle $A_{1,\mathcal{F}}(p)$ and $A_{2,\mathcal{F}}(p)$, Theorem 3.8 and Theorem 4.3 to handle the cardinalities and the conductors, and Theorem 7.8 to handle the sieving) we have proved

Theorem 7.9 (Rational Surfaces Density Theorem) *Consider a one-parameter family of elliptic curves of rank r over $\mathbb{Q}(t)$ that is a rational surface. Assume GRH, $j(t)$ is non-constant, and the ABC or Square-Free Sieve conjecture if $\Delta(t)$ has an irreducible polynomial factor of degree at least 4. Let f_i be an even Schwartz function of small but non-zero support σ_i and $m = deg\, C(t)$. For the 1-level density, $\sigma < \min(\frac{1}{2}, \frac{2}{3m})$. For the 2-level density, $\sigma_1 + \sigma_2 < \frac{1}{3m}$. Assume the Birch and Swinnerton-Dyer conjecture for interpretation purposes. Possibly after passing to a subsequence,*

$$\begin{aligned} D_{1,\mathcal{F}}(f_1) &= \widehat{f_1}(0) + \frac{1}{2}f_1(0) + rf_1(0) \\ D_{1,\mathcal{F}}^{(r)}(f_1) &= \widehat{f_1}(0) + \frac{1}{2}f_1(0). \end{aligned} \tag{7.55}$$

and

$$\begin{aligned} D_{2,\mathcal{F}}(f) &= \prod_{i=1}^{2}\left[\widehat{f_i}(0) + \frac{1}{2}f_i(0)\right] + 2\int_{-\infty}^{\infty}|u|\widehat{f_1}(u)\widehat{f_2}(u)du \\ &\quad -2\widehat{f_1f_2}(0) - f_1(0)f_2(0) + (f_1f_2)(0)N(\mathcal{F},-1) \\ &\quad +(r^2-r)f_1(0)f_2(0) + r\widehat{f_1}(0)f_2(0) + rf_1(0)\widehat{f_2}(0) \\ D_{2,\mathcal{F}}^{(r)}(f_1) &= \prod_{i=1}^{2}\left[\widehat{f_i}(0) + \frac{1}{2}f_i(0)\right] + 2\int_{-\infty}^{\infty}|u|\widehat{f_1}(u)\widehat{f_2}(u)du \\ &\quad -2\widehat{f_1f_2}(0) - f_1(0)f_2(0) + (f_1f_2)(0)N(\mathcal{F},-1). \end{aligned} \tag{7.56}$$

The 2-level non-family is SO(even) *(*SO(odd)*, O) if all curves are even (odd, the signs are equidistributed).*

Thus, for small support, the 1-level non-family density agrees with the predictions of Katz and Sarnak; the 2-level non-family density agrees with Katz and Sarnak's predictions up to the distribution of the signs of the functional equations.

We will study several families with constant sign and obtain examples agreeing with Katz and Sarnak's predictions. Further, we will also investigate several families with $j(t)$ and $M(t)$ non-constant. Conjecturally (see Helfgott [Hel]), these families have equidistribution of sign, and we observe the 2-level non-family density agrees with O (as predicted).

Part III

Modified 1- and 2-Level Densities

8 Modified 1- and 2-Level Densities, All Curves

8.1 Introduction

Consider the family $\mathcal{F} = \{E : y^2 = x^3 + ax + b\}$, with $a \in [-N^2, N^2]$, $b \in [-N^3, N^3]$, and conductors $N_E = C(a,b)$. We expect the logarithm of most of the conductors to be like $6 \log N$. Later we sieve and study $\mathcal{F}_M$, the subset of almost minimal curves, of size $|\mathcal{F}_M| = \frac{4N^5}{\zeta(10)} + O(N^3)$.

Definition 8.1 (Almost Minimal Family of All Curves) *Let $\mathcal{F}$ be the family of all elliptic curves, parametrized as above. Let $\mathcal{F}_M$ be the subset of almost minimal curves, namely, if $p^4|a$ then $p^6 \nmid b$. The curves are minimal except possibly at the primes 2 and 3.*

Handling the conductor dependence is beyond our techniques; unlike the one-parameter family cases, we do not have monotonicity at our disposal. We can evaluate all needed sums of $a_{a,b}(p)$'s by looking at complete sums, but as the conductors vary, we have to study factors such as $\frac{\log p}{\log N_E}$ $f(\frac{\log p}{\log N_E})$ $a_{a,b}(p)$. We are unable to pull the summation on a and b past the test functions, which is how we obtain cancellation. To surmount this, we study the modified level densities.

Definition 8.2 (Average log-conductor) $\log M = \frac{1}{|\mathcal{F}_M|}\sum_{E \in \mathcal{F}_M} \log C(a,b)$*, the average of the logarithms of the conductors.*

Definition 8.3 (Modified n-Level Density) $D'_{n,\mathcal{F}_M}(f)$ *differs from the n-level density $D_{n,\mathcal{F}_M}(f)$ in that each curve's zeros are rescaled by $\log M$ (a global quantity) instead of $\log C(a,b)$ (a local quantity). This leads to a correction term of $\frac{\log M - \log C(a,b)}{\log M}\widehat{f}_i(0)$ on the primes' side.*

Instead of scaling the local 1-level densities associated to each curve by $\log C(a,b)$, we scale by $\log M$. This has the advantage of giving factors such as $\frac{\log p}{\log M}$ $f(\frac{\log p}{\log M})$ $a_{a,b}(p)$, and we can easily move the summations on a and b past the test function.

Unfortunately, we now have sums such as $\frac{\log C(a,b) - \log M}{\log M}$. We use the Modified Explicit Formula (Theorem A.31). Let $L_M = \frac{\log M}{2\pi}$.

$$\begin{aligned}\sum_{\gamma_{E^{(j)}_{a,b}}} f(L_M \gamma_{E^{(j)}_{a,b}}) \quad &= \quad \frac{\log C(a,b)}{\log M}\widehat{f}(0) + f(0) - \; 2\sum_p \frac{1}{p}\frac{\log p}{\log M}\widehat{f}_1\Big(\frac{\log p}{\log M}\Big)a_E(p) \\ &\quad -2\sum_p \frac{1}{p^2}\frac{\log p}{\log M}\widehat{f}\Big(\frac{2\log p}{\log M}\Big)a_E^2(p) + O(\frac{\log\log M}{\log M}). \qquad (8.1)\end{aligned}$$

The proof is similar to that of the Explicit Formula, Theorem A.29. For the modified 1-level density, this introduces no difficulty. When we sum over all curves in the family, $\frac{1}{|\mathcal{F}_M|}\sum_{E\in\mathcal{F}_M}\frac{\log C(a,b)}{\log M} = 1$ from the definition of $\log M$. Thus, the proof of the modified 1-level density is straightforward.

Complications arise in the modified 2-level density, as we have the product of two 1-level densities. Summing over all curves in the family yield cross terms, and we must sum terms ranging from $\left(\frac{\log C(a,b)}{\log M}\right)^2$ to $\frac{\log C(a,b)}{\log M}a_{a,b}^r(p)$.

We write $\frac{\log C(a,b)}{\log M}$ as $1-\frac{\log M-\log C(a,b)}{\log M}$. As in the proof of Theorem E.1, we bring $\frac{\log M-\log C(a,b)}{\log M}$ over to the zeros' side. Summing over all curves yields, on the zeros' side,

$$\frac{1}{|\mathcal{F}_M|}\sum_{E\in\mathcal{F}_M}\left[\prod_{i=1}^{2}\Big(\sum_{\gamma_{E_{a,b}^{(j_i)}}} f_i(L_M\gamma_{E_{a,b}^{(j_i)}})\Big)+\frac{\log M-\log C(a,b)}{\log M}\right]. \tag{8.2}$$

Later we will handle the conductor correction; for now, we calculate the rest of the quantities needed to determine the modified 2-level density, ie, the terms on the primes' side. Initially we ignore the almost minimal condition ($p^4|a \to p^6\nmid b$) and sum over all curves. We then sieve and handle the contributions from the minimal curves. Thus, for now, instead of using $\mathcal{F}_M$ on the primes' side we use $\mathcal{F}$; later we will subtract the contribution from curves in $\mathcal{F}-\mathcal{F}_M$.

One reason we chose to sieve to $\mathcal{F}_M$ is Fouvry, Nair and Tenenbaum [FNT] give a good bound on the number of curves in $\mathcal{F}_M$ whose conductor's logarithm is far from $\log M$; we will need such a bound to handle the conductor correction.

Note: in the definition of $\mathcal{F}_M$, we can either keep or remove the singular curves. A curve is singular if its discriminant is zero. Up to small factors of 2 and 3, $|a|^3 = |b|^2 = c^6$ for some c. For each square $|a|$ in $[0,N^2]$ there is a unique cube $|b|$ in $[0,N^3]$ such that $|a|^3 = |b|^2$. Therefore the number of such curves is $O(N)$, whereas $|\mathcal{F}|$ and $|\mathcal{F}_M|$ are of size N^5. By Lemma B.7, each curve contributes at most $O(\log N)$, so the contribution from the singular curves is bounded by $N\log^2 N$ (we get a $\log^2 N$ if we have $a_{a,b}(p_1)a_{a,b}(p_2)$; otherwise it is just $\log N$). We see we may safely ignore or keep these terms.

8.2 Useful Sums

Lemma 8.4 *Let $a_{a,b}(p_i) = \sum_{x=0}^{p-1} \left(\frac{x^3+ax+b}{p_i}\right)$. Let P be the product of the maximal set of distinct primes. For n odd, the complete sum*

$$\sum_{a=0}^{P-1} \sum_{b=0}^{P-1} a_{a,b}(p_1) \cdots a_{a,b}(p_n) = 0. \tag{8.3}$$

Proof: Find α such that $\prod_{i=1}^{n} \left(\frac{\alpha}{p_i}\right) = -1$. For example, let p be a prime that occurs an odd number of times in the list $p_1, \dots, p_n$. Let ξ be any quadratic non-residue mod p. By the Chinese Remainder Theorem $\exists \alpha$ congruent to ξ mod p, and 1 for every other prime. For each prime, α is invertible; change variables by $x_i \to \alpha x_i, a \to \alpha^2 a, b \to \alpha^3 b$. This changes the sum by a factor $\prod_{i=1}^{n} \left(\frac{\alpha^3}{p_i}\right) = (-1)^3 = -1$, proving the complete sum vanishes. The importance of this lemma is the primes need not be distinct. □

Lemma 8.5 *For $n = 2$ we have*

$$S \;=\; \sum_{a=0}^{p-1} \sum_{b=0}^{p-1} \prod_{i=1}^{2} \sum_{x_i=0}^{p-1} \left(\frac{x_i^3 + ax_i + b}{p}\right) \;=\; p^3 - p^2. \tag{8.4}$$

Proof: We use Equation 2.4 to expand $a_E(p)$:

$$a_E(p) = -G_p^{-1} \sum_{x(p)} \sum_{c=1}^{p} \left(\frac{c}{p}\right) \mathbf{e}\left(\frac{cf_E(x)}{p}\right). \tag{8.5}$$

We take the complex conjugate, which on the RHS introduces a minus sign into the exponential and sends G_p to $\overline{G_p}$, and has no effect on the LHS (which is real). The sum becomes

$$\begin{aligned} S &= (G_p\overline{G_p})^{-1} \sum_{a=0}^{p-1} \sum_{b=0}^{p-1} \prod_{i=1}^{2} \sum_{x_i=0}^{p-1} \sum_{c_i=0}^{p-1} \left(\frac{c_i}{p}\right) \mathbf{e}\left(\frac{(-1)^{i+1}(c_i x_i^3 + c_i a x_i + c_i b)}{p}\right) \\ &= \frac{1}{p} \sum_{x_1,c_1=0}^{p-1} \sum_{x_2,c_2=0}^{p-1} \left(\frac{c_1 c_2}{p}\right) \mathbf{e}\left(\frac{c_1 x_1^3 - c_2 x_2^3}{p}\right) \sum_{a=0}^{p-1} \mathbf{e}\left(\frac{(c_1 x_1 - c_2 x_2)a}{p}\right) \\ &\quad \cdot \sum_{b=0}^{p-1} \mathbf{e}\left(\frac{(c_1 - c_2)b}{p}\right) \end{aligned} \tag{8.6}$$

The b-sum vanishes unless $p|(c_1 - c_2)$, which only happens if $c_1 = c_2 = c$. The a-sum vanishes unless $p|(cx_1 - cx_2)$. As $c \not\equiv 0(p)$ (we have the factor $\left(\frac{c}{p}\right)$) this forces $x_1 = x_2 = x$. As c is non-zero, $\left(\frac{c^2}{p}\right) = 1$, the first exponential factor is 1, and the sums collapse to

$$\begin{aligned} S &= \frac{1}{p}\sum_{c=1}^{p-1} 1 \sum_{x=0}^{p-1} 1 \sum_{a=0}^{p-1} 1 \sum_{b=0}^{p-1} 1 \\ &= \frac{1}{p}(p-1)\cdot p \cdot p \cdot p = p^3 - p^2. \end{aligned} \tag{8.7}$$

8.3 1-Level Density Sums

$$\begin{aligned} D'_{1,\mathcal{F}}(f_1) &= \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\sum_{\gamma_{E^{(j)}_{a,b}}} f_1(L_M\gamma_{E^{(j)}_{a,b}}) \\ &= \widehat{f_1}(0)\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\frac{\log C(a,b)}{\log M} + f_1(0) - 2\sum_p \frac{1}{p}\frac{\log p}{\log M}\widehat{f_1}\Big(\frac{\log p}{\log M}\Big)\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} a_E(p) \\ &\quad -2\sum_p \frac{1}{p^2}\frac{\log p}{\log M}\widehat{f_1}\Big(\frac{2\log p}{\log M}\Big)\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} a_E^2(p) + O\Big(\frac{\log\log M}{\log M}\Big). \end{aligned} \tag{8.8}$$

We evaluate the above sums for $E \in \mathcal{F}$; later we remove the contributions from curves where $p^4|a$, $p^6|b$ to evaluate the sums for $E \in \mathcal{F}_M$.

The first term becomes $\widehat{f_1}(0)\frac{1}{|\mathcal{F}_M|}\sum_{E\in\mathcal{F}_M}\frac{\log C(a,b)}{\log M}$. From the definition of $\log M$, this is $\widehat{f_1}(0)$

We need to calculate $\frac{1}{4N^5}\sum_a\sum_b a_{a,b}(p)$ and $\frac{1}{4N^5}\sum_a\sum_b a_{a,b}^2(p)$. We break each up into $\frac{2N^2}{p}\frac{2N^3}{p}$ complete sums of a mod p, b mod p, plus an incomplete sum. For small support, the incomplete sum does not contribute. By Lemma 8.4, the $a_{a,b}(p)$ term's complete sum vanishes. By Lemma 8.5, the complete sum of $a_{a,b}^2(p)$ is $p^3 - p^2$. As there are $\frac{4N^5}{p^2}$ complete sums, it contributes $p - 1$ (we to divide by $4N^5$, the cardinality of the family). Substituting, we see there is no contribution from the $O(1)$ term, while the p term yields $-\frac{1}{2}f_1(0)$ by Corollary B.3.

We may ignore the contribution of $-p^2$ (from the sum of $a_{a,b}^2(p)$) as it gives a contribution of $\frac{O(1)}{\log M}$. If, however, we start expanding the density in $\frac{1}{\log M}$, then $-p^2$ will give a potential lower order correction term. We say potential as the discarded error terms are of size $\frac{1}{\log M}$ and $\frac{1}{\log M}$! We investigate this observation in more detail later.

8.4 Definitions of Modified Densities

We use the modified Explicit Formula, where we have brought $\frac{\log M - \log C(a,b)}{\log M}$ over to the zeros' side. We will handle this term later; for now, we calculate the terms on the primes' side.

Definition 8.6 *Let $D_{2,\mathcal{F}_M}''(f)$ equal the modified 2-level density $D'_{2,\mathcal{F}_M}(f)$ with the correction terms $\frac{\log M - \log C(a,b)}{\log M}\widehat{f_i}(0)$ moved to the zeros' side.*

As in our calculation of $D_{2,\mathcal{F}}(f)$, it is first easier to determine the modified densities where we sum over all pairs of zeros and then remove pairs where $j_1 = \pm j_2$.

Definition 8.7 *Let $D'^{*}_{2,\mathcal{F}_M}(f)$ equal $D^{*}_{2,\mathcal{F}_M}(f)$ except we do not remove the contributions from $j_1 = \pm j_2$, and similarly for $D_{2,\mathcal{F}_M}''^{*}(f)$.*

We prove, up to negligible error, that the correction terms on the zeros' side don't contribute.

8.5 2-Level Density Sums

We evaluate the above sums for $E \in \mathcal{F}$; later we will remove the contributions from curves where $p^4|a$, $p^6|b$ to evaluate the sums for $E \in \mathcal{F}_M$.

By Lemma 6.6, we have

$$\begin{aligned}
D_{2,\mathcal{F}}''^{*}(f) &= \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\prod_{i=1}^{2}\left[\widehat{f_i}(0) + f_i(0) + S_{i,1} + S_{i,2}\right] \\
&= \prod_{i=1}^{2}\left[\widehat{f_i}(0) + f_i(0)\right] + \\
&\quad \left[\widehat{f_1}(0) + f_1(0)\right]\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{2,1} + \left[\widehat{f_2}(0) + f_2(0)\right]\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{1,1} + \\
&\quad \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{1,1}S_{2,1} + \\
&\quad \left[\widehat{f_1}(0) + f_1(0)\right]\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{2,2} + \left[\widehat{f_2}(0) + f_2(0)\right]\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{1,2} + \\
&\quad \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{1,1}S_{2,2} + \frac{1}{|\mathcal{F}|}S_{1,2}\sum_{E\in\mathcal{F}} S_{2,1} + \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{1,2}S_{2,2}. \qquad (8.9)
\end{aligned}$$

In $S_{i,j}$ the i refers to which prime, and the j to the power of $a_E(p)$; ie, we have the factor $a_E^j(p_i)$.

From our (or Brumer's [Br]) 1-level density investigations, $\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{i,1}$ does not contribute if the support is sufficiently small ($\frac{5}{9}^{th}$ can be established very easily; $\frac{4}{7}^{th}$ with a little more care).

All complete sums of $a_{a,b}(p_1)\cdots a_{a,b}(p_n)$, n odd, vanish. We are therefore left with partial sums, which do not contribute for small support. The odd power terms $(S_{1,1}, S_{2,1}, S_{1,1}S_{2,2}, S_{1,2}S_{2,1})$ do not contribute. From previous investigations, $S_{1,2}$ contributes $-\frac{1}{2}f_1(0)$ and $S_{2,2}$ contributes $-\frac{1}{2}f_2(0)$.

We are left with two terms, $S_{1,1}S_{2,1}$ and $S_{1,2}S_{2,2}$.

$$\begin{aligned}
D_{2,\mathcal{F}}"^{*}(f) &= \prod_{i=1}^{2}\left[\widehat{f_i}(0)+f_i(0)\right] \\
&\quad +\left[\widehat{f_1}(0)+f_1(0)\right]\Big(-\frac{1}{2}f_2(0)\Big)+\left[\widehat{f_2}(0)+f_2(0)\right]\Big(-\frac{1}{2}f_1(0)\Big) \\
&\quad +\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{1,1}S_{2,1}+\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{1,2}S_{2,2} \\
&= \widehat{f_1}\widehat{f_2}(0)+\frac{1}{2}f_1\widehat{f_2}(0)+\frac{1}{2}\widehat{f_1}f_2(0) \\
&\quad +\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{1,1}S_{2,1}+\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{1,2}S_{2,2} \\
&= \widehat{f_1}\widehat{f_2}(0)+\frac{1}{2}f_1\widehat{f_2}(0)+\frac{1}{2}\widehat{f_1}f_2(0)+\frac{1}{4}f_1f_2(0)-\frac{1}{4}f_1f_2(0) \\
&\quad +\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{1,1}S_{2,1}+\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{1,2}S_{2,2} \\
&= \Big[\widehat{f_1}(0)+\frac{1}{2}f_1(0)\Big]\Big[\widehat{f_2}(0)+\frac{1}{2}f_2(0)\Big]-\frac{1}{4}f_1f_2(0) \\
&\quad +\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{1,1}S_{2,1}+\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{1,2}S_{2,2} \qquad (8.10)
\end{aligned}$$

8.5.1 $S_{1,12}=\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{1,1}S_{2,1}$

By Lemma 2.6, $\sum_{a,b(p_1p_2)} a_{a,b}(p_1)\ a_{a,b}(p_2) = A_{1,\mathcal{F}}(p_1)A_{1,\mathcal{F}}(p_2)$ if $p_1 \neq p_2$. Thus there is no contribution (for small support) if $p_1 \neq p_2$. If $p_1 = p_2$ we have $\sum_{a,b(p)} a_{a,b}^2(p)$, which is $A_{2,\mathcal{F}}(p) = p^3 - p^2$ by Lemma Lemma 8.5. For any support, we may ignore the p^2 term, although as previously remarked, it will contribute to lower order correction terms to the densities.

As $|\mathcal{F}| = 4N^5$, we have $\frac{2N^2}{p}\frac{2N^3}{p}$ complete sums and an incomplete sum which will not contribute for small support. Therefore the contribution from $p_1 = p_2$ is, for small support,

$$S_{1,12a} = \Big(\frac{2}{\log M}\Big)^2 \sum_p \frac{\log^2 p}{p^2}\widehat{f_1}\widehat{f_2}\Big(\frac{\log p}{\log M}\Big)\Big(p+O(1)\Big). \qquad (8.11)$$

The $O(1)$ term does not contribute ($\sum_p \frac{\log^2 p}{p^2}$ is finite). By Lemma B.4, $S_{1,12a} = 2\int_{-\infty}^{\infty} |u|\widehat{f_1}(u)$ $\widehat{f_2}(u)du$.

For the family of all elliptic curves, for small support

Lemma 8.8 ($S_{1,12}$ for the Family of All Elliptic Curves)

$$S_{1,12} \quad = \quad 2\int_{-\infty}^{\infty} |u|\widehat{f_1}(u)\widehat{f_2}(u)du. \tag{8.12}$$

8.5.2 $S_{2,12} = \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} S_{1,2}S_{2,2}$

$$\begin{aligned} S_{2,12} &= \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\prod_{i=1}^{2}\sum_{p_i}\frac{-2\log p_i}{\log M}\frac{1}{p_i^2}\widehat{f_i}\Big(2\frac{\log p_i}{\log M}\Big)a_E^2(p_i) \\ &= \prod_{i=1}^{2}\sum_{p_i}\frac{-2\log p_i}{\log M}\frac{1}{p_i^2}\widehat{f_i}\Big(2\frac{\log p_i}{\log M}\Big)T_{2,12}, \\ T_{2,12} &= \frac{1}{|\mathcal{F}|}\prod_{i=1}^{2}\sum_a\sum_b a_{a,b}^2(p_i) \end{aligned} \tag{8.13}$$

For small support, the only contribution will be when a and b are complete sums mod p_1p_2. If $p_1 = p_2 = p$ there is no net contribution. Using Hasse to bound $a_{a,b}^2(p)$ by $4p$ yields $T_{2,12} \leq \frac{1}{4N^5}\frac{2N^2}{p}\frac{2N^3}{p}p^2{\cdot}4p = 4p$. Substituting into $S_{2,12}$ gives a contribution bounded by $\frac{1}{\log^2 M}\sum_p \frac{\log^2 p}{p^4}4p = O(\frac{1}{\log M})$.

Therefore we may assume $p_1 \neq p_2$. We've shown (Lemmas 2.6 and 8.5) $\sum_{a,b(p_1p_2)} a_{a,b}^2(p_1)$ $a_{a,b}^2(p_2) = A_{2,\mathcal{F}}(p_1)A_{2,\mathcal{F}}(p_2) = p_1^3p_2^3 + O(p_1^3p_2^2 + p_1^2p_2^3)$. For all support, there is no contribution from the error term. We now add back $p_1 = p_2$ (which doesn't contribute). Up to negligible error

$$T_{2,12} \quad = \quad \frac{1}{4N^5}\frac{2N^2}{p_1p_2}\frac{2N^3}{p_1p_2}p_1^3p_2^3. \tag{8.14}$$

$$\begin{aligned} S_{2,12} &= \prod_{i=1}^{2}\sum_{p_i}\frac{-2\log p_i}{\log M}\frac{1}{p_i^2}\widehat{f_i}\Big(2\frac{\log p_i}{\log M}\Big)T_{2,12} \\ &= \prod_{i=1}^{2}\sum_{p_i}\frac{-2\log p_i}{\log M}\frac{1}{p_i}\widehat{f_i}\Big(2\frac{\log p_i}{\log M}\Big) \end{aligned} \tag{8.15}$$

By Corollary B.3, up to negligible error,

$$\sum_{p_i} \frac{-2\log p_i}{\log M}\frac{1}{p_i}\widehat{f_i}\Big(2\frac{\log p_i}{\log M}\Big) = -\frac{1}{2}f_i(0). \tag{8.16}$$

Therefore, up to terms which don't contribute,

Lemma 8.9 ($S_{2,12}$ for the Family of All Elliptic Curves)

$$S_{2,12} = \prod_{i=1}^{2}\left(-\frac{1}{2}f_i(0)\right) = \frac{1}{4}f_1f_2(0) \tag{8.17}$$

8.5.3 Expression for $D_{2,\mathcal{F}}"^*(f)$

Adding the contributions from $S_{1,12}$ and $S_{2,12}$ yields

Lemma 8.10

$$\begin{aligned} D_{2,\mathcal{F}}"^*(f) &= \Big[\widehat{f_1}(0)+\frac{1}{2}f_1(0)\Big]\Big[\widehat{f_2}(0)+\frac{1}{2}f_2(0)\Big] \\ &\quad +2\int_{-\infty}^{\infty}|u|\widehat{f_1}(u)\widehat{f_2}(u)du \end{aligned} \tag{8.18}$$

We note the $\widehat{f_i}(0)+\frac{1}{2}f_i(0)$ terms are what we observed in the 1-level densities.

8.6 Sieving for the Family of All Elliptic Curves

Closely following Brumer [Br], we perform the promised sieving, namely, we restrict to pairs (a,b) such that $p^4|a \to p^6 \nmid b$. Except possibly at 2 and 3, the equations are minimal. We divide the pairs into two groups: pairs divisible by a large prime, and pairs divisible by a small prime.

8.6.1 Number of Curves

Before we divided the sums by $|\mathcal{F}| = 4N^5$. Now we divide by slightly less, as the family consists of curves where if $p^4|a, p^6 \nmid b$.

Lemma 8.11 (Number of Curves) *The number of curves in the family $\mathcal{F}_M$ ($p^4|a, p^6\nmid b$) is $\frac{1}{\zeta(10)}4N^5 + O(N^3)$.*

$$|\mathcal{F}_M| = \sum_{d=1}^{N}\mu(d)\cdot\#\Big\{(a,b): d^4|a\in N_a, d^6|b\in N_b\Big\}$$

$$\begin{aligned}
& N_a = [-N^2, N^2]; \quad N_b = [-N^3, N^3] \\
= & \sum_{d=1}^{N} \mu(d) \Big(\frac{2N^2}{d^4} + O(1) \Big) \Big(\frac{2N^3}{d^6} + O(1) \Big) \\
= & \sum_{d=1}^{N} \mu(d) \frac{4N^5}{d^{10}} + O(N^3) \\
= & 4N^5 \sum_{d=1}^{\infty} \mu(d) \frac{1}{d^{10}} + O(N^{1-10}N^5) + O(N^3) \\
= & \frac{1}{\zeta(10)} 4N^5 + O(N^3) \qquad (8.19)
\end{aligned}$$

8.6.2 Performing the Sieving

Consider the pairs (a, b) such that $\exists p$ with $p^4|a, p^6|b$. We must remove the contributions from these pairs from our sums in order to obtain the density functions for the family $\mathcal{F}_M$ (instead of for $\mathcal{F}$).

By inclusion / exclusion, noting that d is at most $\sqrt{N}$, a typical sum that we must remove looks like

$$S_2 = \frac{1}{4N^5/\zeta(10)} \sum_{d=1}^{\sqrt{N}} \mu(d) \sum_{\substack{a=-N^2 \\ d^4|a}}^{N^2} \sum_{\substack{b=-N^3 \\ d^6|b}}^{N^3} \prod_{i=1}^{2} \sum_{p} \frac{\log p_i}{\log M} \widehat{\phi}_i\Big(\frac{\log p_i}{\log M}\Big) \frac{1}{p_i^{r_i}} a_{a,b}^{r_i}(p_i). \qquad (8.20)$$

There is no net contribution from terms with $d > \sqrt{\log N}$. For each $d \geq \sqrt{\log N}$, there are $\frac{2N^2}{d^4}$ choices of a that are multiples of d, and $\frac{2N^3}{d^6}$ choices of b that are multiples of d, for a total of $\frac{4N^5}{d^{10}}$ curves. By Lemma B.6 or Hasse, each curve contributes at most $\log^2 C(a,b) \ll \log^2 N$. Hence the contribution from these pairs is bounded by

$$S_{2,\sqrt{\log N}} \ll \frac{1}{N^5} \sum_{d \geq \sqrt{\log N}}^{\sqrt{N}} \frac{4N^5}{d^{10}} \log^2 N \ll \log^2 N \cdot \log^{-\frac{9}{2}} N. \qquad (8.21)$$

Thus, it is enough to subtract from a sum over curves in $\mathcal{F}$ the contribution from terms with $d \leq \sqrt{\log M}$.

By Lemma B.8 we may assume all primes are greater than $\sqrt{\log N}$, as we may absorb the contribution of the small primes into the error term from each curve, provided we increase it from $O(\frac{1}{\log N})$ to $O(\frac{\log^{\frac{1}{4}} N}{\log N})$.

We analyze as before. If $p_1 \neq p_2$, every time a and b run through a complete set of residues mod $p_1 p_2$ we get $A_{r_1,\mathcal{F}}(p_1) A_{r_2,\mathcal{F}}(p_2)$, unless $(d, p_1 p_2) > 1$, which by the above cannot happen.

$p_1 = p_2$ is handled similarly, contributing only if $r_1 = r_2 = 1$.

Up to manageable error, the a and b-sums give

$$\Big(1 - \frac{1}{\zeta(10)}\Big)\frac{4N^5}{p_1p_2}A_{r_1,\mathcal{F}}(p_1)A_{r_2,\mathcal{F}}(p_2) \tag{8.22}$$

if the primes are distinct, and a similar term otherwise. Thus, the amount we lose (from dropping the curves where $p^4|a$, $p^6|b$) exactly equals the change in cardinality from $4N^5$ to $\frac{4N^5}{\zeta(10)}$.

8.7 Modified 1-Level Density

Theorem 8.12 ($D'_{1,\mathcal{F}_M}(f_1)$) *For small support,* $D'_{1,\mathcal{F}_M}(f_1) = \widehat{f_1}(0) + \frac{1}{2}f_1(0)$.

This follows immediately from the above, as in the 1-level density, we can easily handle the conductor contribution (by definition, it sums to zero).

8.8 Modified 2-Level Density, I

We subtract from $D_{2,\mathcal{F}_M}"^*(f)$ the contribution from $j_1 = \pm j_2$. By Lemma 6.6, this is $2D'_{1,\mathcal{F}_M}(f_1f_2)$ $-\ N(\mathcal{F}_M,-1)\ f_1(0)f_2(0)$, or $2\widehat{f_1f_2}(0) + (f_1f_2)(0) - N(\mathcal{F}_M,-1)f_1(0)f_2(0)$.

Therefore

Lemma 8.13

$$\begin{aligned} D_{2,\mathcal{F}_M}"(f) &= \prod_{i=1}^{2}\Big[\widehat{f_i}(0) + \frac{1}{2}f_i(0)\Big] + 2\int_{-\infty}^{\infty}|u|\widehat{f_1}(u)\widehat{f_2}(u)du + \\ &\quad -2\widehat{f_1f_2}(0) - f_1(0)f_2(0) + N(\mathcal{F}_M,-1)f_1(0)f_2(0). \end{aligned} \tag{8.23}$$

8.9 Handling the Variation in the Conductors

8.9.1 Preliminaries

We now handle the variation in the conductors. Recall (Equation 8.2) this entails analyzing

$$\frac{1}{|\mathcal{F}_M|}\sum_{E\in\mathcal{F}_M}\Bigg[\prod_{i=1}^{2}\Big(\sum_{\gamma_{E^{(j_i)}_{a,b}}} f_i\Big(\frac{\log M}{2\pi}\gamma_{E^{(j_i)}_{a,b}}\Big)\Big) + \frac{\log M - \log C(a,b)}{\log M}\Bigg]. \tag{8.24}$$

We know the modified 1-level density:

$$\frac{1}{|\mathcal{F}_M|} \sum_{E \in \mathcal{F}_M} \sum_{\gamma_{E^{(j)}_{a,b}}} f_1(L_M \gamma_{E^{(j)}_{a,b}}) = \widehat{f}_1(0) + \frac{1}{2} f_1(0). \tag{8.25}$$

The idea of the proof is, for most pairs (a, b), $\frac{\log M - \log C(a,b)}{\log M}$ is small, and the cross product of this and the 1-level density won't contribute. For the remaining curves, they are so few they yield no net contribution.

As in the proof of Theorem E.1, there exist positive functions g_i ($i = 1, 2$) such that g_i is an even Schwartz function whose Fourier Transform is supported in the same interval as that of f_i and $g_i(x) \geq |f_i(x)|$. As the g_i satisfy the necessary conditions, we may apply the modified 1-level density theorem to the g_i's.

8.9.2 Variation in Sizes of the Conductors

Fouvry, Nair and Tenenbaum [FNT] show that $\forall \epsilon$, if N is sufficiently large, then the average of the logarithm of the conductors for the family of almost minimal curves, $\mathcal{F}_M$, satisfies

$$(1 - \epsilon) \log N^6 \leq \log M \leq \log N^6 + O(1). \tag{8.26}$$

For convenience, we rewrite this as

$$(1 - \epsilon^2) \log N^6 \leq \log M \leq \log N^6 + O(1), \tag{8.27}$$

where we consider the subset of all curves such that, if $p^4 | a$, then $p^6 \nmid b$. The percentage of such curves is $\frac{1}{\zeta(10)} \approx .999006$.

By Theorem E.1, errors of size $O(\frac{1}{\log N})$ (or slightly larger) for an individual curve are harmless. As $a \in [-N^2, N^2]$, $b \in [-N^3, N^3]$ and the discriminant is at most of size N^6, up to a few factors of 2 and 3, the largest our conductors can be is $(N^6)^2$.

The discriminant is $\Delta(a, b) = -16(4a^3 + 27b^2)$. Let's compare $\Delta(a, b)$ to $C(a, b)$. For $p > 3$, the conductor $C(a, b)$ has p to the first power if $p | \Delta(a, b)$, $p \nmid a$; if $p | \Delta$ and $p | a$, then $p^2 | \Delta$ and $C(a, b)$ has p to the second power ([Kn]). In both cases, we have at least as many powers of p in $\Delta \approx N^6$ as we do in $C(a, b)$. Thus primes greater than 3 cannot lead to the conductor being more than the discriminant. Further, the powers of 2 and 3 in $C(a,b)$ are universally bounded. Hence we may assume the conductors are at most $(1+\epsilon)\log N^6$, and the average of the logarithms of the conductors is at least $(1-\epsilon^2)\log N^6$.

If at least $\sqrt{\epsilon}|\mathcal{F}_M|$ curves have conductors at most $(1-\sqrt{\epsilon})\log N^6$, the maximum $\log M$ could be is $\sqrt{\epsilon}\cdot(1-\sqrt{\epsilon})\ \log N^6\ +(1-\sqrt{\epsilon})\ (1+\epsilon)\log N^6 = (1-\epsilon\sqrt{\epsilon})\log N^6$. As $\epsilon < 1$, $1-\epsilon\sqrt{\epsilon} < 1-\epsilon^2$, contradicting the lower bound for the average of the conductors. Therefore

Lemma 8.14 *There at most $\sqrt{\epsilon}|\mathcal{F}_M|$ curves with conductor less than $(1-\sqrt{\epsilon})\log N^6$, and at least $(1-\sqrt{\epsilon})|\mathcal{F}_M|$ curves with conductors in $[(1-\sqrt{\epsilon})\log N^6,\ (1+\epsilon)\log N^6]$.*

Definition 8.15 *Let $\mathcal{C}_2$ be the set of curves with conductor at most $\sqrt{\epsilon}N^5$, and $\mathcal{C}_1$ the remaining curves.*

8.9.3 Contribution from $\mathcal{C}_1$, the Large Conductors

We first analyze the contribution from the curves with large conductor, ie, the at least $(1-\sqrt{\epsilon})|\mathcal{F}_M|$ curves with conductors in $[(1-\sqrt{\epsilon})\log N^6,\ (1+\epsilon)\log N^6]$.

As $\log M \in [(1-\epsilon)\log N^6, \log N^6 + O(1)]$, for these curves

$$\Big|\frac{\log M - \log C(a,b)}{\log M}\Big| \ll \sqrt{\epsilon} + \frac{1}{\log N}. \tag{8.28}$$

We have three terms to bound. First, we do the reinforcement term, where the conductor correction hits itself:

$$\begin{aligned}\frac{1}{|\mathcal{F}_M|}\sum_{E\in\mathcal{C}_1}\Big(\frac{\log M - \log C(a,b)}{\log M}\Big)^2 &\ll \frac{1}{N^5}\sum_{E\in\mathcal{C}_1}\Big(\sqrt{\epsilon}+\frac{1}{\log N}\Big)^2 \\ &\ll O\Big(\sqrt{\epsilon}+\frac{1}{\log N}\Big).\end{aligned} \tag{8.29}$$

We now handle the two cross terms; by symmetry it is enough to do one. We have

$$\frac{1}{|\mathcal{F}_M|}\sum_{E\in\mathcal{C}_1}\Big(\frac{\log M - \log C(a,b)}{\log M}\Big)\sum_{\gamma_{E_{a,b}^{(j_2)}}} f_2(L_M\gamma_{E_{a,b}^{(j_2)}}). \tag{8.30}$$

Inserting absolute values, we obtain a bound for the above by passing from $|f_2|$ to g_2. We replace the conductor term with

$$\max_{E\in\mathcal{C}_1}\left|\frac{\log M-\log C(a,b)}{\log M}\right| \ll \sqrt{\epsilon}+\frac{1}{\log N}. \tag{8.31}$$

We are left with

$$\begin{aligned}
&\ll \Big(\sqrt{\epsilon}+\frac{1}{\log N}\Big)\frac{1}{|\mathcal{F}_M|}\sum_{E\in\mathcal{C}_1}\sum_{\gamma_{E_{a,b}^{(j_2)}}} g_2(L_M\gamma_{E_{a,b}^{(j_2)}})\\
&\ll \Big(\sqrt{\epsilon}+\frac{1}{\log N}\Big)\frac{1}{|\mathcal{F}_M|}\sum_{E\in\mathcal{F}_M}\sum_{\gamma_{E_{a,b}^{(j_2)}}} g_2(L_M\gamma_{E_{a,b}^{(j_2)}})\\
&\ll \Big(\sqrt{\epsilon}+\frac{1}{\log N}\Big)D'_{1,\mathcal{F}_M}(g_2) = O\Big(\sqrt{\epsilon}+\frac{1}{\log N}\Big). \qquad (8.32)
\end{aligned}$$

It is essential that we are able to majorize $|f_2|$ with a positive function g_2 whose modified 1-level density is known; ie, if supp $\widehat{f_2}\subset(-\sigma_2,\sigma_2)$, supp $\widehat{g}_2\subset(-\sigma_2,\sigma_2)$.

We have proved

Lemma 8.16 (Contributions from the Large Conductors) *Given $\epsilon>0$, the large conductors ($E\in\mathcal{C}_1$) contribute $O\Big(\sqrt{\epsilon}+\frac{1}{\log N}\Big)$.*

8.9.4 Contribution from $\mathcal{C}_2$, the Small Conductors, I

There are again three terms. For $E\in\mathcal{C}_2$, the conductor could be very small. Thus, all we can say about $\frac{\log M-\log C(a,b)}{\log M}$ is that it is $O(1)$.

By Lemma 8.14, $|\mathcal{C}_2|\le\sqrt{\epsilon}|\mathcal{F}_M|$. The reinforcement term is

$$\frac{1}{|\mathcal{F}_M|}\sum_{E\in\mathcal{C}_2}\Big(\frac{\log M-\log C(a,b)}{\log M}\Big)^2 \;\ll\; \frac{|\mathcal{C}_2|}{N^5}\;\le\;\sqrt{\epsilon}. \tag{8.33}$$

We bound the cross terms.

$$S \;=\; \frac{1}{|\mathcal{F}_M|}\sum_{E\in\mathcal{C}_2}\Big(\frac{\log M-\log C(a,b)}{\log M}\Big)\sum_{\gamma_{E_{a,b}^{(j_2)}}} f_2(L_M\gamma_{E_{a,b}^{(j_2)}}). \tag{8.34}$$

Inserting absolute values and replacing $|f_2|$ with g_2 yields

$$S \leq \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{C}_2}\Big|\frac{\log M-\log C(a,b)}{\log M}\Big|\sum_{\gamma_{E_{a,b}^{(j_2)}}} g_2(L_M\gamma_{E_{a,b}^{(j_2)}}). \tag{8.35}$$

We now apply the Modified Explicit Formula, Equation 8.1, to g_2. There are four of terms.

The first is $\frac{\log C(a,b)}{\log M}\widehat{f}_1(0)+f_1(0)=O(1)$. Hitting this with $\Big|\frac{\log M-\log C(a,b)}{\log M}\Big|$ and summing over $E\in\mathcal{C}_2$ is $\ll |\mathcal{C}_2|\leq\sqrt{\epsilon}|\mathcal{F}_M|$. Dividing by $|\mathcal{F}_M|$ gives a contribution of at most $\sqrt{\epsilon}$. A similar argument handles the fourth term, the error which is of size $\frac{\log\log M}{\log M}=O(1)$.

The third term is from the sum of $a_{a,b}^2(p)$. Bounding trivially by Hasse, we see the sum over p is $O(1)$ by Corollary B.3.

We are left with the difficult piece, arising from $a_{a,b}(p)$

8.9.5 Contribution from $\mathcal{C}_2$, the Small Conductors, II

We must bound

$$S_{bad} \leq \frac{1}{|\mathcal{F}_M|}\sum_{E\in\mathcal{C}_2}\Big|\frac{\log M-\log C(a,b)}{\log M}\Big|\Big|\sum_p\frac{1}{p}\frac{\log p}{\log M}\widehat{g}_2\Big(\frac{\log p}{\log M}\Big)a_{a,b}(p)\Big|. \tag{8.36}$$

We apply Cauchy-Schwartz.

$$\begin{aligned} S_{bad} &\leq \frac{1}{|\mathcal{F}_M|}S_1^{\frac{1}{2}}S_2^{\frac{1}{2}},\\ & S_1=\sum_{E\in\mathcal{C}_2}\Big(\frac{\log M-\log C(a,b)}{\log M}\Big)^2\\ & S_2=\sum_{E\in\mathcal{C}_2}\Big|\sum_p\frac{1}{p}\frac{\log p}{\log M}\widehat{g}_2\Big(\frac{\log p}{\log M}\Big)a_{a,b}(p)\Big|^2. \end{aligned} \tag{8.37}$$

As each summand in S_1 is $O(1)$, $S_1\ll|\mathcal{C}_2|=\sqrt{\epsilon}N^5\ll\sqrt{\epsilon}|\mathcal{F}|$.

For S_2, as each summand is positive, we may increase the summation to all $E\in\mathcal{F}$ and not just $E\in\mathcal{C}_2$. We could have increased to $\mathcal{F}_M$, but it is easier to increase to $\mathcal{F}$. We find

$$S_2 \leq \sum_{E\in\mathcal{F}}\Big|\sum_p\frac{1}{p}\frac{\log p}{\log M}\widehat{g}_2\Big(\frac{\log p}{\log M}\Big)a_{a,b}(p)\Big|^2$$

$$\leq \quad |\mathcal{F}|\left[\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\sum_{i=1}^{2}\sum_{p_i}\frac{1}{p_i}\frac{\log p_i}{\log M}\widehat{g}_2\Big(\frac{\log p_i}{\log M}\Big)a_{a,b}(p_i)\right]. \tag{8.38}$$

As the square of a real number is positive, we drop the absolute values above.

We have already proven the boundedness of such sums. If $p_1 = p_2$, we use Hasse to bound $a^2_{a,b}(p)$ by $4p$. For each curve, we are left with $\sum_p \frac{1}{p}\frac{\log p}{\log M}\widehat{g}_2\Big(\frac{\log p_i}{\log M}\Big)$, which is $O(1)$ by Corollary B.3. The introduced $\frac{1}{|\mathcal{F}|}$ factor cancels the number of curves.

If $p_1 \neq p_2$, we break $\sum_{E\in\mathcal{F}} = \sum_{a=-N^2}^{N^2}\sum_{b=-N^3}^{N^3}$ into blocks of size p_1p_2. We have $\frac{2N^2}{p_1p_2}\frac{2N^3}{p_1p_2}$ such blocks. By Lemma 2.6, $\sum_{a,b(p_1p_2)} a_{a,b}(p_1)\ a_{a,b}(p_2) = A_{1,\mathcal{F}}(p_1)A_{1,\mathcal{F}}(p_2)$ if $p_1 \neq p_2$. Thus there is no contribution (for small support) if $p_1 \neq p_2$, as the only contributing term will be the small incomplete sum.

Thus, $S_2 \ll O(|\mathcal{F}|)$. As $|\mathcal{F}_M| = \frac{|\mathcal{F}|}{\zeta(10)}$, substituting into the Cauchy-Schwartz bound yields

Lemma 8.17 $S_{bad} \ll \sqrt{\epsilon}$

Therefore, we have shown

Lemma 8.18 (Contributions from the Small Conductors) *Given $\epsilon > 0$, the small conductors ($E \in \mathcal{C}_2$) contribute $O(\sqrt{\epsilon})$.*

8.9.6 Modified 2-Level Density, II

Combining the above, we have shown the conductor factors contributes at most $\ll \sqrt{\epsilon} + \frac{1}{\log N}$. Therefore, we may remove them in $D_{2,\mathcal{F}}{}''^*(f)$, and we obtain

Theorem 8.19 (Modified 2-Level Density)

$$\begin{aligned} D'_{2,\mathcal{F}_M}(f) \quad &= \quad \prod_{i=1}^{2}\Big[\widehat{f}_i(0)+\frac{1}{2}f_i(0)\Big] + 2\int_{-\infty}^{\infty}|u|\widehat{f}_1(u)\widehat{f}_2(u)du + \\ &\quad -2\widehat{f_1f_2}(0) - f_1(0)f_2(0) + N(\mathcal{F}_M,-1)f_1(0)f_2(0). \end{aligned} \tag{8.39}$$

8.10 Summary of Results

Let $N(\mathcal{F}_M, -1)$ be the percent of curves in $\mathcal{F}_M$ with odd functional equation.

Theorem 8.20 *For the family of all elliptic curves such that $p^4|a \to p^6 \nmid b$, if the support is sufficiently small, the density function (as $|\mathcal{F}_M| \to \infty$) converges to*

$$W_{2,\mathcal{D}}(x_1, x_2) + \delta(x_1)\delta(x_2)N(\mathcal{F}_M, -1) \tag{8.40}$$

Assuming equidistribution of sign in the limit, the density is

$$\widehat{W_{2,\mathcal{F}_M}} = \widehat{W_{2,O}}. \tag{8.41}$$

Thus, assuming equidistribution of sign, the modified 2-level density for the family of almost minimal elliptic curves, with small support, corresponds to the group $\mathcal{G} = O$; further, in order to do the above calculations, we assume only GRH.

Again, modulo the distribution of signs, we confirm Katz and Sarnak's predictions for the 2-level density.

9 Modified 1- and 2-Level Density, One-Parameter Families

9.1 Introduction

In proving the Rational Surfaces Density Theorem (Theorem 7.9), the major difficulty was handling the t-dependence in the conductors. We now determine the modified 1- and 2-level densities for one-parameter families; ie, instead of scaling each curve's zeros by the logarithm of the curve's conductor, we rescale by the average log-conductor. As the proof is almost identical to Theorem 8.19, we only sketch the arguments below.

Similar to before, define

$$\log M = \sum_{t=N}^{2N} \log C(t). \tag{9.1}$$

Unlike the case of almost minimal curves, there is no sieving required. For $D(t)$ square-free, $C(t)$ is a polynomial in t, say of degree k. We show $\log M = \log N^k + O(\log\log N)$, and the number of curves with small conductor is $o(N)$. The rest of the proof mirrors that of Theorem 8.19.

To simplify the presentation, we assume $\forall t$, $\Big(\Delta(t), c_4(t)\Big) = 1$, and $D(t)$ has no factors of degree 12 or more.

9.2 $\nu(d)$

Recall $\nu(d)$ is the number of incongruent solutions to $D(t) \equiv 0 \bmod d^2$. Earlier (Lemma 3.5) we proved $\nu(d) \ll d^\epsilon$ for d square-free. We now extend to all d, modifying the definition of $\nu(d)$.

Definition 9.1 *For this chapter only, $\nu(n)$ is the number of incongruent roots of $D(t) \equiv 0$ mod n.*

We use the following fact (See [Nag], Theorem 53):

Lemma 9.2 *Let δ be the discriminant of a primitive integral polynomial $D(t)$ (not necessarily irreducible). If $p^{\mu_p}||\delta$, then the number of incongruent roots of $D(t) \equiv 0$ mod p^α equals the number of incongruent roots of $D(t) \equiv 0$ mod $p^{2\mu_p+1}$ for all $\alpha \geq 2\mu_p + 1$.*

Note for $\mu_p = 0$ this reduces to Lemma 3.3.

Lemma 9.3 *$\nu(d) \ll d^\epsilon$ for all d.*

Proof: Let $D(t)$ be a degree k primitive irreducible polynomial with discriminant δ. By Lemmas 3.1, 3.2, 3.3 and 9.2, $\nu(p^\alpha)$ is bounded by k for $p \nmid \delta$, and $p^{2\mu_p+1}$ for $p|\delta$. As $p^{\mu_p}||\delta$, for $p|\delta$, $\nu(p^\alpha) \leq \delta^3 k$.

Assume δ has l distinct prime factors. Let $d = \prod_{i=1}^r p_i^{\alpha_i}$ have r distinct prime factors. Then $\nu(d) = \prod_{i=1}^r \nu(p_i^{\alpha_i}) \leq \delta^{3l} k^r$. Let $d_0 = \prod_{p|d} p$. As in the proof of Lemma 3.5, $r = \log_2 \tau(d_0)$, and we get $\nu(d) \ll \tau^{\log_2 k}(d_0) \ll d_0^\epsilon$. As $d_0 \leq d$, we get $\nu(d) \ll d^\epsilon$ for all d.

9.3 $\log M$

Let $D(t)$ be the product of the irreducible polynomial factors of $\Delta(t)$. As we are assuming $\Big(D(t), c_4(t)\Big) = 1$, for t good, $C(t) = D(t)$, up to constants from the bad primes. Before, such inaccuracies were deadly (as we needed monotonicity to bound some of the sums); here, however, these errors are negligible on a logarithmic scale.

Thus, we expect the logarithms of the conductors to be of size $\log N^k$, at least for t good. The conductors decrease when $D(t)$ is divisible by second or higher powers of primes. For a given t, let us write

$$D(t) = \prod_{i=1}^a p_i \prod_{j=1}^b q_j^{2s_j+\delta_j}, \tag{9.2}$$

where all the primes above are distinct, $s_j \geq 1$ and $\delta_j \in \{0,1\}$.

By the ABC or Square-Free Sieve conjecture (or unconditionally if all factors of $D(t)$ are of degree at most 3), there are at most $o(N)$ choices of $t \in [N, 2N]$ such that $D(t)$ is divisible by p^2, $p > \log N$. Thus, these t will contribute at most $o(\log N)$ to $\log M$, and we may now consider the subset of t such that $D(t)$ is not divisible by the square of a prime greater than $\log N$.

If $\prod_j q_j^{2s_j+\delta_j} < \log^3 N$, then the conductor is at least $\log N^k - 3\log\log N + O(1)$ and at most $\log N^k + O(1)$.

We now consider t with $D(t)$ where the q-product is at least $\log^3 N$. As $2s_j + \delta_j \leq 3s_j$,

$$\log^3 N \ \leq \ \prod_{j=1}^b q_j^{2s_j+\delta_j} \ \leq \ \Big(\prod_{j=1}^b q_j^{s_j}\Big)^3. \tag{9.3}$$

Therefore, $q_s = \prod_j q_j^{s_j} \geq \log N$, and each prime $q_j \leq \log N$.

We say a $t \in [N, 2N]$ is of type d if $d^2|D(t)$. The above shows we need to estimate all t that are of type d, with $d > \log N$ and all factors of d are primes less than $\log N$. The above calculation is for a number of type q_s, as q_s^2 divides this $D(t)$. Clearly, if a number is of type d_1 and $d_0|d_1$, the number is of type d_0.

It is therefore sufficient to bound the number of type n numbers, where n is at least $\log N$ and at most $\log^2 N$. The lower bound is clear (as we want q_s to be at least $\log N$). For the upper bound, say for some t, there is a $q_s \geq \log N$ with $q_s^2|D(t)$ and all prime factors of q_s are at most $\log N$. While q_s could be significantly larger than $\log N$, we can find a sub-product with the desired properties by removing factors one at a time. As the largest factor is $\log N$, the largest we can be and unable to remove a factor is $\log^2 N$.

Fix a prime $q < \log N$. The largest power of q we need consider is $q^m = \log^2 N$, or $m = \frac{2 \log\log N}{\log q} < \log N$. Given a q^m, we must consider all multiples $q^m d \in [\log N, \log^2 N]$ with all prime factors of $d \leq \log N$. Clearly we overcount if we consider all $d \in [\log N, \log^2 N]$.

The number of incongruent solutions to $D(t) \equiv 0 \bmod q^{2m}d^2$, is $\frac{N\nu(q^m d)}{q^{2m}d^2} + O(\nu(q^m d))$. By Lemma 9.3, $\nu(n) \ll n^\epsilon$. Thus the number of such t is bounded by

$$\sum_{q=2}^{\log N} \sum_{m=1}^{\log N} \sum_{d=\frac{\log N}{q^m}}^{\log^2 N} \left[N \frac{1}{q^{2m-\epsilon}} \frac{1}{d^{2-\epsilon}} + O\Big(q^{m\epsilon} d^\epsilon\Big)\right]. \tag{9.4}$$

As $q^m d \leq \log^2 N$, the $O(q^{m\epsilon}d^\epsilon)$ piece is $O(\log^6 N)$. The remaining sum is

$$\begin{aligned}
N \sum_{q=2}^{\log N} \sum_{m=1}^{\log N} \frac{1}{q^{2m-\epsilon}} \sum_{d=\frac{\log N}{q^m}}^{\log^2 N} \frac{1}{d^{2-\epsilon}} &\ll N \sum_{q=2}^{\log N} \sum_{m=1}^{\log N} \frac{1}{q^{2m-\epsilon}} \Big(\frac{\log N}{q^m}\Big)^{-1+\epsilon} \\
&\ll \frac{N}{\log^{1-\epsilon} N} \sum_{q=2}^{\log N} \sum_{m=1}^{\log N} \frac{1}{q^m} \\
&\ll \frac{N}{\log^{1-\epsilon} N} \sum_{q=2}^{\log N} \frac{1}{q} \\
&\ll \frac{N}{\log^{1-\epsilon} N} \log\log N. \qquad (9.5)
\end{aligned}$$

We have proved

Lemma 9.4 *The number of $t \in [N, 2N]$ such that $D(t)$ is divisible by d^2, $d > \log N$, is $o(N)$. Further, $\log M = \log N^k + o(\log N)$.*

9.4 Large and Small Conductors

As in the family of all curves, let $\mathcal{C}_1$ be the curves with large conductor, and $\mathcal{C}_2$ the curves with small conductor. The determination of the size of $\log M$ suggests natural definitions for these sets: take $\mathcal{C}_2$ to be all the bad t from above (t with $S(t)$ divisible by the square of a large prime, or by the square of a $d \geq \log N$ made up of powers of primes at most $\log N$).

For $t \in \mathcal{C}_1$, $\frac{\log M - \log C(t)}{\log M} \ll \frac{1+\log\log N}{\log N}$; for $t \in \mathcal{C}_2$, the difference is $O(1)$, but $|\mathcal{C}_2| = o(N)$.

An inspection of Theorem 8.19 shows these were the difficult needed input. The remaining input is simply complete sums and partial densities.

Thus, in an entirely analogous manner, we can show the conductor correction is negligible.

9.5 Modified Density

Theorem 9.5 (Modified 1- and 2-Level Densities) *If $j(t)$ and $M(t)$ are non-constant and $\Big(c_4(t), \Delta(t)\Big) = 1$, for small support, $D^{(r)'}_{1,\mathcal{F}}(f_1) = \widehat{f_1}(0) + \frac{1}{2}f_1(0)$ and $\widehat{W^{(r)'}_{2,\mathcal{F}}} = \widehat{W_{2,O}}$. Again, for small support, we confirm Katz and Sarnak's prediction for the 1-level non-family density, and conditional on the distribution of the signs, we confirm the 2-level non-family density predictions.*

A more cumbersome book-keeping should allow the relaxation of the relatively prime constraint.

9.6 Summary

We comment on the difference in difficulties in determining the n-level density versus the modified n-level density.

For the former, much care is needed to handle the t-dependence of the conductor. To control the error terms, we needed to pass to a manageable subsequence (a union of almost arithmetic sequences) where the conductors were monotone. The monotonicity was the essential input to control the difficult error piece: without it, we could have traversed the interval so many times that the bounds would be useless.

Contrast this with the modified n-level density case. As all curves' zeros are rescaled by $\log M$, the calculations on the prime side are trivial. Some care is needed to calculate the main term of $\log M$ (with good error), as well as how many curves have small conductor. These, however, are standard calculations which only weakly depend on the elliptic curves; in the previous case, we needed to use Tate's algorithm and passing to subsequences to determine the conductors exactly.

Part IV

1- and 2-Level Densities for Families of Constant Sign

10 1- and 2-Level Densities for Families with Constant Sign

10.1 $\mathcal{F} : y^2 = x^3 + 2^4(-3)^3(9t+1)^2$, $9t+1$ Square-Free

Let $\mathcal{F} : y^2 = x^3 + 2^4(-3)^3(9t+1)^2$, $t \in [N, 2N]$, $9t+1$ square-free. For $p \equiv 2(3)$, $x \to x^3$ is an automorphism and $a_t(p) = 0$. Therefore in the sequel we assume all primes are congruent to 1 mod 3, for any sum involving a prime congruent to 2 mod 3 is zero. Note $p \equiv 1(3)$ implies that -3 is a square mod 3.

Given that $p \neq 2, 3$ and $p \equiv 1(3)$, let a be a square-root of -3 mod p. Change variables: $t \to 3^{-2}(t-1)$ to go from $2^4(-3)^3(9t+1)^2$ to $2^4(-3)^3t^2$. Then change variables $t \to 2^{-2}a^{-3}t$. Thus, for $p > 3$, complete sums of $y^2 = x^3 + t^2$ equal those from the original curve.

10.1.1 ϵ_t, $C(t)$ and $|\mathcal{F}|$

We show $y^2 = x^3 + 2^4(-3)^3D^2$ is equivalent to $y^3 = x^3 + Dz^3$. Start with $y^3 = x^3 + Dz^3$.

$$\begin{array}{rclll}
3x(y^2+xy) & = & -x^3 - Dz^3 & \text{from} & x \to x+y \\
3x(y+\frac{1}{2}x)^2 & = & -\frac{1}{4}x^3 - Dz^3 & \text{from} & y \to y - \frac{1}{2}x \\
3xy^2 & = & -x^3 - 2^2Dz^3 & \text{from} & y \to \frac{1}{2}y \\
3y^2z & = & -z^3 - 2^2Dx^3 & \text{from} & x \to z,\ z \to x \\
y^2z & = & -2^2Dx^3 - 3^3z^3 & \text{from} & y \to \frac{1}{9}y,\ x \to \frac{1}{3}x \\
y^2z & = & -x^3 - 2^4 \cdot 3^3D^2z^3 & \text{from} & y \to \frac{y}{2^2D^2}, x \to \frac{x}{2^2D} \\
y^2z & = & \quad x^3 + 2^4 \cdot (-3)^3 \cdot D^2z^3 & \text{from} & x \to -x.
\end{array} \tag{10.1}$$

If $p \neq 2, 3$ the above calculations are permissible. Let $E_1 : y^3 = x^3 + Dz^3$ and $E_2 : y^2z = x^3 + 2^4(-3)^3D^2z^3$. For $p = 2$, $a_2(E_1) = 0$ and $a_2(E_2) = 0$. For $p = 3$, $a_3(E_1) = 0$ and $a_3(E_2) = 0$.

Therefore in calculating a_p we may use either E_1 or E_2.

We proved this equivalence as Birch and Stephens [BS] calculate the sign of the functional equation for $y^3 = x^3 + Dz^3$, D cube-free. It is

Theorem 10.1 (Birch-Stephens)

$$\epsilon_{E_D} = -w_3 \prod_{p \neq 3} w_p, \tag{10.2}$$

where $w_3 = -1$ if $D \equiv \pm 1, \pm 3(9)$ and 1 otherwise, $w_p = -1$ if $p|D, p \equiv 2(3)$ and 1 otherwise, and D is cube-free.

Consider our choice of $D = D(t) = 9t+1$. Mod 9 this is 1, so $-w_3$ is 1. Assume a prime congruent to 2 mod 3 divides $9t+1$. If there were only one such prime, the remaining primes would be congruent to 1 mod 3, and the product over all primes dividing $9t+1$ would be congruent to 2 mod 3, a contradiction. Hence the number of primes congruent to 2 mod 3 dividing $9t+1$ is even. For $9t+1$ square-free, this proves the functional equation is even.

By Lemma D.4, $C(t) = 3^3(9t+1)^2$ for $9t+1$ square-free. $\delta_D = 1$, $k = 1$, $a_k = 9$ so $\mathcal{P} = \{2, 3\}$. As $\nu(2) = 1$ and $\nu(3) = 0$, by Theorem 3.8 $c_{\mathcal{F}} > 0$.

10.1.2 $A_{1,\mathcal{F}}(p)$

For $p > 3$ (using the change of variables mentioned) and $p \equiv 1$ mod 3:

$$\begin{aligned}
-A_{1,\mathcal{F}}(p) &= \sum_{t(p)} a_t(p) \\
&= \sum_{t(p)} \sum_{x(p)} \left(\frac{x^3 + 2^4(-3)^3(9t+1)^2}{p} \right) \\
&= \sum_{t(p)} \sum_{x(p)} \left(\frac{x^3 + t^2}{p} \right) \\
&= \sum_{t=1}^{p-1} \sum_{x(p)} \left(\frac{x^3 + t^2}{p} \right) \\
&= \sum_{t=1}^{p-1} \sum_{x(p)} \left(\frac{t^2}{p} \right) \left(\frac{tx^3 + 1}{p} \right) \\
&= \sum_{t(p)} \sum_{x(p)} \left(\frac{tx^3 + 1}{p} \right) - p \\
&= p - p = 0. \qquad (10.3)
\end{aligned}$$

10.1.3 $A_{2,\mathcal{F}}(p)$

If $p \equiv 2(3)$ then $a_t^2(p) = 0$. Assume $p \equiv 1(3)$.

$$A_{2,\mathcal{F}}(p) = \sum_{t(p)} a_t^2(p)$$

$$
\begin{aligned}
&= \sum_{t(p)}\sum_{x(p)}\sum_{y(p)} \left(\frac{x^3+2^4(-3)^3(9t+1)^2}{p}\right)\left(\frac{y^3+2^4(-3)^3(9t+1)^2}{p}\right) \\
&= \sum_{t(p)}\sum_{x(p)}\sum_{y(p)} \left(\frac{x^3+t^2}{p}\right)\left(\frac{y^3+t^2}{p}\right) \\
&= \sum_{t=1}^{p-1}\sum_{x(p)}\sum_{y(p)} \left(\frac{x^3+t^2}{p}\right)\left(\frac{y^3+t^2}{p}\right) \\
&= \sum_{t=1}^{p-1}\sum_{x(p)}\sum_{y(p)} \left(\frac{t^4}{p}\right)\left(\frac{tx^3+1}{p}\right)\left(\frac{ty^3+1}{p}\right) \\
&= \sum_{x(p)}\sum_{y(p)}\sum_{t(p)} \left(\frac{tx^3+1}{p}\right)\left(\frac{ty^3+1}{p}\right) - p^2. \qquad (10.4)
\end{aligned}
$$

We use inclusion / exclusion to reduce to $xy \neq 0$. If $x = 0$, the t and y-sums give p. If $y = 0$, the t and x-sums give p. We subtract the doubly counted contribution from $x = y = 0$, which gives p. Thus

$$
A_{2,\mathcal{F}}(p) = \sum_{x=1}^{p-1}\sum_{y=1}^{p-1}\sum_{t(p)} \left(\frac{tx^3+1}{p}\right)\left(\frac{ty^3+1}{p}\right) + 2p - p - p^2. \qquad (10.5)
$$

By Lemma C.1, the t-sum is $(p-1)\left(\frac{x^3y^3}{p}\right)$ if $p|(x^3-y^3)^2$ and $-\left(\frac{x^3y^3}{p}\right)$ otherwise. As $p = 6m+1$, let g be a generator of the multiplicative group $\mathbf{Z}/p\mathbf{Z}$. Solving $g^{3a} \equiv g^{3b}$ yields $b = a$, $a + 2m$, or $a + 4m$. Thus, $x^3 \equiv y^3$ three times, and in each instance y equals x times a square (1, g^{2m}, g^{4m}).

$$
\begin{aligned}
A_{2,\mathcal{F}}(p) &= \sum_{x=1}^{p-1}\sum_{\substack{y=1 \\ y^3\equiv x^3}}^{p-1} p - \sum_{x=1}^{p-1}\sum_{y=1}^{p-1}\left(\frac{x^3y^3}{p}\right) + p - p^2 \\
&= (p-1)3p + p - p^2 \\
&= 2p^2 - 2p = 2p^2 + O(p). \qquad (10.6)
\end{aligned}
$$

From Michel's Theorem, Theorem 2.4, we expect $A_{2,\mathcal{F}}(p) = p^2 + O(p^{\frac{3}{2}})$; however, his theorem is only applicable for non-constant $j(t)$. As $j(t)$ is constant, we must directly compute $A_{2,\mathcal{F}}(p)$. Further, as $a_t(p)$ trivially vanishes for half of the primes, we expect and observe twice the predicted contribution at the other primes. Finally, we will see later that the correction term to $A_{2,\mathcal{F}}(p)$ contributes a potential lower order term to the density functions.

By Dirichlet's Theorem for Primes in Arithmetic Progressions (using Lemma B.1 instead of Corollaries B.2 and B.3), we see the factors of 2 compensate for the restriction to primes congruent to 1 mod 3, and this will be harmless in the applications.

10.1.4 $D_{1,\mathcal{F}}(f)$ and $D_{2,\mathcal{F}}(f)$

We have shown the family satisfies the conditions of Theorem 7.9 with $r = 0$. Therefore

Theorem 10.2 ($D_{1,\mathcal{F}}(f_1)$ and $D_{2,\mathcal{F}}(f)$) *For small support, $D_{1,\mathcal{F}}(f_1) = \widehat{f}_1(0) + \frac{1}{2}f_1(0)$. As every curve in our family has even functional equation, $c(\mathcal{F}) = +$, $N(\mathcal{F}, -1) = 0$, and*

$$\widehat{W_{2,\mathcal{F}}} = \widehat{W_{2,\mathrm{O}^+}}. \tag{10.7}$$

10.2 $\mathcal{F} : y^2 = x^3 \pm 4(4t + 2)x$, $4t + 2$ Square-Free

Let $\mathcal{F} : y^2 = x^3 + 4(4t+2)x$, $4t+2$ square-free. We need to study sums of $\left(\frac{x^3 \pm 4(4t+2)x}{p}\right)$. For $p > 2$, changing variables by $t \to t - 2^{-1}$, $t \to \pm 16^{-1}t$, we are led to study sums of $\left(\frac{x^3+tx}{p}\right)$. If $p \equiv 3 \bmod 4$ then $\left(\frac{-1}{p}\right) = -1$. Changing variables $x \to -x$ shows $a_t(p) = \sum_{x(p)} \left(\frac{f_t(x)}{p}\right)$ vanishes; therefore, in the sequel we only consider $p \equiv 1 \bmod 4$.

10.2.1 ϵ_t, $C(t)$ and $|\mathcal{F}|$

Birch and Stephens [BS] calculate the sign of the functional equation for this family. For general D, D not divisible by 4 or any fourth power, the sign of the functional equation for the curve $y^2 = x^3 + 4Dx$ is

$$w_\infty w_2 \prod_{p^2 || D} w_p, \tag{10.8}$$

where $w_\infty = \mathrm{sgn}(-D)$, $w_2 = -1$ if $D \equiv 1, 3, 11, 13 \bmod 16$ and 1 otherwise, $w_p = -1$ for $p \equiv 3(4)$, and $w_p = 1$ for other $p \geq 3$.

By restricting to positive, even, square-free D, we force the sign of the functional equation to be odd. Hence $\epsilon_D = -1$ if $D = 4t + 2$, D square-free. If we had taken $D = -(4t + 2)$, $4t + 2$ square-free, we would have found $\epsilon_D = +1$.

By Lemma D.5, for $D(t) = 4t + 2$ square-free, $C(t) = 2^6(4t + 2)^2$. A similar calculation yields this for $D(t) = -(4t+2)$. $\delta_D = 1$, $k = 1$, $a_k = 4$ so $\mathcal{P} = \{2\}$. As $\nu(2) = 0$, by Theorem 3.8 $c_{\mathcal{F}} > 0$.

10.2.2 $A_{1,\mathcal{F}}(p)$

For $p > 2$:

$$A_{1,\mathcal{F}}(p) \quad = \quad -\sum_{t(p)}\sum_{x(p)}\left(\frac{x^3+tx}{p}\right). \tag{10.9}$$

If $x = 0$ we get zero; for $x \neq 0$, changing variables $t \to x^{-1}t$ yields 0. Hence $A_{1,\mathcal{F}}(p) = 0$.

10.2.3 $A_{2,\mathcal{F}}(p)$

$$\begin{aligned} A_{2,\mathcal{F}}(p) \quad &= \quad \sum_{t(p)}\sum_{x(p)}\sum_{y(p)}\left(\frac{x^3+tx}{p}\right)\left(\frac{y^3+ty}{p}\right) \\ &= \quad \sum_{t(p)}\sum_{x(p)}\sum_{y(p)}\left(\frac{xy}{p}\right)\sum_{t(p)}\left(\frac{t^2+(x^2+y^2)t+x^2y^2}{p}\right). \end{aligned} \tag{10.10}$$

Let $\delta = (x^2+y^2)^2 - 4x^2y^2 = (x^2-y^2)^2$ be the discriminant of the t quadratic. By Lemma C.2, the t-sum is $p-1$ if $p|\delta$ and -1 otherwise. As we have a sum of $\left(\frac{xy}{p}\right)$, the -1 washes out. We are left with

$$A_{2,\mathcal{F}}(p) \quad = \quad p \sum_{\substack{x,y \\ p|x^2-y^2}} \left(\frac{xy}{p}\right). \tag{10.11}$$

$x^2 - y^2 = (x-y)(x+y)$. For a non-zero x, there are two y such that $p|\delta$: $y = \pm x$. If $p \equiv 3(4)$ then $\left(\frac{-1}{p}\right) = -1$ and $A_{2,\mathcal{F}}(p) = 0$. If $p \equiv 1(4)$ then $\left(\frac{-1}{p}\right) = 1$ and the sum over x and y ($2p-2$ terms) yields $2p(p-1)$.

10.2.4 $D_{1,\mathcal{F}}(f)$ and $D_{2,\mathcal{F}}(f)$

For the family $\mathcal{F}_{\pm} : y^2 = x^3 \pm 4(4t+2)x$, $4t+2$ square-free, $c(\mathcal{F}) = \mp$ (ie, all curves in $\mathcal{F}_-$ have even sign, in $\mathcal{F}_+$ odd sign. We have shown the families satisfy the conditions of Theorem 7.9 with $r = 0$. Therefore

Theorem 10.3 ($D_{1,\mathcal{F}}(f_1)$ and $D_{2,\mathcal{F}}(f)$) *For small support, $D_{1,\mathcal{F}}(f_1) = \widehat{f_1}(0) + \frac{1}{2}f_1(0)$. Further,* *the* 2*-level densities are*

$$\widehat{W_{2,\mathcal{F}_\pm}} = \widehat{W_{2,O^\mp}}. \tag{10.12}$$

10.3 $\mathcal{F} : y^2 = x^3 + tx^2 - (t+3)x + 1$

For this family (due to Washington)

$$\begin{aligned} c_4(t) &= 2^4(t^2+3t+9) \\ \Delta(t) &= 2^4(t^2+3t+9)^2 \\ j(t) &= 2^8(t^2+3t+9). \end{aligned} \tag{10.13}$$

Washington ([Wa]) proved the rank is odd for t^2+3t+9 square-free, assuming the finiteness of the Tate-Shafarevich group. Rizzo [Ri] proved the rank is odd for all t. While $j(t)$ is non-constant, $M(t) = 1$ ($M(t)$ is the product of all irreducible polynomials dividing $\Delta(t)$ but not $c_4(t)$). Thus, Helfgott's results on equidistribution of sign are not applicable.

10.3.1 ϵ_t, $C(t)$ and $|\mathcal{F}|$

For sieving convenience, we replace t with $12t+1$. Let $D(t) = 144t^2+60t+13$. By Lemma D.10, for $D(t)$ square-free, $C(t) = 2^3(144t^2+60t+13)$.

$\delta_D = -2^4 3^5$, $k = 2$, $a_k = 2^4 3^2$ so $\mathcal{P} = \{2,3\}$. $D(t)$ is a primitive integral polynomial. For $p \nmid 6$, by Lemma 3.3 the number of incongruent solutions of $D(t) \equiv 0 \bmod p^2$ equals the number of incongruent solutions of $D(t) \equiv 0 \bmod p$. As $\nu(2) = \nu(3) = 0$, by Theorem 3.8, $c_{\mathcal{F}} > 0$.

In determining $A_{r,\mathcal{F}}(p)$ below, for $p > 3$ we may use t instead of $12t+1$ in the complete sums.

10.3.2 $A_{1,\mathcal{F}}(p)$

$$\begin{aligned} A_{1,\mathcal{F}}(p) &= -\sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\left(\frac{x^3-3x+1+tx(x-1)}{p}\right) \\ &= -\sum_{x=2}^{p-1}\sum_{t=0}^{p-1}\left(\frac{x^3-3x+1+tx(x-1)}{p}\right) - \sum_{t=0}^{p-1}\left(\frac{1}{p}\right) - \sum_{t=0}^{p-1}\left(\frac{-1}{p}\right) \\ &= -\sum_{x=2}^{p-1}\sum_{t=0}^{p-1}\left(\frac{(x^3-3x+1)+t}{p}\right) - p - p\left(\frac{-1}{p}\right) \end{aligned}$$

$$= \quad -p\left[1+\left(\frac{-1}{p}\right)\right]. \tag{10.14}$$

Hence $A_{1,\mathcal{F}}(p)$ is $-2p$ for $p \equiv 1(4)$ and 0 for $p \equiv 3(4)$. Thus the average rank over $\mathbb{Q}(t)$ is 1 (see Rosen-Silverman, Theorem 1.2)

10.3.3 $A_{2,\mathcal{F}}(p)$

If we use the Gauss sum expansion (Equation 2.4) to calculate $A_{2,\mathcal{F}}(p)$, we are quickly led to determining when p divides $(x^3-3x+1)\ y(y-1)-\ (y^3-3y+1)\ x(x-1)$. It is not sufficient to determine how often p divides this; we then need to sum over sum x and y. We therefore apply Michel's Theorem, and immediately obtain $A_{2,\mathcal{F}}(p) = p^2 + O(p^{\frac{3}{2}})$.

10.3.4 $D^{(1)}_{1,\mathcal{F}}(f)$ and $D^{(1)}_{2,\mathcal{F}}(f)$

Recall $D^{(1)}_{1,\mathcal{F}}(f_1)$ and $D^{(1)}_{2,\mathcal{F}}(f)$ are the 1- and 2-level densities with the contribution from a single family zero removed.

The conditions of Theorem 7.9 are satisfied with $r = 1$. Therefore

Theorem 10.4 ($D^{(1)}_{1,\mathcal{F}}(f)$ and $D^{(1)}_{2,\mathcal{F}}(f)$) *For small support, $D^{(1)}_{1,\mathcal{F}}(f_1) = \widehat{f_1}(0) + \frac{1}{2}f_1(0)$. Further, the 2-level density of the non-family zeros is*

$$\widehat{W^{(1)}_{2,\mathcal{F}}} = \widehat{W_{2,\mathrm{O}^-}}. \tag{10.15}$$

10.4 Summary of Examples with $j(t)$ Constant

As the 1-level density functions for SO(even), O, and SO(odd) all agree in the interval $[-1,1]$, we are unable to use the 1-level density to distinguish these candidate symmetry groups; however, as expected, the 2-level density is able to distinguish the three groups.

We have found four families where the observed density agrees with the density of one (and only one) symmetry group. As expected, after removing the contribution from the family zeros, the symmetry group is determined by the distribution of signs in the family, verifying Katz and Sarnak's predictions.

Only GRH was assumed (except for Washington's family, where the Birch and Swinnertyon-Dyer conjecture was assumed for interpretation purposes only). We are able to handle the dependence of the conductors on t, the error terms, and calculate the sign of the functional equations.

Part V

1- and 2-Level Densities of Rational Surfaces of Rank ≤ 6

11 General Ideas of the Methods

11.1 Introduction

We study several one-parameter families investigated by Fermigier [Fe2], as well as some new ones. Consider 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 $\mathbb{Q}(t)$. By choosing the polynomials appropriately, we can force rational points on the curve, and hence construct families of curves of rank $1, 2, 3$ and 4 (and by looking at two new constructions, of rank 5, 6 and possibly 7 and 8) over $\mathbb{Q}(t)$. By evaluating these polynomials at integers, we get families of elliptic curves over $\mathbb{Q}$. By Silverman's Specialization Theorem, for large t the rank of E_t over $\mathbb{Q}$ is at least that of the family over $\mathbb{Q}(t)$.

In order to apply the Rational Surfaces Density Theorem (Theorem 7.9) to calculate the 1- and 2-level densities, for a given family it is sufficient to show

1. $A_{1,\mathcal{F}}(p) = -rp + O(1)$, $A_{2,\mathcal{F}}(p) = p^2 + O(p^{\frac{3}{2}})$.

2. For $D(t)$ good (usually square-free), $C(t)$ is a monotone polynomial.

3. Let $\mathcal{F} = \{t \in [N, 2N] :\ D(t)$ 'good'$\}$; $|\mathcal{F}| = c_{\mathcal{F}}N + o(N)$, $c_{\mathcal{F}} > 0$.

We construct families where $A_{1,\mathcal{F}}(p)$ is $rp + O(1)$. If Tate's conjecture is true for the family, then r may be interpreted as the rank of the family over $\mathbb{Q}(t)$. As rational surfaces are the only cases where Tate's conjecture is known, we mostly confine ourselves to rational surfaces.

For families with non-constant $j(t)$, Michel's Theorem (Theorem 2.4) yields $A_{2,\mathcal{F}}(p) = p^2 + O(p^{\frac{3}{2}})$. Sometimes we show by direct calculation that $A_{2,\mathcal{F}}(p) = p^2 + m_{\mathcal{F}}p + O(1)$. These terms lead to potential lower order corrections to the n-level densities.

$D(t)$ will be the product of the irreducible polynomial factors of the discriminant $\Delta(t)$. Our proof of Theorem 7.9 requires the conductors to be monotone. Thus, it is not enough to control $C(t)$ up to a bounded number of powers of 2 and 3; we need $C(t)$ exactly. For many families (including rational surfaces), this is doable, especially upon a change of variables $t \to ct + t_0$. By controlling $\Big(c_4(t), D(t)\Big)$ for $D(t)$ good, for such t, $C(t)$ is a polynomial. See the Conductor-Cardinality Theorem, Theorem 4.3.

Consider $g(t) = 4t^5 + t(t+1)(t+2)(t+3) + 12$; $g(t)$ is primitive and irreducible over $\mathbb{Q}(t)$, but it is never square-free as it is always divisible by 4. By changing variables we can, however, control how often it is divisible by 2. We would never obtain a positive percent of t yield $g(t)$ square-free, but we can obtain a positive percent of t good.

Invoking Theorem 4.3 is costly, as it requires passing to a small subsequence. If the following condition is met, we may use Theorem 3.8 instead, and obtain a positive percent of t are good without costly sieving. Let δ_D be the discriminant of $D(t)$ and $p_0 = \max\Big(\{p : p | a_k \delta_D\} \cup \{p : p \leq \sqrt{k}\}\Big)$. If $\forall p \leq p_0$, $\nu(p) \leq p^2 - 1$, by Theorem 3.8 a positive percent of t give $D(t)$ square-free.

11.2 Rosen-Silverman Theorem

For unity of presentation, we recall Rosen and Silverman's Theorem Let $\mathcal{E}$ be the family $y^2 = x^3 + A(t)x + B(t)$, $t \in \mathbb{Z}$. For each t, we have the elliptic curve E_t, with

$$a_t(p) = -\sum_{x=0}^{p-1} \left(\frac{x^3 + A(t)x + B(t)}{p}\right). \tag{11.1}$$

Define

$$A_{\mathcal{E}}(p) = \frac{1}{p}\sum_{t=0}^{p-1} a_t(p) = \frac{1}{p} A_{1,\mathcal{F}}(p). \tag{11.2}$$

Recall an elliptic surface is rational if and only if one of the following holds

1. $0 < \max\{3\text{deg } A(t), 2\text{deg } B(t)\} < 12$.

2. $3\text{deg } A(t) = 2\text{deg } B(t) = 12$ and $\text{ord}_{t=0} t^{12}\Delta(t^{-1}) = 0$

See [RSi], pages $46 - 47$ for more details. Rosen and Silverman [RSi] prove

Theorem 11.1 *Let $\mathcal{E} : y^2 = x^3 + A(t)x + B(t)$, and assume Tate's conjecture (known for rational surfaces) for the surface. Then*

$$\lim_{X \to \infty} \frac{1}{X} \sum_{p \leq X} -A_{\mathcal{E}}(p) \log p = \text{rank } \mathcal{E}(\mathbb{Q}(t)). \tag{11.3}$$

For many of the families we construct, $A_{\mathcal{E}}(p)$ is $-r + O(\frac{1}{p})$. Therefore the above and the Prime Number Theorem allow us to conclude that this constant is the rank over $\mathbb{Q}(t)$. Recall the Prime Number Theorem states $\sum_{p<X} \log p = X$ plus lower order terms, significantly lower assuming RH.

Hence we must study

$$A_{1,\mathcal{F}}(p) = pA_{\mathcal{E}}(p) = -\sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\left(\frac{f_t(x)}{p}\right). \tag{11.4}$$

If we show this sum equals $-rp$ for all p, then the family will have rank r over $\mathbb{Q}(t)$ if $A(t)$ and $B(t)$ have small degrees. 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 show $A_{1,\mathcal{F}}(p) = -c_1 p$ for half of the primes and $-c_2 p$ for the other half. By Dirichlet's Theorem on Primes in Arithmetic Progression (primes are well distributed in congruence classes), this will imply the rank is $r = \frac{c_1+c_2}{2}$.

11.3 Other Methods to Construct Families with Rank

The methods developed in this thesis to construct families of a given rank are based on the Rosen-Silverman Theorem. By forcing $A_{\mathcal{E}}(p)$ to be essentially constant, provided our family is a rational surface, we can immediately calculate the rank. If the degrees of the defining polynomials are too large, our results are conditional on Tate's conjecture.

Mestre ([Mes2], [Mes3]) has developed a powerful method to construct families of rank 11 and 12 over $\mathbb{Q}(t)$. Searching within such a family, Nagao [Na2] has found an elliptic curve of rank at least 21.

Mestre considers a 6-tuple of integers a_i. Let $q(x) = \prod_{i=1}^{6}(x - a_i)$ and $p(t,x) = q(x-t)q(x+t)$. There exist polynomials $g(t,x)$ of degree 6 in x and $r(t,x)$ of degree at most 5 in x such that $p(t,x) = g^2(t,x) - r(t,x)$.

Consider the curve $y^2 = r(t,x)$. If $r(t,x)$ is of degree 3 or 4 in x, we obtain an elliptic curve, with points $P_{\pm i}(t) = \Big(\pm t + a_i, g(\pm t + a_i)\Big)$.

The reason this is an elliptic curve is as follows: for $x_{\pm i} = \pm t + a_i$, $p(t, x_{\pm i}) = 0$. Thus, $r(t, x_{\pm i}) = g^2(t, x_{\pm i}) - p(t, x_{\pm i}) = g^2(t, x_{\pm i})$. Therefore, we can solve $y^2 = r(t, x_{\pm i})$. If $r(t,x)$ has degree 4, we may need to change variables to make the coefficient of x^4 a perfect square (see [Mor], [Na2]). Two 6-tuples that work (see [Na2]) are $(-17, -16, 10, 11, 14, 17)$ and $(399, 380, 352, 47, 4, 0)$.

Finally, Shioda [Sh] gives explicit constructions for not only families of rank $2, 4, 6, 7$ and 8 over $\mathbb{Q}(t)$, but generators of the Mordell-Weil groups.

11.4 Outline of the Calculations

In the following chapters we calculate the 1- and 2-level densities for many rational families. While we may immediately apply the Rational Surfaces Density Theorem (Theorem 7.9), proving the theorem for all surfaces at once necessitated passing to a very small subsequence. To obtain better results for a particular example requires a more detailed analysis of the actual equations. We do this in the sequel.

Further, if we simply use Michel's Theorem, we obtain $A_{2,\mathcal{F}}(p) = p^2 + O(p^{\frac{3}{2}})$. For many families, by direct calculation we find $A_{2,\mathcal{F}}(p) = p^2 - m_{\mathcal{F}}p + O(1)$. This allows us to start calculating potential lower order correction terms to the density functions.

In all the calculations below, we need to determine $A_{1,\mathcal{F}}(p)$, $A_{2,\mathcal{F}}(p)$, $j(t)$, $M(t)$ (the product of the irreducible factors of $\Delta(t)$ not dividing $c_4(t)$), a positive percent of t give $D(t)$ (the product of the irreducible factors of $\Delta(t)$) good, and the conductors $C(t)$ for t good.

For convenience,

Definition 11.2 *$c_{\mathcal{F}} > 0$ denotes a positive percent of t are good, and are attainable by sieving (inclusion / exclusion) with negligible contribution from $d > \log^l n$; $|\mathcal{F}| = c_{\mathcal{F}}N + o(N)$, $c_{\mathcal{F}} > 0$.*

12 1- and 2-Level Densities for Rank 0 Rational Surfaces

12.1 $y^2 = x^3 + (t+1)x^2 + tx$

For the family $y^2 = x^3 + (t+1)x^2 + tx$ we have

$$\begin{aligned}
c_4(t) &= 16t^2 - 16t + 16 \\
\Delta(t) &= 16\Big(t \cdot (t-1)\Big)^2 \\
j(t) &= 256\frac{t^6 - 3t^5 + 6t^4 - 7t^3 + 6t^2 - 3t + 1}{t^2(t-1)^2} \\
M(t) &= t(t-1) \qquad (12.1)
\end{aligned}$$

By Lemma D.6, for $t(t-1)$ square-free, the conductors are $C(t) = 2^4 t(t-1)$. $\delta_D = 1$, $k = 2$, $a_k = 1$. As $\mathcal{P}$ is empty, by Theorem 3.8, $c_{\mathcal{F}} > 0$. As $j(t)$ and $M(t)$ are non-constant, by Helfgott's work ([Hel]) we expect the signs to be equidistributed (for all t and for t good).

12.1.1 $A_{1,\mathcal{F}}(p)$ and $A_{2,\mathcal{F}}(p)$

We calculate the complete t-sums of $a_t(p)$ and $a_t^2(p)$. Note we can write the family as $y^2 = x^2(x+1) + x(x+1)t$.

$$A_{1,\mathcal{F}}(p) = \sum_{t(p)} a_t(p) = -\sum_{t=0}^{p-1}\sum_{x=0}^{p-1} \left(\frac{x^2(x+1) + x(x+1)t}{p}\right). \qquad (12.2)$$

If x equals 0 or -1, then the t-sum is zero. Otherwise we change variables $t \to x^{-1}(x-1)^{-1}t$ and again get zero from the t-sum. Hence $A_{1,\mathcal{F}}(p)$ vanishes.

$$\begin{aligned}
A_{2,\mathcal{F}}(p) &= \sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\sum_{y=0}^{p-1} \left(\frac{x^2(x+1) + x(x+1)t}{p}\right)\left(\frac{y^2(y+1) + y(y+1)t}{p}\right) \\
&= \sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\sum_{y=0}^{p-1} \left(\frac{x(x+1)y(y+1)}{p}\right)\left(\frac{t+x}{p}\right)\left(\frac{t+y}{p}\right) \\
&= \sum_{x=1}^{p-2}\sum_{y=1}^{p-2} \left(\frac{x(x+1)y(y+1)}{p}\right)\sum_{t=0}^{p-1}\left(\frac{(t+x)(t+y)}{p}\right) \qquad (12.3)
\end{aligned}$$

By Lemma C.1, the t-sum is $p-1$ if $x = y$ and -1 otherwise. Thus

$$\begin{aligned}
A_{2,\mathcal{F}}(p) &= \sum_{x=1}^{p-2}\left(\frac{x^2(x+1)^2}{p}\right)p - \sum_{x=1}^{p-2}\sum_{y=1}^{p-2}\left(\frac{x(x+1)y(y+1)}{p}\right) \\
&= (p-2)p - \Big(\sum_{x=0}^{p-1}\left(\frac{x(x+1)}{p}\right)\Big)^2 \\
&= p^2-2p-(-1)^2 = p^2-2p-1, \qquad (12.4)
\end{aligned}$$

where the last line follows again from Lemma C.1. Therefore $A_{2,\mathcal{F}}(p) = p^2-2p-1$.

12.1.2 $D_{1,\mathcal{F}}(f)$ and $D_{2,\mathcal{F}}(f)$

The conditions of the Rational Surfaces Density Theorem are satisfied with $r = 0$. Therefore

Theorem 12.1 ($D_{1,\mathcal{F}}(f_1)$ and $D_{2,\mathcal{F}}(f)$) *For small support, $D_{1,\mathcal{F}}(f_1) = \widehat{f_1}(0) + \frac{1}{2}f_1(0)$. Further, the 2-level density is $\widehat{W_{2,\mathcal{F}}} = \widehat{W_{2,O}}$.*

We assumed GRH and as $j(t)$ and $M(t)$ are non-constant, we assumed the Square-Free Sieve and the Polynomial Moebius conjectures to obtain equidistribution in sign for good t.

12.2 $y^2 + xy = x^3 + x^2 + tx$

This is one of Fermigier's examples (see [Fe2]). We rewrite this as $y^2 = x^3 + 5x^2 + 16tx = f_t(x)$.

$$\begin{aligned}
c_4(t) &= -2^4(48t-25) \\
j(t) &= \frac{-110592t^3 + 172800t^2 - 90000t + 15625}{-64t^3 + 25t^2} \\
\Delta(t) &= -2^{12}t^2(64t-25) = -2^{12}tD(t) \\
M(t) &= t(64t-25). \qquad (12.5)
\end{aligned}$$

To determine the conductors, we study the primes $p|\Delta(t)$. If $p|c_4(t)$, the reduced curve has a cusp, and contributes p^2 to the conductor, else it has a node and contributes p. Except for $p = 2$ or 5, no prime dividing t divides $c_4(t)$.

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

For $p \geq 5$, every reduced curve has a node. Let $\tau = 2\cdot 3\cdot 5t + 1$. Then $5 \nmid c_4(\tau)\Delta(\tau)$, $\Big(c_4(\tau), D(\tau)\Big) = 1$, $\Big(c_4(\tau), \Delta(\tau)\Big) = 2^4$, $2^{12}||\Delta(\tau)$, and for $D(\tau)$ square-free, $3||\Delta(\tau)$. The last follows from, mod 3, $64\tau - 25 \equiv 64 - 25 = 39$.

We could also have changed variables $\tau = 2 \cdot 3 \cdot 5t + 11$, and then $3 \nmid D(\tau)$. As all the families we consider will have discriminants divisible by 2, we need to apply Tate's Algorithm anyway, and consider just the first change of variables.

Hence, for the family $E_t : y^2 = x^3 + 5x^2 + 16(30t+1)x$, for $\Big(30t+1\Big)\Big(25 - 64(30t+1)\Big)$ square-free, by Lemma D.7, $C(t) = \Big(30t+1\Big)\Big(64(30t+1) - 25\Big)$. $\delta_D = 2^2 3^2 5^6$, $k = 2$, $a_k = 2^8 3^2 5^2$ so $\mathcal{P} = \{2, 3, 5\}$. As $\nu(2) = 0$, $\nu(3) = 3$, and $\nu(5) = 0$, by Theorem 3.8, $c_{\mathcal{F}} > 0$.

12.2.1 $A_{1,\mathcal{F}}(p)$ and $A_{2,\mathcal{F}}(p)$

We calculate $A_{1,\mathcal{F}}(p)$ for a large number of families. Consider instead the family $y^2 = x^3 + 5x^2 + 16x(c_1 t + c_0)$, $c_1 \neq 0$. For $p > |c_1|$:

$$\begin{aligned} A_{1,\mathcal{F}}(p) &= -\sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\left(\frac{x^3 + 5x^2 + 16x(c_1 t + c_0)}{p}\right) \\ &= -\sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{16xt + x^3 + 5x^2}{p}\right) \\ &= -\sum_{x\neq 0}\sum_{t=0}^{p-1}\left(\frac{16xt + x^3 + 5x^2}{p}\right) \\ &= -\sum_{x\neq 0}\sum_{t=0}^{p-1}\left(\frac{t + x^3 + 5x^2}{p}\right) = 0. \qquad (12.6) \end{aligned}$$

Thus this family has rank 0 over $\mathbb{Q}(t)$. As $j(t)$ is non-constant, we use Michel's Theorem to handle $A_{2,\mathcal{F}}(p)$; it would be a difficult direct calculation.

12.2.2 $D_{1,\mathcal{F}}(f)$ and $D_{2,\mathcal{F}}(f)$

The conditions of Theorem 7.9 are satisfied with $r = 0$. As $j(t)$ and $M(t)$ are non-constant, we conditionally obtain equidistribution of sign (for all t and for t good).

The conditions of the Rational Surfaces Density Theorem are satisfied with $r = 0$. Therefore

Theorem 12.2 ($D_{1,\mathcal{F}}(f_1)$ and $D_{2,\mathcal{F}}(f)$) *For small support, $D_{1,\mathcal{F}}(f_1) = \widehat{f_1}(0) + \frac{1}{2}f_1(0)$. Further, the 2-level density is $\widehat{W_{2,\mathcal{F}}} = \widehat{W_{2,O}}$.*

We assumed GRH, and the Square-Free Sieve and Polynomial Moebius conjectures to handle the signs.

12.3 $y^2 + xy + 2y = x^3 + x^2 + tx + 1$

We consider a more exotic example from Fermigier, where $A_{1,\mathcal{F}}(p) = pA_{\mathcal{E}}(p)$ is not constant. Consider $y^2+xy+2y = x^3+x^2+tx+1$, which on rewriting becomes $y^2 = x^3+5x^2+16(t+1)x+128$.

$$\begin{aligned}
c_4(t) &= -2^4(48t+23) = -2^4c(t) \\
j(t) &= \frac{-110592t^3 - 158976t^2 - 76176t - 12167}{-64t^3 - 167t^2 + 578t - 1297} \\
\Delta(t) &= -2^{12}(64t^3 + 167t^2 - 578t + 1297) = -2^{12}D(t) \\
M(t) &= 64t^3 + 167t^2 - 578t + 1297 \qquad (12.7)
\end{aligned}$$

We study $h(t) = \Big(c_4(t), \Delta(t)\Big)$. Except for powers of 2, this reduces to studying $\Big(c(t), D(t)\Big)$. As

$$\frac{D(t)}{c(t)} = \frac{9216t^2 + 19632t - 92639}{6912} + \frac{11095561}{6912c(t)}, \qquad (12.8)$$

if $p|h(t)$, $p|6912D(t) - (9216t^2 + 19632t - 92639)c(t) = 11095561 = 3331^2$. If $3331|c(t)$, then $t \equiv 2012(3331)$; if $3331|D(t)$ then $t \equiv 2012, 3312(3331)$. We change variables $\tau = 2^2 \cdot 3 \cdot 3331t + 1$, which yields $\Big(c_4(t), \Delta(t)\Big) = 2^4$, $2^{13}||D(\tau)$ and $3\nmid D(\tau)$.

Possibly after passing to a subsequence, by Theorem 4.3 we can handle the conductors and the cardinality. The only troublesome prime is $p = 2$.

12.3.1 $A_{1,\mathcal{F}}(p)$ and $A_{2,\mathcal{F}}(p)$

We calculate $A_{1,\mathcal{F}}(p)$ for a large number of families. Consider instead the family $y^2 = x^3 + 5x^2 + 16x + 128 + 16x(c_1t + c_0)$, $c_1 \neq 0$. For $p > |c_1|$:

$$\begin{aligned}
A_{1,\mathcal{F}}(p) &= -\sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\left(\frac{x^3 + 5x^2 + 16x + 128 + 16x(c_1t + c_0)}{p}\right) \\
&= -\sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{16xt + x^3 + 5x^2 + 16x + 128}{p}\right) \\
&= -\sum_{x\neq 0}\sum_{t=0}^{p-1}\left(\frac{t + x^3 + 5x^2 + 16x + 128}{p}\right) - \sum_{t=0}^{p-1}\left(\frac{128}{p}\right)
\end{aligned}$$

$$= \quad -p\left(\frac{2}{p}\right) \tag{12.9}$$

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 two contribute $+1$, and two contribute -1, for no net contribution.

Thus this family has rank 0 over $\mathbb{Q}(t)$. As $j(t)$ is non-constant, we may use Michel's Theorem to calculate $A_{2,\mathcal{F}}(p)$.

12.3.2 $D_{1,\mathcal{F}}(f)$ and $D_{2,\mathcal{F}}(f)$

The conditions of Theorem 7.9 are satisfied with $r = 0$. As $j(t)$ and $M(t)$ are non-constant, we conditionally obtain equidistribution of sign (for all t and for t good).

The conditions of the Rational Surfaces Density Theorem are satisfied with $r = 0$. Therefore

Theorem 12.3 ($D_{1,\mathcal{F}}(f_1)$ and $D_{2,\mathcal{F}}(f)$) *For small support, $D_{1,\mathcal{F}}(f_1) = \widehat{f_1}(0) + \frac{1}{2}f_1(0)$. Further, the 2-level density is $\widehat{W_{2,\mathcal{F}}} = \widehat{W_{2,O}}$.*

We assumed GRH, and the Square-Free Sieve and Polynomial Moebius conjectures to handle the signs.

13 1- and 2-Level Densities for Rank 1 Rational Surfaces

13.1 $y^2 = x^3 + x^2 + t$

Let $\mathcal{F} : y^2 = x^3 + x^2 + t$. As $\Delta(t) = -16t(27t+4)$ and $c_4(t) = 16$, by sieving to $t(27t+4)$ square-free, the conductors will be manageable. The only common factors of t and $27t+4$ are 2 and 4, because if d divides both, then $d|(27t+4) - 27t$. To escape this complication, we study $y^2 = x^3 + x^2 + 2t + 1$. It is easier to calculate the conductors if we additionally send t to $6t$. Thus, we study $y^2 = x^3 + x^2 + 12t + 1$.

$$\begin{aligned}
c_4(t) &= 16 \\
\Delta(t) &= -16(3888t^2 + 696t + 31) = -16(12t+1)(324t+31) \\
j(t) &= -\frac{256}{3888t^2 + 696t + 31} \\
M(t) &= (12t+1)(324t+31). \qquad (13.1)
\end{aligned}$$

We sieve to square-free $D(t) = (12t+1)(324t+31)$. Assume there is a common factor d. Then $d|(324t+31) - 27(2t+1)$, or $d|4$. As both factors of $\Delta(t)$ are odd, there are no common divisors of $12t+1$ and $324t+31$.

For $D(t)$ square-free, by Lemma D.9, $C(t) = 2^3(12t+1)(324t+31)$. $\delta_D = 2^8 3^2$, $k = 2$, $a_k = 2^4 3^5$ so $\mathcal{P} = \{2, 3\}$. As $\nu(2) = \nu(3) = 0$, by Theorem 3.8, $c_{\mathcal{F}} > 0$.

13.1.1 $A_{1,\mathcal{F}}(p)$, $A_{2,\mathcal{F}}(p)$

For $p > 3$,

$$\begin{aligned}
A_{1,\mathcal{F}}(p) &= -\sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\left(\frac{x^3 + x^2 + 12t + 1}{p}\right) \\
&= -\sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{(x^3 + x^2) + t}{p}\right) = 0. \qquad (13.2)
\end{aligned}$$

As $p > 3$, we immediately change $12t + 1$ back to t in $A_{2,\mathcal{F}}(p)$.

$$A_{2,\mathcal{F}}(p) = \sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\left(\frac{t + (x^3 + x^2)}{p}\right)\left(\frac{t + (y^3 + y^2)}{p}\right). \qquad (13.3)$$

The t-sum is $p-1$ if $p|\delta = (x^3+x^2)-(y^3+y^2)$ and -1 otherwise. $\delta = (x-y)(y^2+(x+1)y+x^2+x)$. The solutions of the first factor are $x = y$; for fixed x, the discriminant of the second factor is $(x+1)^2 - 4(x^2+x) = 1-2x-3x^2$. Thus the number of solutions of the second factor, for fixed x, is $1 + \left(\frac{1-2x-3x^2}{p}\right)$. As the discriminant of $1-2x-3x^2$ is 16, summing over x for $p > 2$ yields $p - \left(\frac{-3}{p}\right)$ by Lemma C.2.

We must be careful about double counting. If both factors are congruent to zero, then $3x^2+2x \equiv 0$, or $x \equiv 0, -2 \cdot 3^{-1}$. Hence we always double count two solutions.

$$\begin{aligned} A_{2,\mathcal{F}}(p) &= \left[p + p - \left(\frac{-3}{p}\right) - 2\right]p - \sum_{x=0}^{p-1}\sum_{y=0}^{p-1} 1 \\ &= p^2 - 2p - p\left(\frac{-3}{p}\right). \end{aligned} \tag{13.4}$$

13.1.2 1- and 2-Level Densities

Recall $D_{1,\mathcal{F}}^{(1)}(f_1)$ and $D_{2,\mathcal{F}}^{(1)}(f)$ are the 1- and 2-level densities with the contribution from a single family zero removed. As $j(t)$ and $M(t)$ are non-constant, we expect equidistribution in sign (for all t and for t good).

The conditions of the Rational Surface Density Theorem are satisfied with $r = 1$. Therefore

Theorem 13.1 ($D_{1,\mathcal{F}}^{(1)}(f)$ and $D_{2,\mathcal{F}}^{(1)}(f)$) *For small support, $D_{1,\mathcal{F}}^{(1)}(f_1) = \widehat{f_1}(0) + \frac{1}{2}f_1(0)$. Further, the 2-level density of the non-family zeros is $\widehat{W_{2,\mathcal{F}}^{(1)}} = \widehat{W_{2,O}}$.*

Removing the contribution from the single family zero, the 2-level density of the remaining zeros agrees with that of O for test functions with small support.

To prove the above, we only assume GRH, the Birch and Swinnterton-Dyer conjecture (to interpret the rank), and the Square-Free Sieve and the Polynomial Moebius conjectures (to get equidistribution of sign for good t).

13.2 $y^2 = x^3 + tx^2 + 1$

Consider the family $y^2 = x^3 + 1 + tx^2$. Then

$$\begin{aligned} c_4(t) &= 16t^2 \\ \Delta(t) &= -16(4t^3+27) \end{aligned}$$

$$\begin{aligned} j(t) &= -256\frac{t^6}{4t^3+27} \\ M(t) &= 4t^3+27. \end{aligned} \tag{13.5}$$

If we replace t with $6t+1$, we can easily calculate the conductors for $D(t) = 4(6t+1)^3+27$ square-free. Such a change will not affect the values of $A_{1,\mathcal{F}}(p)$ or $A_{2,\mathcal{F}}(p)$ for $p > 3$. By Lemma D.11, $C(t) = 2^2\Big(4(6t+1)^3+27\Big)$ for $D(t)$ square-free. By Hooley ([Ho], Theorem 3, page 69), as $D(t)$ is an irreducible polynomial, $c_{\mathcal{F}} > 0$.

13.2.1 $A_{1,\mathcal{F}}(p)$

$$\begin{aligned} A_{1,\mathcal{F}}(p) &= -\sum_{t(p)}\sum_{x(p)}\left(\frac{x^3+1+tx^2}{p}\right) \\ &= -\sum_{t(p)}\left(\frac{1}{p}\right) - \sum_{x=1}^{p-1}\sum_{t(p)}\left(\frac{x^3+1+tx^2}{p}\right) \\ &= -p - \sum_{x=1}^{p-1}\sum_{t(p)}\left(\frac{x^3+1+t}{p}\right) = -p. \end{aligned} \tag{13.6}$$

As the family is a rational surface, Theorem 1.2 implies it has rank 1 over $\mathbb{Q}(t)$.

13.2.2 $A_{2,\mathcal{F}}(p)$

We use the Gauss sum expansion (Equation 2.4) to calculate $A_{2,\mathcal{F}}(p)$.

$$\begin{aligned} A_{2,\mathcal{F}}(p) &= \sum_{t(p)}\sum_{x(p)}\sum_{y(p)}\left(\frac{x^3+1+x^2t}{p}\right)\left(\frac{y^3+1+y^2t}{p}\right) \\ &= \sum_{x,y(p)}\sum_{c,d=1}^{p-1}\frac{1}{p}\left(\frac{cd}{p}\right)\mathbf{e}\left(\frac{c(x^3+1)-d(y^3+1)}{p}\right)\sum_{t(p)}\mathbf{e}\left(\frac{(cx^2-dy^2)t}{p}\right). \end{aligned} \tag{13.7}$$

Note c and d are invertible mod p. If the numerator in the t-exponential is non-zero, the t-sum vanishes. If exactly one of x and y vanishes, the numerator is not congruent to zero mod p. Hence either or neither are zero. If both are zero, the t-sum gives p, the c-sum gives G_p, the d-sum gives $\overline{G}_p$, for a total contribution of p.

Assume x and y are non-zero. Then $d = c(x^2y^{-2})$ (otherwise the t-sum is zero). The t-sum yields p, and we have

$$\begin{aligned} A_{2,\mathcal{F}}(p) &= \sum_{x,y=1}^{p-1}\sum_{c=1}^{p-1}\frac{1}{p}\left(\frac{x^2y^2}{p}\right)\mathbf{e}\left(\frac{cy^{-2}(x^3y^2+y^2-x^2y^3-x^2)}{p}\right)p+p \\ &= \sum_{x,y=1}^{p-1}\sum_{c=1}^{p-1}\left(\frac{x^2y^2}{p}\right)\mathbf{e}\left(\frac{cy^{-2}(x-y)(x^2y^2-(x+y))}{p}\right)+p \\ &= \sum_{x,y=1}^{p-1}\sum_{c=0}^{p-1}\left(\frac{x^2y^2}{p}\right)\mathbf{e}\left(\frac{cy^{-2}(x-y)(x^2y^2-(x+y))}{p}\right)+p-\sum_{x,y=1}^{p-1}\left(\frac{x^2y^2}{p}\right) \\ &= \sum_{x,y=1}^{p-1}\sum_{c=0}^{p-1}\mathbf{e}\left(\frac{cy^{-2}(x-y)(x^2y^2-(x+y))}{p}\right)+p-(p-1)^2. \end{aligned} \tag{13.8}$$

If $g(x,y) = (x-y)(x^2y^2-(x+y)) \equiv 0(p)$ then the c-sum is p, otherwise it is 0. We are left with counting how often $g(x,y) \equiv 0$ for x, y non-zero.

A few words must be said about why we cooked up this family. If, instead of x^2t we had xt, we would have found the condition $d = c(x/y)$. As we have $\left(\frac{cd}{p}\right)$ this would lead to $\left(\frac{c^2}{p}\right)\left(\frac{xy}{p}\right)$ times a similar c-exponential. It would not be sufficient to find how often a similar $g(x,y)$ vanished; we would need to know at which x and y (or, slightly weaker, the value of $\left(\frac{xy}{p}\right)$.

Clearly, whenever $x = y$, $g(x,y) \equiv 0$; therefore there are $p-1$ solutions from this term. For x non-zero, each such pair contributes p, for a total contribution of $(p-1)p$.

Consider now $x^2y^2 \equiv x+y$, which we may rewrite as a quadratic: $x^2y^2-y-x \equiv 0$. By Lemma C.3 (the Quadratic Formula mod p), if the discriminant $1+4x^3$ is a square mod p there are roots; if it is not a square mod p there are no roots. The roots would be

$$y \equiv \frac{1 \pm \sqrt{1+4x^3}}{2x^2}, \tag{13.9}$$

where the square-root and divisions are operations mod p. If $1+4x^3$ is a non-zero square, there will be two distinct choices for y. If $1+4x^3 \equiv 0$, there is one choice for y, and if $1+4x^3$ is not a square mod p, there are no y such that $x^2y^2 \equiv x+y$.

First, a note about our previous conditions. Neither x nor y is allowed to be zero. If $y = 0$ then $x^2y^2 = x+y$ reduces to $x = 0$ (similarly if $x = 0$). Hence we do not need to worry about our solutions violating x, y non-zero.

From the above, we've seen that for a given non-zero x, the number of non-zero y with $x^2y^2 \equiv x + y$ is $1 + \left(\frac{4x^3+1}{p}\right)$. Hence the number of non-zero pairs with $x^2y^2 \equiv x + y$ is

$$\sum_{x \neq 0} \left(1 + \left(\frac{4x^3+1}{p}\right)\right) = p - 1 + \sum_{x=0}^{p} \left(\frac{4x^3+1}{p}\right) - 1. \tag{13.10}$$

Each of these pairs contributes p. Thus, these pairs contribute $p^2 - 2p + p\sum_x \left(\frac{4x^3+1}{p}\right)$.

We must be careful about double counting. If both $x - y \equiv 0$ and $x^2y^2 \equiv x + y$, then we find $x^4 \equiv 2x$. As $x \neq 0$, we obtain $x^3 \equiv 2$. If 2 has a cube root mod p, we have double counted three solutions; if it does not, we have counted correctly. Let $h_{3,p}(2)$ denote the number of cube roots of 2 modulo p.

Thus

$$\begin{aligned} A_{2,\mathcal{F}}(p) &= p^2 - 2p + p\sum_{x(p)} \left(\frac{4x^3+1}{p}\right) + p(p-1) - ph_{3,p}(2) + p - (p-1)^2 \\ &= p^2 - ph_{3,p}(2) - 1 + p\sum_{x(p)} \left(\frac{4x^3+1}{p}\right) = p^2 + O(p^{\frac{3}{2}}). \end{aligned} \tag{13.11}$$

The elliptic curve $y^2 = 4x^3 + 1$ is equivalent to $y^2 = x^3 + 16$. This curve has analytic rank 0: $L(E, 1) = .5968$. It does have complex multiplication, and for $p \equiv 2(3)$, $a_E(p) = 0$. For the other p, the angles of $\frac{a_E(p)}{2\sqrt{p}}$ are uniformly distributed. Hence we expect no net contribution from the $\left(\frac{4x^3+1}{p}\right)$ term, though this does show that the bound in Michel's theorem is sharp. If $p \equiv 2(3)$, as $x \to x^3$ is an automorphism, $h_{3,p}(2) = 1$. Thus, at least half the time, $A_{2,\mathcal{F}}(p) = p^2 - 3p - 1$.

Lemma 13.2

$$A_{2,\mathcal{F}}(p) = \sum_{t(p)} a_{E_t}^2(p) = p^2 + O(p^{\frac{3}{2}}). \tag{13.12}$$

13.2.3 1- and 2-Level Densities

As $j(t)$ and $M(t)$ are non-constant, we expect equidistribution in sign (for all t and for t good).

The conditions of the Rational Surface Density Theorem are satisfied with $r = 1$. Therefore

Theorem 13.3 ($D_{1,\mathcal{F}}^{(1)}(f)$ and $D_{2,\mathcal{F}}^{(1)}(f)$) *For small support,* $D_{1,\mathcal{F}}^{(1)}(f_1) = \widehat{f_1}(0) + \frac{1}{2}f_1(0)$. *Further,* *the 2-level density of the non-family zeros is* $\widehat{W^{(1)}_{2,\mathcal{F}}} = \widehat{W_{2,O}}$.

To prove the above, we only assume GRH, the Birch and Swinnterton-Dyer conjecture (to interpret the rank), and the Square-Free Sieve the Polynomial Moebius conjectures (to get equidistribution of sign for good t).

13.2.4 Generalization to Related Families

Let $\mathcal{F}_1$ be the family $y^2 = x^3+1+x^2t$. Consider the natural generalization $\mathcal{F}_{\alpha,\beta} : y^2 = x^3+\alpha+\beta x^2 t$. Consider primes which do not divide $\alpha\beta$. Before we found

$$A_{1,\mathcal{F}}(p) \;=\; -\sum_{t(p)}\sum_{x(p)} \left(\frac{x^3+1+x^2t}{p}\right) \;=\; -\sum_{t(p)} \left(\frac{1}{p}\right) \;=\; -p. \tag{13.13}$$

Now $A_{1,\mathcal{F}}(p) = -\sum_{t(p)} \left(\frac{\alpha}{p}\right)$. If α is a square, then we again get $A_{1,\mathcal{F}}(p) = -p$. If, however, $\left(\frac{\alpha}{p}\right)$ is equally distributed among 1 and -1, we get 0 and the rank of the family is zero. For example, take $\alpha = -1$. Then if $p \equiv 1(4)$ we get p and for $p \equiv 3(4)$ we get 0.

For $A_{2,\mathcal{F}}(p)$, we needed to study how often $(x-y)\ (x^2y^2-(x+y))$ was congruent to zero mod p. Now we have $(x-y)\ (x^2y^2-\alpha(x+y))$. Again, the contribution from $x=y$ and $x^2y^2 \equiv \alpha(x+y)$ is at most $3p$, as these two conditions force $x^4 \equiv 2\alpha x$, which has at most 3 non-zero solutions.

We now study

$$\begin{aligned} 0 &\equiv x^2\cdot y^2 - \alpha y - \alpha x \\ y(x) &\equiv \frac{\alpha \pm \sqrt{\alpha^2+4\alpha x^3}}{2x^2} \end{aligned} \tag{13.14}$$

Again, $x=0$ forces $y=0$ and vice versa, and the number of solutions is controlled by

$$\sum_{x=1}^{p-1}\left(1+\left(\frac{4\alpha x^3+\alpha^2}{p}\right)\right) = p-1+\left(\frac{\alpha}{p}\right)\sum_{x=1}^{p-1}\left(\frac{4x^3+\alpha}{p}\right). \tag{13.15}$$

Again, there will be $p+O(\sqrt{p})$ solutions.

We see that β has no effect on our sums (not surprising, as for fixed β, β may be absorbed by t); however, α strongly effects our results. If α is always a square, there is non-zero rank. If $\left(\frac{\alpha}{p}\right)$ is equidistributed between 1 and -1, then there is no rank.

13.3 General Rank 1 Construction

More generally, consider the family $y^2 = x^3 + Ax^2 + (Bt+C)x + D^2$. Then for $D \neq 0$, $p \nmid BD$:

$$\begin{aligned} A_{1,\mathcal{F}}(p) &= -\sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{Bxt + x^3 + Ax^2 + Cx + D^2}{p}\right) \\ &= -\sum_{x\neq 0}\sum_{t=0}^{p-1}\left(\frac{t + x^3 + Ax^2 + Cx + D^2}{p}\right) - p\left(\frac{D^2}{p}\right) \\ &= -p. \end{aligned} \tag{13.16}$$

Thus this family has rank 1 over $\mathbb{Q}(t)$. In general one expects $j(t)$ to be non-constant (so Michel's Theorem gives $A_{2,\mathcal{F}}(p)$). We expect (in general) that $M(t)$ is non-constant, hence we expect the generic such family has equidistribution of sign. The Rational Surfaces Density Theorem is applicable, and we predict the 2-level non-family density to be $\widehat{W_{2,O}}$, again agreeing with Katz and Sarnak's predictions.

To prove the above, we only assume GRH, the Birch and Swinnterton-Dyer conjecture (to interpret the rank), and the Square-Free Sieve and the Polynomial Moebius conjectures (to get equidistribution of sign for good t).

14 1- and 2-Level Densities for Rank 2 Rational Surfaces

14.1 $y^2 = x^3 - t^2x + t^2$

Consider the family $y^2 = x^3 - t^2x + t^2$. Then

$$\begin{aligned} c_4(t) &= 2^4 \cdot 3t^2 \\ \Delta(t) &= 2^4t^4(4t^2-27) \\ j(t) &= \frac{6912}{4t^2-27} \\ M(t) &= 4t^2-27. \end{aligned} \tag{14.1}$$

14.1.1 $A_{1,\mathcal{F}}(p)$

$$\begin{aligned} -A_{1,\mathcal{F}}(p) &= -\sum_{t(p)} a_t(p) \ = \ \sum_{t(p)}\sum_{x(p)} \left(\frac{x^3-t^2x+t^2}{p}\right) \\ &= \sum_{t=1}^{p-1}\sum_{x(p)} \left(\frac{x^3-t^2x+t^2}{p}\right) \ = \ \sum_{t=1}^{p-1}\sum_{x(p)} \left(\frac{t^3x^3-t^3x+t^2}{p}\right) \\ &= \sum_{t=1}^{p-1}\sum_{x(p)} \left(\frac{t^2}{p}\right)\left(\frac{t(x^3-x)+1}{p}\right) \\ &= \sum_{t(p)}\sum_{x(p)} \left(\frac{t(x^3-x)+1}{p}\right) - \sum_{x(p)}\left(\frac{1}{p}\right) \\ &= \sum_{t(p)}\sum_{x=0,\pm1} \left(\frac{t(x^3-x)+1}{p}\right) + \sum_{t(p)}\sum_{\substack{x(p)\\ x\neq 0,\pm1}} \left(\frac{t(x^3-x)+1}{p}\right) - p \\ &= \sum_{t(p)}\sum_{x=0,\pm1} \left(\frac{1}{p}\right) + \sum_{\substack{x(p)\\ x\neq 0,\pm1}}\sum_{t(p)} \left(\frac{t+1}{p}\right) - p \\ &= 3p + 0 - p \ = \ 2p. \end{aligned} \tag{14.2}$$

We isolate a useful sum:

Lemma 14.1

$$\sum_{t(p)}\sum_{x(p)} \left(\frac{tx^3-tx+1}{p}\right) = 3p. \tag{14.3}$$

14.1.2 $A_{2,\mathcal{F}}(p)$

$$\begin{aligned}
A_{2,\mathcal{F}}(p) &= \sum_{t(p)} a_t^2(p) \\
&= \sum_{t(p)} \sum_{x,y(p)} \left(\frac{x^3 - t^2x + t^2}{p}\right)\left(\frac{y^3 - t^2y + t^2}{p}\right) \\
&= \sum_{t=1}^{p-1} \sum_{x,y(p)} \left(\frac{x^3 - t^2x + t^2}{p}\right)\left(\frac{y^3 - t^2y + t^2}{p}\right) \\
&= \sum_{t=1}^{p-1} \sum_{x,y(p)} \left(\frac{t^3x^3 - t^3x + t^2}{p}\right)\left(\frac{t^3y^3 - t^3y + t^2}{p}\right) \\
&= \sum_{t=1}^{p-1} \sum_{x,y(p)} \left(\frac{t^4}{p}\right)\left(\frac{t(x^3 - x) + 1}{p}\right)\left(\frac{t(y^3 - y) + 1}{p}\right) \\
&= \sum_{t=0}^{p-1} \sum_{x,y(p)} \left(\frac{t(x^3 - x) + 1}{p}\right)\left(\frac{t(y^3 - y) + 1}{p}\right) - \sum_{x,y(p)} \left(\frac{1}{p}\right) \\
&= \sum_{x,y(p)} \sum_{t(p)} \left(\frac{t(x^3 - x) + 1}{p}\right)\left(\frac{t(y^3 - y) + 1}{p}\right) - p^2. \qquad (14.4)
\end{aligned}$$

In Lemma C.2 we showed that, if a and b are not both zero,

$$\sum_{t=0}^{p-1} \left(\frac{at^2 + bt + c}{p}\right) = \begin{cases} (p-1)\left(\frac{a}{p}\right) \ if \ p \mid b^2 - 4ac \\ -\left(\frac{a}{p}\right) \ otherwise \end{cases} \qquad (14.5)$$

In $A_{2,\mathcal{F}}(p)$ we have

$$\begin{aligned}
a &= (x^3 - x)(y^3 - y) = y(x^2 - 1)x(y^2 - 1) \\
b &= (x^3 - x) + (y^3 - y) \\
c &= 1 \\
\delta(x, y) &= b^2 - 4ac = \Big((x^3 - x) - (y^3 - y)\Big)^2. \qquad (14.6)
\end{aligned}$$

We use inclusion / exclusion on $x^3 - x$ and $y^3 - y$ vanishing. Assume first that $x^3 - x$ equals zero (happens three ways: $x = 0, \pm 1$). Then we have $\sum_t \left(\frac{t(y^3-y)+1}{p}\right)$, which is $3p$ from our $A_{1,\mathcal{F}}(p)$ computation, giving $3 \cdot 3p$. Similarly we get $3 \cdot 3p$ if $y^3 - y$ is zero. We subtract the doubly counted $x^3 - x \equiv y^3 - y \equiv 0$ (nine ways), each of which gives $\sum_t \left(\frac{1}{p}\right) = p$. Hence the contribution from at least one of $x^3 - x$ and $y^3 - y$ vanishing is $9p$.

Assume $x, y \notin \{0, \pm 1\}$. When is $\delta(x,y) = (x^3 - x) - (y^3 - y) \equiv 0(p)$?

$$\delta(x,y) \quad = \quad (x-y)\cdot(x^2+xy+y^2-1). \tag{14.7}$$

Therefore

$$A_{2,\mathcal{F}}(p) = \sum_{\substack{x,y\neq 0,\pm 1\\ \delta(x,y)\equiv 0}} p\left(\frac{(x^3-x)(y^3-y)}{p}\right) - \sum_{x,y\neq 0,\pm 1}\left(\frac{(x^3-x)(y^3-y)}{p}\right) + 9p - p^2. \tag{14.8}$$

Clearly, $\delta(x,y) \equiv 0(p)$ if $x = y$, which happens $p - 3$ times. If $x = y$ then the second factor is $3x^2 - 1$, which is congruent to zero at most twice.

When is $\delta_2(x,y) = x^2 + xy + y^2 - 1 \equiv 0$? By the Quadratic Formula mod p (Lemma C.3):

$$y = \frac{-x \pm \sqrt{4-3x^2}}{2}, \tag{14.9}$$

which reduces to finding when $4 - 3x^2$ is a square mod p. We get two values of y if it is equivalent to a non-zero square, one value if it is equivalent to zero, and no values if it is not equivalent to a square. When solving $\delta_2(x,y) \equiv 0(p)$, we make sure such $y \notin \{0, \pm 1\}$. If $y = 0$, $x = \pm 1$; $y = 1$, $x = 0$,-1;y = -1,x = $0, 1$. Therefore, we don't get an excluded y (and similarly if we reverse the rolls of y and x). Thus the number of solutions to $\delta_2(x,y) \equiv 0(p)$ is

$$\begin{aligned}\sum_{x=2}^{p-2}\left[1 + \left(\frac{4-3x^2}{p}\right)\right] \quad &= \quad p - 3 + \sum_{x=2}^{p-2}\left(\frac{4-3x^2}{p}\right) \\ &= \quad p - 6 + \sum_{x(p)}\left(\frac{4-3x^2}{p}\right).\end{aligned} \tag{14.10}$$

We again use Lemma C.2. The discriminant now is $0^2 - 4\cdot(-3)\cdot 4$. For $p \geq 5$, p does not divide the discriminant, hence this sum is $-\left(\frac{-3}{p}\right)$.

Thus, for $x \neq 0, \pm 1$, the number of solutions with $x^2 + xy + y^2 \equiv 1$ is $p - 6 - \left(\frac{-3}{p}\right)$; the number with $x - y \equiv 0$ is $p - 3$. At most two of the pairs (x,y) satisfying $x^2 + xy + y^2 - 1 \equiv 0(p)$ also satisfy $x = y$. These pairs satisfy $3x^2 \equiv 1$, thus, if $\left(\frac{3}{p}\right) = 1$ we have doubly counted two solutions; if it is -1, there was no double counting. Thus, the number of doubly counted pairs is $1 + \left(\frac{3}{p}\right)$, and the total number of pairs is

$$2p - 10 - \left(\frac{-3}{p}\right) - \left(\frac{3}{p}\right). \tag{14.11}$$

When $x = y \neq 0, \pm 1$, clearly $\left(\frac{(x^3-x)(y^3-y)}{p}\right) = 1$. Hence these terms contribute 1.

Consider $x \neq y$ and $x^2 + xy + y^2 - 1 \equiv 0$. Thus $x, y \neq 0, \pm 1$. Then $y^2 - 1 \equiv -x(x+y)$ and $x^2 - 1 \equiv -y(x+y)$ and

$$\left(\frac{(x^3-x)(y^3-y)}{p}\right) = \left(\frac{x(x^2-1)y(y^2-1)}{p}\right) = \left(\frac{x^2y^2(x+y)^2}{p}\right). \tag{14.12}$$

As long as $x \neq -y$, this is 1. If $x = -y$ then we would have $x^2 - x^2 + x^2 - 1 \equiv 0$. This implies $x = \pm 1$, which cannot happen as $x, y \neq 0, \pm 1$. Therefore all pairs have their Legendre factor $+1$, and we need only count how many such pairs there are. We've previously shown this to be $p + O(1)$, therefore

$$\begin{aligned} A_{2,\mathcal{F}}(p) &= p\left[2p - 10 - \left(\frac{-3}{p}\right) - \left(\frac{3}{p}\right)\right] - \sum_{x,y \neq 0,\pm 1} \left(\frac{(x^3-x)(y^3-y)}{p}\right) + 9p - p^2 \\ &= p^2 - p - \left[\sum_{x(p)} \left(\frac{(x^3-x)}{p}\right)\right]^2 - \left[\left(\frac{-3}{p}\right) + \left(\frac{3}{p}\right)\right]p. \end{aligned} \tag{14.13}$$

As $x^3 - x$ is a non-singular elliptic curve, by Hasse its sum above is bounded by $4p$. It has complex multiplication and analytic rank 0. For $p \equiv 3 \bmod 4$ its $a_E(p) = 0$ (change variables $x \to -x$); for the remaining p, the angles of $\frac{a_E(p)}{2\sqrt{p}}$ are uniformly distributed. Hence $A_{2,\mathcal{F}}(p) = p^2 + O(p)$.

Lemma 14.2

$$A_{2,\mathcal{F}}(p) = p^2 - p - \left[\sum_{x(p)} \left(\frac{(x^3-x)}{p}\right)\right]^2 - \left[\left(\frac{-3}{p}\right) + \left(\frac{3}{p}\right)\right]p \;=\; p^2 + O(p). \tag{14.14}$$

The reason this calculation succeeds is we have a very tractable expression for $x(x^2-1)y(y^2-1)$ when $x^2+xy+y^2-1 \equiv 0$ mod p. It was non-trivial to find a family with high rank over $\mathbb{Q}(t)$ and $A_{2,\mathcal{F}}(p)$ computable.

We isolate a useful result:

Lemma 14.3 *The number of pairs (x, y), $x, y \neq 0, \pm 1$, such that $\delta(x, y) = (x^3 - x) - (y^3 - y) \equiv 0(p)$ is $2p - 10 - \left(\frac{-3}{p}\right) - \left(\frac{3}{p}\right)$.*

14.1.3 1- and 2-Level Densities

If we replace t with $6t+1$, we can easily calculate the conductors for $D(t) = (6t+1)\Big(4(6t+1)^2-27\Big)$ square-free. Such a change will not affect the values of $A_{1,\mathcal{F}}(p)$ or $A_{2,\mathcal{F}}(p)$ for $p > 3$. By Lemma D.12, $C(t) = 2^2(6t+1)^2 \cdot (4(6t+1)^2 - 27)$ for $D(t)$ square-free. By Hooley ([Ho], Theorem 3, page 69), $c_{\mathcal{F}} > 0$.

As $j(t)$ and $M(t)$ are non-constant, we expect equidistribution in sign (for all t and for t good). The conditions of the Rational Surface Density Theorem are satisfied with $r = 2$. Therefore

Theorem 14.4 ($D^{(2)}_{1,\mathcal{F}}(f)$ and $D^{(2)}_{2,\mathcal{F}}(f)$) *For small support, $D^{(2)}_{1,\mathcal{F}}(f_1) = \widehat{f_1}(0) + \frac{1}{2}f_1(0)$. Further, the 2-level density of the non-family zeros is $\widehat{W^{(2)}_{2,\mathcal{F}}} = \widehat{W_{2,O}}$.*

To prove the above, we only assume GRH, the Birch and Swinnterton-Dyer conjecture (to interpret the rank), and the Square-Free Sieve and the Polynomial Moebius conjectures (to get equidistribution of sign for good t). Note the calculations should also work for $y^2 = x^3 - t^2x + \alpha^2 t^2$.

14.2 $y^2 = x^3 - t^2x + t^4$

Consider the family $y^2 = x^3 - t^2x + t^4$. Then

$$\begin{aligned} c_4(t) &= 2^4 \cdot 3t^2 \\ \Delta(t) &= 2^4 t^6 (27t^2 - 4) \\ j(t) &= -\frac{6912}{27t^2 - 4} \\ M(t) &= 27t^2 - 4. \end{aligned} \tag{14.15}$$

14.2.1 $A_{1,\mathcal{F}}(p)$

$$\begin{aligned}
-A_{1,\mathcal{F}}(p) &= -\sum_{t(p)} a_t(p) \;=\; \sum_{t(p)}\sum_{x(p)} \left(\frac{x^3-t^2x+t^4}{p}\right) \\
&= \sum_{t=1}^{p-1}\sum_{x(p)} \left(\frac{x^3-t^2x+t^4}{p}\right) \;=\; \sum_{t=1}^{p-1}\sum_{x(p)} \left(\frac{t^3x^3-t^3x+t^4}{p}\right) \\
&= \sum_{t=1}^{p-1}\sum_{x(p)} \left(\frac{t^3}{p}\right)\left(\frac{x^3-x+t}{p}\right) \\
&= \sum_{x(p)}\sum_{t(p)} \left(\frac{t}{p}\right)\left(\frac{t+(x^3-x)}{p}\right). \qquad (14.16)
\end{aligned}$$

From Lemma C.1, the t-sum is $p-1$ if $p|(x^3-x)$ and -1 otherwise. Thus each of $x=0,1$ and -1 contribute $p-1$, everything else contributes -1, for a total contribution of $3(p-1)+(p-3)(-1)=2p$.

Lemma 14.5

$$A_{1,\mathcal{F}}(p) \;=\; \sum_{t(p)} a_t(p) = -2p. \qquad (14.17)$$

14.2.2 $A_{2,\mathcal{F}}(p)$

$$\begin{aligned}
A_{2,\mathcal{F}}(p) &= \sum_{t(p)} a_t^2(p) \\
&= \sum_{t(p)}\sum_{x,y(p)} \left(\frac{x^3-t^2x+t^4}{p}\right)\left(\frac{y^3-t^2y+t^4}{p}\right) \\
&= \sum_{t=0}^{p-1}\sum_{x,y(p)} \left(\frac{t^6}{p}\right)\left(\frac{(x^3-x)+t}{p}\right)\left(\frac{(y^3-y)+t}{p}\right) \\
&= \sum_{t(p)}\sum_{x,y(p)} \left(\frac{(x^3-x)+t}{p}\right)\left(\frac{(y^3-y)+t}{p}\right) \\
&\quad - \sum_{x,y(p)} \left(\frac{(x^3-x)}{p}\right)\left(\frac{(y^3-y)}{p}\right) \\
&= \sum_{t(p)}\sum_{x,y(p)} \left(\frac{(x^3-x)+t}{p}\right)\left(\frac{(y^3-y)+t}{p}\right) - \left[\sum_{x(p)} \left(\frac{x^3-x}{p}\right)\right]^2. \qquad (14.18)
\end{aligned}$$

The t-sum involves a quadratic in t. Its discriminant is

$$\begin{aligned} \delta^2(x,y) &= \Big((x^3-x)+(y^3-y)\Big)^2 - 4(x^3-x)(y^3-y) \\ &= \Big((x^3-x)-(y^3-y)\Big)^2. \end{aligned} \tag{14.19}$$

By Lemma C.2, the t sum is $p-1$ if $\delta(x,y) \equiv 0(p)$ and -1 otherwise. Hence

$$\begin{aligned} A_{2,\mathcal{F}}(p) &= p \sum_{\substack{x,y(p) \\ \delta(x,y)\equiv 0}} 1 - \sum_{x,y(p)} 1 - \left[\sum_{x(p)} \left(\frac{x^3-x}{p}\right)\right]^2 \\ &= p\Big|\{(x,y) : \delta(x,y) \equiv 0(p)\}\Big| - p^2 - \left[\sum_{x(p)} \left(\frac{x^3-x}{p}\right)\right]^2. \end{aligned} \tag{14.20}$$

By Lemma 14.3, the number of such pairs with $x, y \neq 0, \pm 1$ is $2p - 10 - \left(\frac{-3}{p}\right) - \left(\frac{3}{p}\right)$. There are 9 pairs from $x, y = 0, \pm 1$. Therefore

Lemma 14.6

$$A_{2,\mathcal{F}}(p) = p^2 - p - \left[\left(\frac{-3}{p}\right) + \left(\frac{3}{p}\right)\right]p - \left[\sum_{x(p)} \left(\frac{x^3-x}{p}\right)\right]^2 = p^2 + O(p). \tag{14.21}$$

14.2.3 1- and 2-Level Densities

If we replace t with $6t+1$, we can calculate the conductors for $D(t) = (6t+1)\cdot(27(6t+1)^2-4)$ square-free. Such a change will not affect the values of $A_{1,\mathcal{F}}(p)$ or $A_{2,\mathcal{F}}(p)$ for $p > 3$. By Lemma D.13, for $D(t)$ square-free, $C(t) = 2^2(6t+1)^2 \cdot (27(6t+1)^2+4)$. By Hooley ([Ho], Theorem 3, page 69), $c_{\mathcal{F}} > 0$.

As $j(t)$ and $M(t)$ are non-constant, we expect equidistribution in sign (for all t and for t good). The conditions of the Rational Surface Density Theorem are satisfied with $r = 2$. Therefore

Theorem 14.7 ($D^{(2)}_{1,\mathcal{F}}(f)$ and $D^{(2)}_{2,\mathcal{F}}(f)$) *For small support, $D^{(2)}_{1,\mathcal{F}}(f_1) = \widehat{f_1}(0) + \frac{1}{2}f_1(0)$. Further, the 2-level density of the non-family zeros is $\widehat{W^{(2)}_{2,\mathcal{F}}} = \widehat{W_{2,O}}$.*

To prove the above, we only assume GRH, the Birch and Swinnterton-Dyer conjecture (to interpret the rank), and the Square-Free Sieve and the Polynomial Moebius conjectures (to get equidistribution of sign for good t).

14.3 $y^2 + xy = x^3 + tx^2 - (3+2t)x + 1$

Consider Fermigier's example $y^2 + xy = x^3 + tx^2 - (3+2t)x + 1$, or $y^2 = (4x^2 - 32x)t + x^3 + x^2 - 48x + 64 = f_t(x)$. Note $4x^2 - 32x$ equals zero for $x = 0, 8$, and both $f_t(0)$ and $f_t(8)$ are squares.

$$\begin{aligned}
\Delta(t) &= 2^{14}(16t^4 + 168t^3 + 481t^2 + 630t + 272) = 2^{14}D(t) \\
c_4(t) &= 2^4(16t^2 + 104t + 145) = 2^4 c(t) \\
j(t) &= \frac{4096t^6 + \cdots + 3048625}{64t^4 + \cdots + 1088} \\
M(t) &= 16t^4 + 168t^3 + 481t^2 + 630t + 272. \qquad (14.22)
\end{aligned}$$

For $p > 3$ we calculate $h(t) = \Big(c(t), D(t)\Big)$. $D(t) \equiv 570t + 997 \bmod c(t)$. Thus, if $p | h(t)$ then

$$p | D(t) - (t^2 + 4t - 5)c(t) = 570t + 997 = h_1(t). \qquad (14.23)$$

As $c(t) \equiv \frac{978121}{81225} \bmod h_1(t)$ and $p | c(t)$ and $p | h_1(t)$ we have

$$p | 81225c(t) - (2280t + 10832)h_1(t) = 978121 = 23^2 43^2. \qquad (14.24)$$

The only possible common factors (greater than 3) are 23 and 43. If $23 | c(t)$ then $16t^2 + 104t + 145 \equiv 0 \bmod 23$, which implies $t \equiv 8$ or $20 \bmod 23$. If $D(t) \equiv 0 \bmod 23$ then $t \equiv 20 \bmod 23$. If $c(t) \equiv 0 \bmod 43$, $t \equiv 11$ or 4; if $D(t) \equiv 0 \bmod 43$, $t \equiv 11$.

Thus, it is possible for both 23 and 43 to divide $\Big(c(t), D(t)\Big)$. For convenience in calculating the conductors for square-free $D(t)$, we change variables to $\tau = 2 \cdot 3 \cdot 23 \cdot 43t + 1$. $D(\tau)$ and $c(\tau)$ are never divisible by 2, 3, 23 or 43. $3 \nmid \Delta(\tau)$, $\Big(c_4(\tau), \Delta(\tau)\Big) = 2^4$, and $2^{14} || \Delta(\tau)$.

Possibly after passing to a subsequence, by Theorem 4.3 we can handle the conductors and the cardinality. The only troublesome prime is $p = 2$.

14.3.1 $A_{1,\mathcal{F}}(p)$ and $A_{2,\mathcal{F}}(p)$

We calculate $A_{1,\mathcal{F}}(p)$ for a large number of families. Consider instead the family $y^2 = x^3 + x^2 - 48x + 64 + (4x^2 - 32x)(c_1 t + c_0)$, $c_1 \neq 0$. For $p > |c_1|$:

$$\begin{aligned} A_{1,\mathcal{F}}(p) &= -\sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{x^3+x^2-48x+64+(4x^2-32x)(c_1t+c_0)}{p}\right) \\ &= -\sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{(4x^2-32x)t+x^3+x^2-48x+64}{p}\right) \\ &= -\sum_{x\neq 0,8}\sum_{t=0}^{p-1}\left(\frac{t+x^3+x^2-48x+64}{p}\right)-\sum_{t=0}^{p-1}\left[\left(\frac{64}{p}\right)+\left(\frac{256}{p}\right)\right] \\ &= 0-2p. \end{aligned} \tag{14.25}$$

Thus this family has rank 2 over $\mathbb{Q}(t)$. As $j(t)$ is non-constant, we can use Michel's Theorem to calculate $A_{2,\mathcal{F}}(p)$.

14.3.2 1- and 2-Level Densities

As $j(t)$ and $M(t)$ are non-constant, we expect equidistribution in sign (for all t and for t good). The conditions of the Rational Surface Density Theorem are satisfied with $r = 2$. Therefore

Theorem 14.8 ($D_{1,\mathcal{F}}^{(2)}(f)$ and $D_{2,\mathcal{F}}^{(2)}(f)$) *For small support, $D_{1,\mathcal{F}}^{(2)}(f_1) = \widehat{f_1}(0) + \frac{1}{2}f_1(0)$. Further, the 2-level density of the non-family zeros is $\widehat{W_{2,\mathcal{F}}^{(2)}} = \widehat{W_{2,O}}$.*

To prove the above, we only assume GRH, the Birch and Swinnterton-Dyer conjecture (to interpret the rank), the Square-Free Sieve conjecture to handle the sieving (as $D(t)$ has an irreducible factor of degree 4), and the Square-Free Sieve and the Polynomial Moebius conjectures (to get equidistribution of sign for good t). This is our first example of a family where the sieving to good t is conditional.

14.4 General Rank 2 Construction

We show how to construct families of elliptic curves with rank 2 over $\mathbb{Q}(t)$. 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 equal.

Theorem 14.9 (Families of Rank 2) *Let $f(x) = a(x-r_1)(x-r_2)$, $h(x) = (x-B)(x-r_1)(x-r_2)+C^2$,$r_i$ integral. $y^2 = h(x)+f(x)t$ has rank 2 over $\mathbb{Q}(t)$ if $r_1 \neq r_2$ and rank 1 otherwise.*

Proof: Substituting yields

$$y^2 = a(x-r_1)(x-r_2)t+(x-B)(x-r_1)(x-r_2)+C^2 = f_t(x). \tag{14.26}$$

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

$$\begin{aligned}
A_{1,\mathcal{F}}(p) &= -\sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{f_t(x)}{p}\right) \\
&= -\sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{a(x-r_1)(x-r_2)t+(x-B)(x-r_1)(x-r_2)+C^2}{p}\right) \\
&= -\sum_{x\neq r_1,r_2}\sum_{t=0}^{p-1}\left(\frac{t+(x-B)(x-r_1)(x-r_2)+C^2}{p}\right) \\
&\quad -\sum_{t=0}^{p-1}\left[\left(\frac{f_t(r_1)}{p}\right)+\left(\frac{f_t(r_2)}{p}\right)\right] \\
&= 0-2p. \qquad (14.27)
\end{aligned}$$

If the two roots are equal we get $-p$.

Note our choice of f and h force two rational points on the curve, (r_1, C) and (r_2, C); however, we don't know if they are independent, or even in the infinite part of the Mordell-Weil group. However, by Rosen-Silverman (Theorem 2.3), as $A_{1,\mathcal{F}}(p) = pA_{\mathcal{E}}(p) = -2p$, the family has rank 2 over $\mathbb{Q}(t)$.

15 1- and 2-Level Densities for Rank 3 Rational Surfaces

15.1 $y^2 = x^3 + 5x^2 + (4-x)(4t)^2 = f_t(x)$

Consider Fermigier's example $y^2 = x^3 + 5x^2 + (4-x)(4t)^2 = f_t(x)$, where

$$\begin{aligned}
\Delta(t) &= 2^{12}t^2(64t^4 - 767t^2 - 125) = 2^{12}tD(t) = 2^{12}t^2d(t) \\
c_4(t) &= 2^4(48t^2+25) = 2^4c(t) \\
j(t) &= \frac{110592t^6 + \cdots + 15625}{64t^6 - 767t^4 - 125t^2} \\
M(t) &= t(64t^4 - 767t^2 - 125). \qquad (15.1)
\end{aligned}$$

We will replace t with $\tau = mt+1$ to make $\Big(D(mt+1), c(mt+1)\Big) = 1$. Clearly the only possible common divisor of $c(t)$ and t^2 is 25; if $5|m$ then they will be relatively prime.

Assume $p > 5$ and $p|c(t)$ and $p|d(t)$. Then $p|144d(t) - (192t^2 - 2401)c(t) = 42025$. We chose these values as $\frac{144d(t)}{c(t)} = 192t^2 - 2401 + \frac{42025}{c(t)}$. As $42025 = 5^2 \cdot 41^2$, the candidates for p are 5 and 41.

Assume $41|c(t)$. Then $7t^2 \equiv -25 \bmod 41$, or $t^2 \equiv 14 \bmod 41$; as 14 is not a square mod 41, we see $\forall t$, $41 \nmid c_4(t)$. Hence the only possible common divisor is 5. If we change to $5kt+1$, clearly $c(t)$ and $D(t)$ will be relatively prime.

To ease the conductor calculations, we consider $\tau = 2 \cdot 3^3 \cdot 5t + 1$. Mod 3, $D(\tau) \equiv 1+1+1$. Mod 9, $D(\tau) \equiv 1 + 7 + 1$. Mod 27, $D(\tau) \equiv 10 + 16 + 10 \equiv 9$.

$d(\tau) = 64(270t+1)^4 - 767(270t+1)^2 - 125$. Mod 4 we have $-767 - 125$, which is divisible by 4. Mod 8 we have $(6t+1)^2 + 3 \equiv 4t^2 + 4t + 4 = 4t(t+1) + 4 \equiv 4$.

Hence $3^2||D(\tau)$, $2^{14}\Delta(\tau)$. We consider the family

$$\begin{aligned}
y^2 &= x^3 + 5x^2 + (4-x)16(270t+1)^2 \\
c_4(t) &= 2^4\Big(48(270t+1)^2 + 25\Big) \\
\Delta(t) &= 2^{12}(270t+1)^2\Big(64(270t+1)^4 - 767(270t+1)^2 - 125\Big) \\
D(t) &= (270t+1)\Big(64(270t+1)^4 - 767(270t+1)^2 - 125\Big) \\
& \quad 2^{14}||\Delta(t),\ 3^2||\Delta(t) \\
& \quad 2^2||D(t),\ 3^2||D(t). \qquad (15.2)
\end{aligned}$$

For $\frac{D(t)}{36}$ square-free, by Lemma D.14, $C(t) = \frac{|D(t)|}{6}$. Thus, for t sufficiently large, the conductors will be given by a monotone polynomial.

15.1.1 $A_{1,\mathcal{F}}(p)$ and $A_{2,\mathcal{F}}(p)$

We calculate $A_{1,\mathcal{F}}(p)$ for a large number of families. Consider instead the family $y^2 = x^3 + 5x^2 + (4-x)16(c_1t+c_0)^2$, $c_1 \neq 0$. For $p > |c_1|$:

$$\begin{aligned} A_{1,\mathcal{F}}(p) &= -\sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{x^3+5x^2+(4-x)16(c_1t+c_0)^2}{p}\right) \\ &= -\sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{(4-x)t^2+x^3+5x^2}{p}\right). \end{aligned} \tag{15.3}$$

To investigate $A_{1,\mathcal{F}}(p)$ we use the lemma on Quadratic Legendre Sums (Lemma C.2). The quadratic t polynomial has discriminant $-4(4-x)(x^3+5x^2)$, which is congruent to zero mod p for $x = 0$, 4 and -5. For $x = 4$ we get $p\left(\frac{144}{p}\right)$, for $x = 0$ or -5 we get $(p-1)\left(\frac{4-x}{p}\right)$, and for the other $p-3$ we get $-\left(\frac{4-x}{p}\right)$.

$$\begin{aligned} A_{1,\mathcal{F}}(p) &= -\sum_{x=4}\sum_{t=0}^{p-1}\left(\frac{144}{p}\right) - \sum_{x=0,-5}\sum_{t=0}^{p-1}\left(\frac{4-x}{p}\right) - \sum_{x\neq 0,4,-5}\sum_{t=0}^{p-1}\left(\frac{4-x}{p}\right) \\ &= -p-(p-1)\left(\frac{4}{p}\right)-(p-1)\left(\frac{9}{p}\right)+\sum_{x\neq 0,4,-5}\left(\frac{4-x}{p}\right) \\ &= -3p. \end{aligned} \tag{15.4}$$

Thus this family has rank 3 over $\mathbb{Q}(t)$. As $j(t)$ is non-constant, we may use Michel's Theorem to calculate $A_{2,\mathcal{F}}(p)$.

15.1.2 $|\mathcal{F}|$

Recall $D(t) = (270t+1)\cdot(64(270t+1)^4 - 767(270t+1)^2 - 125) = D_\alpha(t)D_\beta(t)$. We need to sieve to $\frac{D(t)}{36}$ square-free. Thus, we study divisibility by p^2, $p \geq 5$.

Clearly $\Big(D_\alpha(t), D_\beta(t)\Big) = 1$: the only possible common prime divisor is 5, and $5 \nmid D_\alpha(t)$. For every prime $p \geq 7$, $D_\alpha(t)$ has one root mod p; it has no roots for $p \leq 5$.

The discriminant of $D_\beta(t)$ is $2^{22}3^{40}5^{15}41^6$. Mod 5, $D_\beta(t) \equiv 4+3 \equiv 2$. Thus, $D_\beta(t) \not\equiv 0$ mod 5.

Mod 41, $D_\beta(t) \equiv 10t^4+29t^3+13t^2+37t+33$, which is never equivalent to zero mod 41. Thus, there are no t where $41^2|D(t)$.

As the degree of $D(t)$ is 5, we need to check solutions of $D(t) \equiv 0 \bmod p$ for $p \leq \sqrt{5}$, which was done above. Hence Theorem 3.8 is applicable, and $c_{\mathcal{F}} > 0$.

15.1.3 1- and 2-Level Densities

As $j(t)$ and $M(t)$ are non-constant, we expect equidistribution in sign (for all t and for t good). The conditions of the Rational Surface Density Theorem are satisfied with $r = 3$. Therefore

Theorem 15.1 ($D^{(3)}_{1,\mathcal{F}}(f)$ and $D^{(3)}_{2,\mathcal{F}}(f)$) *For small support, $D^{(3)}_{1,\mathcal{F}}(f_1) = \widehat{f_1}(0) + \frac{1}{2}f_1(0)$. Further, the 2-level density of the non-family zeros is $\widehat{W^{(3)}_{2,\mathcal{F}}} = \widehat{W_{2,O}}$.*

To prove the above, we only assume GRH, the Birch and Swinnterton-Dyer conjecture (to interpret the rank), the Square-Free Sieve conjecture to handle the sieving (as $D(t)$ has an irreducible factor of degree 4), and the Square-Free Sieve and the Polynomial Moebius conjectures (to get equidistribution of sign for good t).

15.2 General Rank 3 Construction

In the next chapter we give a construction for rank 4 families. By taking two of the roots equal, we obtain a construction for rank 3 families.

16 1- and 2-Level Densities for Rank 4 Rational Surfaces

16.1 $y^2 = x^3 + 41x^2 + 184x + 144 - 16t^2x = f_t(x)$

Consider Fermigier's example $y^2 = x^3 + 41x^2 + 184x + 144 - 16t^2x = f_t(x)$.

$$\begin{aligned}
\Delta(t) &= 2^{12}(64t^6 - 527t^4 - 19913t^2 + 44100) = 2^{12}D(t) \\
c_4(t) &= 2^4(48t^2 + 1129) = 2^4c(t) \\
j(t) &= \frac{110592t^6 + \cdots + 1439069689}{64t^6 + \cdots + 44100} \\
M(t) &= 64t^6 - 527t^4 - 19913t^2 + 44100. \qquad (16.1)
\end{aligned}$$

We calculate $h(t) = \Big(c(t), D(t)\Big)$ for $p \geq 5$. $D(t) \equiv \frac{-4229291089}{6912}$ mod $c(t)$. Thus, if $p|h(t)$,

$$p|6912D(t) - (9216t^4 - 292656t^2 + 4016041)c(t) = -4229291089 = -65033^2. \qquad (16.2)$$

If $c(t) \equiv 0$ mod 65033, $t \equiv 18305$ or 46728. If $D(t) \equiv 0$ mod 65033, $t \equiv 45605$, 19428, 18305 or 46728.

To facilitate the conductor calculations, let $\tau = 2^2 3^3 65033t + 1$. Then $\Big(c_4(\tau), \Delta(\tau)\Big) = 2^4$, $2^{14}||\Delta(\tau)$, and as $D(\tau) \equiv -9$ mod 27), $3^2||\Delta(\tau)$. Clearly we cannot sieve to $D(\tau)$ square-free; instead we sieve to $D'(t) = \frac{D(\tau)}{4\cdot 9}$ square-free; note $\Big(D'(t), 6\Big) = 1$.

16.2 $A_{1,\mathcal{F}}(p)$ and $A_{2,\mathcal{F}}(p)$

To investigate $A_{1,\mathcal{F}}(p) = -\sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{f_t(x)}{p}\right)$ we use the lemma on Quadratic Legendre Sums (Lemma C.2). More generally, consider $y^2 = x^3 + 41x^2 + 184x + 144 - 16(c_1t + c_0)^2x = f_{c_1t+c_0}(x)$, $c_1 \neq 0$. For $p > |c_1|$, we may replace $c_1t + c_0$ by t in complete t-sums mod p. 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 such x is 3. When $x = 0$ we have $\sum_{t=0}^{p-1}\left(\frac{144}{p}\right) = p$. Hence

$$\sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{f_t(x)}{p}\right) = 3(p-1)+3+p = 4p, \tag{16.3}$$

Thus this family has rank 4 over $\mathbb{Q}(t)$. As $j(t)$ is non-constant, we may use Michel's Theorem to calculate $A_{2,\mathcal{F}}(p)$.

16.2.1 $|\mathcal{F}|$

We sieve to $D'(t) = \frac{D(\tau)}{4\cdot 9}$ square-free. $\Big(D'(t), 6\Big) = 1$, $D'(t) = 2^{16}3^{16}65033^6t^6 + \cdots + 659$ and is primitive irreducible. The discriminant is $\delta = 2^{54}3^{76}5^27^265033^{36}$.

Let $\nu(p)$ be the number of incongruent solutions to $D'(t) \equiv 0 \bmod p^2$. The only factors of $a_k\delta$ are $2, 3, 5, 7$ and 65033, and $\sqrt{\text{deg}D'(t)} = \sqrt{6} < 3$. If we show for these primes that $\nu(p) < p^2 - 1$, then by Theorem 3.8 a positive percent of t give $D'(t)$ square-free.

$\nu(2) = \nu(3) = 0$, $\nu(5) = 5$ ($t \equiv 1, 6, 11, 16$ or $21 \bmod 25$), $\nu(7) = 7$ ($t \equiv 3, 10, 17, 24, 31, 38$ or $45 \bmod 49$), and $\nu(65033) = 0$.

Hence, by Theorem 3.8, a positive percent of t yield $D'(t)$ square-free. By Lemma D.15, for $D'(t)$ square-free, $C(t) = 6|D'(t)|$. Hence the conductors are given by a monotone polynomial.

16.2.2 1- and 2-Level Densities

As $j(t)$ and $M(t)$ are non-constant, we expect equidistribution in sign (for all t and for t good). The conditions of the Rational Surface Density Theorem are satisfied with $r = 4$. Therefore

Theorem 16.1 ($D^{(4)}_{1,\mathcal{F}}(f)$ and $D^{(4)}_{2,\mathcal{F}}(f)$) *For small support, $D^{(4)}_{1,\mathcal{F}}(f_1) = \widehat{f_1}(0) + \frac{1}{2}f_1(0)$. Further, the 2-level density of the non-family zeros is $\widehat{W^{(4)}_{2,\mathcal{F}}} = \widehat{W_{2,O}}$.*

To prove the above, we only assume GRH, the Birch and Swinnterton-Dyer conjecture (to interpret the rank), the Square-Free Sieve conjecture to handle the sieving (as $D(t)$ has an irreducible factor of degree 6), and the Square-Free Sieve and the Polynomial Moebius conjectures (to get equidistribution of sign for good t).

16.3 General Rank 4 Construction

We now give a construction that will generate rank 4 families. 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 16.2 (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 $y^2 = f_t(x)$ has rank 4 over $\mathbb{Q}(t)$.*

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 the lemma on Quadratic Legendre Sums (Lemma C.2) we have (for $f(x) \not\equiv 0 \bmod p$)

$$\sum_{t=0}^{p-1} \left(\frac{f(x)t^2 + 2g(x)t - h(x)}{p}\right) = \begin{cases} -\left(\frac{f(x)}{p}\right) & D_t(x) \not\equiv 0(p) \\ (p-1)\left(\frac{f(x)}{p}\right) & D_t(x) \equiv 0(p) \end{cases} \tag{16.4}$$

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 3.

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

$$\sum_{x=0}^{p-1}\sum_{t=0}^{p-1} \left(\frac{f_t(x)}{p}\right) = 3(p-1) + p + 3 = 4p. \tag{16.5}$$

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

$$\begin{aligned} D_t(x) &= 4x\Big(x(x+b)^2 + (3x^3 + Bx^2 + Cx - D^2)\Big) \\ &= 16x(x^3 + \frac{B+2b}{4}x^2 + \frac{C+b^2}{4}x - \frac{D^2}{4}) \end{aligned} \tag{16.6}$$

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 $B = -4(r_1^2 + r_2^2 + r_3^2) - 2b$, $C = 4(r_1^2 r_2^2 + r_1^2 r_3^2 + r_2^2 r_3^2) - b^2$, and $D^2 = 4r_1^2 r_2^2 r_3^2$. Taking $x = 0, r_1, r_2$, and r_3 yield four rational points on the curve.

We may write the curve as

$$y^2 = x^3 + [2t + B(r,b)]x^2 + [3C(r,b) - 6bt - 3t^2]x + 9D^2(r,b). \tag{16.7}$$

We note that this method of construction cannot be used to yield families of rank 7 or more over $\mathbb{Q}(t)$ 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 rank 6. However, by looking at $y^2 = f(x)$ for f a good quartic, it might be possible to construct rank 8 families.

17 1- and 2-Level Densities for (Conditional) Rank 5 Surfaces

17.1 Idea of the Construction

We construct a family with rank 5 by modifying the rank 4 construction. Let

$$\begin{aligned}
y^2 = f_t(x) &= x^2t^2 + 2g(x)t - h(x) \\
g(x) &= x^3 + ax^2 + bx + c, \ c \neq 0 \\
h(x) &= Ax^3 + Bx^2 + Cx + D \\
D_t(x) &= g(x)^2 + x^2h(x). \qquad (17.1)
\end{aligned}$$

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 $A_{1,\mathcal{F}}(p)$.

We 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 the lemma on Quadratic Legendre Sums (Lemma C.2)

$$\sum_{t=0}^{p-1}\left(\frac{x^2t^2+2g(x)t-h(x)}{p}\right) = \begin{cases} (p-1)\left(\frac{x^2}{p}\right) & \text{if } p \mid D_t(x) \\ -1\left(\frac{x^2}{p}\right) & \text{otherwise} \end{cases} \qquad (17.2)$$

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

$$\begin{aligned}
\sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{f_t(x)}{p}\right) &= \sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{x^2t^2+2g(x)t-h(x)}{p}\right) \\
&= \sum_{x=0}\sum_{t=0}^{p-1}\left(\frac{f_t(x)}{p}\right) + \sum_{\substack{x=1 \\ D_t(x)=0}}^{p-1}\sum_{t=0}^{p-1}\left(\frac{f_t(x)}{p}\right) + \sum_{\substack{x=1 \\ xD_t(x)\neq 0}}^{p-1}\sum_{t=0}^{p-1}\left(\frac{f_t(x)}{p}\right) \\
&= 0 + 6(p-1) + (p-7)(-1) \\
&= 5p + 1. \qquad (17.3)
\end{aligned}$$

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.

$$\begin{aligned}
D_t(x) &= g(x)^2 + x^2 h(x) \\
&= (x^3 + ax^2 + bx + c)^2 + x^2(Ax^3 + Bx^2 + Cx + D) \\
&= x^6 + (A + 2a)x^5 + (B + a^2 + 2b)x^4 + (C + 2ab + 2c)x^3 \\
&\quad + (D + 2ac + b^2)x^2 + (2bc)x + c^2 \\
&=^? x^6 + R_5x^5 + R_4x^4 + R_3x^3 + R_2x^2 + R_1x + R_0 \\
&= (x + r_1)(x + r_2)(x + r_3)(x + r_4)(x + r_5)(x + r_6). \qquad (17.4)
\end{aligned}$$

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 equal 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 $(2t - A)^2$.

$$\begin{aligned}
f_t(x) &= (2t - A)x^3 + x^2t^2 + (2ax^2 + 2bx + 2c)t - Bx^2 - Cx - D \\
F_t(x) &= x^3 + x^2t^2 + (2ax^2 + 2bx(2t - A) + 2c(2t - A)^2)t \\
&\quad -Bx^2 - Cx(2t - A) - D(2t - A)^2 \\
&= x^3 + (t^2 + 2at - B)x^2 + (2bt - C)(2t - A)x \\
&\quad +(2ct - D)(2t - A)^2. \qquad (17.5)
\end{aligned}$$

Now we study $-A_{1,\mathcal{F}}(p)$ arising from $F_t(x)$, assuming that we can find coefficients so that $D_t(x)$ has six distinct non-zero roots.

$$\begin{aligned}
\sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\left(\frac{F_t(x)}{p}\right) &= \sum_{2t\neq A}\sum_{x=0}^{p-1}\left(\frac{F_t(x)}{p}\right) + \sum_{2t=A}\sum_{x=0}^{p-1}\left(\frac{F_t(x)}{p}\right) \\
&\quad 2t \neq A, \quad x \to (2t - A)x \\
&\quad \text{as } 2t - A \neq 0, \left(\frac{(2t - A)^2}{p}\right) = 1, \text{pull out } (2t - A)^2
\end{aligned}$$

$$\begin{aligned}
&= \sum_{2t\neq A}\sum_{x=0}^{p-1}\left(\frac{f_t(x)}{p}\right) + \sum_{x=0}^{p-1}\left(\frac{x^3+(\frac{A^2}{4}+aA-B)x^2}{p}\right) \\
&= \sum_{2t\neq A}\sum_{x=0}^{p-1}\left(\frac{f_t(x)}{p}\right) + O(1) \\
&= \sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\left(\frac{f_t(x)}{p}\right) - \sum_{2t-A=0}\sum_{x=0}^{p-1}\left(\frac{f_t(x)}{p}\right) + O(1) \\
&= 5p + O(1) + O(1) - \sum_{x=0}^{p-1}\left(\frac{f_{A/2}(x)}{p}\right) \\
&= 5p + O(1) - \sum_{x=0}^{p-1}\left(\frac{x^2\frac{A^2}{4}+(ax^2+bx+c)A-Bx^2-Cx-D}{p}\right) \\
&= 5p + O(1) - \sum_{x=0}^{p-1}\left(\frac{(aA+\frac{A^2}{4}-B)x^2+(bA-C)x+(cA-D)}{p}\right).
\end{aligned} \tag{17.6}$$

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

$$D_2(x) = (bA-C)^2 - 4(aA+\frac{A^2}{4}-B)(cA-D) \not\equiv 0(p). \tag{17.7}$$

17.2 Determining Admissible Constants $a, \dots, D$

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.

$$\begin{aligned}
\Phi(x) &= (x+4)(x+6)(x+8)(x+1)(x-6)(x-8) \\
&= x^6+5x^5-96x^4-500x^3+1904x^2+11520x+9216 \\
&= x^6+R_5x^5+R_4x^4+R_3x^3+R_2x^2+R_1x+R_0.
\end{aligned} \tag{17.8}$$

This gives (on taking $a = 0$)

$$b = 60, c = 96, A = 5, B = -216, C = -692, D = -1696. \tag{17.9}$$

Therefore

$$\begin{aligned} g(x) &= x^3 + 60x + 96 \\ h(x) &= 5x^3 - 216x^4 - 692x - 1696 \\ D_t(x) &= x^6 + 5x^5 - 96x^4 - 500x^3 + 1904x^2 + 11520x + 9216 \\ &= x^6 + R_5x^5 + R_4x^4 + R_3x^3 + R_2x^2 + R_1x + R_0 \end{aligned} \tag{17.10}$$

and

$$\begin{aligned} D_2(x) &= (bA - C)^2 - 4(aA + \frac{A^2}{4} - B)(cA - D) \\ &= (60 * 5 + 692)^2 - (5^2 + 4 * 216)(96 * 5 + 1696) \\ &= -950400. \end{aligned} \tag{17.11}$$

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

$$\begin{aligned} &(6, 6t + 112),\ (8, 8t + 136),\ (-1, t + 35), \\ &(-4, 4t - 52),\ (-6, 6t - 80),\ (-8, 8t - 112). \end{aligned} \tag{17.12}$$

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

$$\begin{aligned} D_t(x) &= x^6 + (A + 2a)x^5 + (B + a^2 + 2b)x^4 + (C + 2ab + 2c)x^3 \\ &\quad + (D + 2ac + b^2)x^2 + (2bc)x + c^2 \\ &= x^6 + R_5x^5 + R_4x^4 + R_3x^3 + R_2x^2 + R_1x + R_0 \\ &= (x + r_1)(x + r_2)(x + r_3)(x + r_4)(x + r_5)(x + r_6). \end{aligned} \tag{17.13}$$

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

$$2bc = R_1 = r_1r_2r_3r_4r_5 + \cdots + r_2r_3r_4r_5r_6$$

$$c^2 = R_0 = r_1r_2r_3r_4r_5r_6. \tag{17.14}$$

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

$$\begin{aligned} c &= rr_2r_3, \quad 2bc = -2r^2r_2^2r_3 - 2r^2r_2r_3^2 + r^2r_2^2r_3^2 + r_2^2r_3^2 \\ & \text{try } r = 2 \\ 4b &= r_2r_3 + 4r_2r_3 - 8r_3 - 8r_2. \end{aligned} \tag{17.15}$$

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 rank of only 4. This phenomenon may be worth investigating.

17.3 General Rank 5 Construction

Theorem 17.1 (Constructing Rank 5 Families) *There exist integers a, b, c, A, B, C, D so that, assuming Tate's conjecture, 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 rank 5. We may take $a = 0, b = 60, c = 96, A = 5, B = -216, C = -692, D = -1696$, obtaining*

$$\begin{aligned} y^2 &= x^3 + (t^2 + 2at - B)x^2 + (2bt - C)(2t - A)x \\ &\quad +(2ct - D)(2t - A)^2 \\ c_4(t) &= 16t^4 + 4608t^2 - 37632t + 912576 \\ c_6(t) &= -64t^6 + 27648t^4 - 437760t^3 + 2431872t^2 + 73930752t \\ &\quad -\ 896845824 \\ j(t) &= \frac{16t^{12} + \ldots + 2968705818602496}{-192t^9 + \cdots - 100241750000} \\ \Delta(t) &= -41952t^9 + \ldots - 25661888000000 \\ M(t) &= -41952t^9 + \ldots - 25661888000000. \end{aligned} \tag{17.16}$$

As the above is not a rational surface, Tate's conjecture is not known for the surface. While we may calculate $A_{1,\mathcal{F}}(p) = -5p + O(1)$, we cannot unconditionally interpret this as the rank over $\mathbb{Q}(t)$.

For concreteness, we explicitly list a curve of rank at least 5. By a more delicate analysis (ie, doing a better job of choosing coefficients a through D so that the method works), we are led to

$$y^2 = x^3 - 15823x + 767122. \tag{17.17}$$

Five points on the curve are:

$$\begin{array}{lll} P[1] = (81, 130) & P[2] = (83, 160) & P[3] = (74, 38) \\ P[4] = (71,\ 40) & P[5] = (69,\ 62) & \end{array}$$

As the determinant of the height matrix is approximately 32.5, the points are independent; hence the Mordell-Weil group has rank at least 5. The curve has odd sign.

17.4 1- and 2-Level Densities

As $j(t)$ and $M(t)$ are non-constant, we expect equidistribution in sign (for all t and for t good). Even though this is not a rational surface, as the discriminant is of degree less than 12, Theorem 4.3 is applicable to handle the sieving and to calculate the conductors.

The conditions of the Rational Surface Density Theorem are satisfied with $r = 5$. Therefore

Theorem 17.2 ($D_{1,\mathcal{F}}^{(5)}(f)$ and $D_{2,\mathcal{F}}^{(5)}(f)$) *For small support, $D_{1,\mathcal{F}}^{(5)}(f_1) = \widehat{f_1}(0) + \frac{1}{2}f_1(0)$. Further, the 2-level density of the non-family zeros is $\widehat{W_{2,\mathcal{F}}^{(5)}} = \widehat{W_{2,O}}$.*

To prove the above, we assume GRH, the Birch and Swinnterton-Dyer conjecture and Tate's conjecture (to interpret the rank), the Square-Free Sieve conjecture to handle the sieving (as $D(t)$ has an irreducible factor of degree 9), and the Square-Free Sieve and the Polynomial Moebius conjectures (to get equidistribution of sign for good t).

18 1- and 2-Level Densities for Rank 6 Rational Surfaces

18.1 Idea of the Construction

We construct a family of rank 6 by modifying the rank 5 construction. Let

$$\begin{aligned} y^2 = f_t(x) &= x^3t^2 + 2g(x)t - h(x) \\ g(x) &= x^3 + ax^2 + bx + c,\ c \neq 0 \\ h(x) &= (A-1)x^3 + Bx^2 + Cx + D \\ D_t(x) &= g(x)^2 + x^3h(x). \end{aligned} \tag{18.1}$$

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 rank. 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 $-A_{1,\mathcal{F}}(p) = \sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{f_t(x)}{p}\right)$. 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 the lemma on Quadratic Legendre Sums (Lemma C.2)

$$\sum_{t=0}^{p-1}\left(\frac{x^3t^2+2g(x)t-h(x)}{p}\right) = \begin{cases} (p-1)\left(\frac{x^3}{p}\right) & \text{if } p \mid D_t(x) \\ -1\left(\frac{x^3}{p}\right) & \text{otherwise} \end{cases} \tag{18.2}$$

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 in better shape then the rank 5 case, as there we had $\left(\frac{x^2}{p}\right)$. Summing 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

$$\begin{aligned} -A_{1,\mathcal{F}}(p) &= \sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{f_t(x)}{p}\right) = \sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{x^3t^2+2g(x)t-h(x)}{p}\right) \\ &= \sum_{x=0}\sum_{t=0}^{p-1}\left(\frac{f_t(x)}{p}\right) + \sum_{x:D_t(x)=0}\sum_{t=0}^{p-1}\left(\frac{f_t(x)}{p}\right) + \sum_{x:xD_t(x)\neq 0}\sum_{t=0}^{p-1}\left(\frac{f_t(x)}{p}\right) \\ &= 0 \ + \ 6(p-1) \ - \sum_{x:xD_t(x)\neq 0}\left(\frac{x^3}{p}\right) \ = \ 6p. \end{aligned} \tag{18.3}$$

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

$$\begin{aligned}
D_t(x) &= g(x)^2 + x^3 h(x) \\
&= (x^3 + ax^2 + bx + c)^2 + x^3((A-1)x^3 + Bx^2 + Cx + D) \\
&= Ax^6 + (B+2a)x^5 + (C + a^2 + 2b)x^4 + (D + 2ab + 2c)x^3 \\
&\quad + (2ac + b^2)x^2 + (2bc)x + c^2 \\
&= A\Big(x^6 + \frac{B+2a}{A}x^5 + \frac{C+a^2+2b}{A}x^4 + \frac{D+2ab+2c}{A}x^3 \\
&\quad + \frac{2ac+b^2}{A}x^2 + \frac{2bc}{A}x + \frac{c^2}{A}\Big) \\
&= A(x^6 + R_5x^5 + R_4x^4 + R_3x^3 + R_2x^2 + R_1x + R_0) \\
&= A(x+r_1)(x+r_2)(x+r_3)(x+r_4)(x+r_5)(x+r_6) = A\Phi(x).
\end{aligned} \tag{18.4}$$

18.2 Determining Admissible Constants $a, \ldots, D$

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

$$\begin{aligned}
2ac + b^2 &= R_2 A \\
2bc &= R_1 A \\
c^2 &= R_0 A.
\end{aligned} \tag{18.5}$$

We can always send $A \to Aw^2$. This rescales b and c by w, and instead of $2ac + b^2 = R_2A$ we have $2ac + b^2w = R_2Aw$. Taking $w = 2c$ simplifies our work to solving $a + b^2 = R_2A$, 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 $2bc = R_1A$ yields $b = R_1$. We now send $A \to Aw^2 = (4R_0) \cdot (2c)^2 = 64R_0^3$. Thus we obtain:

$$\begin{array}{rclcrcl} c^2 & = & 64R_0^4 & \to & c & = & 8R_0^2 \\ 2bc & = & 64R_0^3R_1 & \to & b & = & 4R_0R_1 \\ 2ac+b^2 & = & 64R_0^3R_2 & \to & a & = & 4R_0R_2-R_1^2. \end{array} \tag{18.6}$$

Take $r_i = -\rho_i^2 = -i^2$. Then

$$\begin{aligned} A\Phi(x) &= A(x-1)(x-4)(x-9)(x-16)(x-25)(x-36) \\ &= A\Big(x^6 - 91x^5 + 3003x^4 - 44473x^3 \\ &\quad +296296x^2 - 773136x + 518400\Big) \\ &= A\Big(x^6 + \frac{B+2a}{A}x^5 + \frac{C+a^2+2b}{A}x^4 + \frac{D+2ab+2c}{A}x^3 \\ &\quad + \frac{2ac+b^2}{A}x^2 + \frac{2bc}{A}x + \frac{c^2}{A}\Big) \\ &= A(x^6 + R_5x^5 + R_4x^4 + R_3x^3 + R_2x^2 + R_1x + R_0). \end{aligned} \tag{18.7}$$

We find, for these choices of roots, that

$$R_0 = 518400, R_1 = -773136, R_2 = 296296. \tag{18.8}$$

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

$$\begin{array}{rcrcr} A & = & 64R_0^3 & = & 8916100448256000000 \\ c & = & 8R_0^2 & = & 2149908480000 \\ b & = & 4R_0R_1 & = & -1603174809600 \\ a & = & 4R_0R_2 - R_1^2 & = & 16660111104 \end{array} \tag{18.9}$$

We now solve for B, C, D, getting

$$\begin{array}{rcrcr} B & = & R_5A - 2a & = & -811365140824616222208 \\ C & = & R_4A - a^2 - 2b & = & 26497490347321493520384 \\ D & = & R_3A - 2ab - 2c & = & -343107594345448813363200 \end{array} \tag{18.10}$$

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

$$\begin{aligned} t^2+2t-A+1 &= (t+1-\sqrt{A})(t+1+\sqrt{A}) \\ &= (t-t_1)(t-t_2) \\ &= (t-2985983999)(t+2985984001). \end{aligned} \tag{18.11}$$

$$\begin{aligned} f_t(x) &= t^2x^3+(2x^3+2ax^2+2bx+2c)t-(A-1)x^3-Bx^2-Cx-D \\ &= (t^2+2t-A+1)x^3+(2at-B)x^2+(2bt-C)x+(2ct-D) \\ F_t(x) &= x^3+(2at-B)x^2+(2bt-C)(t^2+2t-A+1)x \\ &\quad +(2ct-D)(t^2+2t-A+1)^2. \end{aligned} \tag{18.12}$$

Now we study the $-A_{1,\mathcal{F}}(p)$ arising from $F_t(x)$.

$$\begin{aligned} \sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\left(\frac{F_t(x)}{p}\right) &= \sum_{t\neq t_1,t_2}\sum_{x=0}^{p-1}\left(\frac{F_t(x)}{p}\right)+\sum_{t=t_1,t_2}\sum_{x=0}^{p-1}\left(\frac{F_t(x)}{p}\right) \\ &\quad t\neq t_1,t_2,\quad x\to(t^2+2t-A+1)x \\ &\quad \text{as } (t^2+2t-A+1)\neq 0, \left(\frac{(t^2+2t-A+1)^2}{p}\right)=1, \\ &\quad \text{pull out } (t^2+2t-A+1)^2 \text{ from the first term} \\ &= \sum_{t\neq t_1,t_2}\sum_{x=0}^{p-1}\left(\frac{f_t(x)}{p}\right)+\sum_{t=t_1,t_2}\sum_{x=0}^{p-1}\left(\frac{x^3+(2at-B)x^2}{p}\right) \\ &= \sum_{t\neq t_1,t_2}\sum_{x=0}^{p-1}\left(\frac{f_t(x)}{p}\right)+O(1) \\ &= \sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\left(\frac{f_t(x)}{p}\right)-\sum_{t=t_1,t_2}\sum_{x=0}^{p-1}\left(\frac{f_t(x)}{p}\right)+O(1) \\ &= 6p+O(1)+O(1)+\sum_{t=t_1,t_2}\sum_{x=0}^{p-1}\left(\frac{f_t(x)}{p}\right) \\ &= 6p+O(1)+\sum_{t=t_1,t_2}\sum_{x=0}^{p-1}\left(\frac{(2at-B)x^2+(2bt-C)x+(2ct-D)}{p}\right). \end{aligned} \tag{18.13}$$

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

$$D(t) = (2bt - C)^2 - 4(2at - B)(2ct - D) \not\equiv 0(p). \tag{18.14}$$

Calculating yields

$$\begin{aligned} D(t_1) &= 4291243480243836561123092143580209905401856 \\ &= 2^{32}3^{25}7^{5}11^{2}13 \cdot 19 \cdot 29 \cdot 31 \cdot 47 \cdot 67 \cdot 83 \cdot 97 \cdot 103 \\ D(t_2) &= 4291243816662452751895093255391719515488256 \\ &= 2^{33}3^{12}7 \cdot 11 \cdot 13 \cdot 41 \cdot 173 \cdot 17389 \cdot 805873 \cdot 9447850813. \end{aligned} \tag{18.15}$$

Hence, except for finitely many primes (coming from factors of $D(t_i)$, $a, \dots, D$), $-A_{\mathcal{E}}(p) = 6p + O(1)$ as desired.

18.3 General Rank 6 Construction

Theorem 18.1 (Constructing Rank 6 Families) *We can find integers a, b, c, A, B, C, D so that the family $y^2 = x^3t^2 + 2g(x)t - h(x)$, $g(x) = x^3 + ax^2 + bx + c$ and $h(x) = (A-1)x^3 + Bx^2 + Cx + D$, has rank 6 over $\mathbb{Q}(t)$. In particular, with the choices of a through D above we have:*

$$\begin{aligned} y^2 &= x^3 + (2at - B)x^2 + (2bt - C)(t^2 + 2t - A + 1)x \\ &\qquad +(2ct - D)(t^2 + 2t - A + 1)^2 \\ c_4(t) &= 2^{19}3^{7}7^{1}13^{1}(1475t^3 + 12359745382011t^2 \\ &\quad - 48601106039970532404 03t \\ &\quad - 7735999878503076170786750620939) \\ c_6(t) &= -2^{25}3^{11}(625t^5 + \cdots + 4280\dots8201) \\ j(t) &= \frac{50141357421875t^9 + \cdots - 7233\dots6875}{-1171875t^{10} + \cdots - 5944\dots1875} \\ \Delta(t) &= -2^{44}3^{18}5^{6}(75t^{10} + \dots + 3804\dots0875 \\ &= -2^{44}3^{18}5^{6}(t \pm \sqrt{A} + 1)^2(75t^6 + \cdots + 4785\dots0875). \end{aligned} \tag{18.16}$$

Note this ia a rational surface, and Rosen-Silverman's theorem is applicable.

For concreteness, we explicitly list a curve of rank at least 6. By a more delicate analysis (ie, doing a better job of choosing coefficients a through D so that the method works), we are led to

Theorem 18.2 *$y^2 = x^3 + Ax + B$ has rank at least 6, where*

$$\begin{aligned} A &= 112318704018571 7205972 \\ B &= 507868938591179376397860 31372848 \end{aligned}$$

Six points on the curve are:

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

As the determinant of the height matrix is approximately $880,000$, the points are independent; hence the Mordell-Weil group has rank at least 6. The curve has even sign.

18.4 1- and 2-Level Densities

As $j(t)$ and $M(t)$ are non-constant, we expect equidistribution in sign (for all t and for t good). The conditions of the Rational Surface Density Theorem are satisfied with $r = 6$. Therefore

Theorem 18.3 ($D^{(6)}_{1,\mathcal{F}}(f)$ and $D^{(6)}_{2,\mathcal{F}}(f)$) *For small support, $D^{(6)}_{1,\mathcal{F}}(f_1) = \widehat{f_1}(0) + \frac{1}{2}f_1(0)$. Further, the 2-level density of the non-family zeros is $\widehat{W^{(6)}_{2,\mathcal{F}}} = \widehat{W_{2,O}}$.*

To prove the above, we assume GRH, the Birch and Swinnterton-Dyer conjecture (to interpret the rank), the Square-Free Sieve conjecture to handle the sieving (as $D(t)$ has an irreducible factor of degree 10), and the Square-Free Sieve and the Polynomial Moebius conjectures (to get equidistribution of sign for good t).

19 More Attempts for Families with $r = 6$, 7 and 8

19.1 Families of Rank 6

We give another construction for a family of rank 6 by modifying our construction from the rank 5 and 6 cases.

Let

$$\begin{aligned}
y^2 = f_t(x) &= x^4t^2 + 2g(x)t - h(x) \\
g(x) &= x^4 + ax^3 + bx^2 + cx + d, \;\; d \neq 0 \\
h(x) &= -x^4 + Ax^3 + Bx^2 + Cx + D \\
D_t(x) &= g(x)^2 + x^4h(x). \qquad (19.1)
\end{aligned}$$

The idea is similar to before. We try and find choices of the free coefficients such that $D_t(x) = \prod_1^7(\alpha^2x - \rho_i)$, with each root non-zero. For $x = 0$, we have $\sum_t \left(\frac{2dt-D}{p}\right)$, which vanishes. By Lemma C.2, for x a root of D_t we have a contribution of $(p-1)\left(\frac{x^4}{p}\right) = (p-1)\left(\frac{\rho_i^4\alpha^{-8}}{p}\right) = p-1$; for all other x a contribution of $-\left(\frac{x^4\alpha^{-8}}{p}\right) = -1$. Hence summing over x and t yields $7(p-1) + \sum_{x\neq\rho_i,0} -1 = 6p$. 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 $\mathbb{Q}$ and obtain an elliptic curve.

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

$$\begin{aligned}
D_t(x) &= (2a + A)x^7 + (a^2 + 2b + B)x^6 + (2c + 2ab + C)x^5 \\
&\quad + (b^2 + 2ac + 2d + D)x^4 + (2bc + 2ad)x^3 \\
&\quad + (2bd + c^2)x^2 + (2cd)x + d^2 \\
&= \prod_{i=1}^{7}(\alpha^2x - \rho_i) \\
&= \sum_{k=0}^{7} x^k(-1)^{k+1}\alpha^{2k}R_k. \qquad (19.2)
\end{aligned}$$

If $\prod_{i=1}^7 \rho_i = -\square$, 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

$$\begin{aligned} d^2 &= -R_0 \\ 2cd &= (2d)^2 R_1 \\ 2bd + c^2 &= -(2d)^4 R_2 \\ 2bc + 2ad &= (2d)^6 R_3. \end{aligned} \tag{19.3}$$

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

$$\begin{aligned} d &= 12,\ c = -864,\ b = -2740608,\ a = 192844800 \\ D &= -1013478801432, \\ C &= 169376669763264 \\ B &= -183270506625785088 \\ A &= 21035720122782898176. \end{aligned} \tag{19.4}$$

Hence we can find integer coefficients such that

$$y^2 = (t+1)^2 x^4 + \dots \tag{19.5}$$

We quote the following theorem (Mordell [Mor], page 77; also see Nagao [Na2], page 212):

Theorem 19.1 *Let $a_4, a_3, a_2, a_1, a_0 \in \mathbb{Q}, a_4 \neq 0$. Then E and E' are isomorphic over $\mathbb{Q}(\sqrt{a_4})$, 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

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

As the coefficient of x^4 is a perfect square, we see we again obtain a family with rank 6 over $\mathbb{Q}(t)$.

19.2 Families of Rank $7, 8$

19.2.1 Probable Construction of Rank 7, 8 Families

We can modify the previous construction

$$\begin{aligned} y^2 &= x^3t^2 + 2g(x)t - h(x) \\ g(x) &= x^4 + ax^3 + bx^2 + cx + d, \ d \neq 0 \\ h(x) &= Ax^4 + Bx^3 + Cx^2 + Dx + E \end{aligned} \tag{19.6}$$

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 $8p$. As the coefficient of t^2 is x^3, we won't lose p from summing over non-roots of $D_t(x)$. By specializing to certain $t = a_2s^2 + a_1s + a_0$ 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 $A_{1,\mathcal{F}}(p)$ (because of the replacement $t \to a_2s^2 + a_1s + a_0$), so for this method to be applicable we would need another way to determine its rank over $\mathbb{Q}(s)$, even though we can construct eight points on it for all s.

$$\begin{aligned} D_t(x) &= x^8 + (2a + A)x^7 + (a^2 + 2b + B)x^6 + (2c + 2ab + C)x^5 \\ &\quad + (b^2 + 2ac + 2d + D)x^4 + (2bc + 2ad + E)x^3 \\ &\quad + (2bd + c^2)x^2 + (2cd)x + d^2 \\ &= \prod_{i=1}^{8}(x - \alpha^2\rho_i^2) \\ &= \sum_{k=0}^{8} x^k(-1)^k\alpha^{16-2k}R_k. \end{aligned} \tag{19.7}$$

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

$$\begin{aligned} d^2 &= \alpha^{16}R_0 \\ 2cd &= -\alpha^{14}R_1 \\ 2bd + c^2 &= \alpha^{12}R_2. \end{aligned} \tag{19.8}$$

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

$$\begin{aligned} d &= \alpha^8 r_0 \\ c &= -\frac{\alpha^6 R_1}{2r_0} \\ b &= \frac{\alpha^4 R_2}{2r_0} - \frac{\alpha^4 R_1^2}{8r_0^3}. \end{aligned} \tag{19.9}$$

Taking $\alpha = 2r_0$ yields d, b, c integral. If we take two of the roots to be the same, we should get a family of rank 7. If the one-parameter family is a rational surface, then by Rosen-Silverman we can unconditionally calculate the rank; if the defining polynomials have large degrees, our results are conditional on Tate's conjecture.

19.2.2 8 Rational Points on the Curves

We list the 8 points the previous construction forces on the curves. Consider a quadratic $\alpha t^2+\beta t+\gamma$, with discriminant $\beta^2 - 4\alpha\gamma = 0$. Then the two roots are equal, and we may factor the quadratic as $\alpha(t + \frac{\beta}{2\alpha})^2$. If α is a perfect square, we may rewrite as $\Big(\sqrt{\alpha} \cdot (t + \frac{\beta}{2\alpha})\Big)^2$.

For our family, we have the quadratic

$$\begin{aligned} q_x(t) &= \alpha(x)t^2 + \beta(x)t + \gamma(x) \\ &\quad \alpha(x) = x^3,\ \beta(x) = 2g(x),\ \gamma(x) = -h(x) \\ &\quad \text{discriminant} = 4\Big(g^2(x) - x^3h(x)\Big). \end{aligned} \tag{19.10}$$

We've chosen $g(x)$ and $h(x)$ such that the discriminant has 8 distinct perfect square roots, say $x_i = r_i^2$. For these eight roots, $\alpha(x)$ is a perfect square, and the discriminant of the quadratic in t is zero. Thus, we find 8 points on our curves:

$$P_i(t) = \left(r_i^2, \rho_i^3 \Big(t - \frac{2g(r_i)}{2r_i^3} \Big) \right). \tag{19.11}$$

We now change variables: $t \to a_2 s^2 + a_1 s + a_0$. This yields 8 points $P_i(s)$, and for appropriate choices of a_1, a_2 and a_3, for each s the curve will be isomorphic to an elliptic curve over $\mathbb{Q}$.

To determine a lower bound for the geometric rank of this family, we need only compute the determinant of the height matrix of the points $P_i(s)$ over $\mathbb{Q}(s)$. If we can find appropriate polynomials $g(x)$ and $h(x)$ such that there are eight perfect square roots of the discriminant and the eight points $P_i(s)$ are linearly independent, then we will have constructed an at least rank 8 family.

Part VI

Using the Modified 2-Level Density to Bound Excess Rank

20 Bounding Excess Rank

20.1 Preliminaries

For $n = 1$ and 2, consider the test functions

$$\begin{aligned}
\widehat{f_i}(u) &= \frac{1}{2}\Big(\frac{1}{2}\sigma_n - \frac{1}{2}|u|\Big),\ |u| \leq \sigma \\
f_i(x) &= \frac{\sin^2(2\pi\frac{1}{2}\sigma_n x)}{(2\pi x)^2}. \qquad (20.1)
\end{aligned}$$

If $n = 1$, $i = 1$; if $n = 2$, $i = 1$ or 2. These are the test function pairs used in the n-level densities. We expect $\sigma_2 = \frac{\sigma_1}{2}$; unfortunately, we are only able to prove σ_2 may be taken as large as $\frac{\sigma_1}{4}$.

Note $f_i(0) = \frac{\sigma_n^2}{4}$, $\widehat{f_i}(0) = f_i(0)\frac{1}{\sigma_n}$.

Lemma 20.1

$$-2\widehat{f_1 f_2}(0) = -\frac{4}{3\sigma_2}f_1(0)f_2(0). \qquad (20.2)$$

Proof:

$$\begin{aligned}
-2\widehat{f_1 f_2}(0) &= -2\int_{-\infty}^{\infty} f_1(u)f_2(u)du \\
&= -2\int_{-\infty}^{\infty} \widehat{f_1}(u)\widehat{f_2}(u)du \\
&= -2\int_{-\sigma_2}^{\sigma_2} \frac{1}{4^2}(\sigma_2 - |u|)^2 du \\
&= -4\frac{1}{4^2}\int_0^{\sigma_2}(\sigma_2 - u)^2 du \\
&= -4\frac{\sigma_2^3}{3\cdot 4^2} \\
&= -\frac{4}{3\sigma_2}f_1(0)f_2(0). \qquad (20.3)
\end{aligned}$$

Lemma 20.2

$$2\int_{-\infty}^{\infty}|u|\widehat{f_1}(u)\widehat{f_2}(u)du = \frac{1}{3}f_1(0)f_2(0). \qquad (20.4)$$

Proof:

$$\begin{aligned}
2\int_{-\infty}^{\infty}|u|\widehat{f}_1(u)\widehat{f}_2(u)du &= 2\cdot 2\int_0^{\sigma_2} u\frac{1}{4^2}(\sigma_2-u)^2du \\
&= 4\frac{1}{4^2}\int_0^{\sigma_2}(u\sigma_2^2-2u^2\sigma_2+u^3) \\
&= 4\frac{1}{4^2}\frac{\sigma_2^4}{12} \\
&= \frac{1}{3}f_1(0)f_2(0). \qquad (20.5)
\end{aligned}$$

We note the following fact:

Lemma 20.3

$$\prod_{i=1}^{2}\Big[\widehat{f}_i(0)+\frac{1}{2}f_i(0)\Big] \;=\; \Big(\frac{1}{\sigma_2^2}+\frac{1}{\sigma_2}+\frac{1}{4}\Big)f_1(0)f_2(0). \qquad (20.6)$$

In all arguments below, we assume the Birch and Swinnerton-Dyer conjecture so that we may interpret families of rank r over $\mathbb{Q}(t)$ as collections of curves whose L-functions have at least r zeros at the critical point. For simplicity, we consider generic families, ie, families where we expect equidistribution in sign. The arguments can easily be adapted to any family where the proportion of even to odd curves is known. All families considered are assumed to satisfy the conditions of the Rational Surfaces Density Theorem (Theorem 7.9); in particular, any rational surface is permissible below.

20.2 Bounds on Excess Rank from the 1-Level Density

For a family with rank r, $D_{1,\mathcal{F}}(f)=\widehat{f}(0)+\frac{1}{2}f(0)+rf(0)$.

For notational convenience, by even (odd) we mean a curve whose rank r_E satisfies r_E-r is even (odd); ie, even (odd) rank above the rank of the family.

Let P_0 be the probability that an even curve has rank at least $r+2a_0$, and P_1 the probability that an odd curve has rank at least $r+1+2b_0$.

Recall $D_{1,\mathcal{F}}(f)=\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\sum_{\gamma_E} f(\frac{\log N_E}{2\pi}\gamma_E)$, where γ_E is the imaginary part of the zeros. Note we could have used the modified 1-level density instead, and rescaled each curve's zeros by $\log M$, the average log-conductor. The proof would proceed similarly. Then

$$\begin{aligned}\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} r_E f(0) &\leq \widehat{f_1}(0) + \frac{1}{2}f_1(0) + rf_1(0)\\ \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} r_E &\leq \frac{1}{\sigma_1} + \frac{1}{2} + r. \end{aligned} \tag{20.7}$$

Thus the average rank is bounded by $r + \frac{1}{2}$ plus $\frac{1}{\sigma_1}$. Unfortunately, for many families, we only know the 1-level density for very small σ_1, which results in terrible bounds.

Assuming the Restricted Sign conjecture, half the time we have even functional equation, half odd. Of the even curves, $1 - P_0$ have rank less than or equal to $r + 2a_0 - 2$; we will get a lower bound by replacing these ranks with r. P_0 will have rank at least $r + 2a_0$; we replace these ranks with $r + 2a_0$.

Similarly for the odd curves we have $1 - P_1$ contributing $r + 1$ and P_1 contributing $r + 1 + 2b_0$. Thus

$$\begin{aligned}\frac{1}{\sigma_1} + \frac{1}{2} + r &\geq \frac{1}{2}\Big[(1-P_0)r + P_0(r+2a_0)\Big] + \frac{1}{2}\Big[(1-P_1)(r+1) + P_1(r+1+2b_0)\Big]\\ &= \frac{1}{2} + r + a_0P_0 + a_1P_1\\ \frac{1}{\sigma_1} &\geq a_0P_0 + b_0P_1. \end{aligned} \tag{20.8}$$

If we take $a_0 = b_0$, we get a bound for the probability of the rank being at least $r + 2a_0$, namely $\frac{1}{a_0\sigma_1}$. In general we obtain:

Theorem 20.4 (1-Level Density Bounds for Excess Rank)

$$\begin{aligned} P_0 &\leq \frac{1}{a_0\sigma_1}\\ P_1 &\leq \frac{1}{b_0\sigma_1} \end{aligned} \tag{20.9}$$

20.3 First Bound on Excess Rank from the 2-Level Density

We have the following expansion for the 2-level density:

$$D_{2,\mathcal{F}}(f) = D^*_{2,\mathcal{F}}(f) - 2D_{1,\mathcal{F}}(f_1f_2) + f_1(0)f_2(0)N(\mathcal{F},-1)$$

$$\begin{aligned} D^*_{2,\mathcal{F}}(f) &= \prod_{i=1}^{2}\Big[\widehat{f_i}(0)+\frac{1}{2}f_i(0)\Big]+2\int|u|\widehat{f_1}(u)\widehat{f_2}(u)du \\ &\quad +r\widehat{f_1}(0)f_2(0)+rf_1(0)\widehat{f_2}(0)+(r^2+r)f_1(0)f_2(0) \\ D(1,f) &= \widehat{f}(0)+\frac{1}{2}f(0)+rf(0). \end{aligned} \tag{20.10}$$

The difference between $D_{2,\mathcal{F}}(f)$ and $D^*_{2,\mathcal{F}}(f)$ is that $D_{2,\mathcal{F}}(f)$ involves sums over zeros with $j_1 \neq j_2$, and $D^*_{2,\mathcal{F}}(f)$ is over all zeros.

Our expansion for $D^*_{2,\mathcal{F}}(f)$ implies

$$\begin{aligned} \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} r_E^2 &\leq \frac{1}{\sigma_2^2}+\frac{1}{\sigma_2}+\frac{1}{4}+\frac{1}{3}+\frac{2r}{\sigma_2}+r^2+r \\ &= \frac{1}{\sigma_2^2}+\frac{2r+1}{\sigma_2}+\frac{1}{12}+r^2+r+\frac{1}{2}\equiv_{\text{def}} B_2^*(r). \end{aligned} \tag{20.11}$$

This gives a weak bound for the average of the squares of the ranks. By Silverman's Specialization Theorem, eventually all curves have rank at least r.

Again, call a curve of rank $r+2a_0$ 'even'. Similar to the 1-level investigations, let P_0 be the probability that an even curve has rank $r_E \geq r+2a_0$, and let P_1 be the probability that an odd curve has rank at least $r+1+2b_0$. Assuming the Restricted Sign conjecture we find

$$\begin{aligned} B_2^*(r) &\geq \frac{1}{2}\Big[(1-P_0)r^2+P_0(r+2a_0)^2\Big] \\ &\quad +\frac{1}{2}\Big[(1-P_1)(r+1)^2+P_1(r+1+2b_0)^2\Big] \\ &\geq \frac{r^2}{2}+\frac{1}{2}\Big[P_0(4a_0r+4a_0^2)\Big]+\frac{(r+1)^2}{2}+\frac{1}{2}\Big[P_1(4b_0(r+1)+4b_0^2)\Big] \\ &\geq r^2+r+\frac{1}{2}+2(a_0r+a_0^2)P_0+2(b_0(r+1)+b_0^2)P_1. \end{aligned} \tag{20.12}$$

Thus we find

Theorem 20.5 (First 2-Level Density Bounds for Excess Rank)

$$\begin{aligned} P_0 &\leq \frac{\frac{1}{2\sigma_2^2}+\frac{1}{24}+\frac{r+\frac{1}{2}}{\sigma_2}}{a_0(a_0+r)} \\ P_1 &\leq \frac{\frac{1}{2\sigma_2^2}+\frac{1}{24}+\frac{r+\frac{1}{2}}{\sigma_2}}{b_0(b_0+r+1)}. \end{aligned} \tag{20.13}$$

For $\sigma_2 = \frac{\sigma_1}{4}$ and $r = 0$ and $a_1 = 1$, we see this is *worse* than what we had in the 1-level density. However, for fixed $\sigma_2 = \frac{\sigma_1}{4}$ and r, as we increase a_0 we eventually do get a better bound. Quickly for large a_0 it falls off proportional to $\frac{1}{(a_0\sigma_1)^2}$, which is superior to the $\frac{1}{a_0\sigma_1}$ from the 1-level density.

20.4 Second Bound on Excess Rank from the 2-Level Density

Still assuming the Restricted Sign conjecture, we now use $D_{2,\mathcal{F}}(f)$ instead of $D^*_{2,\mathcal{F}}(f)$. For $j_1 \neq \pm j_2$, if the curve has r_E zeros, and r_E is even, we get a contribution of $r_E(r_E - 2)$, as each zero is matched with $r_E - 2$ others. If r_E is odd, there are $r_E - 1$ non-special zeros, each matched with $r_E - 2$ others. For the special zero, it is matched with $r_E - 1$ others. Thus the total contribution is $(r_E - 1)(r_E - 2) + (r_E - 1) = r_E(r_E - 2) + 1$.

Instead of $B_2^*(2)$ we have

$$\begin{aligned}
B_2(r) &= B_2^*(r) - \frac{1}{f_1(0)f_2(0)}\left(2D_{1,\mathcal{F}}(f_1f_2) - \frac{1}{2}f_1(0)f_2(0)\right) \\
&= B_2^*(r) - \frac{2\widehat{f_1f_2}(0) + (1+2r)f_1(0)f_2(0) - \frac{1}{2}f_1(0)f_2(0)}{f_1(0)f_2(0)} \\
&= B_2^*(r) - \frac{4}{3\sigma_2} - 1 - 2r + \frac{1}{2} \\
&= 2\Big(\frac{1}{2\sigma_2^2} + \frac{1}{24} + \frac{r}{\sigma_2} - \frac{1}{6\sigma_2}\Big) + r^2 - r. \qquad (20.14)
\end{aligned}$$

Therefore

$$B_2(r) \;\geq\; \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} r_E(r_E - 2) + \frac{1}{|\mathcal{F}|}\sum_{\substack{E\in\mathcal{F}\\ \epsilon_E\ odd}} 1. \qquad (20.15)$$

Assume r is even (r odd is handled similarly). Then an even curve of rank $r + 2a_0$ contributes $(r+2a_0)(r-2+2a_0)$. An odd curve of rank $r+1+2b_0$ contributes $(r+1+2b_0)(r+1-2+2b_0)+1$. Going through similar calculations as before, we find the contribution from the even curves is

$$\frac{r(r-2)}{2} \;+\; 2P_0 \cdot a_0(a_0 + r - 1) \qquad (20.16)$$

and the contribution from the odd curves (assuming half the curves are odd) is

$$\frac{(r+1)(r-1)}{2} \ + \ 2P_1 \cdot b_0(b_0+r) \ + \ \frac{1}{2}. \tag{20.17}$$

Substituting yields

Theorem 20.6 (Second 2-Level Density Bounds for Excess Rank)

$$\begin{aligned} P_0 &\leq \frac{\frac{1}{2\sigma_2^2} + \frac{1}{24} + \frac{r}{\sigma_2} - \frac{1}{6\sigma_2}}{a_0(a_0+r-1)} \\ P_1 &\leq \frac{\frac{1}{2\sigma_2^2} + \frac{1}{24} + \frac{r}{\sigma_2} - \frac{1}{6\sigma_2}}{b_0(b_0+r)}, \end{aligned} \tag{20.18}$$

where $a_0 \neq 1$ *if* $r = 0$.

A straightforward calculation shows, for $\sigma_2 = \frac{\sigma_1}{4}$ and $r = 0$, this is a better estimate once a_0 is greater than $\frac{\sigma_1^2+8\sigma_1+192}{24\sigma_1}$. If $r = 1$, it is a better estimate once a_0 is greater than $\frac{\sigma_1^2+80\sigma_1+192}{24\sigma_1}$. Again, we note decay proportional to $\frac{1}{(a_0\sigma_1)^2}$.

Note the numerator is never negative. The smallest it can be is when $r = 0$. Standard calculus gives the minimum of the numerator occurs at $\sigma_2 = 6$ and is $\frac{1}{18}$. (Write the numerator as $\frac{\sigma_2^2-4\sigma_2+12}{24\sigma_2}$ and note the two roots are complex).

20.5 Third Bound on Excess Rank from the 2-Level Density

Let E be a curve in a family of rank r over $\mathbb{Q}(t)$. Let z_E denote the number of extra zeros beyond the r family zeros at the critical point. Let $D_{1,E}(f)$ denote the 1-level density from the curve E. Then $D_{1,\mathcal{F}}(f) = \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} D_{1,E}(f)$.

We have $\sum_{j_1}\sum_{j_2} f_1(L\gamma_{E_{j_1}})f_2(L\gamma_{E_{j_2}})$. Let j_1 be one of the r family critical point zeros. Letting j_2 vary we get a contribution of $f_1(0)D_{1,E}(f_2)$ for each of the r family zeros. Interchanging j_1 and j_2 we get a contribution of $D_{1,E}(f_1)f_2(0)$ for each of the r family.

So far, the only double counting of zeros is when j_1 and j_2 are both a family zero. Thus we must subtract off $r^2 f_1(0)f_2(0)$.

We now consider the contributions from the other z_E zeros. We've already taken into account the contribution from j_1 one of the z_E zeros and j_2 one of the r family zeros (and vice-versa).

Thus, for a given curve, a lower bound of the contribution from all pairs (j_1, j_2) is

$$rf_1(0)D_{1,E}(f_2) + rD_{1,E}(f_1)f_2(0) - r^2 f_1(0)f_2(0) + z_E^2. \tag{20.19}$$

Summing over all $E \in \mathcal{F}$, the first two terms yield

$$\begin{aligned}
\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} rf_1(0)D_{1,E}(f_2) &= rf_1(0)\Big(\frac{1}{\sigma_2} + \frac{1}{2} + r\Big)f_2(0) \\
\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} rD_{1,E}(f_1)f_2(0) &= r\Big(\frac{1}{\sigma_2} + \frac{1}{2} + r\Big)f_1(0)f_2(0).
\end{aligned} \tag{20.20}$$

Combining the terms, we get

$$2r\Big(\frac{1}{\sigma_2} + \frac{1}{2} + r\Big) - r^2 + \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} z_E^2 \;\; \leq \;\; \frac{1}{\sigma_2^2} + \frac{2r+1}{\sigma_2} + \frac{1}{12} + \frac{1}{2} + r^2 + r = B_2^*(r) \tag{20.21}$$

Therefore

$$\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} z_E^2 \;\; \leq \;\; \frac{1}{\sigma_2^2} + \frac{1}{\sigma_2} + \frac{1}{12} + \frac{1}{2}. \tag{20.22}$$

Going through similar calculations, assuming the Restricted Sign conjecture, we find

Theorem 20.7 (Third 2-Level Density Bounds for Excess Rank)

$$\begin{aligned}
P_0 &\leq \frac{\frac{1}{2\sigma_2^2} + \frac{1}{24}}{a_0^2} + \frac{1}{2a_0}\frac{1}{a_0\sigma_2} \\
P_1 &\leq \frac{\frac{1}{2\sigma_2^2} + \frac{1}{24}}{b_0 + b_0^2} + \frac{1}{2(1+b_0)}\frac{1}{b_0\sigma_2}
\end{aligned} \tag{20.23}$$

Note, for $r = 0$, this is the same as our first attempt.

For $\sigma_2 = \frac{\sigma_1}{4}$, this is a better bound than the 1-level density once a_0 is greater than $\frac{\sigma_1^2+48\sigma_1+192}{24\sigma_1}$. It is a better bound than the first 2-level bound, if $r \neq 0$, once a_0 is greater than $\frac{\sigma_1^2+48\sigma_1+192}{96\sigma_1}$. If $r \geq 1$, it is a better bound than the second 2-level bound once a_0 is greater than $\frac{3(r-1)}{3r-2}\frac{\sigma_1^2+48\sigma_1+192}{96\sigma_1}$.

20.6 Summary

In all of the above, the bounds for excess rank decay like $\frac{1}{a_0^2}$ or $\frac{1}{b_0^2}$. For different values of r, σ_2, and a_0 and b_0, different approximations will yield better results. For fixed $r \geq 1$, the third attempt is the best as a_0 and b_0 tend to infinity.

Note this result is much weaker than what other authors (in particular, Heath-Brown and Brumer [BHB3]) have shown. They've proved there exist absolute constants, for the family of all elliptic curves, such that there the decay is bounded by $\beta \cdot a_0^{-\alpha a_0}$, $\beta \cdot b_0^{-\alpha b_0}$.

Our methods and results are almost assuredly better for specific choices of a_0 and b_0. Unfortunately, the supports of the test functions are too small for these bounds to yield useful information on the number of curves with rank slightly above the family rank (the case of interest in numerical investigations).

Part VII

Potential Lower Order Correction Terms to the Densities and Excess Rank

21 Potential Lower Order Terms in the 1-Level Densities

21.1 Introduction

In the Rational Surfaces Density Theorem (Theorem 7.9), we showed, for small support, rational elliptic surfaces of rank r over $\mathbb{Q}(t)$ have for their 1-level density

$$D_{1,\mathcal{F}}(f) \;=\; \widehat{f}(0) \;+\; \frac{1}{2}f(0) \;+\; rf(0). \tag{21.1}$$

Following Fermigier [Fe2], who studied many one-parameter families with $A_{\mathcal{E}}(p)$ constant, and Heath-Brown and Brumer, who studied the family of all elliptic curves, we look more closely at some families.

The 1-level density is

$$\begin{aligned} D_{1,\mathcal{F}}(f) \quad &= \quad \widehat{f}(0) + f(0) - 2\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\sum_{p}\frac{\log p}{\log N_E}\frac{1}{p}\widehat{f}\Big(\frac{\log p}{\log N_E}\Big)a_t(p) \\ &\qquad -2\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\sum_{p}\frac{\log p}{\log N_E}\frac{1}{p^2}\widehat{f}\Big(2\frac{\log p}{\log N_E}\Big)a_t(p)^2, \end{aligned} \tag{21.2}$$

Following Rosen and Silverman (Theorem 1.2) the sums of $a_t(p)$ contribute $rf(0)$. Michel proved for non-constant $j(t)$ that

$$A_{2,\mathcal{F}}(p) = \sum_{t(p)} a_t(p)^2 = p^2 + O(p^{\frac{3}{2}}). \tag{21.3}$$

The main term of $A_{2,\mathcal{F}}(p)$ will contribute in the limit, while the error term will not.

In the families we study below, the first sum (Equation 21.2) always contributes $rf(0)$. The main term from the second sum contributes $-\frac{1}{2}f(0)$. As we are only investigating the 1- and not the 2-level density, if instead of scaling each curve's zeros by the logarithm of its conductor we instead used the average of the logarithms of the conductors, we can ignore all conductor arguments. To simplify the discussion below, we use the average log-conductor.

For a great many families, we can do better than Michel's $O(p^{\frac{3}{2}})$ bound for the error term. Many families (including the family of all elliptic curves) investigated have a correction of size $-m_{\mathcal{F}}p + O(1)$, where $m_{\mathcal{F}} > 0$. As there is a negative sign in the second sum, this results in a positive contribution to the 1-level density, of size $\frac{1}{\log N}$. In the limit this will of course be drowned out; however, for small N it will be present.

For many families with constant $A_{\mathcal{E}}(p)$ and rank r, Fermigier [Fe2] observed that approximately 32% had rank r, 18% rank $r+2$, and 48% rank $r+1$, 2% rank $r+3$. The Excess Rank question is: will the 18% persist for large values of N? Using Fermigier's numbers, we expect the average rank to be about $r + \frac{1}{2} + .40$.

The correction term we observe from sums of $a_t^2(p)$ leads to deriving (when we look at small values of N) a higher bound for the average rank.

21.2 Contributions from Sub-Families

A strong possible explanation for the observed excess rank is the presence of sub-families of higher rank. These families' contributions will be dwarfed in the limit, but noticeable for small N.

Consider an elliptic curve $E : y^2 = x^3 + ax + b$ over $\mathbb{Q}$ and its family of twists $E_d : dy^2 = x^3+ax+b$ by square-free d. Assuming the Restricted Sign conjecture for twists, Gouvéa and Mazur [GM] prove that there exist positive constants $C_0(\epsilon, E)$ and $C_1(\epsilon, E)$ such that, if $N \geq C_0(\epsilon, E)$, the number of square-free $d \leq N$ with the rank of E_d even and at least 2 is at least $C_1(\epsilon, E)N^{\frac{1}{2}-\epsilon}$.

Similarly, Mai [Mai] considered $E_d : x^3 + y^3 = d$ for cube-free d. Assuming the Restricted Sign conjecture for cubic twists, he proved there exist positive constants $C_2(\epsilon, E)$ and $C_3(\epsilon, E)$ such that, if $N \geq C_2(\epsilon, E)$, the number of cube-free $|d| \leq N$ with the rank of E_d even and at least 2 is at least $C_3(\epsilon, E)N^{\frac{2}{3}-\epsilon}$.

Stewart and Top [ST] generalize these results and remove the dependence on the Restricted Sign conjecture, though at the cost of weaker bounds. They prove:

Theorem 21.1 (Cubic Twists) *For the family $x^3 + y^3 = d$, there exists a universal constant C_4 such that, for cube-free $|d| \leq N$, if $N \geq 657$, at least $C_4 N^{\frac{1}{6}}$ curves have rank at least* 3.

Theorem 21.2 (Quadratic Twists) *Let E be an elliptic curve over $\mathbb{Q}$ with $j(E) \neq 0, 1728$, and let E_d be a quadratic twist. There exist constants $C_5(E)$ and $C_6(E)$ such that, for square-free $|d| \leq N$, if $N \geq C_5(E)$, then at least $C_6(E)N^{\frac{1}{7}} \cdot \log^{-2} N$ have rank even and at least* 2.

In all of the above results, there is very slow decay with respect to N. The cardinality in these families is a multiple of N. Thus, we have contributions ranging from $N^{\frac{1}{7}}/N$ to $N^{\frac{1}{2}}/N$ to $N^{\frac{2}{3}}/N$. Taking $N = 100$, 1000 and 10000 yields

N	$N^{-\frac{6}{7}}$	$N^{-\frac{1}{2}}$	$N^{-\frac{2}{3}}$
100	.0193	.1000	.2154
1000	.0027	.0316	.1000
10000	.0004	.0100	.0464

In Fermigier's [Fe2] investigations, N ranges from 250 to 1000. Thus, it is very likely, depending on the size of the constants (and the true values of the exponents) that there may be higher rank sub-families of cardinality N^c lurking within our families, $0 < c < 1$. While not contributing in the limit, they will be very noticeable for small values of N.

To determine the analytic rank (the order of vanishing of $L(s, E)$ at the critical point $s = 1$) requires studying sums of the coefficients $a_E(n)$ for $n \leq \sqrt{N_E} \log N_E$. See, for example, [Cr]. As the conductors grow polynomially in our families, it already requires several hours to investigate families for t up to 1000. It thus seems unlikely that we will be able to attain large enough ranges of t to get past the contributions of these possibly lower cardinality sub-families.

21.3 Caveats to Determining Lower Order Corrections

The potential lower order corrections, arising from lower order terms in the sums of the second moments of $a_E^2(p)$, could be masked by the errors propagating through our derivations. We have errors of the size $\frac{1}{\log N}$ and $\frac{\log \log N}{\log N}$ arising from the Explicit Formula. To truly observe lower order corrections to the densities, a significantly more delicate analysis is needed in the Explicit Formula.

The conductor dependence in the Gamma factors of the Explicit Formula is easily managed. The real difficulty is handling the primes which divide the discriminant and the sums of $a_E^m(p)$, $m \geq 3$.

We save a full analysis for a future project, and content ourselves with observing a potential lower order density term. While we only discuss potential contributions to the 1-level density, the same terms will propagate and contribute to the 2-level density.

21.4 Corrections to $A_{2,\mathcal{F}}(p)$

Family:$y^2 =$	$A_{1,\mathcal{F}}(p)$	$A_{2,\mathcal{F}}(p)$
All Curves	0	$p^3 - p^2$
$x^3 + 2^4(-3)^3(9t+1)^2$	0	$\begin{cases} 2p^2-2p & p\equiv 2(3) \\ 0 & p\equiv 1(3) \end{cases}$
$x^3 \pm 4(4t+2)x$	0	$\begin{cases} 2p^2-2p & p\equiv 1(4) \\ 0 & p\equiv 3(3) \end{cases}$
$x^3 + (t+1)x^2 + tx$	0	$p^2 - 2p - 1$
$x^3 + x^2 + 2t + 1$	0	$p^2 - 2p - \left(\frac{-3}{p}\right)$
$x^3 + tx^2 + 1$	$-p$	$p^2 - ph_{3,p}(2) - 1 + c_{3/2}(p)$
$x^3 - t^2x + t^2$	$-2p$	$p^2 - p - c_1(p) - c_0(p)$
$x^3 - t^2x + t^4$	$-2p$	$p^2 - p - c_1(p) - c_0(p)$

where

$$\begin{aligned} c_{3/2}(p) &= p\sum_{x(p)}\left(\frac{4x^3+1}{p}\right) \\ c_1(p) &= \left[\sum_{x(p)}\left(\frac{x^3-x}{p}\right)\right]^2 \\ c_0(p) &= \left(\frac{-3}{p}\right) + \left(\frac{3}{p}\right), \end{aligned} \tag{21.4}$$

and $h_{3,p}(2)$ is the number of cube roots of 2 modulo p.

21.5 Potential Lower Order Correction from $A_{2,\mathcal{F}}(p)$

We analyze the contribution to the modified 1-level density from the first order correction to $A_{2,\mathcal{F}}(p)$. Consider a correction term of $-m_{\mathcal{F}}p$, $m_{\mathcal{F}} > 0$. We sum from $t = N$ to $2N$, which means we have $\frac{N}{p}$ full sums and one partial sum (which will be an even lower order contribution).

Substituting into the 1-level density yields

$$\begin{aligned} C_2 &= \frac{2}{N}\sum_p \frac{\log p}{\log M}\widehat{f}\Big(2\frac{\log p}{\log M}\Big)\frac{1}{p^2}\frac{N}{p}m_{\mathcal{F}}p \\ &= \frac{2m_{\mathcal{F}}}{\log M}\sum_p \widehat{f}\Big(2\frac{\log p}{\log M}\Big)\frac{\log p}{p^2}. \end{aligned} \tag{21.5}$$

Thus there is a contribution of size $\frac{1}{\log N}$.

Consider the pair of functions

$$\begin{aligned} \widehat{f}(u) &= \frac{1}{2}\left(\frac{1}{2}\sigma - \frac{1}{2}|u|\right),\ |u| \leq \sigma \\ f(x) &= \frac{\sin^2(2\pi\frac{1}{2}\sigma x)}{(2\pi x)^2}. \end{aligned} \tag{21.6}$$

Note $f(0) = \frac{\sigma^2}{4}$, $\widehat{f}(0) = f(0)\frac{1}{\sigma}$; thus $\sigma = \frac{4f(0)}{\sigma}$.

Then $\widehat{f}\Big(2\frac{\log p}{\log M}\Big) = \frac{\sigma}{4} - \frac{1}{2}\frac{\log p}{\log M}$ for $p \leq M^{\frac{\sigma}{2}}$. The first term contributes

$$\begin{aligned} C_{2,1} &= \frac{2m_{\mathcal{F}}}{\log M}\sum_p^{M^{\frac{\sigma}{2}}} \frac{\sigma}{4}\frac{\log p}{p^2} \\ &= \frac{m_{\mathcal{F}}\sigma}{2\log M}\sum_p^{M^{\frac{\sigma}{2}}} \frac{\log p}{p^2} \\ &\approx \frac{m_{\mathcal{F}}\sigma}{2\log M}\cdot .493, \end{aligned} \tag{21.7}$$

where the last result follows from numerical evaluation: the sum of the first 30,000 primes gives .493088. Therefore the first term contributes

$$C_{2,1} \approx \frac{m_{\mathcal{F}}}{2\log M}\frac{4f(0)}{\sigma}\cdot .493$$

$$\approx \quad \frac{.986 m_{\mathcal{F}}}{\sigma} \frac{1}{\log M} f(0) \tag{21.8}$$

The second term contributes

$$\begin{aligned} C_{2,2} &= -\frac{m_{\mathcal{F}}}{\log^2 M} \sum_{p}^{M^{\frac{\sigma}{2}}} \frac{\log^2 p}{p^2} \\ &\approx -\frac{m_{\mathcal{F}}}{\log^2 M} \cdot .742 \\ &= -\frac{.742 m_{\mathcal{F}}}{\log^2 M} \frac{4}{\sigma^2} f(0) \end{aligned} \tag{21.9}$$

where the last result follows from numerical integration: the sum of the first 30,000 primes gives .741559. Thus $C_{2,2}$ contributes $-\frac{2.966 m_{\mathcal{F}}}{\sigma^2 \log^2 M}$ and we have

$$\begin{aligned} C_2 &= C_{2,1} + C_{2,2} \\ &\approx \left(\frac{.986}{\sigma} - \frac{2.966}{\sigma^2 \log M} \right) \frac{m_{\mathcal{F}}}{\log M} f(0). \end{aligned} \tag{21.10}$$

We've kept the factor $f(0)$ for ease in bounding the average rank. The Explicit Formula relates a sum over zeros to a sum over primes. As our test function f is positive, keeping just the sum over the zeros at the critical point gives an upper bound for the average rank. For each curve, we get $r_E f(0)$, where r_E is the order of vanishing at the critical point.

For these test functions, and recalling that $\widehat{f}(0) = \frac{f(0)}{\sigma}$, we get

$$\begin{aligned} \frac{1}{|\mathcal{F}|} \sum_{E \in \mathcal{F}} r_E f(0) &\leq \frac{f(0)}{\sigma} + (r + \frac{1}{2}) f(0) + \left(\frac{.986}{\sigma} - \frac{2.966}{\sigma^2 \log M} \right) \frac{m_{\mathcal{F}}}{\log M} f(0) \\ \text{Ave Rank} &\leq \frac{1}{\sigma} + r + \frac{1}{2} + \left(\frac{.986}{\sigma} - \frac{2.966}{\sigma^2 \log M} \right) \frac{m_{\mathcal{F}}}{\log M}. \end{aligned} \tag{21.11}$$

For example, for the family of all elliptic curves, Heath-Brown and Brumer proved we may take $\sigma = \frac{4}{7}$. Ignoring the correction term, this leads to a bound for the average rank of 2.25. For the family of all elliptic curves ($m_{\mathcal{F}} = 1$), we can handle conductors of size 10^{12}. This would lead to increasing the bound by .05. In the limit

More generally, for $m_{\mathcal{F}} = 1$ we list below how the additional term depends on σ and M. As the contribution is linear in $m_{\mathcal{F}}$, it is easy to rescale as needed.

Extra Contributions: $m_{\mathcal{F}} = 1$

M	$\sigma = \frac{4}{7}$	$\sigma = 1$	$\sigma = 2$
10^6	.077	.056	.032
10^{12}	.051	.032	.017
10^{18}	.036	.022	.011
10^{24}	.025	.015	.007

Note: We might expect the above 1-level density to hold for all σ, and not merely $\sigma < \frac{4}{7}$. In this case, the lower order terms from the second moment, the sums of $a_E^2(p)$, will *not* contribute to the bound for the average rank, as their contribution vanishes as $\sigma \to \infty$. They will, however, contribute a lower order term to the 1-level density. Also, $M \approx N^m$, where m is the degree of the conductor. If M is small, we have included too many primes in the summations (the above are the limiting values), and the formulas must be modified accordingly.

Let us examine the boost this correction term will give to the upper bound for the average rank. As remarked, if our 1-level density were true for all σ, and not just $\sigma < \sigma_0$, there would be no contribution from the correction term to the second sum, nor would the $\frac{1}{\sigma}$ term contribute, and we would obtain the average rank is bounded by $r + \frac{1}{2}$.

Let us assume we knew the 1-level density up to $\sigma = 1$. The $\frac{1}{\sigma}$ term contributes 1, the lower correction contributes .03 for conductors of size 10^{12}, and we get (for $m_{\mathcal{F}} = 1$) the average rank is bounded by $1 + r + \frac{1}{2} + .03 = r + \frac{1}{2} + 1.03$. This is significantly higher than Fermigier's observed $r + \frac{1}{2} + .40$.

If we were able to prove our 1-level density for $\sigma = 2$, then the $\frac{1}{\sigma}$ term will contribute $\frac{1}{2}$, and the lower order correction will contribute .02 for conductors of size 10^{12}. Thus, the average rank will be bounded by $\frac{1}{2} + r + \frac{1}{2} + .02 = r + \frac{1}{2} + .52$. While the main error contribution is from the $\frac{1}{\sigma}$, there is still a noticeable effect from the correction term to $A_{2,\mathcal{F}}(p)$. Moreover, we are now in the ballpark of Fermigier's bound; of course, we were already there without the potential correction term.

It seems hopeless to think about obtaining a 1-level density for any family of elliptic curves with support greater than 2. Iwawniec, Luo and Sarnak obtain such large support for some of their families, but only because of great averaging formulas over the family. We have no analogue that works as well as the Petersson Formula, and our conductors grow very quickly for these geometric families of elliptic curves.

Thus, from the analytic side, it seems very unlikely that we shall be able to disprove the results of Fermigier. We can, however, see that *assuming this formula for the* 1*-level density*, Fermigier's observed bounds are reasonable, even under the assumption of immensely larger support. There is a slight bump due to low values of t, due to the $\frac{1}{\log M}$ factor in the correction term. This will wash out in the limit, but will be present for small t. It is, of course, dwarfed by the presence of the $\frac{1}{\sigma}$ term.

21.6 Family of All Elliptic Curves

For simplicity, consider the modified 1-level density (rescale by the average log-conductor) for the family of all elliptic curves (no sieving). We sketch how to handle the contributions from the $m \geq 3$ terms (ie, the terms incorporated into the error in the Explicit Formulas).

From the Modified Explicit Formula (Theorem A.31), we must evaluate the higher order terms, namely, sums of $\alpha_E^m(p) + \beta_E^m(p)$ for $m \geq 3$.

For $p \nmid N_E$, $\alpha_E(p) + \beta_E(p) = a_E(p)$ and $\alpha_E(p)\beta_E(p) = p$. By Lemma 8.4, complete sums of $a_E^m(p)$ vanish for m odd, ie

$$\sum_{a=0}^{p-1}\sum_{b=0}^{p-1} a_{a,b}^{2m+1}(p) \;=\; 0. \tag{21.12}$$

For $p \nmid N_E$,

$$\begin{aligned}
\alpha_E^3(p) + \beta_E^3(p) &= a_E^3(p) - 3pa_E(p)\\
\alpha_E^4(p) + \beta_E^4(p) &= a_E^4(p) - 4pa_E^2(p) + 2p^2\\
\alpha_E^5(p) + \beta_E^5(p) &= a_E^5(p) - 5p(\alpha_E^3(p) - \beta_E^3(p)) + 10p^2 a_E(p)\\
\alpha_E^6(p) + \beta_E^6(p) &= a_E^6(p) - 6pa_E^4(p) + 9p^2 a_E^2(p) - 2p^3\\
\alpha_E^7(p) + \beta_E^7(p) &= a_E^7(p) - 7p(\alpha_E^5(p) + \beta_E^5(p)) - 21p^2(\alpha_E^3(p) + \beta_E^3(p)) - 35p^3 a_E(p)\\
\alpha_E^8(p) + \beta_E^8(p) &= a_E^8(p) - 8pa_E^6(p) + 20p^2 a_E^4(p) - 16p^3 a_E^2(p) + 2p^4.
\end{aligned} \tag{21.13}$$

By induction (using Lemma 8.4), it is easy to show that the complete sums of the odd powers vanish. We are left with evaluating complete sums of $a_{a,b}^{2m}(p)$.

Assuming these complete sums are polynomials of degree $m+2$ in p ($\alpha_E^{2m}(p)$ and $\beta_E^{2m}(p)$ are of size p^m; summing over a and b mod p gives an expected size of p^{m+2}), by explicitly calculating the values for a few primes we can read off the coefficients. Some care is required, as we are reading the coefficients mod p, p^2, etc; ie, to obtain the constant term, we look at the complete sum mod p; to obtain the p-term, we look at the complete sum mod p^2, and so on. We numerically find (see also [Bi])

$$\begin{aligned}
\sum_{a=0}^{p-1}\sum_{b=0}^{p-1} a_{a,b}^4(p) &= 3p - 3p^2 - 2p^3 + 2p^4 \\
\sum_{a=0}^{p-1}\sum_{b=0}^{p-1} a_{a,b}^6(p) &= 5p + 4p^2 - 9p^3 - 5p^4 + 5p^5 \\
\sum_{a=0}^{p-1}\sum_{b=0}^{p-1} a_{a,b}^8(p) &= 7p + 13p^2 + 8p^3 - 28p^4 - 14p^5 + 14p^6. \qquad (21.14)
\end{aligned}$$

By Hasse, $\alpha_E^{2m}(p) + \beta_E^{2m}(p) \le 2p^m$, thus its complete sum is of size p^{m+2}.

In general, we have $\frac{1}{N^5}\frac{N^2}{p}\frac{N^3}{p}$ complete sums, and we multiply each complete sum by $\frac{1}{p^{2m}}$ (and other factors) and then sum over the primes.

The main contribution to the potential lower order density correction is from $m = 1$, where the complete sum of $a_E^2(p)$ gives $p^3 - p^2$, with the p^2 term leading to a sum of $\frac{1}{p^2}$.

When $m = 2$, we get another potential term of size $\frac{1}{p^2}$, as $\frac{1}{p^{2\cdot 2}}$ exactly balances p^{2+2}. Note, however, that the test function will be evaluated at $\frac{3\log p}{\log M}$ and not $\frac{2\log p}{\log M}$. The complete sum of the $m = 2$ term is

$$2p^3 - 3p^2 + 3p, \qquad (21.15)$$

the p^4 terms (which yield the main term) exactly cancel each other out. Thus, the $m = 2$ term will contribute a sum of size $\frac{1}{p^3}$ and not of size $\frac{1}{p^2}$.

For $m \ge 3$, the contributions will be of size $\frac{1}{p^3}$ or less.

Hence, subject to proving the expansion formulas, for the family of all elliptic curves (no sieving, rescaling by the average log-conductor), the $m \ge 1$ terms contribute a potential lower order correction, where we sum over the primes terms of size $\frac{1}{p^2}$.

Part VIII

3 and Higher Level Densities

22 3 and Higher Level Densities

22.1 3-Level Density

We analyze the combinatorics needed to determine the 3-level density. $D_{3,\mathcal{F}}(f)$ is defined as a sum over distinct indices; there will be complications due to mixing curves with even and odd functional equations.

22.1.1 Combinatorics

Write L_E for $\frac{\log N_E}{2\pi}$. We define

$$\begin{aligned} D_{3,\mathcal{F}}(f) &= \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\sum_{\substack{j_1,j_2,j_3\\ j_i\neq\pm j_k}} f_1(L_E\gamma_E^{(j_1)})f_2(L_E\gamma_E^{(j_2)})f_3(L_E\gamma_E^{(j_3)}) \\ D^*_{3,\mathcal{F}}(f) &= \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\sum_{j_1}\sum_{j_2}\sum_{j_3} f_1(L_E\gamma_E^{(j_1)})f_2(L_E\gamma_E^{(j_2)})f_3(L_E\gamma_E^{(j_3)}). \end{aligned} \tag{22.1}$$

We want to sum over distinct indices. For non-distinct triples, there are four possibilities. Either all indices are the same, or two are the same and one differs. However, in addition to summing over distinct indices, we want to exclude the case $j_i = -j_k$, and here we have complications due to the sign of the functional equation. For notational convenience, write z_i for $L_E\gamma_E^{(j_i)}$

22.1.2 Even Functional Equation

Assume the curve has even functional equation. Then we can label the zeros with indices $j_i = \pm1, \pm2, \dots$. There are four cases.

Case One: Assume $j_1 = \pm j_2 = \pm j_3$. Hence we must throw out $2\cdot 2\sum_{j_1} f_1f_2f_3(z_1)$.

Case Two: Assume $j_1 = \pm j_2 \neq \pm j_3$. We discard $2\sum_{\substack{j_1,j_3\\ j_1\neq\pm j_3}} f_1f_2(z_1)f_3(z_3)$. This equals $2\sum_{j_1}\sum_{j_3} f_1f_2(z_1)f_3(z_3) - 4\sum_{j_1} f_1f_2f_3(z_1)$.(For each value of j_1, there are two values of j_3 which work).

Case Three: Assume $j_1 = \pm j_3 \neq \pm j_2$. Identical reasoning leads us to discard

$2\sum_{j_1}\sum_{j_2} f_1f_3(z_1)f_2(z_2) - 4\sum_{j_1} f_1f_2f_3(z_1)$.

Case Four: Assume $j_1 \neq \pm j_2 = \pm j_3$. Identical reasoning leads us to discard

$2\sum_{j_1}\sum_{j_2} f_1(z_1)f_2f_3(z_2) - 4\sum_{j_1} f_1f_2f_3(z_1)$.

Collecting all the pieces yields, for a function with even functional equation, that we must discard

$$
\begin{aligned}
D^{\#}_{3,\mathcal{F},even}(f) &= \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\Bigg[2\sum_{j_1}\sum_{j_3} f_1f_2(z_1)f_3(z_3) + 2\sum_{j_1}\sum_{j_2} f_1f_3(z_1)f_2(z_2) \\
&\qquad +2\sum_{j_1}\sum_{j_2} f_1(z_1)f_2f_3(z_2) - 8\sum_{j_1} f_1f_2f_3(z_1)\Bigg]. \qquad (22.2)
\end{aligned}
$$

Define $D^{*}_{2,\mathcal{F},even}(f,g)$ to be the 2-level density sum (over all indices) restricted to even curves, with test functions f and g. We have shown

Lemma 22.1 (Even Functional Equation: Excess Contribution)

$$
\begin{aligned}
D^{\#}_{3,\mathcal{F},even}(f) &= 2\Big(D^{*}_{3,\mathcal{F},even}(f_1f_2,f_3) + D^{*}_{3,\mathcal{F},even}(f_1f_3,f_2) + D^{*}_{3,\mathcal{F},even}(f_1,f_2f_3)\Big) \\
&\quad -8\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\frac{1+\epsilon_E}{2}\sum_{j_1} f_1f_2f_3(z_j). \qquad (22.3)
\end{aligned}
$$

22.1.3 Odd Functional Equation

Assume the curve has odd functional equation. We label the zeros with indices $j_i = 0, \pm1, \pm2, \dots$. There are four cases; however, we must be careful about whether or not an index is zero.

Assume $j_1 = \pm j_2 \neq \pm j_3$; call this sum $S(12;3)$. If there were no zero at the critical point, this would be $2\sum_{\substack{j_1,j_3\\ j_1\neq\pm j_3}} f_1f_2(z_1)f_3(z_3)$, because for each j_1 there are two j_2's. This double counts $j_1 = j_2 = 0$. To remedy this, we must subtract off $j_1 = j_2 = 0$, hence we are left with $2\sum_{\substack{j_1,j_3\\ j_1\neq\pm j_3}} f_1f_2(z_1)f_3(z_3)$ $-f_1f_2(0)\sum_{j_3\neq0} f_3(z_3)$. We fix the last sum by adding back $j_3 = 0$ and then subtracting, yielding $S(12;3) = 2\sum_{\substack{j_1,j_3\\ j_1\neq\pm j_3}} f_1f_2(z_1)f_3(z_3)$ $-f_1f_2(0)\sum_{j_3} f_3(z_3)$ $+f_1f_2f_3(0)$. We now correct the first sum by removing the condition $j_1 \neq \pm j_3$. We add back $j_3 = \pm j_1$ and then subtract.

Consider $\sum_{\substack{j_1,j_3\\ j_1\neq\pm j_3}}$ If $j_1 \neq 0$, we add back $j_3 = \pm j_1$ and then subtract this off, getting $\sum_{j_1\neq0} f_1f_2(z_1)\sum_{j_3} f_3(z_3) - 2\sum_{j_1\neq0} f_1f_2f_3(z_1)$.

If $j_1 = 0$, we add back $j_3 = 0$ and subtract $j_3 = 0$, yielding $\sum_{j_1=0} f_1f_2(z_1)\cdot \sum_{j_3} f_3(z_3) -$ $\sum_{j_1=0} f_1f_2f_3(z_1)$, which is the same as

$$
\sum_{j_1=0} f_1f_2(z_1)\sum_{j_3} f_3(z_3) - 2\sum_{j_1=0} f_1f_2f_3(z_1) + f_1f_2f_3(0). \qquad (22.4)
$$

Combining the above gives

$$\sum_{\substack{j_1,j_3\\ j_1\neq\pm j_3}} f_1f_2(z_1)f_3(z_3) \quad = \quad \sum_{j_1} f_1f_2(z_1)\sum_{j_3} f_3(z_3) - 2\sum_{j_1} f_1f_2f_3(z_1) + f_1f_2f_3(0). \qquad (22.5)$$

We have shown

$$\begin{aligned} S(12;3) \quad &= \quad 2\sum_{j_1} f_1f_2(z_1)\sum_{j_3} f_3(z_3) - 4\sum_{j_1} f_1f_2f_3(z_1) + 2f_1f_2f_3(0) \\ &\quad -f_1f_2(0)\sum_{j_3} f_3(z_3) + f_1f_2f_3(0). \qquad (22.6) \end{aligned}$$

Similarly we can determine the sums $S(13;2), S(23;1)$. Therefore

Lemma 22.2 (Odd Functional Equation, exactly two indices are equal)

$$\begin{aligned} S(\#\#;*) \quad &= \quad S(12;3) + S(13;2) + S(23;1) \\ &= \quad 2\sum_{j_1} f_1f_2(z_1)\sum_{j_3} f_3(z_3) + 2\sum_{j_1} f_1f_3(z_1)\sum_{j_2} f_2(z_2) \\ &\quad +2\sum_{j_1} f_1(z_1)\sum_{j_2} f_2f_3(z_2) \\ &\quad -f_1f_2(0)\sum_{j_3} f_3(z_3) - f_1f_3(0)\sum_{j_2} f_2(z_2) - f_2f_3(0)\sum_{j_1} f_1(z_1) \\ &\quad -12\sum_{j_1} f_1f_2f_3(z_1) + 9f_1f_2f_3(0). \qquad (22.7) \end{aligned}$$

We now handle the case $j_1 = \pm j_2 = \pm j_3$. There are two cases. Assume first that $j_1 \neq 0$. Then this is just $4\sum_{j_1\neq 0} f_1f_2f_3(z_1)$. Assume now that $j_1 = 0$. Then we have $\sum_{j_1=0} f_1f_2f_3(z_1)$. Hence the sum over $j_1 = \pm j_2 = \pm j_3$ is $4\sum_{j_1} f_1f_2f_3(z_1) - 3f_1f_2f_3(0)$. Combining with $S(\#\#;*)$ yields

Lemma 22.3 (Odd Functional Equation: Excess Contribution)

$$\begin{aligned} D^{\#}_{3,\mathcal{F},odd}(f) \quad &= \quad 2\Big(D^*_{2,\mathcal{F},odd}(f_1f_2,f_3) + D^*_{2,\mathcal{F},odd}(f_1f_3,f_2) + D^*_{2,\mathcal{F},odd}(2;f_1,f_2f_3)\Big) \\ &\quad +\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\frac{1-\epsilon_E}{2}\Bigg[-f_1f_2(0)\sum_{j_3} f_3(z_3) - f_1f_3(0)\sum_{j_2} f_2(z_2) - \\ &\quad f_2f_3(0)\sum_{j_1} f_1(z_1) - 8\sum_{j_1} f_1f_2f_3(z_1) + 6f_1f_2f_3(0)\Bigg] \qquad (22.8) \end{aligned}$$

22.1.4 Combinatorial Contributions to $D^*(3)$

We use $D^*_{2,\mathcal{F},even}(f,g) + D^*_{2,\mathcal{F},odd}(f,g) = D^*_{2,\mathcal{F}}(f,g)$. Let ϵ_E be the sign of the functional equation of E. Adding the contributions from the even and odd cases and summing over all curves yields

$$\begin{aligned}
D_{3,\mathcal{F}}(f) &= D^*_{3,\mathcal{F}}(f) - \Big(D^{\#}_{3,\mathcal{F},even}(f) + D^{\#}_{3,\mathcal{F},odd}(f)\Big) \\
&= D^{\#}_{3,\mathcal{F}}(f) - D^{\#}_{3,\mathcal{F},comb}(f) \\
D^{\#}_{3,\mathcal{F},comb}(f) &= 2\Big(D^*_{2,\mathcal{F}}(f_1f_2,f_3) + D^*_{2,\mathcal{F}}(f_1f_3,f_2) + D^*_{2,\mathcal{F}}(f_1,f_2f_3)\Big) \\
&\quad -8\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\frac{1+\epsilon_E}{2}\sum_{j_1} f_1f_2f_3(z_j) + \\
&\quad \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\frac{1-\epsilon_E}{2}\Bigg[-f_1f_2(0)\sum_{j_3} f_3(z_3) - f_1f_3(0)\sum_{j_2} f_2(z_2) \\
&\quad -f_2f_3(0)\sum_{j_1} f_1(z_1) - 8\sum_{j_1} f_1f_2f_3(z_1) + 6f_1f_2f_3(0)\Bigg] \\
&= 2\Big(D^*_{2,\mathcal{F}}(f_1f_2,f_3) + D^*_{2,\mathcal{F}}(f_1f_3,f_2) + D^*_{2,\mathcal{F}}(f_1,f_2f_3)\Big) \\
&\quad -8\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\sum_{j_1} f_1f_2f_3(z_1) \\
&\quad +\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\frac{1-\epsilon_E}{2}\Bigg[-f_1f_2(0)\sum_{j_3} f_3(z_3) \\
&\quad -f_1f_3(0)\sum_{j_2} f_2(z_2) - f_2f_3(0)\sum_{j_1} f_1(z_1) + 6f_1f_2f_3(0)\Bigg]. \qquad (22.9)
\end{aligned}$$

As $\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\sum_{j_1} f_1f_2f_3(z_1) = D_{1,\mathcal{F}}(f_1f_2f_3)(0)$ for small support, we get

Lemma 22.4

$$\begin{aligned}
D^{\#}_{3,\mathcal{F},comb}(f) &= 2\Big(D^*_{2,\mathcal{F}}(f_1f_2,f_3) + D^*_{2,\mathcal{F}}(f_1f_3,f_2) + D^*_{2,\mathcal{F}}(f_1,f_2f_3)\Big) \\
&\quad -8D_{1,\mathcal{F}}(f_1f_2f_3)(0) + \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\frac{1-\epsilon_E}{2}\Bigg[6f_1f_2f_3(0) + f_1f_2(0)\sum_{j_3} f_3(z_3) \\
&\quad +f_1f_3(0)\sum_{j_2} f_2(z_2) + f_2f_3(0)\sum_{j_1} f_1(z_1)\Bigg]. \qquad (22.10)
\end{aligned}$$

This is very different than the 2-level case. There, it was sufficient to know the percentage of curves of even and odd functional equation. We never had to execute sums over these subsets. Here, however, the Restricted Sign conjecture is not enough; we must be able to execute sums over just the even and just the odd curves.

In other words, in the 2-level density case, the sums that arose were all of the form $\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\frac{1-\epsilon_E}{2}f_1f_2(0)$, whereas now we encounter more complicated sums such as $\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\frac{1-\epsilon_E}{2}f_1f_2(0)\sum_j f_3(z_j)$.

22.2 Higher Level Densities

The 4 and Higher Level Densities are determined in a similar manner. For families of constant even sign, see Rubinstein ([Ru]) for the combinatorics; trivial modifications handle families of constant odd sign.

The combinatorics in Rubinstein ([Ru]) are significantly easier, as there is no mixing of sign. In general, for families of elliptic curves, the higher level densities will be tractable for only constant sign families.

To make progress with the higher level densities for families of elliptic curves, significantly more than equidistribution of sign is needed.

Part IX

Appendices

A The Explicit Formula

Let E be a modular elliptic curve (arising from a weight 2 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. 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

$$\Lambda(s) = \epsilon \Lambda(2 - s), \tag{A.1}$$

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

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

We express $\frac{L'(s)}{L(s)}$ in a form convenient for deriving the Explicit Formula. For each prime p, let N_p be the number of points on the reduced elliptic curve E (including infinity), and let $a_p = 1 + p - N_p$. It is well known (see, for example, [Si1], page 240) that

$$\begin{aligned} L(s) &= \prod_{p|\triangle} (1 - a_p p^{-s})^{-1} \prod_{p \nmid \triangle} (1 - a_p p^{-s} + p^{1-2s})^{-1} \\ &= \sum \lambda(n) n^{-s}, \ \lambda(p) = a_p, \end{aligned} \tag{A.3}$$

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

$$\frac{L'(s)}{L(s)} = -\sum_{p|\triangle} \frac{d}{ds} \log(1 - a_p p^{-s}) - \sum_{p \nmid \triangle} \frac{d}{ds} \log(1 - a_p^{-s} + p^{1-2s}). \tag{A.4}$$

Straightforward calculations show the first term equals

$$-\sum_{p|\triangle} \sum_{k=1}^{\infty} \frac{(\log p) a_p^k}{(p^k)^s}. \tag{A.5}$$

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

$$1 - a_p p^{-s} + p^{1-2s} = pu^2 - a_p u + 1 = (1 - \alpha_p u)(1 - \beta_p u), \tag{A.6}$$

where for $p\nmid \Delta$

$$\alpha_p + \beta_p = a_p, \quad \alpha_p \beta_p = p. \tag{A.7}$$

The second term in $\frac{L'(s)}{L(s)}$ is

$$\sum_{p \nmid \triangle} \sum_{k=1}^{\infty} \frac{(\log p)(\alpha_p^k + \beta_p^k)}{(p^k)^s}. \tag{A.8}$$

Combining yields

$$\frac{L'(s)}{L(s)} = -\sum_{p|\triangle} \sum_{k=1}^{\infty} \frac{(\log p) a_p^k}{(p^k)^s} - \sum_{p \nmid \triangle} \sum_{k=1}^{\infty} \frac{(\log p)(\alpha_p^k + \beta_p^k)}{(p^k)^s}. \tag{A.9}$$

A.1 The Explicit Formula

The following derivation is a modification of Rudnick and Sarnak [RS], Proposition 2.1, pages 277 – 278. See also [Mes1].

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

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

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

$$H(s) = \phi\Big(\frac{s-1}{i}\Big). \tag{A.10}$$

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

$$\phi(x) = \int_{\mathbb{R}} \widehat{\phi}(\xi) e^{2\pi i x \xi} d\xi. \tag{A.11}$$

As $\widehat{\phi}$ has compact support, we may extend ϕ to

$$\phi(x+iy) = \int_{\mathbb{R}} \widehat{\phi}(\xi) e^{2\pi i (x+iy)\xi} d\xi. \tag{A.12}$$

Hence $H(s)$ is well defined, with

$$H(x+iy) = \int_{\mathbb{R}} \Big[\widehat{\phi}(\xi) e^{2\pi (x-1)\xi}\Big] e^{2\pi i y \xi} d\xi. \tag{A.13}$$

As $H(x+iy)$ is the Fourier Transform of a function in $\mathcal{S}(\mathbb{R})$, it is rapidly decreasing in $\text{Im}(s) = y$. $H(s)$ and $\Lambda(s)$ are nice entire functions. Consider

$$\mathcal{I} = \frac{1}{2\pi i} \int_{Re(s)=2\frac{1}{2}} \frac{\Lambda'(s)}{\Lambda(s)} H(s) ds. \tag{A.14}$$

We shift contours from $\text{Re}(s) = 2\frac{1}{2}$ to $-\frac{1}{2}$. This picks up the zeros and 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

$$\mathcal{I} = \sum \phi(\gamma) + \frac{1}{2\pi i} \int_{Re(s)=-\frac{1}{2}} \frac{\Lambda'(s)}{\Lambda(s)} H(s) ds. \tag{A.15}$$

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

$$\mathcal{I} = \sum \phi(\gamma) - \frac{1}{2\pi i} \int_{Re(s)=2\frac{1}{2}} \frac{\Lambda'(s)}{\Lambda(s)} H(2-s) ds. \tag{A.16}$$

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

$$\sum \phi(\gamma) = \frac{1}{2\pi i} \int_{Re(s)=2\frac{1}{2}} \frac{\Lambda'(s)}{\Lambda(s)} \Big[H(s) + H(2-s) \Big] ds. \tag{A.17}$$

We can shift the contour above to $\text{Re}(s) = 1$, 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.2) for $\frac{\Lambda'(s)}{\Lambda(s)}$ gives (for $s = 1 + iy, ds = idy$)

$$\begin{aligned} \sum \phi(\gamma) &= \frac{1}{2\pi} \int_{\mathbb{R}} \left[\log\left(\frac{N}{4\pi^2}\right) + 2\frac{\Gamma'(1+iy)}{\Gamma(1+iy)} \right] \phi(y) dy \\ &+ \frac{1}{2\pi i} \int_{\mathbb{R}} \frac{L'(1+iy)}{L(1+iy)} 2\phi(y) ds. \end{aligned} \tag{A.18}$$

We use (A.9) to substitute for $\frac{L'(1+iy)}{L(1+iy)}$; by Hasse $|a_p| < 2\sqrt{p}$. We shift this piece back to $\text{Re}(s) = 2\frac{1}{2}$. By the Dominated Convergence Theorem we can interchange the summations and integration. We then shift back to $\text{Re}(s) = 1$. As

$$\begin{aligned}\int_{\mathbb{R}}\Big(\frac{1}{p^k}\Big)^{1+iy}\phi(y)dy &= \int_{\mathbb{R}}\frac{1}{p^k}\phi(y)e^{-ik\log p\cdot y}dy\\ &= \frac{1}{p^k}\widehat{\phi}\Big(\frac{k\log p}{2\pi}\Big),\end{aligned}\tag{A.19}$$

we obtain the Explicit Formula:

$$\begin{aligned}\sum\phi(\gamma) &= \frac{1}{2\pi}\int_{\mathbb{R}}\left[\log\Big(\frac{N}{4\pi^2}\Big)+2\frac{\Gamma'(1+iy)}{\Gamma(1+iy)}\right]\phi(y)dy\\ &- \frac{1}{2\pi}\sum_{p|\triangle}\sum_{k=1}^{\infty}\frac{2\log p\cdot a_p^k}{p^k}\widehat{\phi}\Big(\frac{1}{2\pi}k\log p\Big)\\ &- \frac{1}{2\pi}\sum_{p\nmid\triangle}\sum_{k=1}^{\infty}\frac{2\log p\cdot(\alpha_p^k+\beta_p^k)}{p^k}\widehat{\phi}\Big(\frac{1}{2\pi}k\log p\Big)\end{aligned}\tag{A.20}$$

A.2 Tractable Explicit Formula

In the previous section, we derived the Explicit Formula for the sum over the zeros of an elliptic curve (assuming GRH). Below we show many of the terms are $O\Big(\frac{1}{\log N}\Big)$ or $O\Big(\frac{\log\log N}{\log N}\Big)$.

Replace $\phi(x)$ by $\phi_r(x)=\phi(rx)$, $r=\frac{\log N}{2\pi}$. A straightforward calculation shows

$$\frac{1}{2\pi}\int_{\mathbb{R}}\left[\log\Big(\frac{N}{4\pi^2}\Big)+2\frac{\Gamma'(1+iy)}{\Gamma(1+iy)}\right]\phi(y)dy\to\int_{\mathbb{R}}\phi(y)dy+O\Big(\frac{1}{\log N}\Big).\tag{A.21}$$

To prove the above, use (see Alfohrs [Al])

$$\frac{\Gamma'(z)}{\Gamma(z)}=C+\log z-\frac{1}{2z}-\int_0^\infty\frac{2u}{u^2+z^2}\frac{du}{e^{2\pi u}-1},\ \text{Re}(z)>0.\tag{A.22}$$

Hence we find

$$\begin{aligned}\sum\phi\Big(\gamma\frac{\log N}{2\pi}\Big) &= \int_{\mathbb{R}}\phi(y)dy-2\sum_{p|\triangle}\sum_{k=1}^{\infty}\frac{\log p}{\log N}\frac{a_p^k}{p^k}\widehat{\phi}\Big(k\frac{\log p}{\log N}\Big)\\ &\quad -2\sum_{p\nmid\triangle}\sum_{k=1}^{\infty}\frac{\log p}{\log N}\frac{\alpha_p^k+\beta_p^k}{p^k}\widehat{\phi}\Big(k\frac{\log p}{\log N}\Big)+O\Big(\frac{1}{\log N}\Big).\end{aligned}\tag{A.23}$$

As $|\alpha_p|,|\beta_p|\leq\sqrt{p}$ and $|a_p|\leq 2\sqrt{p}$, we bound the $k\geq 3$ terms by $\frac{||\phi||_\infty}{\log N}$. For $p\nmid\triangle$, $\alpha_p+\beta_p=a_p$ and $\alpha_p\beta_p=p$. Hence $\alpha_p^2+\beta_p^2=a_p^2-2p$, and

$$\begin{aligned}\sum \phi\Big(\gamma\frac{\log N}{2\pi}\Big) &= \int_{\mathbb{R}} \phi(y)dy - 2\sum_p \sum_{k=1}^{2} \frac{\log p}{\log N}\frac{a_p^k}{p^k}\widehat{\phi}\Big(k\frac{\log p}{\log N}\Big) \\ &\quad -2\sum_{p \nmid \triangle} \frac{\log p}{\log N}\frac{-2p}{p^2}\widehat{\phi}\Big(2\frac{\log p}{\log N}\Big) + O\Big(\frac{1}{\log N}\Big). \qquad (A.24)\end{aligned}$$

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

As the conductor and the discriminant have the same prime factors (if the equation is minimal), we may replace $\triangle$ by N. In the applications our curves will be minimal except possibly at the primes 2 and 3; we may easily add these two primes below.

$\frac{\log p}{p}$ is a decreasing function. The sum is greatest when N is the product of the first n primes. So

$$N = 2 \cdot\ 3 \cdots\ p_n \ \geq\ 2^n \ \rightarrow\ n\ \leq\ \frac{\log N}{\log 2}. \qquad (A.25)$$

As $\sum_{p=2}^{X} \frac{\log p}{p} = \log X + O(1)$ ([Da], page 57) we have

$$\begin{aligned}\frac{1}{\log N}\sum_{p|N} \frac{\log p}{p}\widehat{\phi}\Big(a\frac{\log p}{\log N}\Big) &\ll \frac{1}{\log N}\sum_{p=2}^{\frac{\log N}{a\log 2}} \frac{\log p}{p} \\ &= \frac{1}{\log N}\Big[\log\Big(\frac{\log N}{a\log 2}\Big) + O(1)\Big] \\ &= O\Big(\frac{\log\log N}{\log N}\Big), \qquad (A.26)\end{aligned}$$

yielding the lemma.

The cost of expanding $\sum_{p \nmid \triangle} \frac{\log p}{\log N}\frac{-2p}{p^2}\widehat{\phi}(2\frac{\log p}{\log N})$ to a sum over all primes can be safely absorbed in the error. We now study

$$\begin{aligned}\sum \phi\Big(\gamma\frac{\log N}{2\pi}\Big) &= \int_{\mathbb{R}} \phi(y)dy - 2\sum_p \sum_{k=1}^{2} \frac{\log p}{\log N}\frac{a_p^k}{p^k}\widehat{\phi}\Big(k\frac{\log p}{\log N}\Big) \\ &\quad -2\sum_{p} \frac{\log p}{\log N}\frac{-2p}{p^2}\widehat{\phi}\Big(2\frac{\log p}{\log N}\Big) + O\Big(\frac{\log\log N}{\log N}\Big). \qquad (A.27)\end{aligned}$$

The last sum, by Lemma B.3, is just $4\frac{1}{4}\phi(0) = \phi(0)$. Thus

$$\begin{aligned}\sum \phi\Big(\gamma \frac{\log N}{2\pi}\Big) &= \int_{\mathbb{R}} \phi(y)dy + \phi(0) - 2\sum_p \frac{\log p}{\log N}\frac{a_p}{p}\widehat{\phi}\Big(\frac{\log p}{\log N}\Big) \\ &\quad -2\sum_p \frac{\log p}{\log N}\frac{a_p^2}{p^2}\widehat{\phi}\Big(2\frac{\log p}{\log N}\Big) \ + \ O\Big(\frac{\log\log N}{\log N}\Big). \qquad \text{(A.28)}\end{aligned}$$

We make one final simplification. Recall $a_p = 1 + p - N_p$, where N_p is the number of points (including infinity) on the reduced curve mod p. For the curve $y^2 = f(x)$, $N_p = 1 + \sum_{x=0}^{p-1}\Big(1 + \big(\frac{f(x)}{p}\big)\Big)$. Hence $a_p = -\sum_{x=0}^{p-1}\big(\frac{f(x)}{p}\big)$, and

Theorem A.2 (The Explicit Formula) *Let E be an elliptic curve with conductor N. Then*

$$\begin{aligned}\sum \phi\Big(\gamma \frac{\log N}{2\pi}\Big) &= \widehat{\phi}(y) + \phi(0) - 2\sum_p \frac{\log p}{\log N}\frac{a_p}{p}\widehat{\phi}\Big(\frac{\log p}{\log N}\Big) \\ &\quad -2\sum_p \frac{\log p}{\log N}\frac{a_p^2}{p^2}\widehat{\phi}\Big(\frac{2\log p}{\log N}\Big) + O\Big(\frac{\log\log N}{\log N}\Big). \qquad \text{(A.29)}\end{aligned}$$

If E may be written as $y^2 = f(x)$, $f(x)$ a monic integer cubic in x, then

$$\begin{aligned}\sum \phi\Big(\gamma \frac{\log N}{2\pi}\Big) &= \widehat{\phi}(y) + \phi(0) + 2\sum_p \frac{\log p}{\log N}\frac{1}{p}\widehat{\phi}\Big(\frac{\log p}{\log N}\Big)\sum_{x=0}^{p-1}\Big(\frac{f(x)}{p}\Big) \\ &\quad -2\sum_p \frac{\log p}{\log N}\frac{1}{p^2}\widehat{\phi}\Big(\frac{2\log p}{\log N}\Big)\left[\sum_{x=0}^{p-1}\Big(\frac{f(x)}{p}\Big)\right]^2 + O\Big(\frac{\log\log N}{\log N}\Big)\end{aligned}$$
$$\text{(A.30)}$$

If instead of rescaling the zeros by $\log N$ we rescale by $\log M$, an almost identical proof yields

Theorem A.3 (The Modified Explicit Formula) *Let E be an elliptic curve with conductor N. Then*

$$\begin{aligned}\sum \phi\Big(\gamma \frac{\log M}{2\pi}\Big) &= \frac{\log N}{\log M}\widehat{\phi}(y) + \phi(0) - 2\sum_p \frac{\log p}{\log M}\frac{a_p}{p}\widehat{\phi}\Big(\frac{\log p}{\log M}\Big) \\ &\quad -2\sum_p \frac{\log p}{\log M}\frac{a_p^2}{p^2}\widehat{\phi}\Big(2\frac{\log p}{\log M}\Big) + O\Big(\frac{\log\log M}{\log M}\Big). \qquad \text{(A.31)}\end{aligned}$$

B Sums of Test Functions at Primes

We calculate sums of test functions over primes. $\widehat{F}$, $\widehat{f_i}$ are even Schwartz functions with compact support.

B.1 First Order Sums

Let $\varphi(m)$ be the Euler phi-function (the number of numbers relatively prime to m). If m is prime, $\varphi(m) = m - 1$; if $m = 3$ or 4, $\varphi(m) = 2$.

Lemma B.1 (Sum of $\widehat{F}$ over primes)

$$\frac{1}{\log N} \sum_{p \equiv b(m)} \frac{\log p}{p} \widehat{F}\Big(a \frac{\log p}{\log N}\Big) = \frac{1}{2a\varphi(m)} F(0) + O\Big(\frac{1}{\log N}\Big). \tag{B.1}$$

By RH (or GRH if $m \neq 1$, see [Da]) and partial summation we have

$$\begin{aligned} \sum_{\substack{p \le x \\ p \equiv b(m)}} \log p &= \frac{x}{\varphi(m)} + O(x^{\frac{1}{2}} \log^2(mx)) \\ \sum_{\substack{p \le x \\ p \equiv b(m)}} \frac{\log p}{p} &= \frac{\log x}{\varphi(m)} + O(1). \end{aligned} \tag{B.2}$$

Using partial summation on the p-sum gives

$$\begin{aligned} \sum_{\substack{p \equiv b(m) \\ p \ge p_0}} \frac{\log p}{p} \widehat{F}\Big(a \frac{\log p}{\log N}\Big) &= -\int_{p_0}^{\infty} \Big(\frac{\log x}{\varphi(m)} + O(1)\Big) \frac{d}{dx} \widehat{F}\Big(a \frac{\log x}{\log N}\Big) \\ &= \int_{p_0}^{\infty} \frac{1}{\varphi(m) x} \widehat{F}\Big(a \frac{\log x}{\log N}\Big) + O\Big(\frac{1}{x \log N} \Big|\widehat{F}'\Big(a \frac{\log x}{\log N}\Big)\Big|\Big) \\ &= \frac{\log N}{a} \int_{u_0}^{\infty} \Big[\frac{1}{\varphi(m)} \widehat{F}(u) + O\Big(\frac{1}{\log N} \Big|\widehat{F}'(u)\Big|\Big)\Big] du \\ &= \frac{\log N}{a} \frac{1}{2} \int_{-\infty}^{\infty} \Big[\frac{\widehat{F}(u)}{\varphi(m)} + O\Big(\frac{|\widehat{F}'(u)|}{\log N}\Big)\Big] du + O(u_0 \log N) \\ &= \frac{\log N}{2a\varphi(m)} F(0) + O(1), \end{aligned} \tag{B.3}$$

as $u_0 = \frac{\log p_0}{\log N}$. Dividing by $\log N$ yields the lemma. Using the Prime Number Theorem instead of RH yields the same result, but with worse error term. As GRH is assumed throughout this thesis, we have assumed RH here. □.

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

Corollary B.2 $\frac{1}{\log N} \sum_p \frac{\log p}{p} \widehat{F}\Big(\frac{\log p}{\log N}\Big) = \frac{1}{2}F(0) + O\Big(\frac{1}{\log N}\Big)$.

Corollary B.3 $\frac{1}{\log N} \sum_p \frac{\log p}{p} \widehat{F}\Big(2\frac{\log p}{\log N}\Big) = \frac{1}{4}F(0) + O\Big(\frac{1}{\log N}\Big)$.

B.2 Second Order Sums

Lemma B.4

$$4\sum_p \frac{\log^2 p}{\log^2 M}\frac{1}{p}\widehat{f_1}\widehat{f_2}\Big(\frac{\log p}{\log M}\Big) \quad = \quad 2\int_{-\infty}^{\infty} |u|\widehat{f_1}(u)\widehat{f_2}(u)du + O\Big(\frac{1}{\log M}\Big). \tag{B.4}$$

Using $\sum_{p\le x} \log p = x + \text{small}$ and Partial Summation (Integral Version, Lemma 2.2) twice we obtain $\sum_{p\le x} \frac{\log^2 p}{p} = \frac{1}{2}\log^2 x + O(\log x)$. Hence

$$\begin{aligned} S &= \frac{4}{\log^2 M}\sum_p \frac{\log^2 p}{p}\widehat{f_1}\widehat{f_2}\Big(\frac{\log p}{\log M}\Big) \\ &= \frac{-4}{\log^2 M}\int_2^{\infty}\left[\frac{1}{2}\log^2 x + O(\log x)\right]\frac{d}{dx}\widehat{f_1}\widehat{f_2}\Big(\frac{\log x}{\log M}\Big)dx \\ &= S_a + S_b. \end{aligned} \tag{B.5}$$

There is no contribution from S_b. The derivative term looks like $\frac{1}{x\log M}$ times a nice function. The support conditions restrict the integral to M to a power.

$$\begin{aligned} S_b &\ll \frac{1}{\log^2 M}\int_2^{M^\sigma}\frac{1}{\log M}\frac{\log x}{x}dx \\ &\ll \frac{1}{\log^3 M}\log^2 M = O\Big(\frac{1}{\log M}\Big) \\ S_a &= \frac{-4}{\log^2 M}\int_2^{\infty}\frac{1}{2}\log^2 x\frac{d}{dx}\widehat{f_1}\widehat{f_2}\Big(\frac{\log x}{\log M}\Big)dx \\ &= \frac{4}{\log^2 M}\int_2^{\infty}\frac{\log x}{x}\widehat{f_1}\widehat{f_2}\Big(\frac{\log x}{\log M}\Big)dx \\ &= 4\int_2^{\infty}\frac{\log x}{\log M}\widehat{f_1}\widehat{f_2}\Big(\frac{\log x}{\log M}\Big)\frac{dx}{x\log M} \\ &= 4\int_{\frac{\log 2}{\log M}}^{\infty}|u|\widehat{f_1}\widehat{f_2}(u)du \\ &= 2\int_{-\infty}^{\infty}|u|\widehat{f_1}(u)\widehat{f_2}(u)du + O\Big(\frac{1}{\log M}\Big). \end{aligned} \tag{B.6}$$

Repeating the above arguments for $p \equiv b(m)$ yields

Lemma B.5

$$4 \sum_{p \equiv b(m)} \frac{\log^2 p}{\log^2 M} \frac{1}{p} \widehat{f_1} \widehat{f_2}\Big(\frac{\log p}{\log M}\Big) \quad = \quad \frac{2}{\varphi(m)} \int_{-\infty}^{\infty} |u| \widehat{f_1}(u) \widehat{f_2}(u) du + O\Big(\frac{1}{\log M}\Big). \tag{B.7}$$

B.3 Bounding Contributions from Curves

The following lemma is from Brumer [Br], page 451:

Lemma B.6 (Bounding an Individual Sum) *Let E be an elliptic curve with conductor N_E, and let $X > 10 \log N_E$ be a free parameter (we will take X to be (approximately) a power of N_E). Then for $\widehat{\phi}$ a Schwartz function of compact support we have*

$$\Big| \sum_{p \leq X} \frac{\log p}{\log X} \widehat{\phi}\Big(\frac{\log p}{\log X}\Big) \frac{a_E(p)}{p} \Big| \ll \log N_E. \tag{B.8}$$

See also Goldfeld and Hoffstein [GH].

Using Hasse's bound, $|a_E(p)| < 2\sqrt{p}$, we obtain

$$\Big| \sum_{p \leq X} \frac{\log p}{\log X} \widehat{\phi}\Big(2 \frac{\log p}{\log X}\Big) \frac{a_E^2(p)}{p^2} \Big| \ll \widehat{\phi}(0). \tag{B.9}$$

Inserting the above and Lemma B.6 into the Modified Explicit Formula (Theorem A.31) bounds the sum over the zeros of a curve:

Lemma B.7 (Bounding Contributions from a Curve) *For $X > 10 \log N_E$,*

$$\sum_{\gamma} \phi\Big(\gamma \frac{\log X}{2\pi}\Big) \ll \log N_E. \tag{B.10}$$

In all applications, X is significantly greater than $10 \log N_E$.

B.4 Restricting Sums over Primes to $p > \log^l N$

We constantly encounter sums such as

$$\sum_p \frac{\log p}{\log X}\frac{1}{p^r}\widehat{f}\Big(r\frac{\log p}{\log X}\Big)a_t^r(p), \tag{B.11}$$

where $r \in \{1,2\}$ and $\log X$ is either $\log C(t)$ or $\log M$ ($\log M$ is the average of the logarithms of the conductors). For the one-parameter families we consider, $\log M = k\log N + o(\log N)$ (Lemma 9.4).

By Hasse, $a_t^r(p) \le (2\sqrt{p})^r$. The contribution S_l from $p \le \log^l M$ is

$$S_l \ \ll \ \frac{1}{\log X}\sum_{p\le \log^l N}\frac{\log p}{p^{r/2}}. \tag{B.12}$$

Clearly the larger contribution is from $r = 1$. By the Prime Number Theorem, $\sum_{p\le x} \log p \ll x$. By partial summation, $\sum_{p\le x}\frac{\log p}{\sqrt{p}} \ll \sqrt{x}$. Thus

$$S_l \ll \frac{\sqrt{\log^l N}}{\log X}. \tag{B.13}$$

We have shown

Lemma B.8 (Removing Small Primes) *$\forall l < 2$, we may remove the sums over primes $p \le \log^l N$ in the Explicit Formula at a cost of $\frac{\log^{l/2} N}{\log X}$.*

If $X = \log M = k\log N + o(\log N)$ or $X = C(t)$ and $\log C(t) \gg \log N$, the error is $O(\log^{\frac{l}{2}-1} N)$. For $l < 2$, this error is negligible.

B.5 Using the Rank over $\mathbb{Q}(t)$ to Evaluate Sums

In many of the families investigated, $A_{1,\mathcal{F}}(p) = -rp + O(1)$ (or has main term zero half the time, and $-2rp$ the other half). As such, the density sums are easy to evaluate. We consider the more general situation. The arguments below follow those in [Si3].

Lemma B.9 (Using $A_{\mathcal{E}}(p)$ for Sums) *Let $\mathcal{E}$ have rank r over $\mathbb{Q}(t)$ and assume Tate's conjecture for $\mathcal{E}$ (known if $\mathcal{E}$ is a rational surfaces). Then*

$$2\sum_p \frac{\log p}{\log X}\frac{1}{p}\widehat{f}\Big(\frac{\log p}{\log X}\Big)\Big(-A_{\mathcal{E}}(p)\Big) = rf(0). \tag{B.14}$$

Proof:

$$\begin{aligned} S &= \sum_p \frac{\log p}{\log X}\frac{1}{p}\widehat{f}\Big(\frac{\log p}{\log X}\Big)\Big(-A_{\mathcal{E}}(p)\Big) \\ &= \sum_p \Big(-A_{\mathcal{E}}(p)\log p\Big)\frac{1}{p\log X}\widehat{f}\Big(\frac{\log p}{\log X}\Big). \end{aligned} \tag{B.15}$$

Let $a_n = -A_{\mathcal{E}}(p)\log p$ for n prime, and 0 otherwise; let $h(n) = \frac{1}{n\log X}\widehat{f}(\frac{\log n}{\log X})$. Choose B greater than X^σ, where $\widehat{f}$ is supported in $(-\sigma,\sigma)$. Thus the boundary term from partial summation vanishes.

By Rosen-Silverman (Theorem 2.3), $A(u) = ru + o(u)$. In many of our families, $o(u)$ is zero. Differentiating $h(u)$ gives

$$\begin{aligned} h'(u) &= -\frac{1}{u^2\log X}\widehat{f}\Big(\frac{\log u}{\log X}\Big) + \frac{1}{u^2\log^2 X}\widehat{f}'\Big(\frac{\log u}{\log X}\Big) \\ &= \frac{1}{u^2\log X}h_1(u). \end{aligned} \tag{B.16}$$

Thus

$$S = -\int_2^B \Big[ru + o(u)\Big]\frac{1}{u^2\log X}h_1(u). \tag{B.17}$$

The ru piece, by Corollary B.2, contributes $rf(0)$. To see this, integrate by parts (the ru becomes r, $\frac{1}{u^2\log X}h_1(u)$ becomes $h(u)$). We are left with the error term.

The contribution from $u < \log X$ is $\ll \int_2^{\log X}\frac{1}{u\log X} \ll \frac{\log\log X}{\log X}$; $u \geq \log X$ contributes

$$\begin{aligned} -\int_{\log X}^B o(u)\frac{1}{u^2\log X}h_1(u) &\ll \frac{1}{\log X}\int_{\log X}^{X^\sigma}\frac{o(u)}{u}\frac{1}{u}du \\ &\ll \max_{u\in[\log X, X^\sigma]}\frac{o(u)}{u}. \end{aligned} \tag{B.18}$$

As $X \to \infty$, $\frac{o(u)}{u} \to 0$. □

C Character Sums and the Quadratic Formula mod p

C.1 Factorizable Quadratics in Sums of Legendre Symbols

Lemma C.1 *For $p > 2$*

$$S(n) = \sum_{x=0}^{p-1} \left(\frac{n_1 + x}{p}\right)\left(\frac{n_2 + x}{p}\right) = \begin{cases} p-1 & \text{if } p \mid n_1 - n_2 \\ -1 & \text{otherwise} \end{cases} \tag{C.1}$$

Proof: Shifting x by $-n_2$, we need only prove the lemma when $n_2 = 0$. Assume $(n,p) = 1$ as otherwise the result is trivial. For $(a,p) = 1$ we have:

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

Hence

$$\begin{aligned} S(n) &= \frac{1}{p-1}\sum_{a=1}^{p-1}\sum_{x=0}^{p-1} \left(\frac{an+x}{p}\right)\left(\frac{x}{p}\right) \\ &= \frac{1}{p-1}\sum_{a=0}^{p-1}\sum_{x=0}^{p-1} \left(\frac{an+x}{p}\right)\left(\frac{x}{p}\right) - \frac{1}{p-1}\sum_{x=0}^{p-1}\left(\frac{x}{p}\right)^2 \\ &= \frac{1}{p-1}\sum_{x=0}^{p-1}\left(\frac{x}{p}\right)\sum_{a=0}^{p-1}\left(\frac{an+x}{p}\right) - 1 \\ &= 0 - 1 = -1 \end{aligned} \tag{C.3}$$

Where do we use $p > 2$? We used $\sum_{a=0}^{p-1}\left(\frac{an+x}{p}\right) = 0$ for $(n,p) = 1$. This is true for all odd primes (as there are $\frac{p-1}{2}$ quadratic residues, $\frac{p-1}{2}$ non-residues, and 0); for $p = 2$, there is one quadratic residue, no non-residues, and 0. As we never need to use this lemma for $p = 2$ (see Lemma B.8), this complication will not affect any of our proofs.

C.2 General Quadratics in Sums of Legendre Symbols

Lemma C.2 (Quadratic Legendre Sums) *Assume a and b are not both zero mod p and $p > 2$. Then*

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

Proof: Assume $a \not\equiv 0(p)$ as otherwise the proof is trivial. Let $\delta = 4^{-1}(b^2-4ac)$. Then

$$\begin{aligned}
\sum_{t=0}^{p-1}\left(\frac{at^2+bt+c}{p}\right) &= \sum_{t=0}^{p-1}\left(\frac{a^{-1}}{p}\right)\left(\frac{a^2t^2+bat+ac}{p}\right) \qquad \text{(C.5)}\\
&= \sum_{t=0}^{p-1}\left(\frac{a}{p}\right)\left(\frac{t^2+bt+ac}{p}\right)\\
&= \sum_{t=0}^{p-1}\left(\frac{a}{p}\right)\left(\frac{t^2+bt+4^{-1}b^2+ac-4^{-1}b^2}{p}\right)\\
&= \sum_{t=0}^{p-1}\left(\frac{a}{p}\right)\left(\frac{(t+2^{-1}b)^2-4^{-1}(b^2-4ac)}{p}\right)\\
&= \sum_{t=0}^{p-1}\left(\frac{a}{p}\right)\left(\frac{t^2-\delta}{p}\right)\\
&= \left(\frac{a}{p}\right)\sum_{t=0}^{p-1}\left(\frac{t^2-\delta}{p}\right)
\end{aligned}$$

If $\delta \equiv 0(p)$ we get $p-1$. If $\delta = \eta^2, \eta \neq 0$, then by the Lemma C.1

$$\sum_{t=0}^{p-1}\left(\frac{t^2-\delta}{p}\right) = \sum_{t=0}^{p-1}\left(\frac{t-\eta}{p}\right)\left(\frac{t+\eta}{p}\right) = -1. \tag{C.6}$$

We note that $\sum_{t=0}^{p-1}\left(\frac{t^2-\delta}{p}\right)$ is the same for all non-square δ's (let g be a generator of the multiplicative group, $\delta = g^{2k+1}$, change variables by $t \to g^k t$). Denote this sum by S, the set of non-zero 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

$$\begin{aligned}
\sum_{\delta=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{t^2-\delta}{p}\right) &= \sum_{t=0}^{p-1}\left(\frac{t^2}{p}\right) + \sum_{\delta\in\mathcal{R}}\sum_{t=0}^{p-1}\left(\frac{t^2-\delta}{p}\right) + \sum_{\delta\in\mathcal{N}}\sum_{t=0}^{p-1}\left(\frac{t^2-\delta}{p}\right)\\
&= (p-1) + \frac{p-1}{2}(-1) + \frac{p-1}{2}S = 0 \qquad \text{(C.7)}
\end{aligned}$$

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

C.3 Quadratic Formula mod p

We show the Quadratic Formula, properly interpreted, gives the roots of a quadratic congruence mod p. Consider $ax^2 + bx + c \equiv 0 \bmod p$, $a \not\equiv 0$, $p > 2$. There are at most 2 incongruent roots (Lemma 3.1).

For each root x_i mod p there exists an m_i such that $ax_i^2 + bx_i + c + m_i p = 0$. By the usual Quadratic Formula, this implies

$$x_i \quad = \quad \frac{-b \pm \sqrt{b^2 - 4ac - 4am_i p}}{2a}. \tag{C.8}$$

As x_i is an integer, $b^2 - 4ac - 4am_i p = s_i^2$, or $b^2 - 4ac \equiv s_i^2 \bmod p$. Thus, if x_i is a root of the quadratic mod p, $b^2 - 4ac$ is a square mod p. Interpreting the square root as an operation mod p, the Quadratic Formula gives the roots; by direct substitution we see both work.

Conversely, assume there is a root x_i mod p, and $\sqrt{b^2 - 4ac}$ is not equivalent to a square. Repeating the above argument leads to a contradiction.

Thus,

Lemma C.3 (Quadratic Formula mod p) *For a quadratic $ax^2 + bx + c \equiv 0$ mod p, $a \not\equiv 0$, there are two distinct roots if $b^2 - 4ac$ is equivalent to a non-zero square, one root if $b^2 - 4ac \equiv 0$, and no roots if $b^2 - 4ac$ is not equivalent to a square.*

D Calculating Conductors for Various One-Parameter Families

D.1 Introduction

We calculate the conductors $C(t)$ for many families of elliptic curves, $C(t) = \prod_{p|\Delta} p^{f_p(t)}$. For $p > 3$, if the curve is minimal for p then $f_p(t) = 0$ if $p \nmid \Delta(t)$, 1 if $p|\Delta(t)$ and $p \nmid c_4(t)$, and 2 if $p|\Delta(t)$ and $p|c_4(t)$. From [Si1] (Remark 1.1, page 172), if $p > 3$ and $p^{12} \nmid \Delta(t)$, then the equation is minimal at p.

The difficult computations are $p = 2$ and 3. We use Tate's Algorithm (see Cremona [Cr], pages $49 - 52$) to calculate $f_2(t)$ and $f_3(t)$.

We let $T(r, s, h, u)$ denote the standard change of variables $x = u^2x' + r$, $y = u^2y + su^2x + h$. Cremona uses t where we use h; we have changed variables as we use t for our one-parameter family. Hence

$$\begin{aligned}
ua_1' &= a_1 + 2s \\
u^2a_2' &= a_2 - sa_1 + 3r - s^2 \\
u^3a_3' &= a_3 + ra_1 + 2t \\
u^4a_4' &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st \\
u^6a_6' &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1 \\
u^{12}\Delta' &= \Delta
\end{aligned} \tag{D.1}$$

Note that $T(r, s, t, 1)$ does not change Δ, and $T(0, 0, 0, 1)$ is the identity transformation. We record the relation between the a_i's and the b_i's and the c_i's:

$$\begin{aligned}
b_2 &= a_1^2 + 2^2a_2 \\
b_4 &= a_1a_3 + 2a_4 \\
b_6 &= a_3^2 + 2^2a_6 \\
b_8 &= a_1^2a_6 - a_1a_3a_4 + 2^2a_2a_6 + a_2a_3^2 - a_4^2 \\
c_4 &= b_2^2 - 2^3 \cdot 3b_4
\end{aligned}$$

$$\begin{aligned} c_6 &= -b_2^3 + 2^2 \cdot 3^2 b_2 b_4 - 2^3 \cdot 3^3 b_6 \\ \Delta &= -b_2^2 b_8 - 2^3 b_4^3 - 3^3 b_6^2 + 3^2 b_2 b_4 b_6. \end{aligned} \tag{D.2}$$

For notational convenience, we often write a_i (b_i, c_i) for $a_i(t)$ $(b_i(t),\ c_i(t))$ below.

D.2 $C(t)$ for the Family $y^2 = x^3 + 2^4(-3)^3(9t+1)^2$

We calculate $C(t)$ for the $y^2 = x^3 + 2^4(-3)^3(9t+1)^2$, $9t+1$ square-free. $C(t) = \prod_{p|\Delta} p^{f_p(t)}$. If $p \neq 2, 3$ then $f_p(t) = 2$ if $p|9t+1$ and 0 otherwise.

$a_1 = a_2 = a_3 = a_4 = 0$, $a_6 = -3^3 \cdot 2^4 \cdot (9t+1)^2$. Hence $b_2 = b_4 = b_8 = 0$, $b_6 = -2^6 \cdot 3^3 \cdot (9t+1)^2$, $c_4 = 0$, $c_6 = -2^9 \cdot 3^6 \cdot (9t+1)^2$, and $\Delta = -2^{12} \cdot 3^9 \cdot (9t+1)^4$.

D.2.1 $p = 2$

We apply Tate's algorithm.

(3) $n = ord(2, \Delta(t))$. $n = 12 + 4\cdot$ord$(2, 9t+1)$, where ord(p, m) denotes the power of p dividing m.

(4) $n \neq 0$: continue to line 5.

$(5-18)$ $p = 2$, $2|b_2$, so $r = 0$, $h = 0$. Apply $T(0,0,0,1)$.

$(19-28)$ $2|c_4$, $2^2|a_6$, $2^3|b_8$, $2^3|b_6$: continue to line 29.

$(29-33)$ $p = 2$, so $s = 0$, $t = 0$: apply $T(0,0,0,1)$.

$(34-36)$ $b = 0$, $c = 0$, $d = \frac{a_6}{2^3} = -2 \cdot 3^3(9t+1)^2$, $w = 2 \cdot 3^3(9t+1)^2$.

$(37-38)$ $2|w$, $2|x$: continue to line 65.

$(65-69)$ $r = 0$: apply $T(0,0,0,1)$. $x_3 = 0$, $x_6 = -3^3(9t+1)^2$.

(70) $2|x_3^2 + 2^2 x_6$: continue to line 74. Write y as $4k + z$, where $z = 0$, 1 or 2; as $9t+1$ is square-free, $t \not\equiv 3$ mod 4. Then $a_6 = -2^4 \cdot 3^3(36k + 9z + 1)^2$, $x_6 = -3^3(36k + 9z + 1)^2$.

$(74-75)$ $p = 2$ so $t = -2^2(x_6 \bmod 2)$. There are two possibilities: z is even (0, 2) or $z = 1$.

Case One: z is even

If z is even, let $z = 2m$, $m = 0$ or 1. Then $x_6 \equiv 1$ mod 2, hence $h = -2^2$.

(76) $T(0, 0, -2^2, 1)$. This gives $a_3' = -2^3$, $a_6' = -2^4 \cdot 3^3(36k + 18m + 1) - 2^4$, and $\Delta(t)$ is unchanged, $\Delta = -2^{12} \cdot 3^9 \cdot (36y + 18m + 1)^4$, so ord$(2, \Delta) = 12$.

(77) $2^4|a_4$: continue to line 78.

(78) $2^6|a_6$: continue to line 80.

(80) Apply $T(0,0,0,2)$. $a_3' = -1$, $a_6' = \frac{1}{2^2}\Big[-3^3(36k+18z+1)^2 - 1\Big]$, $2^{12}\Delta'(t) = \Delta(t)$. Hence $\Delta'(t) = -3^9 \cdot (36k+18m+1)^4$. Restart the algorithm.

(2) Calculate $b_2, \ldots, \Delta(t)$. $\Delta(t) = -3^9 \cdot (36k+18m+1)^4$.

(3) $n =$ord$(2, \Delta) = 0$.

(4) As $n = 0$, $f_2(t) = 0$.

Therefore there are no factors of 2 in $C(t)$ if $t \equiv 0, 2 \bmod 4$ ($f_2(t) = 0$).

Case Two: $z = 1$

We resume the algorithm on line 75 with $y = 4k + z$ and $z = 1$.

$(75 - 76)$ $h = 0$, apply $T(0,0,0,1)$. Note $a_6 = -2^4 \cdot 3^3(36k+10)^2 = -2^6 \cdot 3^3(18k+5)^2$, $\Delta(t) = -2^{16} \cdot 3^9 \cdot (18k+5)^4$.

$(77 - 78)$ $2^4 | a_4$, $2^6 | a_6$: continue to line 79.

$(79 - 80)$ Apply $T(0,0,0,2)$. $a_6' = -3^3(18k+5)^2$, $2^{12}\Delta'(t) = \Delta(t)$, so $\Delta'(t) = -2^4 \cdot 3^9(18k+5)^4$.

(2) Calculate $b_2, \ldots, \Delta(t)$. $a_6' = -3^3(18k+5)^2$, $a_1, a_2, a_3, a_4, b_2, b_4, b_8, c_4 = 0$, $b_6 = -2^2 3^3(18k+5)^2$, $c_6 = -2^4 \cdot 3^6(18k+5)^2$, $\Delta(t) = -2^4 \cdot 3^9(18k+5)^4$.

(3) $n =$ord$(2, \Delta(t)) = 4$.

(4) $n \neq 0$: continue to line 5.

$(5 - 18)$ $p = 2$, $2 | b_2$ so $r = 0$, $h = 1$. Apply $T(0,0,1,1)$; $a_3' = 2$, $a_6' = -3^3(18k+5)^2 - 1$, $b_6 = -2^2 \cdot 3^3(18k+5)$, $c_4 = 0$.

$(19 - 22)$ $2 | c_4$: continue to line 23.

(23) $2^2 | a_6$: continue to line 24.

(24) $2^3 | b_8$: continue to line 25.

(25) As $2^3 \nmid b_6$, $f_2(t) =$ord$(2, \Delta(t)) - 2 = 4 - 2 = 2$.

Therefore $f_2(t) = 2$ if $t \equiv 1 \bmod 4$. We have shown:

Lemma D.1 *For all square-free* $9t+1$*, if* $E_t : y^2 = x^3 + 2^4 \cdot (-3)^3 \cdot (9t+1)^2$*, then* $f_2(t) = 0$ *if* $t \equiv 0, 2$ *mod* 4 *and* $f_2(t) = 2$ *if* $t \equiv 1$ *mod* 4.

D.2.2 $p = 3$

We again apply Tate's algorithm.

(2) Calculate $b_2, \ldots, \Delta(t)$. $a_1, a_2, a_3, a_4 = 0$, $a_6 = -3^3 \cdot 2^4(9t+1)^2$, $b_2, b_4, b_8 = 0$, $b_6 = -3^3 \cdot 2^6(9t+1)^2$, $c_4 = 04$, $c_6 = 3^6 \cdot 2^9(9t+1)^2$, $\Delta(t) = -3^9 \cdot 2^{12}(9t+1)^2$.

$(3 - 4)$ $n =$ord$(2, \Delta(t)) = 9$. $n \neq 0$: continue to line 5.

$(5-18)$ $p=3$, $3|b_2$ so $r=0$, $h=0$. Apply $T(0,0,0,1)$.

$(19-33)$ $3|c_4$, $3^2|a_6$, $3^3|b_8$, $3^3|b_6$, and $p\neq 2$: continue to line 34. $(34-36)$ $b=0$, $c=0$, $d=-2^4(9t+1)^2$, $w=-3^3\cdot 2^4(9t+1)^2$, $x=0$.

$(37-38)$ $3|w$, $3|x$: continue to line 65.

$(65-68)$ $p=3$ so $r=3\cdot(2^4(9t+1)^2 \bmod 3)=3$. Apply $T(3,0,0,1)$; $a_1', a_3'=0$, $a_2'=3^2$, $a_6'=-3^3\Big[2^4(9t+1)^2-1\Big]$. Hence $a_6'=-3^4(3^3\cdot 2^4t^2+3\cdot 2^5t+5)$.

(69) $x_3=0$, $x_6=\frac{a_6}{3^4}=-(3^3\cdot 2^4t^2+3\cdot 2^5t+5)$.

$(70-72)$ As $3\nmid x_3^2+2^2x_6\equiv 5 \bmod 3$, $f_3(t)=$ord$(3,\Delta)-6=9-6=3$.

We have therefore shown

Lemma D.2 *For all square-free* $9t+1$, $f_3(t)=3$ *for the curve* $y^2=x^3+2^4\cdot(-3)^3(9t+1)^2$.

D.2.3 $C(t)$

Lemma D.3 *Let* $E_t: y^2=x^3+2^4\cdot(-3)^3\cdot(9t+1)^2$, $9t+1$ *square-free. Then* $C(t)=2^{f_2(t)}3^3\cdot\prod_{p|(9t+1),p\neq 2,3}p^2$, *where* $f_2(t)$ *equals* 0 *if* $t\equiv 0,2$ *mod* 4 *and* $f_2(t)$ *equals* 2 *if* $t\equiv 1$ *mod* 4. *Note* $t\not\equiv 3$ *mod* 4 *as* $9t+1$ *is square-free.*

For $p>3$, both cases have $f_p(t)=2$ if $p|9t+1$ and $f_p(t)=0$ otherwise. For $p=3$, $3\nmid(9t+1)^2$, and both cases have $f_3(t)=3$. If $t\equiv 0,2$ mod 4, then $2\nmid(9t+1)^2$, and $C(t)=2^0\cdot 3^3\cdot(9t+1)^2$. If $t\equiv 1$ mod 4, then $2^2\parallel(9t+1)^2$, and $C(t)=2^2\cdot 3^3\prod_{p|(9t+1),p\neq 2,3}p^2=3^3\cdot(9t+1)^2$. Hence

Lemma D.4 *Let* $E_t: y^2=x^3+2^4\cdot(-3)^3\cdot(9t+1)^2$, $9t+1$ *square-free. Then* $C(t)=3^3(9t+1)^2$.

D.3 $C(t)$ for the Family $y^2=x^3\pm 4(4t+2)x$

We calculate the conductors $C(t)$ for the family of elliptic curves $y^2=x^3\pm 4(4t+2)x$, where $4t+2$ is square-free.

We calculate the conductors for $y^2=x^3+4(4t+2)x$. If instead we had $y^2=x^3-4(4t+2)x$, the only differences would be in the sign of a_4, b_4, c_4 and $\Delta(t)$, and a similar argument would yield the same result.

$a_1=a_2=a_3=a_6=0$, $a_4=2^2(2t+1)$, $b_2=b_6=0$, $b_4=2^4(2t+1)$, $b_8=-2^6(2t+1)^2$, $c_4=-2^7\cdot 3(2t+1)$, $c_6=0$, $\Delta(t)=-2^{15}(2t+1)^3$.

D.3.1 $p = 2$

We apply Tate's algorithm.

(3 – 4) $n = \text{ord}(2, \Delta) = 15$, $n > 0$: skip to line 5.

(5 – 18) $p = 2$, $2|b_2$ so $r = h = 0$. Apply $T(0, 0, 0, 1)$.

(19 – 28) $2|c_4$, $2^2|a_6$, $2^3|b_8$, $2^3|b_6$: continue to line 29.

(29 – 33) $p = 2$ so $s = h = 0$. Apply $T(0, 0, 0, 1)$.

(34 – 36) $b = 0$, $c = 2(2t + 1)$, $d = 0$, $w = 2^3(2t + 1)$, $x = 2 \cdot 3(2t + 1)$.

(37 – 38) $2|w$, $2|x$: skip to line 65.

(65 – 68) $r_p = 0$, $r = 0$. Apply $T(0, 0, 0, 1)$.

(69 – 70) $x_3 = x_6 = 0$, $2|(x_3^2 + 4x_6)$: skip to line 74.

(74 – 76) $p = 2$, so $h = 0$. Apply $T(0, 0, 0, 1)$.

(77) $2^4 \nmid a_4$, therefore $f_2(t) = n - 7 = 8$.

D.3.2 $p = 3$

We again apply Tate's algorithm.

(3) $n = \text{ord}(3, \Delta(t)) = \text{ord}(3, (2t + 1)^3)$. As $4t + 2$ is square-free, $\text{ord}(3, (2t + 1)^3)$ is either 0 or 3. If $n = 0$ we are done and $f_3(t) = 0$. Else assume $3||(2t + 1)$ and $n = 3$.

(5 – 18) $p = 3$, $3|b_2$, $r = h = 0$. Apply $T(0, 0, 0, 1)$.

(19 – 23) $3|c_4$, $3^2|a_6$: continue to line 24.

(24) $3^3 \nmid b_8 = -2^6(2t + 1)^2$, therefore $f_3(t) = n - 1 = 2$.

D.3.3 $C(t)$

We calculate $C(t)$ for the curve $y^2 = x^3 \pm 4(4t + 2)x$, $4t + 2$ square-free. If $p > 3$, then $f_p = 2$ if $p|4t + 2$ and 0 otherwise. If $p = 3$ then $f_3 = 2$ if $3||(4t + 2)$ and 0 otherwise. If $p = 2$ then $f_2 = 8$. Note $2||(4t + 2)$. Therefore

Lemma D.5 *Let $E_t : y^2 = x^3 \pm 4(4t + 2)x$, $4t + 2$ square-free. Then $C(t) = 2^6(4t + 2)^2$.*

D.4 $C(t)$ for the Family $y^2 = x^3 + (t + 1)x^2 + tx$

We calculate the conductors $C(t)$ for the family of elliptic curves $y^2 = x^3 + (t + 1)x^2 + tx$, $t(t - 1)$ is square-free.

$a_1 = a_3 = a_6 = 0$, $a_2 = (2t + 1)$, $a_4 = t$, $b_2 = 2^2(t + 1)$, $b_4 = 2t$, $b_6 = 0$, $b_8 = -t^2$, $c_4 = 2^4(t^2 - t + 1)$, $c_6 = -2^5(2t^3 - 3t^3 - 3t + 2)$, $\Delta(t) = 2^4 t^2 (t - 1)^2$.

$C(t) = \prod_{p|\Delta} p^{f_p(t)}$, where for $p > 3$, $f_p = 2$ if $p|c_4(t) = 2^4(t^2 - t + 1)$, and 0 otherwise. Clearly $(\Delta(t), c_4(t)) = 2^4$, as no factors of t divide $t^2 - t + 1$, and no factor of $t - 1$ divides $t^2 - t + 1 = t(t - 1) + 1$. Therefore for $p > 3$, $f_p(t) = 1$.

D.4.1 $p = 2$

We apply Tate's algorithm.

$(3 - 4)$ $n = \text{ord}(2, \Delta(t)) = 6$, $n > 0$: skip to line 5.

$(5 - 18)$ $p = 2$, $2|b_2$ so $r = t$ mod 2, $h = 0$. Apply $T(r, 0, 0, 1)$, which has no affect if $h \equiv 0(2)$. In this case, (19) $2|c_4$: continue to (23). $2^2|a_6$: continue to (24). $2^3 \nmid b_8$, so $f_2(t) = n - 1 = 5$. Assume now $t \equiv 1(2)$. Then on line (18) we apply $T(1, 0, 0, 1)$. This gives $a_1 = 0$, $a_2 = t + 4$, $a_3 = 0$, $a_4 = 3t + 5$, $a_6 = 2t + 2$, $b_8 = 2^2(t + 4)(2t + 2) - (3t + 5)^2$. We don't need to b_2, b_4, or b_6. Note c_4, c_6 and $\Delta(t)$ are unchanged. Also, as $t \equiv 1(2)$ and $t - 1$ is square-free, $t = 4k + 3$.

$(19 - 24)$ $2|c_4$, $2^2|a_6$ (as $t = 4k + 3$), but $2^3 \nmid b_8$. $2^3|2^2(t+4)(2t+2)$, but $(3t+5)^2 = 2^2(6k+7)^2$, which is not divisible by 2^3. Hence $f_2(t) = n - 1 = 5$.

D.4.2 $p = 3$

We again apply Tate's algorithm.

(3) $n = \text{ord}(3, \Delta(t)) = \text{ord}(3, t^2(t - 1)^2)$. As $t(t - 1)$ is square-free, $n = 0$ or 2. If $t \equiv 2(3)$ then $\text{ord}(3, \Delta(t)) = 0$ and $f_3 = 0$. Hence assume $t \equiv 0$ or 1 mod 3, and $n = 2$. In particular, $3 \nmid (t + 1)$.

$(5 - 18)$ $p = 3$, $3 \nmid b_2$, $r = h = 0$. Apply $T(0, 0, 0, 1)$.

(19) $3 \nmid c_4 = 2^4(t + 1)^2 - 3 \cdot 2^4 t$. Thus $f_3(t) = 1$.

D.4.3 $C(t)$

For square-free $t(t - 1)$, $2||t(t - 1)$. As $f_2(t) = 5$ and $f_3(t)$ is the power of 3 dividing $t(t - 1)$ we've shown:

Lemma D.6 *Let $E_t : y^2 = x^3 + (t + 1)x^2 + tx$, $t(t - 1)$ square-free. Then $C(t) = 2^4 t(t - 1)$.*

D.5 $C(t)$ for the Family $y^2 = x^3 + 5x^2 + 16(30t + 1)x$

Earlier we studied $y^2 = x^3 + 5x^2 + 16tx$. For convenience in calculating the conductors, we consider the related family $y^2 = x^3 + 5x^2 + 16(30t + 1)x$. The discriminant is

$$\Delta(t) = 2^{12}\Big(30t+1\Big)^2\Big(25-64(30t+1)\Big) = 2^{12}\Delta_1^2(t)\Delta_2(t). \tag{D.3}$$

We sieve to $\Delta_1(t)\cdot\Delta_2(t)$ square-free. Note $(10, \Delta_1(t)\Delta_2(t)) = 1$.

$a_1 = a_3 = a_6 = 0$, $a_2 = 5$, $a_4 = 2^4(30t+1)$, $b_2 = 2^2\cdot 5$, $b_4 = 2^5(30t+1)$, $b_6 = 0$, $b_8 = 2^8(30t+1)^2$, $c_4 = -2^4(2^5\cdot 3^2\cdot 5t + 23) = -2^4\Big(48(30t+1)-25\Big)$.

$C(t) = \prod_{p|\Delta} p^{f_p(t)}$, where for primes greater than 3, $f_p(t) = 2$ if $p|c_4(t) = 2^4\cdot 3\cdot(6t+1)^2$, and 0 otherwise. $(\Delta(t), c_4(t)) = 2^{12}$. Clearly there are no common factors of $c_4(t)$ and $\Delta_1(t) = 30t+1$. Assume $(c_4(t), \Delta_2(t)) = d > 1$. Then

$$d|3\Big(64(30t+1)-25\Big) - 4\Big(48(30t+1)-25\Big) = 25. \tag{D.4}$$

Thus, $d|5$ but $5\nmid\Delta(t)$. Thus, for $p\geq 5$, $f_p(t) = 1$ if $p|\Delta_1(t)\Delta_2(t)$.

D.5.1 $p = 2$

We apply Tate's algorithm.

$(3-4)$ $n = \text{ord}(2, \Delta(t)) = 12$, $n > 0$: skip to line 5.

$(5-18)$ $p = 2$, $2|b_2$ so $r = 0$ and $h = 0$. Apply $T(0,0,0,1)$.

$(19-28)$ $2|c_4$, $2^2|a_6$, $2^3|b_8$, $2^3|b_6$.

$(29-33)$ $p = 2$ so $s = 1$, $h = 0$. Apply $T(0,1,0,1)$, yielding $a_1 = 2$, $a_2 = 2^2$, $a_3 = 0$, $a_4 = 2^4(30t+1)$, $a_6 = 0$, $b_2 = 2^2\cdot 5$, $b_4 = 2^5(30t+1)$, $b_6 = 0$, $b_8 = 2^8(30t+1)^2$, and the other quantities are unchanged.

$(34-36)$ $b = 2$, $c = 2^2(30t+1)$, $d = 0$, $w = 4(2^2(30t+1)-1)c^2$, $x = 4(90t+2)$.

(37) $2|w$: skip to (38).

(38) $2|x$: skip to (65).

$(65-68)$ $p = 2$ so $rp = -2$, $r = 0$. Apply $T(0,0,0,1)$.

(69) $x_3 = 0$, $x_6 = 0$.

$(70-72)$ $2|(x_3^2 + 4x_6)$: skip to (73).

$(73-76)$ $p = 2$ so $t = 0$, apply $T(0,0,0,1)$.

$(77-80)$ $2^4|a_4$ and $2^6|a_6$: apply $T(0,0,0,2)$ and restart the algorithm. This changes $\Delta(t)$ to $\Delta'(t) = 2^{-12}\Delta(t)$. Before $n = \text{ord}(2,\Delta(t)) = 12$; now $n = \text{ord}(2, \Delta'(t)) = 0$. Thus by line (4) we find $f_2(t) = 0$.

D.5.2 $p = 3$

We apply Tate's algorithm, assuming $\Delta_1(t)\Delta_2(t)$ is square-free.

$(3-4)$ $n = \text{ord}(3, \Delta(t)) = 1$, $n > 0$: skip to line 5.

$(5-18)$ $p = 3$, $3 \nmid b_2$: $r = 2$ and $h = 0$. Apply $T(2, 0, 0, 1)$. Now $a_1 = a_3 = 0$, $a_2 = 11$, $a_4 = 2^4 \cdot 3(10t+1)$, $a_6 = 2^2 \cdot 3 \cdot 5(16t+1)(6t+1)$, $b_2 = 2^2 \cdot 11$, $b_4 = 2^5 \cdot 3(10t+1)$, $b_6 = 2^4 \cdot 3 \cdot 5(16t+1)$, $b_8 = -2^4 \cdot 3(4800t^2 + 80t - 1)$, and the other quantities are unchanged.

(19) $3 \nmid c_4$. Hence $f_3(t) = 1$.

D.5.3 $C(t)$

Lemma D.7 *Let $E_t : y^2 = x^3 + 5x^2 + 16(30t+1)x$, $\Big(30t+1\Big)\Big(25 - 64(30t+1)\Big)$ square-free. Then $C(t) = \Big(30t+1\Big)\Big(64(30t+1) - 25\Big)$.*

D.6 $C(t)$ for the Family $y^2 = x^3 + x^2 + 2t + 1$

We calculate the conductors $C(t)$ for the family of elliptic curves $y^2 = x^3 + x^2 + 2t + 1$, $(2t+1)$ $(54t+31)$ square-free.

$a_1 = a_3 = a_4 = 0$, $a_2 = 1$, $a_6 = 2t+1$, $b_2 = 2^2$, $b_4 = 0$, $b_6 = 2^2(2t+1)$, $b_8 = 2^2(2t+1)$, $c_4 = 2^4$, $c_6 = -2^5(54t+29)$, $\Delta(t) = -2^4(2t+1)(54t+31)$.

$C(t) = \prod_{p|\Delta} p^{f_p(t)}$, where for $p > 3$, $f_p(t) = 2$ if $p|c_4(t) = 2^4$, and 0 otherwise. Clearly $(\Delta(t), c_4(t)) = 2^4$. Therefore, for $p > 3$, $f_p(t) = 1$.

D.6.1 $p = 2$

We apply Tate's algorithm.

$(3-4)$ $n = \text{ord}(2, \Delta) = 4$, $n > 0$: skip to line 5.

$(5-18)$ $p = 2$, $2|b_2$ so $r = 0$, $h = 1$. Apply $T(0, 0, 1, 1)$. This gives $a_1 = 0$, $a_2 = 1$, $a_3 = 2$, $a_4 = 0$, $a_6 = 2t$, $b_8 = 2^2(2t+1)$. We don't need b_2, b_4, or b_6. Note c_4, c_6 and $\Delta(t)$ are unchanged.

$(19-24)$ $2|c_4$. $2^2 \nmid a_6$ if t is odd, in which case we find $f_2(t) = n = 4$. If t is even, $2^2|a_6$ but $2^3 \nmid b_8$. Therefore $f_2(t) = n - 1 = 3$.

D.6.2 $p = 3$

We again apply Tate's algorithm.

(3) $n = \text{ord}(3, \Delta(t)) = \text{ord}(3, 2t+1)$. Thus $n = 0$ or 2. If $t \equiv 0$ or 2 mod (3) then $\text{ord}(3, \Delta(t)) = 0$ and $f_3(t) = 0$. Hence assume $t \equiv 1$ mod 3, and $n = 1$.

$(5 - 18)$ $p = 3$, $3 \nmid b_2$, $r = h = 0$. Apply $T(0, 0, 0, 1)$.

(19) $3 \nmid c_4 = 2^4 t$. Thus $f_3(t) = 1$.

D.6.3 $C(t)$

Lemma D.8 *Let* $E_t : y^2 = x^3 + x^2 + 2t + 1$, $(2t+1)(54t+31)$ *square-free. Then* $C(t) = 2^4(2t+1)(54t+31)$ *if* t *is odd and* $2^3(2t+1)(54t+31)$ *if* t *is even.*

D.7 $C(t)$ for the Family $y^2 = x^3 + x^2 + 12t + 1$

We calculate the conductors $C(t)$ for the family of elliptic curves $y^2 = x^3 + x^2 + 12t + 1$, $(12t + 1)$ $(324t + 31)$ square-free.

$a_1 = a_3 = a_4 = 0$, $a_2 = 1$, $a_6 = 12t + 1$, $b_2 = 2^2$, $b_4 = 0$, $b_6 = 2^2(12t + 1)$, $b_8 = 2^2(12t + 1)$, $c_4 = 2^4$, $c_6 = -2^5(324t + 29)$, $\Delta(t) = -2^4(12t + 1)(324t + 31)^2$. Note $12 = 2^2 \cdot 3$ and $324 = 2^2 \cdot 3^4$.

$C(t) = \prod_{p|\Delta} p^{f_p(t)}$, where for $p > 3$, $f_p = 2$ if $p|c_4(t) = 2^4$, and 0 otherwise. Clearly $(\Delta(t), c_4(t)) = 2^4$. Therefore, for primes greater than 3, $f_p(t) = 1$.

D.7.1 $p = 2$

We apply Tate's algorithm.

$(3 - 4)$ $n = \text{ord}(2, \Delta(t)) = 4$, $n > 0$: skip to line 5.

$(5 - 18)$ $p = 2$, $2|b_2$ so $r = 0$, $h = 1$. Apply $T(0, 0, 1, 1)$. This gives $a_1 = 0$, $a_2 = 1$, $a_3 = 2$, $a_4 = 0$, $a_6 = 12t$, $b_8 = 2^2(12t+1)$. We don't need b_2, b_4, or b_6. Note c_4, c_6 and $\Delta(t)$ are unchanged.

$(19 - 24)$ $2|c_4$, $2^2|a_6$ but $2^3 \nmid b_8$. Therefore $f_2(t) = n - 1 = 3$.

D.7.2 $p = 3$

As $\Delta(t) \equiv 1 \cdot 31 \equiv 1$ mod 3, $3 \nmid \Delta(t)$ and $f_3(t) = 0$.

D.7.3 $C(t)$

Lemma D.9 *Let* $E_t : y^2 = x^3 + x^2 + 12t + 1$, $(12t + 1)(324t + 31)$ *square-free. Then* $C(t) = 2^3(12t + 1)(324t + 31)$.

D.8 $y^2 = x^3 + (12t+1)x^2 - (12t+1+3)x + 1$

We calculate the conductors $C(t)$ for the family of elliptic curves $y^2 = x^3 + (12t+1)x^2 - (12t+4)x + 1$, $144t^2 + 60t + 13$ square-free. We have sent t to $12t$ in Washington's family to simplify the calculations.

$a_1 = a_3 = 0$, $a_2 = 12t+1$, $a_4 = -(12t+4)$, $a_6 = 1$, $b_2 = 2^2(12t+1)$, $b_4 = -2^2(6t+2)$, $b_6 = 2^2$, $b_8 = -2^2 \cdot 3(12t^2+4t+1)$, $c_4 = 2^4(144t^2+60t+13)$, $c_6 = 2^5(24t+5)(144t^2+60t+13)$, $\Delta(t) = 2^4(144t^2+60t+13)^2$.

$C(t) = \prod_{p|\Delta} p^{f_p(t)}$, where for $p > 3$, $f_p = 2$ if $p|c_4(t) = 2^4(144t^2+60t+13)$, and 0 otherwise. Clearly $(\Delta(t), c_4(t)) = 2^4(144t^2+60t+13)$. Therefore, for $p > 3$, $f_p = 2$.

D.8.1 $p = 2$

We apply Tate's algorithm.

$(3-4)$ $n = \text{ord}(2, \Delta(t)) = 4$, $n > 0$: skip to line 5.

$(5-18)$ $p = 2$, $2|b_2$ so $r = 0$, $h = 1$. Apply $T(0,0,1,1)$. This gives $a_1 = 0$, $a_2 = 12t+1$, $a_3 = 2$, $a_4 = -2^2(3t+1)$, $a_6 = 0$, $b_8 = -2^2 \cdot 3(12t^2+4t+1)$. We don't need b_2, b_4, or b_6. Note c_4, c_6 and $\Delta(t)$ are unchanged.

$(19-24)$ $2|c_4$, $2^2|a_6$, $2^3 \nmid b_8$. Therefore $f_2(t) = n - 1 = 3$.

D.8.2 $p = 3$

As $\text{ord}(3, \Delta(t)) = \text{ord}(3, 36t^2 + 30t + 13) = 0$, $f_3(t) = 0$.

D.8.3 $C(t)$

Lemma D.10 *Let* $E_t : y^2 = x^3 + (6t+1)x^2 - (6t+4)x + 1$, $144t^2 + 60t + 13$ *square-free. Then* $C(t) = 2^3(144t^2 + 60t + 13)^2$.

D.9 $C(t)$ for the Family $y^2 = x^3 + (6t+1)x^2 + 1$

Earlier we studied the family $y^2 = x^3 + tx^2 + 1$. For convenience in calculating the conductors, we consider the related family $y^2 = x^3 + (6t+1)x^2 + 1$ with discriminant

$$\Delta(t) = -2^4\Big(4(6t+1)^3 + 27\Big) = -\Delta_1(t)\Delta_2(t). \tag{D.5}$$

We sieve to $\Delta_2(t)$ square-free. Note $(6, \Delta_2(t)) = 1$.

$a_1 = a_4 = a_6 = 0$, $a_2 = 6t+1$, $a_3 = 2$, $b_2 = 2^2(6t+1)$, $b_4 = 0$, $b_6 = 2^2$, $b_8 = 2^2(6t+1)$, $c_4 = 2^4(6t+1)^2$.

$C(t) = \prod_{p|\Delta} p^{f_p(t)}$, where for $p > 3$, $f_p(t) = 2$ if $p|c_4(t) = 2^4(6t+1)^2$, and 0 otherwise. Clearly $(\Delta(t), c_4(t)) = 2^4$, as no factors of $6t+1$ divide $\Delta_2(t)$. Therefore for $p > 3$, $f_p(t) = 1$.

D.9.1 $p = 2$

We apply Tate's algorithm.

$(3-4)$ $n = \text{ord}(2, \Delta(t)) = 4$, $n > 0$: skip to line 5.

$(5-18)$ $p = 2$, $2|b_2$ so $r = 0$ and $h = 1$. Apply $T(0,0,1,1)$. Now $a_1 = a_4 = a_6 = 0$, $a_2 = 6t+1$, $a_3 = 2$, $b_2 = 2^2(6t+1)$, $b_4 = 0$, $b_6 = 2^2$, $b_8 = 2^2(6t+1)$, and the other quantities are unchanged.

$(19-24)$ $2|c_4$, $2^2|a_6$, but $2^3 \nmid b_8$. Hence $f_2(t) = n - 1 = 3$.

D.9.2 $p = 3$

As $(3, \Delta(t)) = 1$, $f_3(t) = 0$. This is one reason we changed from t to $6t+1$.

D.9.3 $C(t)$

Lemma D.11 *Let $E_t : y^2 = x^3 + (6t+1)x^2 + 1$, $4(6t+1)^3 + 27$ square-free. Then $C(t) = 2^2\Big(4(6t+1)^3 + 27\Big)$.*

D.10 $C(t)$ for the Family $y^2 = x^3 - (6t+1)^2x + (6t+1)^2$

Earlier we studied the family $y^2 = x^3 - t^2x + t^2$. For convenience in calculating the conductors, we consider the related family $y^2 = x^3 - (6t+1)^2x + (6t+1)^2$ with discriminant

$$\Delta(t) = 2^4\Big(6t+1\Big)^4\Big(4(6t+1)^2 - 27\Big) = 2^4\Delta_1^4(t)\Delta_2(t). \tag{D.6}$$

We sieve to $\Delta_1(t) \cdot \Delta_2(t)$ square-free. Note $(6, \Delta_1(t)\Delta_2(t)) = 1$.

$a_1 = a_2 = a_3 = 0$, $a_4 = -(6t+1)^2$, $a_6 = (6t+1)^2$, $b_2 = 0$, $b_4 = -2(6t+1)^2$, $b_6 = 2^2(6t+1)^2$, $b_8 = (6t+1)^4$, $c_4 = 2^4 \cdot 3 \cdot (6t+1)^2$.

$C(t) = \prod_{p|\Delta} p^{f_p}$, where for $p > 3$, $f_p(t) = 2$ if $p|c_4(t) = 2^4 \cdot 3 \cdot (6t+1)^2$, and 0 otherwise. Clearly $(\Delta(t), c_4(t)) = 2^4(6t+1)^2$. Thus, for $p > 3$, $f_p(t) = 1$ if $p|\Delta_2(t)$ and $f_p(t) = 2$ if $p|\Delta_1(t)$.

D.10.1 $p = 2$

We apply Tate's algorithm.

$(3-4)$ $n = \text{ord}(2, \Delta(t)) = 4$, $n > 0$: skip to line 5.

$(5-18)$ $p = 2$, $2|b_2$ so $r = 1$ and $h = 1$. Apply $T(1,0,1,1)$. Now $a_1 = a_6 = 0$, $a_2 = 3$, $a_3 = 2$, $a_4 = -2(18t^2+6t-1)$, $b_2 = 2^2 \cdot 3$, $b_4 = -2^2(18t^2+6t-1)$, $b_6 = 2^2$, $b_8 = 2^3(162t^4+108t^3-6t-1)$, and the other quantities are unchanged.

$(19-25)$ $2|c_4$, $2^2|a_6$, $2^3|b_8$, but $2^3 \nmid b_6$. Hence $f_2(t) = n - 2 = 2$.

D.10.2 $p = 3$

As $(3, \Delta(t)) = 1$, $f_3(t) = 0$. This is one reason we changed from t to $6t+1$.

D.10.3 $C(t)$

Lemma D.12 *Let* $E_t : y^2 = x^3 - (6t+1)^2 x + (6t+1)^2$, $\Big(6t+1\Big)\Big(4(6t+1)^2 - 27\Big)$ *square-free. Then* $C(t) = 2^2\Big(6t+1\Big)^2\Big(4(6t+1)^2 - 27\Big)$.

D.11 $C(t)$ for the Family $y^2 = x^3 - (6t+1)^2 x + (6t+1)^4$

Earlier we studied the family $y^2 = x^3 - t^2 x + t^4$. For convenience in calculating the conductors, we consider the related family $y^2 = x^3 - (6t+1)^2 x + (6t+1)^4$ with discriminant

$$\Delta(t) = -2^4\Big(6t+1\Big)^6\Big(27(6t+1)^2 - 4\Big) = -2^4\Delta_1^6(t)\Delta_2(t). \tag{D.7}$$

We sieve to $\Delta_1(t) \cdot \Delta_2(t)$ square-free. Note $(6, \Delta_1(t)\Delta_2(t)) = 1$.

$a_1 = a_2 = a_3 = 0$, $a_4 = -(6t+1)$, $a_6 = (6t+1)^4$, $b_2 = 0$, $b_4 = -2(6t+1)^2$, $b_6 = 2^2(6t+1)^4$, $b_8 = (6t+1)^4$, $c_4 = 2^4 \cdot 3 \cdot (6t+1)^2$.

$C(t) = \prod_{p|\Delta} p^{f_p(t)}$, where for $p > 3$, $f_p(t) = 2$ if $p|c_4(t) = 2^4 \cdot 3 \cdot (6t+1)^2$, and 0 otherwise. Clearly $(\Delta(t), c_4(t)) = 2^4(6t+1)^2$. Thus, for $p > 3$, $f_p(t) = 1$ if $p|\Delta_2(t)$ and $f_p(t) = 2$ if $p|\Delta_1(t)$.

D.11.1 $p = 2$

We apply Tate's algorithm.

$(3-4)$ $n = \text{ord}(2, \Delta(t)) = 4$, $n > 0$: skip to line 5.

$(5-18)$ $p=2$, $2|b_2$ so $r=1$ and $h=1$. Apply $T(1,0,1,1)$. Now $a_1=0$, $a_2=3$, $a_3=2$, $a_4=-2(18t^2+6t-1)$, $a_6=2^2\cdot 3t(3t+1)(6t+1)$, $b_2=2^2\cdot 3$, $b_4=-2^2(18t^2+6t-1)$, $b_6=2^2(1296t^4+864t^3+180t^2+12t+1)$, $b_8=2^3(1782t^4+1188t^3+270t^2+24t+1)$, and the other quantities are unchanged.

$(19-25)$ $2|c_4$, $2^2|a_6$, $2^3|b_8$, but $2^3\nmid b_6$. Hence $f_2(t)=n-2=2$.

D.11.2 $p=3$

As $(3,\Delta(t))=1$, $f_3(t)=0$. This is one reason we changed from t to $6t+1$.

D.11.3 $C(t)$

Lemma D.13 *Let $E_t : y^2=x^3-(6t+1)^2x+(6t+1)^4$, $\Big(6t+1\Big)\Big(27(6t+1)^2-4\Big)$ square-free. Then $C(t)=2^2\Big(6t+1\Big)^2\Big(27(6t+1)^2-4\Big)$.*

D.12 $C(t)$ for the Family $y^2=x^3+5x^2-16(4-x)(270t+1)^2$

$$\begin{aligned} c_4(t) &= 2^4\Big(48(270t+1)^2+25\Big)\\ \Delta(t) &= 2^{12}(270t+1)^2\Big(64(270t+1)^4-767(270t+1)^2-125\Big)\\ D(t) &= (270t+1)\Big(64(270t+1)^4-767(270t+1)^2-125\Big) \end{aligned} \tag{D.8}$$

We sieve to $\frac{D(t)}{36}$ square-free. $a_1=a_2=a_3=0$, $a_4=-(6t+1)$, $a_6=(6t+1)^4$, $b_2=0$, $b_4=-2(6t+1)^2$, $b_6=2^2(6t+1)^4$, $b_8=(6t+1)^4$, $c_4=2^4\cdot 3\cdot(6t+1)^2$.

$C(t)=\prod_{p|\Delta}p^{f_p}$, where for $p>3$, $f_p(t)=2$ if $p|c_4(t)=2^4\cdot 3\cdot(6t+1)^2$, and 0 otherwise. As $(\Delta(t),c_4(t))=2^4$, for $p>3$, $f_p(t)=1$.

D.12.1 $p=2$

We apply Tate's algorithm.

$(3-4)$ $n=\text{ord}(2,\Delta(t))=14$, $n>0$: skip to line 5.

$(5-18)$ $2|b_2$: $r=0$, $h=0$, apply $T(0,0,0,1)$.

$(19-28)$ $2|c_4$, $2^2|a_6$, $2^3|b_8$, $2^3|b_6$.

$(29-33)$ $s=1$, $h=0$: apply $T(0,1,0,1)$.

(34 − 36) $b = 2$, $c = -291600t^2 - 2160t - 4$, $d = 583200t^2 + 4320t + 8$, $w = 27d^2 - b^2 + c^2 + 4b^3d - 18bcd + 4c^3$, $x = 3c - b^2$.

(37 − 38) $2|w$, $2|x$: skip to 66.

(66 − 68) $rp = -2$, $r = 0$: apply $T(0, 0, 0, 1)$.

(69 − 70) $x_3 = 0$, $x_6 = 291600t^2 + 2160t + 4$, $2|x_3^2 + 4x_6$: skip to 74.

(74 − 76) $h = x_6$, $h = 0$: apply $T(0, 0, 0, 1)$.

(77 − 80) $2^4|a_4$, $2^6|a_6$: apply $T(0, 0, 0, 2)$ and restart.

(3 − 4) $n = \text{ord}(2, \Delta(t)) = 2$, $n > 0$: skip to line 5.

(5 − 18) $b_2 = 5$: $2 \nmid b_2$ so $r = 0$, $h = 1$. Apply $T(0, 0, 1, 1)$.

(19) $2 \nmid c_4 = 3499200t^2 + 25920t + 73$: $f_2(t) = 1$.

D.12.2 $p = 3$

(3 − 4) $n = \text{ord}(3, \Delta(t)) = 2$, $n > 0$: skip to line 5.

(5 − 18) $3 \nmid b_2$: $r = 1$, $h = 0$: apply $T(1, 0, 0, 1)$.

(19) $3 \nmid c_4 = 55987200t^2 + 414720t + 1168$: $f_3(t) = 1$.

D.12.3 $C(t)$

Lemma D.14 *Let* $E_t : y^2 = x^3 + 5x^2 - 16(4 - x)(270t + 1)^2$. *Let* $D(t) = (270t + 1) \cdot \Big(64(270t + 1)^4 - 767(270t + 1)^2 - 125\Big)$. *For* $\frac{D(t)}{36}$ *square-free,* $C(t) = \frac{|D(t)|}{6}$.

D.13 $C(t)$ for the Family $y^2 = x^3 + 41x^2 + 184x + 144 - 16\tau^2(t)x$

$y^2 = x^3 + 41x^2 + 184x + 144 - 16\tau^2(t)x = f_\tau(x)$, $\tau = 2^2 3^3 65033t + 1$.

$$\begin{aligned}
\Delta(\tau) &= 2^{12}(64\tau^6 - 527\tau^4 - 19913\tau^2 + 44100 = 2^{12}D(\tau) \\
&= 2^{14}3^2\frac{D(\tau)}{36} = 2^{14}3^2 D_1(t) \\
c_4(\tau) &= 2^4(48\tau^2 + 1129) \\
&= 2^4(2^8 3^7 65033^2 t^2 + 2^7 3^4 65033t + 11 \cdot 107) = 2^4 c(\tau) \\
\tau &= 2^2 3^3 65033t + 1. \qquad \text{(D.1)}
\end{aligned}$$

We sieve to $D'(t) = \frac{D(\tau)}{36}$ square-free. $a_1 = a_2 = a_3 = 0$, $a_4 = -(6t + 1)$, $a_6 = (6t + 1)^4$, $b_2 = 0$, $b_4 = -2(6t + 1)^2$, $b_6 = 2^2(6t + 1)^4$, $b_8 = (6t + 1)^4$, $c_4 = 2^4 \cdot 3 \cdot (6t + 1)^2$.

$C(t) = \prod_{p|\Delta} p^{f_p(t)}$, where for $p > 3$, $f_p = 2$ if $p|c_4(t) = 2^4 \cdot 3 \cdot (6t+1)^2$, and 0 otherwise. As $(\Delta(t), c_4(t)) = 2^4$, for $p > 3$, $f_p(t) = 1$.

D.13.1 $p = 2$

We apply Tate's algorithm.

$(3-4)$ $n = \mathrm{ord}(2, \Delta(t)) = 14$, $n > 0$: skip to line 5.

$(5-18)$ $2|b_2$: $r = 0$, $h = 0$: apply $T(0,0,0,1)$.

$(19-28)$ $2|c_4$, $2^2|a_6 = 2^2 3^2$, $2^3|b_8 = 2^9 3^2$, $2^3|b_6 = 2^6 3^2$.

$(29-33)$ $s = 1$, $h = 0$: apply $T(0,1,0,1)$. $a_2 = 2^3 5$, $a_3 = 0$, $a_4 = 2^3 3(32886967508064t^2 + 9364752t - 7)$, $a_6 = 2^4 3^2$.

$(34-36)$ $b = 2^2 5$, $c = 2 \cdot 3(32886967508064t^2 + 9364752t - 7)$, $d = 2 \cdot 3^2$, $w = 27d^2 - b^2 + c^2 + 4b^3 d - 18bcd + 4c^3$, $x = 3c - b^2$.

$(37-38)$ $2|w$, $2|x$: skip to 66.

$(66-68)$ $rp = -2^2 5$, $r = 0$: apply $T(0,0,0,1)$.

$(69-70)$ $x_3 = 0$, $x_6 = 3^2$, $2|x_3^2 + 4x_6$: skip to 74.

$(74-76)$ $h = x_6 = 9$, $h = -4$: apply $T(0,0,-4,1)$. $a_4 = 2^4(49330451262096t^2 + 14047128t - 11)$, $a_6 = 2^7$.

$(77-80)$ $2^4|a_4$, $2^6|a_6$: apply $T(0,0,0,2)$ and restart. The new discriminant is $\Delta(t) = 2^2 3^2(\text{even}t^6 + \cdots + \text{even}t + 659)$. $a_3 = -1$, $a_4 = -49330451262096t^2 - 14047128t + 11$, $b_2 = 41$.

$(3-4)$ $n = \mathrm{ord}(2, \Delta(t)) = 2$, $n > 0$: skip to line 5.

$(5-18)$ $2 \nmid b_2$ so $r = 1$, $h = 0$. Apply $T(1,0,0,1)$. $c_4(t) = 2^8 3^7 65033^2 t^2 + 2^7 3^4 65033t + 1177$.

(19) $2 \nmid c_4$ so $f_2(t) = 1$.

D.13.2 $p = 3$

$(3-4)$ $n = \mathrm{ord}(3, \Delta(t)) = 2$, $n > 0$: skip to line 5.

$(5-18)$ $3 \nmid b_2 = 2^2 41$: Mod 3, $b_2 \equiv 2$ and $b_4 \equiv 0$. $r = 0$, $h = 0$ (as $a_3 == 0$): apply $T(0,0,0,1)$.

(19) $3 \nmid c_4 \equiv 1 \bmod 3$: $f_3(t) = 1$.

D.13.3 $C(t)$

Lemma D.15 *Let* $E_t : y^2 = x^3 + 41x^2 + 184x + 144 - 16\tau^2(t)x$, $\tau(t) = 2^2 3^3 65033t + 1$. *Let* $D(\tau) = 64\tau^6 - 527\tau^4 - 19913\tau^2 + 44100$. *For* $D_1(t) = \frac{D(\tau)}{36}$ *square-free,* $C(t) = \frac{|D(\tau)|}{6} = 6|D_1(t)|$.

E Handling the Error Terms in the n-Level Densities

Following Rudnick-Sarnak [RS] and Rubenstein [Ru], we handle the error terms in the $(n+1)$-level density, assuming we are able to prove the k-level density theorem ($k \le n$) with error terms. Actually, all we need to show is we can handle the error terms when we sum over all tuples of zeros; simple combinatorics yield the result for tuples of distinct zeros. By the Explicit Formula (Theorem A.29)

$$\sum_{j_i} F_i\Big(\frac{\log N_E}{2\pi}\gamma_E^{(j_i)}\Big) \quad = \quad \mathbf{Good}_i + O\Big((\log N_E)^{-\frac{1}{2}}\Big), \tag{E.1}$$

where $\mathbf{Good}_i$ is the good part of the Explicit Formula, involving $\widehat{F}(0)$, $F(0)$, and sums of $a_E(p)$ and $a_E^2(p)$ for primes $p > \log N$.

Multiplying and summing over i yields

$$\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\prod_{i=1}^{n+1}\left[\sum_{j_i} F_i\Big(\frac{\log N_E}{2\pi}\gamma_E^{(j_i)}\Big) + O\Big((\log N_E)^{-\frac{1}{2}}\Big)\right] \quad = \quad \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\prod_{i=1}^{n+1}\mathbf{Good}_i. \tag{E.2}$$

We proceed by Strong Induction. When $n = 1$, this is the 1-level density, and clearly the Error Term is manageable. Assume now we are able to prove the modified k-level density theorem ($k \le n$) with error terms (ie, the k-level density before we take into account the combinatorics to ensure $j_i \neq \pm j_k$). Multiplying out the LHS yields terms like

$$O\left[\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}(\log N_E)^{-\frac{n+1-k}{2}}\prod_{m=1}^{k}\sum_{j_{m_i}} F_i\Big(\frac{\log N_E}{2\pi}\gamma_E^{(j_{m_i})}\Big)\right]. \tag{E.3}$$

If each function F_i were positive, we could insert absolute values and move $\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}$ past the $\log^{-\frac{n+1-k}{2}} N_E$ factor, as $\log N_E \ll \log N$. The product over m would be a k-level density, which we know is finite as $k \le n$. Hence there is no contribution from this term, and there are only finitely many such terms (trivially at most 2^{n+1}).

If F_i is not positive, we increase the above by replacing F_i with a positive function g_i such that g_i is an even Schwartz function whose Fourier Transform is supported in the same interval as that of F_i and $g_i(x) \geq |F_i(x)|$. As the g_i satisfy the necessary conditions, we may apply the k-level density Theorem to the g_i's. To see that such functions exist, see Rubenstein [Ru], pages $40 - 41$ or Rudnick-Sarnak [RS], pages $302 - 304$.

We have shown:

Theorem E.1 (Handling the Error Terms) *If we are able to do the k-level density calculations for $k \leq n$, then we may ignore the error terms in the $(n+1)$-level density.*

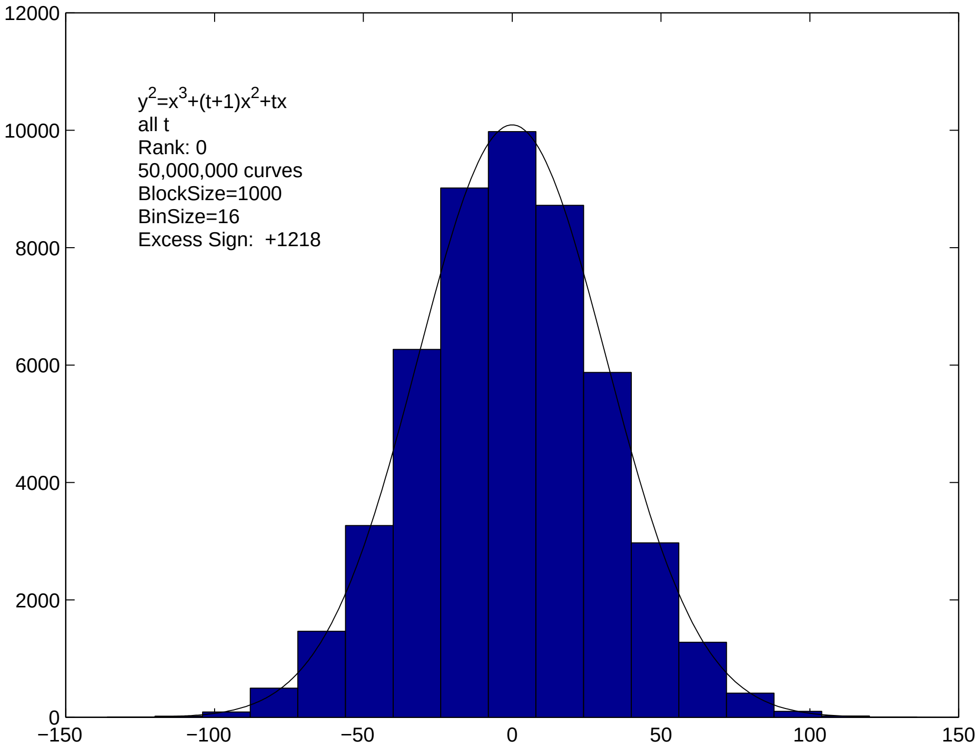
Note: the error need not be $O(\log^{-\frac{1}{2}} N)$; $o(N)$ also works.

F Variation of Sign in One-Parameter Families

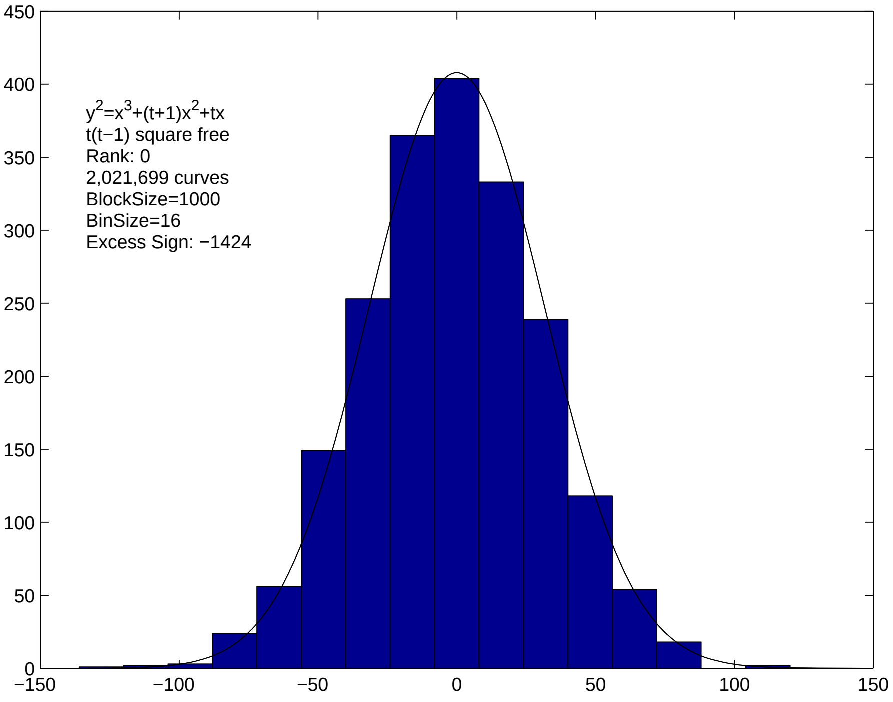
For his junior thesis, Atul Pokharel investigated the Restricted Sign Conjecture by studying the distribution of signs in one-parameter families. A representative family is included below. For N curves, the excess of positive to negative signs in intervals of 1000 was computed, for a total of $\frac{N}{1000}$ blocks. If the signs are randomly distributed, one would expect a histogram bin plot to reveal a Gaussian structure, with mean 0 and standard deviation $\sqrt{1000}$. Note this is a far stronger assumption than equidistribution of sign.

This was tested for many families; further, as in this thesis we sieve to $D(t)$ square-free, the same calculation was performed for the sub-families with $D(t)$ square-free. Restricting t did not seem to change the shape of the observed data. A more sensitive analysis is currently underway.

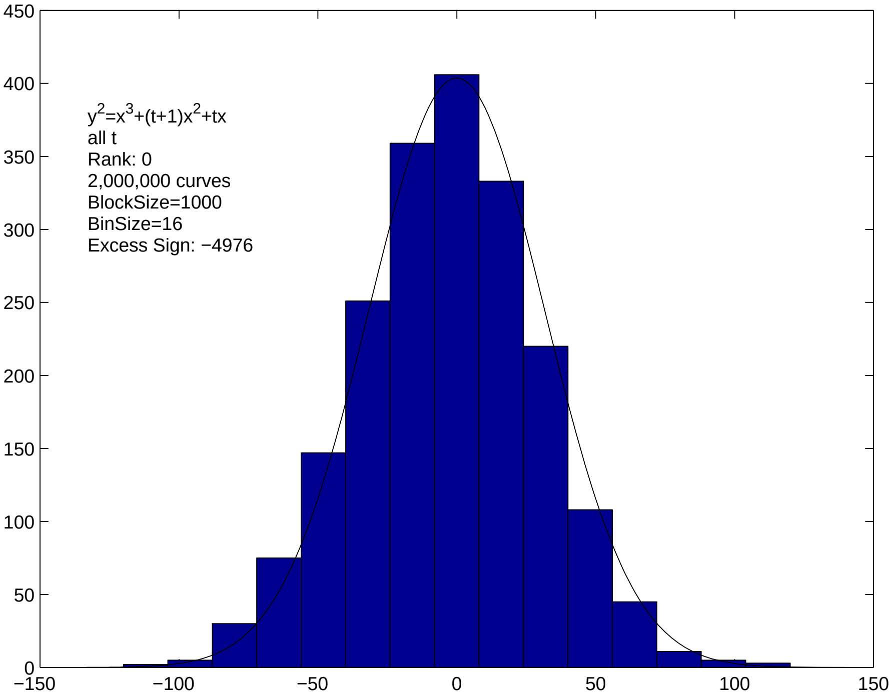
For the family $y^2 = x^3 + (t+1)x^2 + tx$, we sieve to $D(t) = t(t-1)$ square-free. Approximately 32% of t give $D(t)$ square-free. First, the sign of E_t was computed for $t \in [2, 5 \cdot 10^7]$. Histogram plots were prepared without restricting to $D(t)$. Restricting to $D(t)$ square-free requires evaluating $\mu(t)\mu(t-1)$; as this was lengthy (and this is a preliminary verification), we contented ourselves with checking the first $2 \cdot 10^6$ square-free $D(t)$.



Histogram plot: All $t \in [2, 5 \cdot 10^7]$



Histogram plot: $D(t)$ square-free, first $2 \cdot 10^6$ such t.



Histogram plot: All $t \in [2, 2 \cdot 10^6]$.

The observed behavior agrees with the predicted behavior. Note as the number of curves increase (comparing the plot of $5 \cdot 10^7$ points to $2 \cdot 10^6$ points), the fit to the Gaussian improves.

References

[Al] Alfhors, *Complex Analysis*, McGraw-Hill, Inc., New York, 1966.

[BEW] B. Berndt, R. Evans and K. Williams, *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, vol. **21**, Wiley-Interscience Publications, John Wiley & Sons, Inc., New York, 1998.

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

[BS] B. Birch and N. Stephens, *The parity of the rank of the Mordell-Weil group*, Topology **5**, 1966, 295 – 299.

[BSD1] B. Birch and H. Swinnerton-Dyer, *Notes on elliptic curves. I*, J. reine angew. Math. **212**, 1963, 7 – 25.

[BSD2] B. Birch and H. Swinnerton-Dyer, *Notes on elliptic curves. II*, J. reine angew. Math. **218**, 1965, 79 – 108.

[BCDT] C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the modularity of elliptic curves over* $\boldsymbol{Q}$*: wild* 3*-adic exercises*, J. Amer. Math. Soc. **14**, no. 4, 2001, 843 – 939.

[BFFMPW] T. Brody, J. Flores, J. French, P. Mello, A. Pandey, S. Wong, *Random-matrix physics: spectrum and strength fluctuations*, Rev. Mod. Phys. vol. **53**, no. 3, July 1981, 385 – 479.

[Br] A. Brumer, *The average rank of elliptic curves I*, Invent. Math. **109**, 1992, 445 – 472.

[BHB3] A. Brumer and R. Heath-Brown, *The average rank of elliptic curves III*, preprint.

[BHB5] A. Brumer and R. Heath-Brown, *The average rank of elliptic curves V*, preprint.

[BM] A. Brumer and O. McGuinness, *The behaviour of the Mordell-Weil group of elliptic curves*, Bull. AMS **23**, 1991, 375 – 382.

[CW] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnterton-Dyer*, Invent. Math. **39**, 1977, 43 – 67.

[Cr] Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press, 1992.

[Da] H. Davenport, *Multiplicative Number Theory, 2nd edition*, Graduate Texts in Mathematics **74**, Springer-Verlag, New York, 1980, revised by H. Montgomery.

[De] P. Deligne, *La conjecture de Weil. II* Inst. Hautes Études Sci. Publ. Math. **52**, 1980, 137−252.

[Di] F. Diamond, *On deformation rings and Hecke rings*, Ann. Math. **144**, 1996, 137 − 166.

[Fe1] S. Fermigier, *Zéros des fonctions L de courbes elliptiques*, Exper. Math. **1**, 1992, 167 − 173.

[Fe2] S. Fermigier, *Étude expérimentale du rang de familles de courbes elliptiques sur* $\mathbb{Q}$, Exper. Math. **5**, 1996, 119 − 130.

[Fo] G. Folland, *Real Analysis: Modern Techniques and their Applications*, Wiley-Interscience Publications, John Wiley & Sons, New York, 1984.

[FNT] E. Fouvry, M. Nair and G. Tenenbaum, *L'ensemble exceptionnel dans la conjecture de Szpiro*, Bull. Soc. Math. France **120**, 1992, 485 − 506.

[FP] E. Fouvrey and J. Pomykala, *Rang des courbes elliptiques et sommes d'exponentelles*, Monat. Math. **116**, 1993, 111 − 125.

[GM] F. Gouvéa and B. Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc. **4**, 1991, 45 − 65.

[Go] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Number Theory (Proc. Conf. in Carbondale, 1979), Lecture Notes in Math. **751**, Springer-Verlag, 1979, 108 − 118.

[Gr] Granville, *ABC Allows Us to Count Squarefrees*, International Mathematics Research Notices **19**, 1998, 991 − 1009.

[GH] Goldfeld and Hoffstein, *On The Number Of Fourier Coefficients That Determine A Modular Form*, Contemporary Mathematics **143**, 1993, 385 − 393.

[HW] G. Hardy and E. Wright, *An Introduction to the Theory of Numbers*, fifth edition, Oxford Science Publications, Clarendon Press, Oxford, 1995.

[Hej] D. Hejhal, *On the triple correlation of zeros of the zeta function*, Internat. Math. Res. Notices 1994, no. 7, 294 − 302.

[Hel] H. Helfgott, *Average root numbers in families of elliptic curves and the average of the Moebius function on integers represented by a polynomial*, preprint.

[Ho] C. Hooley, *Applications of Sieve Methods to the Theory of Numbers*, Cambridge University Press, Cambridge, 1976.

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics **97**, Springer-Verlag, New York, 1972.

[Iw] H. Iwaniec, *Topics in Classical Automorphic Forms*, American Mathematical Society, Graduate Studies in Mathematics, vol. **17**, Providence, 1997.

[ILS] H. Iwaniec, W. Luo and P. Sarnak, *Low lying zeros of families of L-functions*, Inst. Hautes Études Sci. Publ. Math. **91**, 2000, 55 – 131.

[Ka] N. Katz, *Twisted L-Functions and Monodromy*, Annals of Mathematical Studies **150**, Princeton University Press, Princeton, 2002.

[KS1] N. Katz and P. Sarnak, *Random Matrices, Frobenius Eigenvalues and Monodromy*, AMS Colloquium Publications **45**, AMS, Providence, 1999.

[KS2] N. Katz and P. Sarnak, *Zeros of zeta functions and symmetries*, Bull. AMS **36**, 1999, 1 – 26.

[Kn] A. Knapp, *Elliptic Curves*, Princeton University Press, Princeton, 1992.

[Ko] V. Kolyvagin, *On the Mordell-Weil group and the Shafarevich-Tate group of modular elliptic curves*, Proceedings of the International Congress of Mathematicians, Vol. I, II (Kyoto, 1990), Math. Soc. Japan, Tokyo, 1991, 429 – 436.

[La1] S. Lang, *Algebraic Number Theory*, Graduate Texts in Mathematics **110**, Springer-Verlag, New York, 1986.

[La2] S. Lang, *Real and Functional Analysis*, Graduate Texts in Mathematics **142**, Springer-Verlag, New York, 1993.

[Mai] L. Mai, *The analytic rank of a family of elliptic curves*, Canadian Journal of Mathematics **45**, 1993, 847 – 862.

[Meh] M. Mehta, *Random Matrices,* 2*nd edition*, Academic Press Inc., Boston, 1991.

[Mes1] J. Mestre, *Formules explicites et minorations de conducteurs de varits algbriques*, Compositio Mathematica **58**, 1986, 209 – 232.

[Mes2] J. Mestre, *Courbes elliptiques de rang $\geq$ 11 sur $\boldsymbol{Q}(t)$*, C. R. Acad. Sci. Paris, ser. 1, **313**, 1991, 139 – 142.

[Mes3] J. Mestre, *Courbes elliptiques de rang $\geq$ 12 sur $\boldsymbol{Q}(t)$*, C. R. Acad. Sci. Paris, ser. 1, **313**, 1991, 171 – 174.

[Mi] P. Michel, *Rang moyen de familles de courbes elliptiques et lois de Sato-Tate*, Monat. Math. **120**, 1995, 127 – 136.

[Mir] R. Miranda, *The Basic Theory of Elliptic Surfaces*, Dottorato di Ricerca in Matematica, Dipartmento di Matematica dell'Universit'a di Pisa, ETS Editrice, 1989.

[Mon] H. Montgomery, *The pair correlation of zeros of the zeta function*, Analytic Number Theory, Proc. Sympos. Pure Math. **24**, Amer. Math. Soc., Providence, 1973, 181 – 193.

[Mor] Mordell, *Diophantine Equations*, Academic Press, New York, 1969,

[Na1] K. Nagao, *On the rank of elliptic curve* $y^2 = x^3 - kx$, Kobe J. Math. **11**, 1994, 205 – 210.

[Na2] K. Nagao, *Construction of high-rank elliptic curves*, Kobe J. Math. **11**, 1994, 211 – 219.

[Na3] K. Nagao, $\mathbb{Q}(t)$*-rank of elliptic curves and certain limit coming from the local points*, Manuscr. Math. **92**, 1997, 13 – 32.

[Nag] T. Nagell, *Introduction to Number Theory*, Chelsea Publishing Company, New York, 1981.

[Od1] A. Odlyzko, *On the distribution of spacings between zeros of the zeta function*, Math. Comp. **48**, 1987, no. 177, 273 – 308.

[Od2] A. Odlyzko, *The* 10^{22}*-nd zero of the Riemann zeta function*, Proc. Conference on Dynamical, Spectral and Arithmetic Zeta-Functions, M. van Frankenhuysen and M. L. Lapidus, eds., Amer. Math. Soc., Contemporary Math. series, 2001, http://www.research.att.com/∼amo/doc/zeta.html

[Po] C. Porter (editor), Statistical Theories of Spectra: Fluctuations, Academic Press, 1965.

[Ri] Rizzo, *Average root numbers for a non-constant family of elliptic curves*, preprint.

[Ro] D. Rohrlich, *Variation of the root number in families of elliptic curves*, Compos. Math. **87**, 1993, 119 – 151.

[RSi] M. Rosen and J. Silverman, *On the rank of an elliptic surface*, Invent. Math. **133**, 1998, 43 – 67.

[Ru] M. Rubinstein, *Evidence for a spectral interpretation of the zeros of L-functions*, P.H.D. Thesis, Princeton University, 1998, http://www.ma.utexas.edu/users/miker/thesis/thesis.html.

[Rud] W. Rudin, *Principles of Mathematical Analysis*, third edition, International Series in Pure and Applied Mathematics, McGraw-Hill Inc., New York, 1976.

[RS] Z. Rudnick and P. Sarnak, *Zeros of principal L-functions and random matrix theory*, Duke Journal of Math. **81**, 1996, 269 – 322.

[Sh] T. Shioda, *Construction of elliptic curves with high-rank via the invariants of the Weyl groups*, J. Math. Soc. Japan **43**, 1991, 673 – 719.

[Si1] J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **106**, Springer-Verlag, Berlin - New York, 1986.

[Si2] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **151**, Springer-Verlag, Berlin - New York, 1994.

[Si3] J. Silverman, *The average rank of an algebraic family of elliptic curves*, J. reine angew. Math. **504**, 1998, 227 – 236.

[St1] N. Stephens, *A corollary to a conjecture of Birch and Swinnerton-Dyer*, J. London Math. Soc. **43**, 1968, 146 – 148.

[St2] N. Stephens, *The diophantine equation $X^3 + Y^3 = DZ^3$ and the conjectures of Birch and Swinnerton-Dyer*, J. reine angew. Math. **231**, 1968, 16 – 162.

[ST] C. Stewart and J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms*, Journal of the American Mathematical Society **40**, number 4, 1995.

[Ta] J. Tate, *Algebraic cycles and the pole of zeta functions*, Arithmetical Algebraic Geometry, Harper and Row, New York, 1965, 93 – 110.

[TW] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. Math. **141**, 1995, 553 – 572.

[Wa] L. Washington, *Class numbers of the simplest cubic fields*, Math. Comp. **48**, number 177, 1987, 371 – 384.

[Wig1] E. Wigner, *On the statistical distribution of the widths and spacings of nuclear resonance levels*, Proc. Cambridge Philo. Soc. **47**, 1951, 790 – 798.

[Wig2] E. Wigner, *Statistical Properties of real symmetric matrices*, Canadian Mathematical Congress Proceedings, University of Toronto Press, Toronto, 1957, 174 – 184.

[Wi] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. Math **141**, 1995, 443 − 551.