JOURNAL OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 19, Number 1, Pages 205–250
S 0894-0347(05)00503-5
Article electronically published on September 7, 2005

LOW-LYING ZEROS OF FAMILIES OF ELLIPTIC CURVES

MATTHEW P. YOUNG

1. Introduction

The random matrix model predicts that many statistics associated to zeros of a family of L-functions can be modeled (or predicted) by the distribution of eigenvalues of large random matrices in one of the classical linear groups. If the statistics of a family of L-functions are modeled by the eigenvalues of the group G, then we say that G is the symmetry group (or symmetry type) associated to the family.

The statistic of interest to us in this work is the density of zeros near the central point (also known as the 1-level density). The random matrix model predicts that the distribution of these zeros should be modeled by the eigenvalues nearest 1 for one of the symmetry types G (unitary, symplectic, and orthogonal). All of the different groups G have distinct behavior in this regard. Therefore, computing the 1-level density gives a theoretical way to predict the symmetry type of a family.

The 1-level density has been studied for a wide variety of families of L-functions; see [R], [KS1], [ILS], [Mil] for example.

It is standard to assume the Generalized Riemann Hypothesis (GRH) to study the 1-level density and we do so throughout this work. In particular, it is necessary to use GRH for the application of obtaining a bound on the average analytic rank from a density theorem. In some cases the use of GRH improves the range of the density theorem, which translates to an improved bound on the average rank. Besides these crucial applications of GRH, we have freely assumed GRH even when it could be removed with extra work since it simplifies arguments in some non-essential places.

It is especially interesting to investigate the 1-level density for families of L-functions attached to elliptic curves over the rationals since zeros at the central point have important arithmetic information (by the conjecture of Birch and Swinnerton-Dyer). These investigations have been the main focus of this work.

2. Preliminaries

We begin by collecting some facts and setting the notation we will use. We consider an elliptic curve $E/\mathbb{Q}$ given in general Weierstrass form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1}$$

Received by the editors April 6, 2005.
2000 *Mathematics Subject Classification.* Primary 11M41, 11F30, 11G05, 11G40, 11L20, 11L40.

where each $a_i \in \mathbb{Z}$. Under a change of variables E can be brought into the simpler form

$$y^2 = x^3 + ax + b, \tag{2}$$

where a and b are integers. The canonical change of variables (cf. [Si1], 46-48) uses the parameters b_2, b_4, b_6, c_4, and c_6, where

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6, \end{aligned}$$

and

$$\begin{aligned} c_4 &= b_2^2 - 24b_4, \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6. \end{aligned}$$

The curve (1) is then equivalent to

$$y^2 = x^3 - 27c_4x - 54c_6.$$

When given by the form (2), E has discriminant

$$\Delta = -16(4a^3 + 27b^2),$$

which is necessarily nonzero for the curve E to be elliptic.

The Weierstrass equation for the elliptic curve (1) is not unique. Any two Weierstrass equations for the same curve are related by the admissible change of variables

$$\begin{aligned} x &= u^2x' + r, \\ y &= u^3y' + su^2x' + t, \end{aligned} \tag{3}$$

where u, r, s, and t are integers and $u \neq 0$. Under this change of variables the discriminant transforms by $u^{12}\Delta' = \Delta$. Likewise, $u^4c_4' = c_4$ and $u^6c_6' = c_6$.

A standard technique in studying E is to reduce the equation (1) modulo p for every prime p. Equation (1) is *minimal* for the prime p if the power of p dividing Δ cannot be decreased by an admissible change of variables and (1) is a *global minimal Weierstrass equation* if it is minimal for all primes simultaneously. For any Weierstrass equation there is an admissible change of variables placing it in global minimal Weierstrass form (cf. [Si1], Corollary 8.3). We record here that if the admissible change of variables (3) places (1) in global minimal Weierstrass form then the only primes p dividing u are those for which (1) is not minimal. We remark that for $p > 3$ if the equation (2) is not minimal at p, then $p^4|a$ and $p^6|b$ (and therefore $p^{12}|\Delta$).

Suppose E is given by a global minimal Weierstrass equation (1). The conductor N of E is then defined by

$$N = \prod_{p|\Delta} p^{f_p},$$

where for $p > 3$,

$$f_p = \begin{cases} 1 & \text{if } p \nmid c_4, \text{ i.e. } E \text{ has multiplicative reduction at } p, \\ 2 & \text{if } p|c_4, \text{ i.e. } E \text{ has additive reduction at } p. \end{cases}$$

When $p = 2$ or 3 the definition of f_p is more complicated (cf. [Si2], IV, §10), but it will usually be enough for our purposes that $N|\Delta$ and $f_p \leq 8$ for all primes p. If necessary, the conductor can be computed using Ogg's formula and Tate's algorithm

([Si2], IV, §9). To explicitly display the dependence of N on E we sometimes write N_E for the conductor of E.

Continuing to assume (1) is a global minimal Weierstrass equation for E, the L-function of E is defined by

$$L(s,E)=\prod_{p\nmid\Delta}\left(1-a_pp^{-s}+p^{1-2s}\right)^{-1}\prod_{p|\Delta}\left(1-a_pp^{-s}\right)^{-1}, \tag{4}$$

where

$$a_p=p+1-\#E(\mathbb{F}_p), \tag{5}$$

and $\#E(\mathbb{F}_p)$ is the number of points on E, when reduced (mod p) (including the point at infinity). The central point is at $s=1$ and the critical strip is $\frac{1}{2}<\text{Re }s<\frac{3}{2}$. Since (1) is minimal, the change of variables taking (1) to (2) does not alter a_p for $p>3$. Thus, for any $p>3$, a_p is given by

$$a_p=-\sum_{x\,(\text{mod }p)}\left(\frac{x^3+ax+b}{p}\right).$$

We remark that for primes $p>3$ dividing the conductor we have $a_p=\pm1$ if E has multiplicative reduction at p and $a_p=0$ if E has additive reduction at p. The infinite product (4) converges absolutely and uniformly for Re $s>\frac{3}{2}$, by Hasse's estimate $a_p<2\sqrt{p}$. According to the Shimura-Taniyama conjecture (proved by Wiles *et al* [W], [TW], [BCDT]) there exists a weight two primitive cuspidal newform $f(z)$ on $\Gamma_0(N)$ such that $L(s,E)=L(s,f)$. Furthermore, $L(s,E)$ has analytic continuation to the complex plane and satisfies the functional equation

$$\Lambda(s,E):=\left(\frac{\sqrt{N}}{2\pi}\right)^s\Gamma(s)L(s,E)=\epsilon_E\Lambda(2-s,E),$$

where $\epsilon_E=\pm1$ is the root number of E.

Throughout this work we assume the Generalized Riemann Hypothesis holds, namely that all the nontrivial zeros of an arithmetic L-function lie on its line of symmetry. For our elliptic curve L-functions the zeros have the form $1+i\gamma$, $\gamma\in\mathbb{R}$.

Using the notation of Iwaniec-Luo-Sarnak [ILS] we define for an L-function $L(s,E)$ the quantity

$$D(E;\phi)=\sum_{\gamma_E}\phi\left(\frac{\gamma_E}{2\pi}\log X\right),$$

where ϕ is an even Schwartz class test function whose Fourier transform[1] $\widehat{\phi}$ has compact support (so ϕ extends to an entire function), γ_E runs through the imaginary parts of the nontrivial zeros $\rho_E=1+i\gamma_E$ of $L(s,E)$ (counted with multiplicity), and X is a parameter at our disposal (generally of size N_E; allowing X to be only approximately N_E gives us more freedom in averaging over a family). The scaling factor $(2\pi)^{-1}\log X$ is inserted to normalize the number of zeros counted by the test function ϕ, so that $D(E;\phi)$ should be thought of as representing the density of zeros of $L(s,E)$ near the central point $s=1$. We will be interested in averaging $D(E;\phi)$ over certain families of automorphic forms arising from elliptic curves. Each family we study is of the form

$$\mathcal{F}=\mathcal{F}(\mathcal{A})=\{E_r\}$$

[1]Throughout we denote $\widehat{f}(y)=\int_{-\infty}^{\infty}f(x)e(-xy)dx$, $e(x)=\exp(2\pi ix)$.

where r ranges over a set $\mathcal{A}$, which is a subset of $\mathbb{Z}$ or $\mathbb{Z}\times\mathbb{Z}$, such that each $r\in\mathcal{A}$ naturally defines an elliptic curve E_r over $\mathbb{Q}$. The curve E_r will be defined by a Weierstrass equation whose coefficients are polynomials in r. Our main family will be parameterized by $r=(a,b)\in\mathbb{Z}^2$ where $E_r: y^2=x^3+ax+b$. It may happen that $L(s,E_r)=L(s,E_{r'})$ for $r\neq r'$ trivially because a global minimal Weierstrass equation for E_r equals that of E_r' or more subtly because E_r is isogenous to $E_{r'}$. We take such forms with multiplicity. We expect it should make no statistical difference whether one takes such forms f with multiplicity or not. As a general rule, we can easily make restrictions on r that force E_r to be minimal, but this does not change any statistics (at least in the main term) (see Section 5.6 for a more thorough discussion of this point). We will often suppress the dependence of $\mathcal{F}$ on $\mathcal{A}$.

We study the weighted average

$$\mathcal{D}(\mathcal{F};\phi,w)=\sum_{E\in\mathcal{F}}D(E;\phi)w(E),$$

where $w(E_r):=w(r)$ is a smooth, compactly supported function (a cutoff function) on $\mathbb{R}$ or $\mathbb{R}^2$, whichever is appropriate. To avoid trivialities we assume w does not have total mass zero (i.e. $\widehat{w}(0)\neq 0$), and in particular that w is not identically zero. Here w may take both positive and negative values, yet it is natural to think of w as a bump function approximating the characteristic function of an interval. We measure the weighted sum against the total weight

$$W(\mathcal{F})=\sum_{E\in\mathcal{F}}w(E).$$

Since $D(E;\phi)$ (implicitly) depends on X we scale our cutoff function w by X also, in which case we use the notation w_X to denote the scaling of w by X and W_X to be the total weight scaled by X. The precise scaling depends on the family and is used to pick out curves with conductors N such that $\log N$ is asymptotically $\log X$ on average. Often we simply take curves with discriminant $|\Delta|\asymp X$. Most families of L-functions studied in random matrix theory have either constant conductor or conductors that increase naturally. Families of elliptic curves are different because the conductor behaves erratically as a function of the coefficients of the Weierstrass equation. See [Mil] for a different way of scaling; he scales the zeros by $\log N$ (rather than $\log X$) and passes to a subsequence of curves where the conductor behaves monotonically.

Katz and Sarnak predict that for a natural family $\mathcal{F}$ the average density should satisfy

$$\lim_{X\to\infty}\frac{\mathcal{D}(\mathcal{F};\phi,w_X)}{W_X(\mathcal{F})}=\int_{-\infty}^{\infty}\phi(t)\mathcal{W}(G)(t)dt,$$

where $\mathcal{W}(G)$ is the 1-level scaling density of eigenvalues near 1 for a symmetry group G ($\mathcal{W}$ will in general be a distribution). Such a result is called the *density conjecture* for the family $\mathcal{F}$. We have

$$\mathcal{W}(G)(t)=\begin{cases}1 & \text{if } G=U\\ 1-\frac{\sin 2\pi t}{2\pi t} & \text{if } G=Sp\\ 1+\frac{1}{2}\delta_0(t) & \text{if } G=O\\ 1+\frac{\sin 2\pi t}{2\pi t} & \text{if } G=SO(\text{even})\\ 1+\delta_0(t)-\frac{\sin 2\pi t}{2\pi t} & \text{if } G=SO(\text{odd}),\end{cases}$$

where δ_0 is the Dirac distribution [KS1]. It is more convenient to work with the Fourier transforms of ϕ and $\mathcal{W}$; by the Plancherel theorem it is equivalent to work on the Fourier transform side. We record the Fourier transforms of the above distributions here:

$$\widehat{\mathcal{W}}(G)(t) = \begin{cases} \delta_0(t) & \text{if } G = U \\ \delta_0(t) - \frac{1}{2}\eta(t) & \text{if } G = Sp \\ \frac{1}{2} + \delta_0(t) & \text{if } G = O \\ \delta_0(t) + \frac{1}{2}\eta(t) & \text{if } G = SO(\text{even}) \\ 1 + \delta_0(t) - \frac{1}{2}\eta(t) & \text{if } G = SO(\text{odd}), \end{cases} \tag{6}$$

where

$$\eta(t) = \begin{cases} 1 & \text{if } \ |t| < 1, \\ \frac{1}{2} & \text{if } \ |t| = 1, \\ 0 & \text{if } \ |t| > 1. \end{cases}$$

An important feature is that the Fourier transforms of $\widehat{\mathcal{W}}(O)(t)$, $\widehat{\mathcal{W}}(SO(\text{even}))(t)$, and $\widehat{\mathcal{W}}(SO(\text{odd}))(t)$ all agree for $|t| < 1$ but are distinguishable for $|t| > 1$. Therefore, by the Plancherel Theorem, to distinguish the 1-level densities of these three symmetry types one needs to apply test functions ϕ whose Fourier transforms are supported outside $[-1, 1]$.

Iwaniec, Luo, and Sarnak prove that the family $H_2^\star(N)$ of primitive cusp forms of weight 2 and level N (N square-free), $N \to \infty$, has symmetry type O for test functions ϕ restricted by $\operatorname{supp} \widehat{\phi} \subset (-2, 2)$ (see [ILS]). They also prove the forms with root number $+1$ have symmetry type $SO(\text{even})$ and the forms with root number -1 have symmetry type $SO(\text{odd})$ in the same range. This is relevant for our families because the family of all elliptic curves forms a subfamily of weight two primitive cusp forms. In particular, we do not expect to detect statistics of the root number of the family without obtaining support past $(-1, 1)$. This potential change in behavior at 1 is not surprising in light of the "approximate" functional equation, which states that

$$L(1, E) = \sum_n \frac{a_n}{n} g\left(\frac{2\pi n}{U}\right) + \epsilon_E \sum_n \frac{a_n}{n} g\left(\frac{2\pi n}{V}\right),$$

where g is a test function of a certain kind and $UV = N$. If we take $U > N^{1+\varepsilon}$ (i.e., sum the Fourier coefficients of length greater than N), then the first sum implicitly captures the root number (since the second sum is then small) whereas if $U \leq N^{1-\varepsilon}$, then the root number explicitly occurs in the second sum. After developing the explicit formula we shall see the analogy to this dramatic shift in behavior with a similar sum (except over primes); going past support $(-1, 1)$ is similar to taking U larger than the conductor.

It is more difficult to gain large support for families of elliptic curves than for all cusp forms of weight two because the forms coming from elliptic curves compose a small subfamily of the weight two cusp forms. Very loosely speaking, there are probably around $X^{5/6}$ elliptic curves with conductors $N \asymp X$, whereas there are about X^2 weight two cusp forms of levels $N \asymp X$.

It is an open (and very interesting) question to estimate the number of elliptic curves that have conductor $N \leq X$. Our rough figure of $X^{5/6}$ arises by simply counting the number of positive integers a and b such that $|\Delta| = 16(4a^3 + 27b^2) \asymp X$.

Fouvry, Nair, and Tenenbaum [FNT] have shown that the number of nonisogenous semi-stable elliptic curves with conductor $N \leq X$ is $\gg X^{5/6}$. In the other direction, Duke and Kowalski [DK] (building on work of Brumer and Silverman [BS]) have shown that the number of elliptic curves with conductor $N \leq X$ is $\ll X^{1+\varepsilon}$ for any $\varepsilon > 0$. Any power savings in the exponent in this upper bound would be very interesting because it would show that for almost all levels N there are no elliptic curves with conductor N. Note also that the lack of knowledge in this regard illustrates why we cannot average $D(E;\phi)$ over all elliptic curves with $N_E \leq X$.

We also use the common convention of letting ε denote an arbitrarily small positive constant that may vary from line to line.

3. Summary of results

3.1. **Main results.** Our main results are given in this section.

Theorem 3.1. *Let $\mathcal{F}$ be the family of elliptic curves given by the Weierstrass equations $E_{a,b} : y^2 = x^3 + ax + b$ with a and b positive integers. Let $w \in C_0^\infty(\mathbb{R}^+ \times \mathbb{R}^+)$ (for us $\mathbb{R}^+ = (0,\infty)$) and set $w_X(E_{a,b}) = w\left(\frac{a}{A}, \frac{b}{B}\right)$, where $A = X^{1/3}$, $B = X^{1/2}$ (X a positive real number). Then*

$$\mathcal{D}(\mathcal{F};\phi,w_X) \sim [\widehat{\phi}(0) + \tfrac{1}{2}\phi(0)]W_X(\mathcal{F}) \text{ as } X \to \infty,$$

for ϕ with supp $\widehat{\phi} \subset (-\frac{7}{9}, \frac{7}{9})$.

Note that $W_X(\mathcal{F}) \sim \widehat{w}(0,0)AB$ as $X \to \infty$, so we are taking about $X^{5/6}$ curves from our family. In the language of random matrix theory this theorem shows that the family of all elliptic curves has symmetry type consistent with O, inasmuch as this can be detected without having support outside $(-1,1)$. Furthermore, we have

Theorem 3.2. *Let $\mathcal{F}$ be the family of elliptic curves given by the Weierstrass equations $E_{a,b} : y^2 = x^3 + ax + b^2$ with a and b positive integers. Let $w \in C_0^\infty(\mathbb{R}^+ \times \mathbb{R}^+)$ and set $w_X(E_{a,b}) = w\left(\frac{a}{A}, \frac{b}{B}\right)$, where $A = X^{1/3}$, $B = X^{1/4}$ (X a positive real number). Then*

$$\mathcal{D}(\mathcal{F};\phi,w_X) \sim [\widehat{\phi}(0) + \tfrac{3}{2}\phi(0)]W_X(\mathcal{F}) \text{ as } X \to \infty,$$

for ϕ with supp $\widehat{\phi} \subset (-\frac{23}{48}, \frac{23}{48})$.

Here we are taking approximately $X^{7/12}$ curves from our family. These elliptic curves generally have positive algebraic rank since there is the obvious rational point $Q = (0, b)$ (if Q is torsion the Lutz-Nagell criterion implies $b^2 | 4a^3$, so the number of curves in this family for which Q is torsion is $O(X^{1/3+\varepsilon})$). It is also expected that the root number in this family is evenly distributed between ± 1 so that one might expect that the rank is usually either one or two. These remarks explain the presence of the "extra" $\phi(0)$ contribution above.

Obtaining these two theorems with the stated support crucially requires GRH for Dirichlet L-functions to bound certain character sums. In the course of the proof we also assume GRH for the symmetric square L-functions associated to E, but in practice this could be easily removed simply by using harmonic analysis in the same way we prove Lemma 5.2.

S. J. Miller [Mil] has independently proved density theorems for various families of elliptic curves (along with other things), but more restricted by the support of $\widehat{\phi}$. Brumer [B], Heath-Brown [H-B], Michel [Mic], Silverman [Si3], and others have

proved results on the average rank of certain families of elliptic curves that can now be interpreted to essentially be density theorems. Actually, in order to obtain a density theorem one must asymptotically compute the average of $\log N$ over the family; in order to obtain an upper bound on the average rank only a trivial upper bound (such as $N \leq |\Delta|$) is required. For the family of all elliptic curves the necessary asymptotic formula is not overly difficult, yet for more general families the problem becomes challenging indeed.

Note that if one can apply $\widehat{\phi}$ of large support, then ϕ can be localized near the origin, so the zeros $\rho_E = 1 + i\gamma_E$ are held closer to the central point. Therefore, one challenge for us has been to obtain Theorem 3.1 with the support of $\widehat{\phi}$ as large as possible. Breaking support $(-1, 1)$ would be of interest, since it is at that point that the Fourier transforms of the densities of the groups O, $SO(\text{even})$, and $SO(\text{odd})$ become distinguishable. It appears that the current technology is incapable of producing such a result (even assuming GRH), but we have reasons to expect the following.

Conjecture 3.3. Theorem 3.1 holds for test functions ϕ with no restrictions on the support.

We will provide some justification for this conjecture in Section 7.2 after we prove Theorems 3.1 and 3.2. This conjecture agrees with the folklore conjecture that the root number is equidistributed in the family of all elliptic curves (but see [He1] for an extensive treatment of the variation in sign of the root number). Miller also predicts the symmetry type is O but from an entirely different direction. He considers the 2-level density of the family of all elliptic curves and uses the work and conjectures of Helfgott implying equidistribution of root numbers to predict symmetry type O (the 2-level density can distinguish between the various orthogonal symmetry types using test functions with arbitrarily small support but it is necessary to know the percentage of curves with given root number). Our method is quite different and relies on sharp estimates for the three-variable character sum (27) for large values of P. It is mysterious how the distribution of the root number (essentially controlled by the Möbius function of the polynomial $4a^3 + 27b^2$) is captured by such a character sum.

An easy consequence of Theorem 3.1 is the following.

Corollary 3.4. *The family of all elliptic curves ordered as in Theorem* 3.1 *has average analytic rank* $r \leq 25/14$. *Conjecture* 3.3 *being true implies that* $r \leq 1/2$.

The proof shows that any family with symmetry type O and support in $(-\nu, \nu)$ has average rank bounded by $\frac{1}{2} + \frac{1}{\nu}$. Applying a density theorem to obtain an upper bound on the average rank in this fashion requires the Riemann Hypothesis for all L-functions in the family; the proof involves taking $\phi(x) \geq 0$ for $x \in \mathbb{R}$ so that $D(E; \phi) \geq \phi(0)\text{ord}_{s=1}L(s, E)$ by positivity. Without GRH any contribution to $D(E; \phi)$ from zeros off the critical line may not be real numbers. Using zero density estimates Kowalski and Michel [KM1], [KM2] obtained an upper bound on the average order of vanishing of all weight 2 level q modular L-functions, thereby removing the assumption of GRH for their family. The bound on the average rank is significantly larger than that which is obtained on GRH. It would be interesting to obtain an unconditional (yet weaker) upper bound for the average rank of the family of all elliptic curves.

Brumer [B] showed that the average rank r of all elliptic curves satisfies $r \leq 2.3$ and Heath-Brown [H-B] proved $r \leq 2$, modulo a few minor differences in the choice of test functions and sieving of unpleasant curves. Brumer's and Heath-Brown's results require the GRH for elliptic curve L-functions. It is a standard conjecture of random matrix theory that, once the symmetry type G for the family has been identified, the density theorem should hold for a test function $\widehat{\phi}$ with arbitrarily large support. Random matrix theory predicts that Conjecture 3.3 implies the equidistribution of root numbers (via the 2-level density for instance); it would be interesting to see a direct (number-theoretic) reason for this to be so.

S. J. Miller has observed (private communication) that since $25/14 = 1.78... < 2$ then a positive proportion of curves have analytic rank 0 or 1. Using the famous theorem that says that if the analytic rank is ≤ 1, then the algebraic rank and analytic rank are equal and Ш is finite (due in large part to Kolyvagin [Ko] and Gross-Zagier [GZ]) we obtain

Corollary 3.5. *Assume GRH. Then a positive proportion of elliptic curves ordered as in Theorem* 3.1 *have algebraic rank equal to analytic rank and finite Tate-Shafarevich group.*

3.2. **Further results.** Besides the results recorded in the previous section, we investigate similar density results for a variety of interesting families. In particular we study a number of families with prescribed torsion. See [Ku], Table 3 for the parametrizations of the various torsion structures. Since many of the results follow a general theme we shall give the full details for the family of curves with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ in Section 8.1. The full details of some other torsion families as well as some families with complex multiplication can be found in [Y1][2] or [Y2].

These torsion families have some surprisingly nice properties. For instance, the family of curves with torsion group $\mathbb{Z}/4\mathbb{Z}$ is parameterized by $y^2+xy-by = x^3-bx^2$ with $\Delta = b^4(1+16b)$. As a general rule we cannot prove a density result for a family where the degree of the discriminant is larger than 3. Although the discriminant has degree 5 for this family, it is easily treated because the irreducible factors b and $1+16b$ are linear. In addition the conductor is much smaller than the discriminant ($N \ll b^2$ whereas $|\Delta| \asymp b^5$) so there are many more curves in the family with conductor $\leq X$ than one would expect based on the degree of the discriminant. The other torsion families have similar characteristics that make their study extremely pleasant. The family with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is especially nice because it displays many beautiful symmetries.

In Section 9 we study a thin sequence of quadratic twists with positive rank. This family is challenging because the conductor is essentially a cubic polynomial. Such families of quadratic twists were studied by Rubin and Silverberg [RS] for example.

3.3. **Structure of the paper.** In Section 4 we set up the machinery for proving a density result for a family of elliptic curves. We prove Theorems 3.1 and 3.2 in Sections 5 and 6; some of the more technical details are deferred to the Appendices.

We provide evidence for Conjecture 3.3 in Section 7. This conjecture naturally follows from an assumption that a certain character sum in three variables has square-root cancellation in each variable (one of which is a summation over primes).

[2]Version 3 is the latest version with full details of the torsion families. Other sections of version 3 may differ from the present text.

We lend credence to the conjecture by studying a sum similar to the aforementioned one but where the summation is extended to integers. We obtain a stronger result with this new sum; see Theorem 7.2.

In the remaining sections we prove density results for the interesting families discussed in Section 3.2.

4. General method of proof

In this section we set up some machinery to streamline the proofs of our density theorems.

Suppose we are given a Weierstrass equation (1) (not necessarily minimal) which defines an elliptic curve E with conductor N and L-function $L(s,E)$. To analyze $D(E;\phi)$ we will employ the explicit formula for $L(s,E)$, which for cusp forms of weight two and level N takes the form (see (4.25) in [ILS])

$$D(E;\phi) = \widehat{\phi}(0)\frac{\log N}{\log X} + \frac{1}{2}\phi(0) - P(E;\phi) + O\left(\frac{\log\log|\Delta|}{\log X}\right), \tag{7}$$

where

$$P(E;\phi) = \sum_{p>3} \lambda_E(p)\widehat{\phi}\left(\frac{\log p}{\log X}\right)\frac{2\log p}{p\log X}.$$

Here Δ is the discriminant of the curve defined by (1) (again, Δ is not assumed minimal), X is a scaling parameter (any number ≥ 2 at our disposal), and

$$\lambda_E(p) = -\sum_{x \,(\mathrm{mod}\ p)} \left(\frac{x^3+ax+b}{p}\right) \tag{8}$$

if the Weierstrass equation (1) defining E is put into the form (2). Actually, the sum $P(E;\phi)$ in [ILS] is restricted by $p \nmid N$ and assumes that $\lambda_E(p)$ is the coefficient (5) of p^{-s} in the Dirichlet series expansion of $L(s,E)$. We claim that the modifications in $P(E;\phi)$ are acceptable because the discrepancy in the formula (7) is absorbed by the error term. To prove this we first note that if $p \nmid \Delta$ and (2) is in global minimal Weierstrass form, then $\lambda_E(p)$ is exactly the coefficient (5). Furthermore, the character sum defining the quantity $\lambda_E(p)$ is left unchanged by a change of variables placing (2) in global minimal Weierstrass form. Therefore the terms agree for $p \nmid \Delta$. On the other hand, the terms where $p|\Delta$ are absorbed by the error term. It is worthwhile to note that the error term in (7) is derived by using the Riemann Hypothesis for the symmetric-square L-function $L(s,\mathrm{sym}^2(E))$ to handle terms of the form $\lambda_E(p^2)$. The formula (7) holds for individual E. In practice one could eliminate the use of the GRH by averaging over families; we have used the Riemann Hypothesis for simplicity and brevity since we are assuming it for other reasons anyway. Michel has some general results that would be applicable for this problem [Mic].

Next we sum over the family. We compute

$$\mathcal{D}(\mathcal{F};\phi,w_X) = \widehat{\phi}(0)\sum_{E\in\mathcal{F}}\frac{\log N_E}{\log X}w_X(E) + \frac{1}{2}\phi(0)W_X(\mathcal{F}) - \mathcal{P}(\mathcal{F};\phi,w_X) + O\left(\frac{W_X(\mathcal{F},\Delta)}{\log X}\right),$$

where

$$\mathcal{P}(\mathcal{F};\phi,w_X)=\sum_{E\in\mathcal{F}}P(E;\phi)w_X(E)$$

and

$$W_X(\mathcal{F},\Delta)=\sum_{E\in\mathcal{F}}|w_X(E)|\log\log|\Delta|.$$

In general $\log\log|\Delta|$ will be $\ll\log\log X$, so this will be a true error term.

With all of our families we will take X and w_X so that

$$\sum_{E\in\mathcal{F}}\frac{\log N_E}{\log X}w_X(E)\sim W_X(\mathcal{F})\quad\text{as } X\to\infty. \tag{9}$$

It is generally highly nontrivial to prove that such an asymptotic holds; often it amounts to having control on the square divisors of a polynomial of high degree. This is a significant barrier to producing density theorems with families of high rank. We call (9) the *conductor condition* for the family $\mathcal{F}$.

The idea in most cases is to approximate N_E with numbers R_E which have the same prime divisors as N_E but are easier to compute (often $R_E=|\Delta|$, the discriminant of the elliptic curve). Then X and w_X will be chosen so that X is approximately R_E for E in the support of w_X. For an example, with the family $y^2=x^3+ax+b$ given in Theorem 3.1 we have w_X scaled so that $a\asymp X^{1/3}$, $b\asymp X^{1/2}$, $|\Delta|\asymp X^{5/6}$, and we take $R_E=|\Delta|$.

The following lemma will streamline many of our arguments to show (9) holds.

Lemma 4.1. *Let $\mathcal{F}=\{E_r\}$ be a family of elliptic curves with notation as in Section 2. Let $\Delta(r)$ be the discriminant of the curve E_r. Suppose that there exists an integer polynomial $R(r)$ dividing $\Delta(r)$ such that each irreducible factor of $\Delta(r)$ divides $R(r)$. Further suppose*

$$\sum_{E\in\mathcal{F}}\sum_{\substack{p^\alpha||R_E\\ \alpha>0}}|w_X(E)|\log p^{\alpha-1}+\sum_{E\in\mathcal{F}}\sum_{\substack{p||R_E\\ p^2|N_E\\ p>3}}|w_X(E)|\log p\ll|W_X(\mathcal{F})| \tag{10}$$

uniformly in X, where we have defined $R_E=R(r)$ for $E=E_r$. Suppose $R(r)\asymp X$ for all E_r in the support of w_X. Then we have

$$\sum_{E\in\mathcal{F}}\frac{\log N_E}{\log X}w_X(E)=W_X(\mathcal{F})+O\left(\frac{|W_X(\mathcal{F})|}{\log X}\right).$$

Remark. Both sums in (10) have an interpretation. For the first sum to be small there must not be many large square divisors of R_E (i.e. R_E is not too large). For the second sum to be small it must be rare for a prime to divide R_E to lower order than N_E (i.e. R_E is not too small). In most applications $N_E|R_E$, so the second sum will be void. In general we can handle the first sum as long as all of the irreducible factors of $R(r)$ are of degree 3 or less.

Proof. Suppose $R(d)$ is as above. Then

$$W_X(\mathcal{F})-\sum_{E\in\mathcal{F}}\frac{\log N_E}{\log X}w_X(E)=\sum_{E\in\mathcal{F}}\frac{\log(X/R_E)}{\log X}w_X(E)+\sum_{E\in\mathcal{F}}\frac{\log(R_E/N_E)}{\log X}w_X(E).$$

Since we are assuming $R_E \asymp X$ the first sum is trivially $\ll |W_X(\mathcal{F})| (\log X)^{-1}$. The second sum is

$$\frac{1}{\log X} \sum_{E \in \mathcal{F}} \sum_{\substack{p^\alpha || R_E \\ p^\beta || N_E}} w_X(E) \log p^{\alpha - \beta},$$

by using the additivity of the logarithm to separate the prime factors of R_E and N_E (these primes p have nothing to do with the explicit formula of course). Note $\beta \leq 8$ for all p, and $\beta \leq 2$ for $p > 3$. First consider the terms with $\beta > 0$. By taking the terms with $\alpha > \beta$ and $\alpha < \beta$ separately it is clear the contribution is

$$\ll \frac{1}{\log X} \sum_{E \in \mathcal{F}} \sum_{\substack{p^\alpha || R_E \\ \alpha > 0}} |w_X(E)| \log p^{\alpha - 1} + \frac{1}{\log X} \sum_{E \in \mathcal{F}} \sum_{\substack{p || R_E \\ p^2 | N_E \\ p > 3}} |w_X(E)| \log p + O\left(\frac{|W_X(\mathcal{F})|}{\log X} \right),$$

the error term coming from $\alpha < \beta$ and $p \leq 3$ (in which case β may be larger than 2).

Now consider those terms with $\beta = 0$ (and hence $\alpha > 0$). Since $p | \Delta$ but $p \nmid N$ this implies that the equation (1) defined by r is not minimal at p and therefore $\alpha \geq 12$, so we may absorb these terms into the first sum which consists of $p^\alpha || R_E, \alpha > 0$. □

For any individual family we will need to estimate $\mathcal{P}(\mathcal{F}; \phi, w_X)$ using (ad hoc) techniques applicable to the family. In its evaluation we will often make use of the following identity (Poisson Summation (mod l)).

Proposition 4.2. *Let w be a Schwartz-class function, D a positive real number, and a an integer. Then the following holds:*

$$\sum_{\substack{d \in \mathbb{Z} \\ d \equiv a \, (\mathrm{mod}\ l)}} w\left(\frac{d}{D}\right) = \frac{D}{l} \sum_{h \in \mathbb{Z}} e\left(\frac{ha}{l}\right) \widehat{w}\left(\frac{hD}{l}\right). \tag{11}$$

For a reference see (4.24) of [IK] for instance.

5. Proof of Theorem 3.1

By the discussion in Section 4, to prove Theorem 3.1 we need to show

$$\mathcal{P}(\mathcal{F}; \phi, w_X) \ll \frac{W_X(\mathcal{F})}{\log X} \asymp \frac{AB}{\log X}$$

and to show the conductor condition (9) holds.

5.1. The conductor condition.

In this section we show (9) holds.

Lemma 5.1. *Let $\mathcal{F}, A, B$, and w be as in Theorem 3.1. Then we have*

$$\sum_{E \in \mathcal{F}} \frac{\log N_E}{\log X} w_X(E) = \left\{ 1 + O\left(\frac{1}{\log X} \right) \right\} W_X(\mathcal{F}).$$

Proof. We apply Lemma 4.1. We take the polynomial $R(d)$ for $d = (a, b)$ to be given by $R(d) = 16(4a^3 + 27b^2)$. Note $R(d) = |\Delta(d)|$. Recall that $A = X^{1/3}$ and $B = X^{1/2}$ so that $R(d) \asymp X$ since $a \asymp A$ and $b \asymp B$. The sum

$$\sum_{E \in \mathcal{F}} \sum_{\substack{p || R_E \\ p^2 | N_E}} w_X(E) \log p$$

is empty since $N|\Delta$. The other term is

$$\sum_{E \in \mathcal{F}} \sum_{\substack{p^\alpha || R_E \\ \alpha > 0}} w_X(E) \log p^{\alpha-1} = \sum_a \sum_b \sum_{\substack{p^\alpha || 16(4a^3+27b^2) \\ \alpha > 0}} w\left(\frac{a}{A}, \frac{b}{B}\right) \log p^{\alpha-1}$$

by definition. First suppose $p > 3$. Interchange the order of summation and for each prime p define γ by $p^\gamma || a$. We first consider the terms where $\alpha < 3\gamma$. For these cases $p^\alpha || b^2$ (so α is necessarily even). We employ the change of variables $a = p^\gamma a'$, $b = p^{\alpha/2} b'$ and obtain (we often use primes to indicate that a summation is carried out with certain coprimality conditions in place which should be apparent from the context; in the next formula the restriction is $(a', p) = (b', p) = 1$)

$$\begin{aligned}
&\sum_{\substack{p^\alpha \ll X \\ \alpha > 0}} \sum_{\alpha/3 < \gamma \ll \log A} \sideset{}{'}\sum_{a'} \sideset{}{'}\sum_{b'} w\left(\frac{p^\gamma a'}{A}, \frac{p^{\alpha/2} b'}{B}\right) \log p^{\alpha-1} \\
&\quad \ll \sum_{\substack{p^\alpha \ll X \\ \alpha > 0}} \sum_{\alpha/3 < \gamma \ll \log A} \left(1 + \frac{A}{p^\gamma}\right)\left(1 + \frac{B}{p^{\alpha/2}}\right) \log p^{\alpha-1} \\
&\quad \ll \sum_{\substack{p^\alpha \ll X \\ \alpha > 0}} \left(\log A + \frac{A}{p^{[\alpha/3]+1}} + \frac{B \log A}{p^{\alpha/2}} + \frac{AB}{p^{\alpha/2+[\alpha/3]+1}}\right) \log p^{\alpha-1}.
\end{aligned}$$

This sum is

$$\ll \sqrt{X} \log A + A \log X + B(\log X)^2 + AB \ll X^{5/6},$$

because

$$\sum_{\substack{p^\alpha \le Z \\ \alpha > 0}} \log p^{\alpha-1} \ll \sqrt{Z} \quad \text{and} \quad \sum_{\substack{p^\alpha \\ \alpha > r}} \frac{\log p^{\alpha-1}}{p^{\alpha/r}} \ll 1.$$

Now we consider the terms with $\alpha > 3\gamma$. In this case $p^{3\gamma} || b^2$ (so γ is necessarily even). We employ the change of variables $a \to p^\gamma a'$, $b \to p^{3\gamma/2} b'$ and obtain

$$\sum_{\substack{p^\alpha \ll X \\ \alpha > 0}} \sum_{0 \le \gamma < \alpha/3} \sideset{}{'}\sum_{\substack{a' \\ p^{\alpha-3\gamma} || (4a'^3 + 27b'^2)}} \sideset{}{'}\sum_{b'} w\left(\frac{p^\gamma a'}{A}, \frac{p^{3\gamma/2} b'}{B}\right) \log p^{\alpha-1}.$$

We split the summation over b' into progressions $(\mathrm{mod}\ p^{\alpha-3\gamma})$. Since $(p, a') = (p, b') = 1$ we get that for each a' the number of solutions (in $b' \pmod p$) to the

congruence $4a'^3 + 27b'^2 \equiv 0 \pmod{p^{\alpha-3\gamma}}$ is bounded by 2. Therefore we obtain

$$\sum_{\substack{p^\alpha \ll X \\ \alpha>0}} \sum_{0\le\gamma<\alpha/3} \left(1+\frac{A}{p^\gamma}\right)\left(1+\frac{Bp^{-3\gamma/2}}{p^{\alpha-3\gamma}}\right)\log p^{\alpha-1} \ll \sum_{\substack{p^\alpha \ll X \\ \alpha>0}} \left(\alpha + A + \frac{B}{p^{\alpha-\frac{3}{2}[\alpha/3]}} + \frac{AB}{p^{\alpha-\frac{1}{2}[\alpha/3]}}\right)\log p^{\alpha-1},$$

which is bounded by $X^{5/6}$ by the same type of reasoning used for the case $\alpha > 3\gamma$ (check $\alpha = 2$ and $\alpha \ge 3$ separately).

The case $\alpha = 3\gamma$ proceeds much the same as above; this case is even simpler than before.

The primes 2 and 3 are handled in the same way as above, so we merely summarize the changes. For $p = 3$ we may assume $\alpha \ge 4$ by trivially estimating the terms with $\alpha \le 3$. The estimation for $\alpha < 3\gamma$ is the same as before after the change of variables $\alpha \to \alpha + 3$. The estimation for $\alpha \ge 3\gamma$ is as before after the change of variables $\gamma \to \gamma + 1$. For $p = 2$ we may assume $\alpha \ge 6$. After cancelling 2^6 in the discriminant congruence we are left in a very similar case to $p = 3$. □

5.2. **The central estimate.** We will have proved Theorem 3.1 once we have proved

Lemma 5.2. *Set $A = X^{1/3}$ and $B = X^{1/2}$. Then*

$$\sum_a \sum_b P(E;\phi) w\left(\frac{a}{A},\frac{b}{B}\right) \ll \frac{X^{5/6}}{\log X}$$

provided supp $\widehat{\phi} \subset (-\frac{7}{9},\frac{7}{9})$.

This lemma is the heart of the matter.

Proof. We calculate

$$\sum_a \sum_b P(E;\phi) w\left(\frac{a}{A},\frac{b}{B}\right) = \sum_{p>3} \frac{2\log p}{p\log X}\widehat{\phi}\left(\frac{\log p}{\log X}\right) \sum_a \sum_b \lambda_{a,b}(p) w\left(\frac{a}{A},\frac{b}{B}\right).$$

Apply Poisson summation (mod p) in the summation over a and b and obtain

$$\sum_a \sum_b \lambda_{a,b}(p) w\left(\frac{a}{A},\frac{b}{B}\right) = \frac{AB}{p^2} \sum_h \sum_k \sum_{\substack{\alpha \,(\mathrm{mod}\ p) \\ \beta \,(\mathrm{mod}\ p)}} \sum \lambda_{\alpha,\beta}\, e\left(\frac{\alpha h + \beta k}{p}\right) \widehat{w}\left(\frac{hA}{p},\frac{kB}{p}\right).$$

The summation over α and β is evaluated in Section 5.3 (the evaluation is completely straightforward). Using Lemma 5.6 we continue, obtaining (below ε_p is the sign of the Gauss sum)

$$-\frac{AB}{\log X} \sum_{p>3} \varepsilon_p \frac{2\log p}{p^{3/2}} \widehat{\phi}\left(\frac{\log p}{\log X}\right) \sum_h \sum_k \left(\frac{k}{p}\right) e\left(\frac{-h^3\bar{k}^2}{p}\right) \widehat{w}\left(\frac{hA}{p},\frac{kB}{p}\right). \tag{12}$$

We remark at this point that if we estimate this sum trivially we get a bound of the order (summing p up to P, say)

$$\frac{AB}{\log X} \sum_{p\le P} \frac{\log p}{p^{3/2}} \left(1+\frac{p}{A}\right)\left(1+\frac{p}{B}\right) \ll (AB + BP^{1/2} + P^{3/2})(\log X)^{-1},$$

which is $O\left(AB(\log X)^{-1}\right)$ when $P \leq X^{5/9}$. Brumer essentially obtained this result [B]. To get larger support we need to prove there is quite a lot of cancellation in the three variable character sum (12). By exploiting some cancellation in this sum Heath-Brown [H-B] has improved Brumer's result to the support range $(-2/3, 2/3)$. Note that any improvement on Heath-Brown's result shows that the average rank is strictly less than two.

The first step is to eliminate the variation in ε_p. To do so we sum separately over the progressions $p \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 4$. Effectively, it suffices to replace ε_p by $\psi_4(p)$, a Dirichlet character (mod 4). Now break up the summation in (12) into dyadic segments using a smooth partition of unity. It suffices to consider sums of the form

$$\sum_{\substack{H\leq h<2H\\ K\leq k<2K\\ P\leq p<2P}}\sum\sum \frac{\log p}{p^{3/2}}\psi_4(p)\left(\frac{k}{p}\right)e\left(\frac{-h^3\bar{k}^2}{p}\right)\widehat{\phi}\left(\frac{\log p}{\log X}\right)\widehat{w}\left(\frac{hA}{p},\frac{kB}{p}\right)g(h,k,p), \tag{13}$$

where g is a smooth compactly supported function arising from the partition of unity. We assume that the restrictions on p, h, and k are redundant, following from the support of g. It suffices to show that every sum of type (13) is $\ll X^{-\varepsilon}$, with the implied constant depending only on $w, ||g||_\infty, ||g'||_\infty$, etc. In addition we have to account for the contribution to (12) of $h = 0$, but this contribution is negligible by trivial estimations.

Let $S(H, K, P)$ be the sum given by (13) (in the notation we suppress the dependence on the test functions).

Using the bound $\widehat{w}(x, y) \ll_M (1+|x|)^{-M}(1+|y|)^{-M}$ we may assume that $H \ll_\varepsilon (P/A)^{1+\varepsilon}$ and $K \ll_\varepsilon (P/B)^{1+\varepsilon}$.

It will be necessary to use different techniques of estimation in different ranges. As a first step, we have the bound

$$\sum_{P\leq p<2P}\left|\sum_{H\leq h<2H} e\left(\frac{h^3\bar{k}^2}{p}\right)\right| \ll \left(H^{3/4}P + HP^{3/4} + H^{1/4}P^{5/4}\right)(HKP)^{\varepsilon}. \tag{14}$$

The proof is standard by Weyl's method. If we apply this to (13) (after using partial summation to separate the variables) we get the bound

$$S(H, K, P) \ll \left(H^{3/4}KP^{-1/2} + HKP^{-3/4} + H^{1/4}KP^{-1/4}\right)X^{\varepsilon}, \tag{15}$$

which is useful in some ranges.

To cover the ranges where (15) is insufficient we continue with (13).

We prefer to sum over relatively prime h and k, so we define $d = (h^3, k^2)$ and let d_0 be the least positive integer such that $d|d_0^3$. Since $d_0|h$ we may set $h = d_0h_0$. The condition $(h^3, k^2) = d$ is equivalent to $(h_0, k^2/d) = 1$ and $(d_0^3/d, k^2/d) = 1$. Then

$$\sum_h\sum_k e\left(\frac{-h^3\bar{k}^2}{p}\right) = \sum_k \sum_{\substack{d|k^2\\ (h_0,k^2/d)=1\\ (d_0^3/d,k^2/d)=1}}\sum_{h_0} e\left(\frac{-h_0^3(d_0^3/d)\overline{(k^2/d)}}{p}\right).$$

The point is that everything in the exponential is coprime with k^2/d (besides possibly $\overline{k^2/d}$) . Now we may employ the following elementary reciprocity formula

$$\frac{\bar{u}}{v}+\frac{\bar{v}}{u}\equiv\frac{1}{uv}\pmod 1, \tag{16}$$

where $u,v,\bar{u},\bar{v}$ are integers such that $(u,v)=1, u\bar{u}\equiv 1 \pmod v$, and $v\bar{v}\equiv 1 \pmod u$. This reciprocity law was also employed by [H-B] in his work on this problem. In our application $u=k^2/d$ and $v=p$. Now $S(H,K,P)$ has transformed into

$$\sum_{\substack{K\le k<2K\\ P\le p<2P}}\sum_{d|k^2}\sum_{\substack{\frac{H}{d_0}\le h_0<2\frac{H}{d_0}\\ (h_0,\frac{k^2}{d})=1\\ (\frac{d_0^3}{d},\frac{k^2}{d})=1}}\left(\frac{k}{p}\right)\psi_4(p)e\left(\frac{h_0^3(d_0^3/d)\bar{p}}{k^2/d}\right)e\left(\frac{-h_0^3d_0^3}{pk^2}\right)U(h_0,d_0,k,p), \tag{17}$$

where

$$U(h_0,d_0,k,p)=g(h_0d_0,k,p)\widehat{w}\left(\frac{h_0d_0A}{p},\frac{kB}{p}\right)\frac{2\log p}{p^{3/2}\log X}\widehat{\phi}\left(\frac{\log p}{\log X}\right).$$

To separate the variables we use the following expansion of additive characters into multiplicative characters via Gauss sums (see (3.11) of [IK], e.g.):

$$e\left(\frac{h_0^3(d_0^3/d)\bar{p}}{k^2/d}\right)=\frac{1}{\phi(k^2/d)}\sum_{\chi \,(\mathrm{mod}\ k^2/d)}\tau(\chi)\overline{\chi}(h_0^3(d_0^3/d)\bar{p}) \tag{18}$$

(valid because of the coprimality conditions), obtaining the identity

$$S(H,K,P)=\sum_{K\le k<2K}\sum_{d|k^2}\frac{1}{\phi(k^2/d)}\sum_{\chi \,(\mathrm{mod}\ k^2/d)}\tau(\chi)\overline{\chi}(d_0^3/d)Q(d,k,\chi), \tag{19}$$

where

$$Q(d,k,\chi)=\sum_{P\le p<2P}\sum_{\frac{H}{d_0}\le h_0<2\frac{H}{d_0}}\psi_4(p)\chi(p)\left(\frac{k}{p}\right)\overline{\chi}^3(h_0)e\left(\frac{-h_0^3d_0^3}{pk^2}\right)U(h_0,d_0,k,p).$$

Our goal is to get a good bound for $Q(d,k,\chi)$ and estimate the rest trivially.

We wish to apply Lemma 5.7 to $Q(d,k,\chi)$. To do so we must define a number of parameters and check that the conditions of Lemma 5.7 are satisfied. We set

$$F(u,v)=\left(\frac{v}{P}\right)^{-3/2}g(ud_0,k,v)\widehat{w}\left(\frac{ud_0A}{v},\frac{kB}{v}\right)\widehat{\phi}\left(\frac{\log v}{\log X}\right). \tag{20}$$

The character $\chi(u)$ in Lemma 5.7 is replaced by $\overline{\chi}^3(u)$ (with modulus $l_1=\frac{k^2}{d}$), while the character $\psi(v)$ in Lemma 5.7 is $\chi(v)\psi_4(v)(k/v)$ (with modulus $l_2=\mathrm{lcm}(4,k^*,\frac{k^2}{d})$, where k^* is the conductor of $(\frac{k}{v})$), $q=-\frac{k^2}{d_0^3}$, $U=\min\left\{\frac{H}{d_0},\frac{P}{d_0A}\right\}$, and $V=P$. We have

Claim. The test function $F(u,v)$ defined by (20) satisfies the conditions of Lemma 5.7 with $U=\min\{H/d_0,P/d_0A\}$ and $V=P$.

Proof of claim. The proof is a straightforward calculation. The only slightly thorny issue is that differentiation of $\widehat{w}$ with respect to v introduces a factor $(ud_0A/v)^{\alpha}$. This can be absorbed (for M large enough) by the bound of $(1+u/(v/d_0A))^{-M}$ on any partial derivative of $\widehat{w}$. □

To apply Lemma 5.7 to $Q(d,k,\chi)$ we must first extend the summation over p to prime powers instead of just primes. It is easy to see by trivial estimations that we can extend the summation to prime powers without changing the bound for $Q(d,k,\chi)$. Therefore we have

Corollary 5.3. *If $\chi\psi_4(k/\cdot)$ and χ^3 are nonprincipal, then*

$$Q(d,k,\chi) \ll P^{-1}\left(\frac{H}{d_0}\right)^{1/2}\left(1+\frac{H^{3/2}}{P^{1/2}k}\right)X^{\varepsilon}. \tag{21}$$

If $\chi\psi_4(k/\cdot)$ is principal but not χ^3, then a factor $P^{1/2}$ is lost. If χ^3 is principal but not $\chi\psi_4(k/\cdot)$, then a factor $(H/d_0)^{1/2}$ is lost.

Note. We use the standard notions of 'saving' and 'losing.' Namely, if we have an upper bound β in a certain situation, then we say that we lose a factor Y in another situation if the bound βY holds in this new situation. Likewise, we say that we have saved Y if the bound βY^{-1} holds.

Having obtained the bound for $Q(d,k,\chi)$ we apply it to $S(H,K,P)$. We have four cases according to which characters are principal. Let $S = S_1+S_2+S_3+S_4$, where S_1 corresponds to the terms where both characters are nonprincipal, S_2 corresponds to the terms where χ^3 is nonprincipal but $\chi\psi_4(k/\cdot)$ is not, S_3 corresponds to the terms where both characters are principal, and S_4 corresponds to the remaining terms where $\chi = \psi_4(k/\cdot)$ is nonprincipal.

Case 1. To bound the sum S_1 we apply Corollary 5.3 to (19), obtaining the bound

$$\begin{aligned} S_1 &\ll \sum_{K\le k<2K}\sum_{d\mid k^2}\frac{1}{\phi(k^2/d)}\sum_{\chi \,(\mathrm{mod}\ k^2/d)} P^{-1}\left(\frac{H}{d_0}\right)^{1/2}\left(1+\frac{H^{3/2}}{P^{1/2}k}\right)X^{\varepsilon}\,|\tau(\chi)| \\ &\ll H^{1/2}P^{-1}\left(1+\frac{H^{3/2}}{P^{1/2}K}\right)X^{\varepsilon}\sum_{K\le k<2K} k\sum_{d\mid k^2}\frac{1}{(dd_0)^{1/2}} \\ &\ll H^{1/2}P^{-1}\left(K^2+H^{3/2}KP^{-1/2}\right)X^{\varepsilon}. \end{aligned}$$

We require this bound to be $\ll X^{-\varepsilon}$. Using $H \ll (P/A)^{1+\varepsilon}$ and $K \ll (P/B)^{1+\varepsilon}$ shows the requirement is $P \ll X^{7/9-\varepsilon}$. The existence of $7/9$ here exhibits the limit of our method.

The cases where one or both of the characters are principal are tedious to carry out but do not pose a significant barrier to obtaining larger support.

It remains to bound the sum (19) when one or both of the characters are principal. The loss of cancellation in these cases will be made up for by the rarity of principal characters. First, $\overline{\chi}^3$ is trivial for $\ll k^{\varepsilon}$ characters χ. The character $\chi\psi_4(k/\cdot)$ is trivial for only the character $\chi = \psi_4(k/\cdot)\chi_0$. Therefore the only way both characters are trivial is if χ is trivial and $(k/\cdot)\psi_4$ is trivial (which forces k to be a square).

Case 2. In case $\overline{\chi}^3$ is trivial but not $\chi\psi_4(k/\cdot)$ we lose $(H/d_0)^{1/2}$ (from the loss of cancellation) but save $\phi(k^2/d)$ (from the rarity of such characters), which gives

the bound

$$S_2 \ll HP^{-1}\left(1+\frac{H^{3/2}}{P^{1/2}K}\right)X^{\varepsilon}\sum_{k}k^{-1}\sum_{d|k^2}\frac{\sqrt{d}}{d_0}$$
$$\ll HP^{-1}\left(1+\frac{H^{3/2}}{P^{1/2}K}\right)K^{1/3}X^{\varepsilon}$$

using only the obvious bound $d_0^{-1} \le d^{-1/3}$ (from $d|d_0^3$). Using $H \ll (P/A)^{1+\varepsilon}$ and $1 \ll K \ll (P/B)^{1+\varepsilon}$ and requiring this bound on S_2 to be $O(X^{-\varepsilon})$ means we must require $P \ll X^{5/6-\varepsilon}$.

Case 3. In case both characters are trivial we know k is a square and that $|\tau(\chi)| \le 1$. Using (19) and bounding $Q(d,k,\chi)$ trivially by PH/d_0 we easily get the bound of

$$S_3 \ll HP^{-1/2}X^{\varepsilon}\sum_{\substack{k=\square\\ K\le k<2K}}k^{-2}\sum_{d|k^2}\frac{d}{d_0} = HP^{-1/2}X^{\varepsilon}\sum_{(K)^{1/2}\le l<(2K)^{1/2}}l^{-4}\sum_{d|l^4}\frac{d}{d_0}.$$

Notice that if $a|d$, then $a/a_0 \le d/d_0$ (look at each prime separately). Therefore we have

$$S_3 \ll HP^{-1/2}X^{\varepsilon}\sum_{K^{1/2}\le l<(2K)^{1/2}}\prod_{p|l}p^{-2}$$
$$\ll HP^{-1/2}K^{-1/2}X^{\varepsilon},$$

which is $\ll X^{-\varepsilon}$ when $K \gg PX^{-2/3+\varepsilon}$. To handle $K \ll PX^{-2/3+\varepsilon}$ we simply apply Weyl's bound (14) when $k=\square$, $K \le k < 2K$. We thus obtain the bound

$$S_3 \ll \left(H^{3/4}P^{-1/2}+HP^{-3/4}+H^{1/4}P^{-1/4}\right)K^{1/2}X^{\varepsilon},$$

which is $\ll X^{-\varepsilon}$ (using $H \ll (P/A)^{1+\varepsilon}$ and $K \ll PX^{-2/3+\varepsilon}$) when $P \ll X^{7/9-\varepsilon}$. We expect that use of current technology would allow us to take P larger than $X^{7/9}$ here, but since we are restricted to $7/9$ elsewhere we do not pursue such a result.

Case 4. In the last case where $\chi\psi_4(k/\cdot)$ is trivial but $\overline{\chi}^3$ is not we lose $P^{1/2}$ but save $\phi(k^2/d)$. We get further savings by noticing that $\psi_4(k/\cdot)$ has conductor k^* equal to the square-free part of k (up to a factor of 2 or 4). Therefore $k^*|(k^2d^{-1})$ and hence $d|(k^2(k^*)^{-1})$. We get the bound

$$S_4 \ll H^{1/2}P^{-1/2}\left(1+\frac{H^{3/2}}{P^{1/2}K}\right)X^{\varepsilon}\sum_{K\le k<2K}k^{-1}\sum_{d|(k^2(k^*)^{-1})}\left(\frac{d}{d_0}\right)^{1/2}.$$

As before, $(d/d_0)^{1/2}$ is increasing with respect to divisibility, so we get the bound

$$S_4 \ll H^{1/2}P^{-1/2}\left(1+\frac{H^{3/2}}{P^{1/2}K}\right)X^{\varepsilon}\sum_{K\le k<2K}k^{-1}\prod_{p^2|k}p$$
$$\ll H^{1/2}P^{-1/2}X^{\varepsilon}\left(1+\frac{H^{3/2}}{P^{1/2}K}\right).$$

For this bound to be $\ll X^{-\varepsilon}$ it is necessary and sufficient that

$$H^2K^{-1} \ll PX^{-\varepsilon}. \tag{22}$$

We use a different method to estimate $Q(d,k,\chi)$ that works well for small k. In our current case we have

$$Q(d,k,\chi)=\sum_{\substack{P\le p<2P\\(p,k)=1}}\sum_{H/d_0\le h_0<2H/d_0} e\left(\frac{-h_0^3d_0^3}{pk^2}\right)\bar\chi^3(h_0)U(h_0,d_0,k,p).$$

We exploit cancellation in $\sum_{h_0}c_{h_0}e(-h_0^3d_0^3/pk^2)$ with arbitrary complex coefficients c_n. Precisely, we use the following.

Lemma 5.4. *Let c_n be complex numbers satisfying $|c_n|\le 1$ and let*

$$R(N,P,d_0,k)=\sum_{P\le p<2P}\left|\sum_{N\le n<2N} e\left(\frac{n^3d_0^3}{pk^2}\right)c_n\right|.$$

Then

$$R(N,P,d_0,k)\ll N^{1/2}P+N^{1/4}P^{5/4}k^{1/2}d_0^{-3/4}.$$

This is a special case of a more general result, which is stated and proved in Appendix B; specifically, we apply Lemma B.1 with $f(x)=x^3$, $g(x)=x^{-1}$, and $Y=N^3d_0^3P^{-1}k^{-2}$.

Applying Lemma 5.4 to $Q(d,k,\chi)$ via partial summation gives (actually one must separate the variables h_0 and p in $U(h_0d_0,k,p)$ before applying Lemma 5.4, which can be done in any standard way with no cost)

Corollary 5.5. *If $\chi\psi_4(k/\cdot)$ is principal and $\overline{\chi}^3$ is nonprincipal, then*

$$Q(d,k,\chi)\ll\left(\frac{H}{d_0}\right)^{1/2}P^{-1/2}+P^{-1/4}H^{1/4}k^{1/2}d_0^{-1}X^{\varepsilon}.$$

Applying Corollary 5.5 to S_4 gives the bound

$$S_4\ll\sum_{K\le k<2K}\sum_{d\mid k^2}d^{1/2}k^{-1}\left(\frac{H^{1/2}}{d_0^{1/2}P^{1/2}}+\frac{H^{1/4}k^{1/2}}{P^{1/4}d_0}X^{\varepsilon}\right).$$

Using the same techniques as before to estimate the sum over d gives the bound

$$S_4\ll\frac{H^{1/2}K^{1/2}}{P^{1/2}}X^{\varepsilon}+\frac{H^{1/4}K^{1/2}}{P^{1/4}}X^{\varepsilon}.$$

Using only $H\ll(P/A)^{1+\varepsilon}$ and $K\ll(P/B)^{1+\varepsilon}$ shows that the first term is $\ll X^{-\varepsilon}$ when $P\ll X^{5/6-\varepsilon}$. For the second term in the above bound to be sufficient we must have $K\ll P^{1/2}H^{-1/2}X^{-\varepsilon}(*)$. Assuming (22) does not hold (i.e. $H^2K^{-1}\gg PX^{-\varepsilon}$) and using $H\ll(P/A)^{1+\varepsilon}$ we see that (*) holds when $P\ll X^{5/6-\varepsilon}$. Having considered all possible cases the proof is complete. □

5.3. **A complete character sum.** In this section we evaluate a character sum which arose in our averaging. Set

$$\lambda_{a,b}(p)=-\sum_{x\,(\mathrm{mod}\ p)}\left(\frac{x^3+ax+b}{p}\right).$$

Note that this is $\lambda_E(p)$ for the elliptic curve given by the equation $y^2=x^3+ax+b$. Next, for any integers h and k define

$$T(h,k;p)=\sum_{\alpha\,(\mathrm{mod}\ p)}\sum_{\beta\,(\mathrm{mod}\ p)}\lambda_{\alpha,\beta}(p)e\left(\frac{\alpha h+\beta k}{p}\right).$$

Lemma 5.6. *Let $p > 2$ be prime and $\bar{k}$ be defined by $k\bar{k} \equiv 1 \pmod p$ if $(k,p) = 1$ and $\bar{0} = 0$. Then we have*

$$T(h,k;p) = -\varepsilon_p p^{3/2} \left(\frac{k}{p}\right) e\left(\frac{-h^3\bar{k}^2}{p}\right),$$

where ε_p is the sign of the Gauss sum.

Proof. By definition,

$$T(h,k;p) = -\sum_{x \,(\mathrm{mod}\ p)} \sum_{\alpha \,(\mathrm{mod}\ p)} \sum_{\beta \,(\mathrm{mod}\ p)} \left(\frac{x^3+\alpha x+\beta}{p}\right) e\left(\frac{\alpha h+\beta k}{p}\right).$$

The change of variables $\beta \to \beta - x^3 - \alpha x$ gives

$$\begin{aligned} T(h,k;p) &= \sum_{x \,(\mathrm{mod}\ p)} e\left(\frac{-x^3k}{p}\right) \sum_{\alpha \,(\mathrm{mod}\ p)} e\left(\frac{\alpha(h-xk)}{p}\right) \sum_{\beta \,(\mathrm{mod}\ p)} \left(\frac{\beta}{p}\right) e\left(\frac{\beta k}{p}\right) \\ &= -\varepsilon_p p^{3/2} \left(\frac{k}{p}\right) e\left(\frac{-h^3\bar{k}^2}{p}\right). \end{aligned}$$

□

5.4. **An estimate for an incomplete character sum in two variables.** In this section we establish a general estimate for a character sum in two variables that will be applied in our work. Precisely we have

Lemma 5.7. *Let $F(u,v)$ be a smooth function satisfying*

$$\left|F^{(\alpha_1,\alpha_2)}(u,v)u^{\alpha_1}v^{\alpha_2}\right| \le C(\alpha_1,\alpha_2)\left(1+\frac{|u|}{U}\right)^{-2}\left(1+\frac{|v|}{V}\right)^{-2} \tag{23}$$

for any $\alpha_1, \alpha_2 \ge 0$, the superscripts on F denoting partial differentiation. Then

$$\sum_u \sum_v \chi(u)\psi(v)\Lambda(v) e\left(\frac{u^c}{vq}\right) F(u,v) \ll U^{\frac{1}{2}} V^{\frac{1}{2}} \left(1+\frac{U^c}{V|q|}\right)^{1/2} (l_1 l_2 UV)^{\varepsilon}$$

where χ and ψ are nonprincipal Dirichlet characters to the moduli l_1 and l_2, respectively, Λ is the von Mangoldt function, q is a nonzero rational number, c is a positive integer, and ε is any positive number, the implied constant depending only on ε, c, and the numbers $C(\alpha_1,\alpha_2)$. In case χ is principal but not ψ the same bound holds but with $U^{1/2}$ lost. In case ψ is principal but not χ the same bound holds but with $V^{1/2}$ lost.

Recall that we are assuming the Riemann Hypothesis for all Dirichlet L-functions; this lemma, of course, relies heavily on the GRH.

Proof. First assume χ and ψ are nonprincipal. To begin, by Mellin inversion,

$$\begin{aligned} &\sum_u \sum_v \chi(u)\psi(v)\Lambda(v) e\left(\frac{u^c}{vq}\right) F(u,v) \\ &\qquad = \left(\frac{1}{2\pi i}\right)^2 \int_{(1/2+\varepsilon)} \int_{(1/2+\varepsilon)} L(s_1,\chi)\frac{L'}{L}(s_2,\psi) H(s_1,s_2)\,ds_1\,ds_2, \end{aligned}$$

where

$$H(s_1,s_2) = \int_0^\infty \int_0^\infty e\left(\frac{u^c}{vq}\right) F(u,v) u^{s_1} v^{s_2} \frac{du\,dv}{uv}.$$

Our goal is to obtain the bound

$$H(s_1,s_2) \ll \frac{U^{\sigma_1}V^{\sigma_2}}{|(s_1/c+s_2)(s_1/c+s_2+1)|\,|s_2|^{1+\varepsilon}}\left(1+\frac{U^c}{V|q|}\right)^{1/2}$$

for $\operatorname{Re} s_1 = \sigma_1$, $\operatorname{Re} s_2 = \sigma_2$, $\sigma_j = 1/2+\varepsilon$ or $1+\varepsilon$, and use the GRH for the bound $L(s_1,\chi)\frac{L'}{L}(s_2,\psi) \ll |s_1 s_2 l_1 l_2|^{\varepsilon/2}$. Putting these two estimates together will prove the desired result. The full details of the proof of the bound for $H(s_1,s_2)$ are contained in Appendix A.

In the cases where one of the characters is principal we integrate over the line $\operatorname{Re} s_j = 1+\varepsilon$ instead of $\operatorname{Re} s_j = 1/2+\varepsilon$ for the appropriate variable. The bounds on the L-functions are the same. This accounts for the square-root loss. The proof is now solely dependent on the details of Appendix A. □

5.5. **Proof of Corollary 3.4.** We follow an easy calculation in [ILS]. Take $w \geq 0$ and set

$$p_m(X) = \frac{1}{W_X(\mathcal{F})} \sum_{\substack{E\in\mathcal{F}\\ \operatorname{ord}_{s=1}L(s,f)=m}} w_X(E).$$

We define the (weighted) average analytic rank r by

$$r = \lim_{X\to\infty} \sum_{m=1}^{\infty} m p_m(X)$$

if the limit exists. Our method provides a bound on the lim sup of the above quantity. By taking a test function ϕ such that $\phi(x) \geq 0$, $\phi(0) = 1$, and support of $\widehat{\phi}$ contained in $[-\nu,\nu]$ we derive by Theorem 3.1 and the Plancherel theorem that

$$\sum_{m=1}^{\infty} m p_m(X) \leq g + o(X),$$

where

$$g = \int_{-\infty}^{\infty} \widehat{\phi}(y)\widehat{\mathcal{W}}(O)(y)dy.$$

This uses GRH for all elliptic curve L-functions so that by positivity we can drop all zeros not at the central point. If there were zeros off the central point, then $\phi(\gamma\frac{\log X}{2\pi})$ could be complex and the argument would fail.

By taking the Fourier pair

$$\phi(t) = \left(\frac{\sin(\pi\nu t)}{\pi\nu t}\right)^2, \quad \widehat{\phi}(y) = \frac{1}{\nu}\left(1-\frac{|y|}{\nu}\right)$$

we obtain $g = \frac{1}{\nu}+\frac{1}{2}$. Taking ν less than $7/9$ and letting $X\to\infty$ shows $r \leq 25/14+\varepsilon$ for any $\varepsilon > 0$. An identical calculation works for $\nu < 1+\delta$ and completes the proof. It is shown in Appendix A of [ILS] that this choice of test function is optimal for support $\nu < 1$.

A standard argument would allow us to remove the smooth weighting of the family and obtain the same upper bound for the average rank of the family $y^2 = x^3+ax+b$ where $|a| \leq X^{1/3}$, $|b| \leq X^{1/2}$.

5.6. **A note on minimality.** In this section we investigate the family given in Theorem 3.1 with the restriction that there are no primes q such that both $q^4|a$ and $q^6|b$. This condition ensures that the equation $E : y^2 = x^3 + ax + b$ is minimal for all $p > 3$. The result is the same as that stated in Theorem 3.1; we omit the precise statement for brevity.

The conductor condition (i.e. the analogue of Lemma 5.1) follows directly from Lemma 5.1.

The sum over the Fourier coefficients is hardly complicated by the divisibility restrictions. We easily have

$$\begin{aligned}\sum_{\substack{a\\ q^4|a\Rightarrow q^6\nmid b}}\sum_{b} P(E;\phi)w\left(\frac{a}{A},\frac{b}{B}\right) &= \sum_{p>3}\frac{2\log p}{p\log X}\widehat{\phi}\left(\frac{\log p}{\log X}\right)\sum_{\substack{a\\ q^4|a\Rightarrow q^6\nmid b}}\sum_{b}\lambda_{a,b}(p)w\left(\frac{a}{A},\frac{b}{B}\right)\\ &= \sum_{p>3}\frac{2\log p}{p\log X}\widehat{\phi}\left(\frac{\log p}{\log X}\right)\sum_{d}\mu(d)\sum_{a}\sum_{b}\lambda_{ad^4,bd^6}(p)w\left(\frac{ad^4}{A},\frac{bd^6}{B}\right)\\ &= \sum_{p>3}\frac{2\log p}{p\log X}\widehat{\phi}\left(\frac{\log p}{\log X}\right)\sum_{\substack{d\le\log X\\ (d,p)=1}}\mu(d)\sum_{a}\sum_{b}\lambda_{ad^4,bd^6}(p)w\left(\frac{ad^4}{A},\frac{bd^6}{B}\right)+o(AB).\end{aligned}$$

Completing the sum over a and $b \pmod p$ leads to the sum

$$AB\sum_{p>3}\sum_{\substack{d\le\log X\\ (d,p)=1}}\mu(d)\sum_{h}\sum_{k}\sum_{\alpha}\sum_{\beta}\lambda_{\alpha d^4,\beta d^6}(p)e\left(\frac{\alpha h+\beta k}{p}\right)\Phi(h,k,p)+o(AB),$$

where

$$\Phi(h,k,p)=\frac{2\log p}{p\log X}\widehat{\phi}\left(\frac{\log p}{\log X}\right)\widehat{w}\left(\frac{hA}{d^4p},\frac{kB}{d^6p}\right).$$

Applying the change of variables $\alpha\to\alpha d^{-4}$, $\beta\to\beta d^{-6}$ gives

$$AB\sum_{p>3}\frac{1}{p^2}\sum_{\substack{d\le\log X\\ (d,p)=1}}\frac{\mu(d)}{d^{10}}\sum_{h}\sum_{k}T(h\overline{d}^4,k\overline{d}^6;p)\Phi(h,k,p)+o(AB),$$

where T is given by Lemma 5.6. Applying Lemma 5.6 we obtain the sum

$$\frac{-AB}{\log X}\sum_{p>3}\varepsilon_p\frac{2\log p}{p^{3/2}}\widehat{\phi}\left(\frac{\log p}{\log X}\right)\sum_{\substack{d\le\log X\\ (d,p)=1}}\frac{\mu(d)}{d^{10}}\sum_{h}\sum_{k}\left(\frac{k}{p}\right)e\left(\frac{-h^3\bar{k}^2}{p}\right)\widehat{w}\left(\frac{hA}{d^4p},\frac{kB}{d^6p}\right).$$

Now simply remove the restriction $(d,p)=1$ and move the summation over d to the outside. We are back to the problem of estimating (12) except with slightly smaller A and B. We can simply use the same bounds as before; the presence of d contributes at worst bounded powers of $\log X$. Since we showed that each sum of type (13) is $\ll X^{-\varepsilon}$ we can use the same proof as for Lemma 5.2.

It is possible to impose minimality restrictions on the Weierstrass equations for other families. Since no interesting features arise we have limited our discussions to this brief note.

6. Proof of the density theorem for the main rank one family

In this section we prove Theorem 3.2. The proof will proceed much the same as Theorem 3.1 but the arguments will be more intricate.

6.1. **The conductor condition.** To show (9) holds we will apply Lemma 4.1. We take $R(d) = 16(4a^3 + 27b^4)$. Then $R(d) = |\Delta(d)| \asymp X$. All we need to show is

Proposition 6.1. *Let $A = X^{1/3}$ and $B = X^{1/4}$. Then*

$$\sum_a \sum_b \sum_{p^\alpha || \Delta} \frac{\log p^{\alpha-1}}{\log X} w\left(\frac{a}{A}, \frac{b}{B}\right) \ll \frac{X^{7/12}}{\log X},$$

where $\Delta = -16(4a^3 + 27b^4)$.

Proof. We may assume $\alpha = 2$ because a similar argument to that used in the proof of Lemma 5.1 with the roles of a and b switched will provide the necessary estimation for $\alpha \geq 3$. We may further assume $p > 3$ and that $(a, p) = (b, p) = 1$. We now make two separate arguments to handle p relatively small and p relatively large. For the former, we have

Lemma 6.2. *For $P = X^{1/3}$,*

$$\sum_{3 < p \leq P} \sum_{\substack{(a,p)=1 \\ \Delta \equiv 0 \,(\mathrm{mod}\ p^2)}} \sum_{(b,p)=1} \frac{\log p}{\log X} w\left(\frac{a}{A}, \frac{b}{B}\right) \ll \frac{X^{7/12}}{\log X},$$

the implied constant depending only on w.

For the latter we have

Lemma 6.3. *For $P = X^{11/36+\varepsilon}$*

$$\sum_{p \geq P} \sum_{\substack{a \\ p^2 || \Delta}} \sum_b \frac{\log p}{\log X} w\left(\frac{a}{A}, \frac{b}{B}\right) \ll \frac{X^{7/12}}{\log X},$$

the implied constant depending only on ε and w.

Since $11/36 < 1/3$ these two lemmas will allow us to take ε small enough to close the gap and complete the proof of Proposition 6.1. □

Proof of Lemma 6.2. By breaking the summation over a into congruence classes $(\mathrm{mod}\ p^2)$ we easily obtain the bound

$$\ll \sum_{p \leq P} \sum_{b \ll B} \left(1 + \frac{A}{p^2}\right) \frac{\log p}{\log X} \ll \frac{AB}{\log X} \left(1 + \frac{P}{A}\right),$$

which is sufficient provided $P \ll A = X^{1/3}$, as claimed. □

Proof of Lemma 6.3. By majorizing $|w|$ by a smooth nonnegative function with slightly larger support we may assume $w \geq 0$. The conditions on p imply that if

we write $|\Delta|$ as d^2l with l squarefree, then $d \geq P$. Therefore we have

$$\sum_{p\geq P}\sum_{\substack{a\\ p^2||\Delta}}\sum_{b}\frac{\log p}{\log X}w\left(\frac{a}{A},\frac{b}{B}\right) \leq \sum_{d\geq P}\sum_{\substack{a\\ |\Delta|=d^2l\\ l \text{ squarefree}}}\sum_{b} w\left(\frac{a}{A},\frac{b}{B}\right)$$
$$\leq \sum_{\substack{l\ll XP^{-2}\\ l \text{ squarefree}}}\sum_{a}\sum_{\substack{b\\ |\Delta|=d^2l}} w\left(\frac{a}{A},\frac{b}{B}\right).$$

Now define $s=(a,l)$. Since s is squarefree we must have $s|b$. Define $l=sl'$, $a=sa'$, and $b=sb'$. Then the condition on the discriminant is $4s^2a'^3+27s^3b'^4=(d/4)^2l'$. Since l is squarefree we have $(s,l')=1$, which implies $s|4^{-1}d$. Thus the condition is reduced to $4a'^3+27sb'^4=(d/4s)^2l'$. The important feature is that $(a',l')=(s,l')=1$ and $(b',l')=1$ or 2. Set $l'=(2,l')(3,l')l''$, $a'=(3,a')a''$, $b'=(2,b')b''$, and $s=(2,s)s'$. Then the discriminant condition becomes

$$\frac{4}{(2,l')}\frac{(3,a')^3}{(3,l')}(a'')^3+\frac{27}{(3,l')}\frac{(2,s)(2,b')^4}{(2,l')}s'(b'')^4=(d/4s)^2l''.$$

By taking all the possible combinations of values for $(2,l'),(3,l'),(3,a'),\ldots$, we are left with finitely many equations of the form $c_1a^3+c_2sb^4=u^2l$ with the condition $(c_1c_2abs,l)=1$. Therefore we are reduced to estimating sums of the type

$$\sum_{s\leq L}\sum_{\substack{l\leq L/s\\ l \text{ squarefree}}}{}' \sum_{\substack{a\\ c_1a^3+c_2sb^4=u^2l}}{}'\sum_{b}{}' w\left(\frac{as}{A},\frac{bs}{B}\right),$$

where $L\asymp XP^{-2}$ and the primes indicate the summation is restricted by $(c_1c_2abs,l)=1$. For squarefree l set

$$S(s,l)=\sum_{\substack{a\\ c_1a^3+c_2sb^4=u^2l}}{}'\sum_{b}{}' w\left(\frac{as}{A},\frac{bs}{B}\right).$$

Let $\mathcal{Q}$ be a set of primes q of size $q\asymp Q$ (some fixed proportion), with Q at our disposal (it will be chosen to be X^η for η small). We detect the condition that an integer m is a square by evaluating the Legendre symbol $\left(\frac{m}{q}\right)$ for $q\in\mathcal{Q}$ (a kind of amplification technique). We obtain

$$S(s,l)=\sum_{\substack{c_1a^3+c_2sb^4=cl\\ c=\square}}{}'\sum{}' w\left(\frac{as}{A},\frac{bs}{B}\right)$$
$$=\frac{1}{|\mathcal{Q}|^2}\sum_{\substack{c_1a^3+c_2sb^4=cl\\ c=\square}}{}'\sum{}'\left|\sum_{q\in\mathcal{Q}}\left(\frac{c}{q}\right)\right|^2 w\left(\frac{as}{A},\frac{bs}{B}\right)$$
$$+\frac{1}{|\mathcal{Q}|^2}\sum_{\substack{c_1a^3+c_2sb^4=cl\\ c=\square}}{}'\sum{}'|\{q\in\mathcal{Q}:q|c\}|^2\,w\left(\frac{as}{A},\frac{bs}{B}\right).$$

Simplifying it becomes

$$S(s,l) \le \frac{1}{|\mathcal{Q}|^2} \sideset{}{'}\sum_{\substack{a \\ c_1a^3+c_2sb^4 \equiv 0 \,(\mathrm{mod}\ l)}}\sideset{}{'}\sum_{b} \left|\sum_{q\in\mathcal{Q}} \left(\frac{(c_1a^3+c_2sb^4)l}{q}\right)\right|^2 w\left(\frac{as}{A},\frac{bs}{B}\right) + \frac{1}{|\mathcal{Q}|^2} \sideset{}{'}\sum_{\substack{c_1a^3+c_2sb^4=cl \\ c=\square}}\sideset{}{'}\sum |\{q\in\mathcal{Q} : q|cl\}|^2 w\left(\frac{as}{A},\frac{bs}{B}\right),$$

since in the first sum we have relaxed the condition that c is a square. For the second sum, notice that since $q \asymp Q$ and $cl \ll X$,

$$|\{q\in\mathcal{Q} : q|cl\}| \ll \frac{\log X}{\log Q}.$$

Therefore the second sum is $\ll (\log X/\log Q)^2|\mathcal{Q}|^{-2}S(s,l)$. If we let $S'(s,l)$ be the first sum above, then

$$S(s,l) \le \left(1-\frac{\log^2 X}{|\mathcal{Q}|^2\log^2 Q}\right)^{-1} S'(s,l).$$

Our choices of $\mathcal{Q}$ and Q will show $S(s,l) \ll S'(s,l)$, so we consider $S'(s,l)$. We expand the summation over q and obtain

$$S'(s,l) = \frac{1}{|\mathcal{Q}|^2}\sum_{q_1\in\mathcal{Q}}\sum_{q_2\in\mathcal{Q}}\sideset{}{'}\sum_{c_1a^3+c_2sb^4\equiv 0\,(\mathrm{mod}\ l)}\sideset{}{'}\sum \left(\frac{(c_1a^3+c_2sb^4)l}{q_1q_2}\right) w\left(\frac{as}{A},\frac{bs}{B}\right).$$

Let $S_2 = S_2(s,l,q_1,q_2)$ be the above summation over a and b. Set $r = q_1q_2$ and apply Poisson summation in a and b $(\mathrm{mod}\ lr)$. We get $S_2 =$

$$\frac{AB}{l^2r^2s^2}\sum_h\sum_k \sideset{}{'}\sum_{\substack{u\,(\mathrm{mod}\ lr) \\ c_1u^3+c_2sv^4\equiv 0\,(\mathrm{mod}\ l)}}\sideset{}{'}\sum_{v\,(\mathrm{mod}\ lr)} \left(\frac{(c_1u^3+c_2sv^4)l}{r}\right) e\left(\frac{hu+kv}{rl}\right)\widehat{w}\left(\frac{hA}{lrs},\frac{kB}{lrs}\right).$$

Using the Chinese remainder theorem we write $u = u_1r+u_2l$ with u_1 given $(\mathrm{mod}\ l)$ and u_2 given $(\mathrm{mod}\ r)$, and similarly for v. Then we get

$$S_2 = \frac{AB}{l^2r^2s^2}\sum_h\sum_k U(l,r,s)\widehat{w}\left(\frac{hA}{lrs},\frac{kB}{lrs}\right) \sideset{}{'}\sum_{\substack{u_1 \\ c_1u_1^3+c_2rsv_1^4\equiv 0\,(\mathrm{mod}\ l)}}\sideset{}{'}\sum_{v_1} e\left(\frac{hu_1+kv_1}{l}\right),$$

where

$$U(l,r,s) = \sum_{u_2\,(\mathrm{mod}\ r)}\sum_{v_2\,(\mathrm{mod}\ r)} \left(\frac{c_1u_2^3+c_2lsv_2^4}{r}\right) e\left(\frac{hu_2+kv_2}{r}\right).$$

Apply the change of variables $u_1 \to v_1u_1$ and obtain

$$\begin{aligned} S_2 &= \frac{AB}{l^2r^2s^2}\sum_h\sum_k U(l,r,s)\widehat{w}\left(\frac{hA}{lrs},\frac{kB}{lrs}\right) \sideset{}{'}\sum_{\substack{u_1 \\ c_1u_1^3+c_2rsv_1\equiv 0\,(\mathrm{mod}\ l)}}\sideset{}{'}\sum_{v_1} e\left(\frac{v_1(hu_1+k)}{l}\right) \\ &= \frac{AB}{l^2r^2s^2}\sum_h\sum_k U(l,r,s)\widehat{w}\left(\frac{hA}{lrs},\frac{kB}{lrs}\right) \sideset{}{'}\sum_{u_1\,(\mathrm{mod}\ l)} e\left(\frac{-c_1\overline{c_2rs}u_1^3(hu_1+k)}{l}\right), \end{aligned}$$

since $(c_1c_2rs, l) = 1$. It is easy to see that the exponential sum of u_1 modulo l factors into exponential sums of the form

$$\sum_{x \,(\mathrm{mod}\ p)}{}' e\left(\frac{\alpha_p x^3(hx+k)}{p}\right),$$

where $l = \prod_p p$ and $(\alpha_p, p) = 1$. A corollary of the Riemann Hypothesis for curves (cf. [Sch], Corollary 2F) implies that the summation over x is $O(p^{1/2})$ (the implied constant absolute), unless both h and k are zero $(\mathrm{mod}\ p)$, in which case the sum is exactly $p-1$. Therefore the summation over u_1 is $\ll l^{1/2}(h,k,l)^{1/2}\tau(l)$, unless $h = k = 0$, in which case the bound is l. Clearly $U(l,r,s) \ll r^{3/2} + r^2\delta_{q_1q_2}$, so we get the bound

$$\begin{aligned} S_2 &\ll \frac{AB}{l^2r^2s^2}(r^{\frac{3}{2}} + r^2\delta_{q_1q_2})\left(l^{\frac{1}{2}+\varepsilon}\sum_{\substack{h\\(h,k)\neq(0,0)}}\sum_{k}(h,k,l)^{\frac{1}{2}}\left(1+\frac{hA}{lrs}\right)^{-2}\left(1+\frac{kB}{lrs}\right)^{-2} + l\right) \\ &\ll \frac{AB}{l^2r^2s^2}(r^{\frac{3}{2}} + r^2\delta_{q_1q_2})\left(l^{\frac{1}{2}+\varepsilon}\frac{l^2r^2s^2}{AB} + l^{\frac{1}{2}+\varepsilon}\frac{lrs(A+B)}{AB} + l\right) \\ &\ll (r^{\frac{3}{2}} + r^2\delta_{q_1q_2})\left(l^{\frac{1}{2}+\varepsilon} + l^{-\frac{1}{2}+\varepsilon}\frac{A}{rs} + \frac{AB}{lr^2s^2}\right), \end{aligned}$$

the symmetric occurences of A and B being destroyed in the final inequality since $B \ll A$ (recall that $A = X^{1/3}$ and $B = X^{1/4}$). Therefore

$$S'(s,l) \ll Q^3\left(1+\frac{Q}{|\mathcal{Q}|}\right)\left(l^{1/2+\varepsilon} + l^{-1/2+\varepsilon}\frac{A}{sQ^2} + \frac{AB}{ls^2Q^4}\right).$$

On summation over $l \ll Ls^{-1}$ and $s \leq L$ we get

$$\sum_{s\leq L}\sum_{l\leq Ls^{-1}} S'(s,l) \ll \left(1+\frac{Q}{|\mathcal{Q}|}\right)\left(Q^3L^{3/2+\varepsilon} + AQL^{1/2+\varepsilon} + \frac{AB\log L}{Q}\right).$$

We take $Q = X^{\varepsilon}$ and $|\mathcal{Q}| \gg \sqrt{Q}$ (which implies $S(s,l) \ll S'(s,l)$). The necessary bound on this sum is $\ll X^{7/12-\varepsilon}$, which means the requirement on L is $L \ll X^{7/18-\varepsilon}$. Since $L \asymp X/P^2$ the requirement on P is $P \geq X^{11/36+\varepsilon}$. Now the proof of Lemma 6.3 is complete. □

6.2. **Estimating the sum of the Fourier coefficients.** In this section we evaluate $\mathcal{P}(\mathcal{F}; \phi, w_X)$ for the family given in Theorem 3.2. This is accomplished with

Lemma 6.4. *Set $A = X^{1/3}$ and $B = X^{1/4}$. Then*

$$\sum_a\sum_b -P(E;\phi)w\left(\frac{a}{A},\frac{b}{B}\right) = \phi(0)W_X(\mathcal{F}) + O\left(\frac{X^{7/12}}{\log X}\right)$$

provided supp $\widehat{\phi} \subset (-\frac{23}{48}, \frac{23}{48})$.

We mimic the proof of Lemma 5.2. The details are similar, so we often condense our arguments.

Proof. On Poisson summation,

$$\sum_a \sum_b P(E;\phi) w\left(\frac{a}{A}, \frac{b}{B}\right)$$
$$= AB \sum_{p>3} \frac{2\log p}{p^3 \log X} \widehat{\phi}\left(\frac{\log p}{\log X}\right) \sum_h \sum_k T'(h,k;p) \widehat{w}\left(\frac{hA}{p}, \frac{kB}{p}\right),$$

where

$$T'(h,k;p) = \sum_{\alpha \,(\mathrm{mod}\ p)} \sum_{\beta \,(\mathrm{mod}\ p)} \lambda_{\alpha,\beta^2}(p) e\left(\frac{\alpha h + \beta k}{p}\right).$$

The complete sum T' can be evaluated explicitly; the calculation is made with Lemma 6.6. The $\delta(h)\delta(k)p^2$ term in T' gives the extra $\phi(0)W_X(\mathcal{F})$ (by the Prime Number Theorem). The p term is negligible via trivial estimations. We are left with estimating the sum

$$AB \sum_{p>3} \sum_h \sum_k \varepsilon_p \frac{2\log p}{p^{3/2} \log X} \widehat{\phi}\left(\frac{\log p}{\log X}\right) \left(\frac{-h}{p}\right) e\left(\frac{\bar{h}^3 k^4 \bar{2}^6}{p}\right) \widehat{w}\left(\frac{hA}{p}, \frac{kB}{p}\right).$$

Estimating this sum trivially obtains our result for support up to 7/18.

To get larger support we need to show there is cancellation in the sum. We estimate it in exactly the same way we did in the proof of Lemma 5.2. First replace ε_p by a character $\psi_4 \pmod 4$. Then break up the sum into dyadic segments using partitions of unity. It suffices to consider sums of the type

(24)
$$\sum_{\substack{H \le h < 2H \\ K \le k < 2K \\ P \le p < 2P}} \sum \sum \psi_4(p) \left(\frac{-h}{p}\right) e\left(\frac{\bar{h}^3 k^4 \bar{2}^6}{p}\right) \frac{\log p}{p^{3/2}} \widehat{\phi}\left(\frac{\log p}{\log X}\right) \widehat{w}\left(\frac{hA}{p}, \frac{kB}{p}\right) g(h,k,p),$$

where g is a function arising from the partitions of unity. The contribution from $k = 0$ is negligible by trivial estimations. Let $S(H,K,P)$ be the sum given by (24). It suffices to show $S(H,K,P) \ll X^{-\varepsilon}$.

Using the bound $\widehat{w}(x,y) \ll (1+|x|)^{-M}(1+|y|)^{-M}$ we may assume that $H \ll (P/A)^{1+\varepsilon}$ and $K \ll (P/B)^{1+\varepsilon}$.

In order to sum over coprime integers we set $d = (k^4, 2^6 h^3)$ and define d_0 to be the least positive integer such that $d | d_0^4$. Since $d_0 | k$ we may set $k = d_0 k_0$. The condition $(k^4, 2^6 h^3) = d$ is equivalent to the two conditions $(d_0^4/d, 2^6 h^3/d) = 1$ and $(k_0, 2^6 h^3/d) = 1$. Therefore $S(H,K,P)$ is

$$\sum_{\substack{H \le h < 2H \\ P \le p < 2P}} \sum_{\substack{d | 2^6 h^3 \\ \left(\frac{d_0^4}{d}, \frac{2^6 h^3}{d}\right) = 1}} \sum_{\substack{\frac{K}{d_0} \le k_0 < 2\frac{K}{d_0} \\ \left(k_0, 2^6 \frac{h^3}{d}\right) = 1}} \psi_4(p) \left(\frac{-h}{p}\right) e\left(\frac{(d_0^4/d) k_0^4 \overline{(2^6 h^3/d)}}{p}\right) U(k_0, d, h, p),$$

where

$$U(k_0, d, h, p) = g(h, k_0 d_0, p) \widehat{w}\left(\frac{hA}{p}, \frac{d_0 k_0 B}{p}\right) \frac{\log p}{p^{3/2}} \widehat{\phi}\left(\frac{\log p}{\log X}\right).$$

We apply the elementary reciprocity formula and the expansion of the exponential into multiplicative characters as in the proof of Lemma 5.2 and obtain

$$S(H,K,P)=\sum_{H\le h<2H}\sum_{d|2^6h^3}\frac{1}{\phi(2^6h^3/d)}\sum_{\chi\,(\mathrm{mod}\ 2^6h^3/d)}\tau(\chi)\bar{\chi}(d_0^4/d)Q(d,h,\chi), \tag{25}$$

where

$$Q(d,h,\chi)=\sum_{P\le p<2P}\sum_{K/d_0\le k_0<2K/d_0}\psi_4(p)\chi(p)\left(\frac{-h}{p}\right)\bar{\chi}^4(k_0)e\left(\frac{d_0^4k_0^4}{2^6ph^3}\right)U(k_0,d,h,p).$$

Since the arguments are now extremely similar to those used in the proof of Lemma 5.2 we will be brief. We apply Lemma 5.7 to $Q(d,h,\chi)$ and obtain

Lemma 6.5. *If $\chi\psi_4(-h/\cdot)$ and χ^4 are nonprincipal, then*

$$Q(d,h,\chi)\ll P^{-1}K^{1/2}d_0^{-1/2}\left(1+\frac{K^4}{PH^3}\right)^{1/2}X^{\varepsilon}.$$

If χ^4 is principal but $\chi\psi_4(-h/\cdot)$ is not principal we lose a factor $K^{1/2}d_0^{-1/2}$.

Let $S=S_1+S_2+S_3$, where S_1 corresponds to the terms where both characters are nonprincipal, S_2 corresponds to the terms where χ^4 is principal but $\chi\psi_4(-h/\cdot)$ is not principal, and S_3 corresponds to the remaining terms where $\chi\psi_4(-h/\cdot)$ is principal (and necessarily χ^4 is principal).

Case 1. We apply Lemma 6.5 to S_1 and obtain the bound

$$\begin{aligned}S_1&\ll P^{-1}K^{1/2}\left(1+\frac{K^4}{PH^3}\right)^{1/2}X^{\varepsilon}\sum_{H\le h<2H}\sum_{d|2^6h^3}h^{3/2}(dd_0)^{-1/2}\\&\ll P^{-1}H^{5/2}K^{1/2}\left(1+\frac{K^2}{P^{1/2}H^{3/2}}\right)X^{\varepsilon},\end{aligned}$$

which is $\ll X^{-\varepsilon}$ when $P\ll X^{23/48-\varepsilon}$.

Case 2. Applying Lemma 6.5 to S_2 gives

$$\begin{aligned}S_2&\ll P^{-1}K\left(1+\frac{K^4}{PH^3}\right)^{1/2}X^{\varepsilon}\sum_{H\le h<2H}h^{-3/2}\sum_{d|2^6h^3}d^{1/2}d_0^{-1}\\&\ll P^{-1}K\left(1+\frac{K^2}{P^{1/2}H^{3/2}}\right)X^{\varepsilon}.\end{aligned}$$

Using only $K\ll(P/B)^{1+\varepsilon}$ and $H\gg 1$ shows this is $\ll X^{-\varepsilon}$ when $P\ll X^{1/2-\varepsilon}$.

Case 3. Now consider the case where $\chi\psi_4(-h/\cdot)$ (and hence χ^4) are principal. Since $\psi_4(-h/\cdot)$ has conductor h^* equal to the squarefree part of h (up to a factor of 2 or 4) we get extra savings from the restriction $d|2^6h^3(h^*)^{-1}$. Thus χ has its conductor of size $h^*\ll h$, so $|\tau(\chi)|\ll h^{1/2}$. We therefore have the bound

$$\begin{aligned}S_3&\ll P^{-1/2}H^{-5/2}KX^{\varepsilon}\sum_{H\le h<2H}\sum_{d|2^6h^3/h^*}\frac{d}{d_0}\\&\ll P^{-1/2}KX^{\varepsilon}\prod_p\left(1+p^{-3/2}+\dots\right),\end{aligned}$$

which is $\ll X^{-\varepsilon}$ when $P\ll X^{1/2-\varepsilon}$ since the infinite product converges. Having considered all possible cases the proof is complete. □

6.3. **A complete character sum.** As in the proof of Theorem 3.1 we need to evaluate a complete character sum. We do this now. Set

$$T'(h,k;p)=\sum_{\alpha \,(\mathrm{mod}\ p)}\sum_{\beta\,(\mathrm{mod}\ p)}\lambda_{\alpha,\beta^2}(p)e\left(\frac{\alpha h+\beta k}{p}\right).$$

We have

Lemma 6.6. *Let $p>2$ be prime and $\bar{h}$ be defined by $h\bar{h}\equiv 1 \pmod p$ if $(h,p)=1$ and $\bar{0}=0$. Then we have*

$$T'(h,k;p)=-p^2\delta(h)\delta(k)-\varepsilon_p p^{3/2}\left(\frac{-h}{p}\right)e\left(\frac{k^4\bar{h}^3\bar{2}^6}{p}\right)+p,$$

where δ is the Kronecker delta function $(\mathrm{mod}\ p)$.

Proof. By definition,

$$\begin{aligned}T'(h,k;p)&=-\sum_{x\,(\mathrm{mod}\ p)}\sum_{\alpha\,(\mathrm{mod}\ p)}\sum_{\beta\,(\mathrm{mod}\ p)}\left(\frac{x^3+\alpha x+\beta^2}{p}\right)e\left(\frac{\alpha h+\beta k}{p}\right)\\&=-\sum_{\alpha}\sum_{\beta}\left(\frac{\beta^2}{p}\right)e\left(\frac{\alpha h+\beta k}{p}\right)-\sum_{x\neq 0}\sum_{\alpha}\sum_{\beta}\left(\frac{x^3+\alpha x+\beta^2}{p}\right)e\left(\frac{\alpha h+\beta k}{p}\right)\\&=T_1'+T_2',\end{aligned}$$

say. We easily have

$$T_1'=\begin{cases}-p(p-1) & \text{if } h\equiv k\equiv 0 \pmod p,\\ p & \text{if } h\equiv 0, k\not\equiv 0 \pmod p,\\ 0 & \text{if } h\not\equiv 0 \pmod p.\end{cases}$$

The sum T_2' is, after the linear change of variables $\alpha\to\alpha-x^2-\beta^2\bar{x}$, given by

$$\begin{aligned}T_2'&=-\sum_{x\neq 0}\left(\frac{x}{p}\right)\sum_{\beta}e\left(\frac{-h\beta^2\bar{x}+\beta k-hx^2}{p}\right)\sum_{\alpha}\left(\frac{\alpha}{p}\right)e\left(\frac{\alpha h}{p}\right)\\&=-\varepsilon_p p^{1/2}\left(\frac{h}{p}\right)\sum_{x\neq 0}\left(\frac{x}{p}\right)e\left(\frac{-hx^2}{p}\right)\sum_{\beta}e\left(\frac{-h\beta^2\bar{x}+\beta k}{p}\right)\\&=-\varepsilon_p p^{1/2}\left(\frac{h}{p}\right)\sum_{x\neq 0}\left(\frac{x}{p}\right)e\left(\frac{-hx^2}{p}\right)\sum_{\beta}e\left(\frac{-hx\beta^2+xk\beta}{p}\right)\ (\text{from } \beta\to x\beta).\end{aligned}$$

To evaluate the summation over β we apply the formula

$$\sum_{x\,(\mathrm{mod}\ p)}e\left(\frac{ax^2+bx}{p}\right)=\begin{cases}\varepsilon_p\sqrt{p}\left(\frac{a}{p}\right)e\left(\frac{-\bar{a}b^2\bar{4}}{p}\right) & \text{if } (a,p)=1,\\ p & \text{if } a\equiv b\equiv 0 \pmod p,\\ 0 & \text{otherwise.}\end{cases}\tag{26}$$

We obtain

$$T_2'=-\varepsilon_p^2 p\left(\frac{h^2}{p}\right)\left(\frac{-1}{p}\right)\sum_{x\neq 0}e\left(\frac{-hx^2+k^2\bar{h}\bar{4}x}{p}\right).$$

Applying (26) again we obtain

$$T_2' = -p\left(\frac{h^2}{p}\right)\left(\varepsilon_p\sqrt{p}\left(\frac{-h}{p}\right)e\left(\frac{\bar{h}^3k^4\bar{2}^6}{p}\right)-1\right).$$

Gathering terms and simplifying we finish the proof of the lemma. □

7. Conjecturally enlarging the support for the family of all elliptic curves

7.1. **A conjecture on the size of a character sum.** In this section we investigate heuristically the behavior of $\mathcal{D}(\mathcal{F};\phi,w_X)$ for the family given in Theorem 3.1 when we extend the support of $\widehat{\phi}$ outside the range $(-1,1)$. Recall that this is the splitting point for the symmetry types O, $SO(\text{even})$, and $SO(\text{odd})$. We predict that the symmetry type is O. To provide evidence for this conjecture, we need to argue that

$$\sum_a\sum_b P(E;\phi)w\left(\frac{a}{A},\frac{b}{B}\right) = o(AB)$$

for $\widehat{\phi}$ with large support. From (12) and (17) the problem is basically reduced to estimating the following character sum:

$$\sum_{k\le K}\sum_{h\le H}\sum_{p\le P}\left(\frac{k}{p}\right)e\left(\frac{h^3}{pk^2}\right)e\left(\frac{h^3\bar{p}}{k^2}\right), \tag{27}$$

with certain relations on the sizes of H, K, and P. One of the relations is $H^3/PK^2 \asymp 1$, so for heuristic purposes we ignore the $e(h^3/pk^2)$ term.

Conjecture 7.1. There exist $\delta > 0$ and $\varepsilon > 0$ such that if $k \le P$, k is not a square (i.e. the character $(k/\cdot)$ is nonprincipal), and $H = P^{2/3+\delta}$, then

$$\sum_{h\le H}\sum_{p\le P}\left(\frac{k}{p}\right)e\left(\frac{h^3\bar{p}}{k^2}\right) \ll P^{1-3\delta/2-\varepsilon}.$$

On summation over $k \le P^{1/2+3\delta/2}$ this conjecture would indicate that Theorem 3.1 remains true with test functions whose Fourier transforms $\widehat{\phi}$ have support outside of $(-1,1)$. The extent to which the support could exceed $(-1,1)$ would depend on the value of δ. Precisely, we would obtain support up to $(1-3\delta)^{-1}$. The heuristic used in Section 7.2 lends support to the value $\delta = 1/48$, which would give support up to $16/15$.

7.2. **Evidence for Conjecture 7.1.** To lend support for Conjecture 7.1 we investigate the same sum but with p ranging over positive integers coprime with k instead of primes. We have

Theorem 7.2. *Let $H = P^{2/3+\delta}$, $k \asymp K = H^{3/2}P^{-1/2}$. Then for any $\varepsilon > 0$ we have*

$$\sum_h{}' \sum_m \left(\frac{m}{k}\right)e\left(\frac{h^3\bar{m}}{k^2}\right)w\left(\frac{h}{H},\frac{m}{P}\right) \ll_\varepsilon P^{5/6+c\delta+\varepsilon},$$

where the prime indicates the summation is restricted to $(h,k) = 1$ and c is a positive constant (the proof gives $c = 13/2$).

Taking $\delta < \frac{1}{6}(c+\frac{3}{2})^{-1}$ and ε small enough will show that the sum is $\ll P^{1-3\delta/2-\varepsilon}$ for positive δ and ε. The value $c = 13/2$ allows us to take any $\delta < 1/48$.

Proof. Let $S = S(k)$ be the sum to be estimated. By Poisson summation in m (mod k^2),

$$\begin{aligned} S &= \sideset{}{'}\sum_h \sum_m \left(\frac{m}{k}\right) e\left(\frac{h^3\bar{m}}{k^2}\right) w\left(\frac{h}{H}, \frac{m}{P}\right) \\ &= \frac{P}{k^2}\sideset{}{'}\sum_h \sum_l \sum_{x \,(\mathrm{mod}\ k^2)} \left(\frac{x}{k}\right) e\left(\frac{h^3\bar{x}+lx}{k^2}\right) w\left(\frac{h}{H}, \frac{\widehat{lP}}{k^2}\right), \end{aligned}$$

where the hat over the second variable indicates we have taken the Fourier transform in that variable only. Recall $K^2 = H^3/P = P^{1+3\delta}$, so $k^2/P \asymp P^{3\delta}$. Now write $x = y(1+kz)$ where y and z range over representatives (mod k). Then $\bar{x} = \bar{y}(1-kz)$ where $\bar{y}$ is the multiplicative inverse of y(mod k^2). We obtain

$$\begin{aligned} S &= \frac{P}{k^2}\sideset{}{'}\sum_h \sum_l w\left(\frac{h}{H}, \frac{\widehat{lP}}{k^2}\right) \sum_{y \,(\mathrm{mod}\ k)} \sum_{z \,(\mathrm{mod}\ k)} \left(\frac{y}{k}\right) e\left(\frac{h^3\bar{y}(1-kz)+ly(1+kz)}{k^2}\right) \\ &= \frac{P}{k^2}\sideset{}{'}\sum_h \sum_l w\left(\frac{h}{H}, \frac{\widehat{lP}}{k^2}\right) \sum_{y \,(\mathrm{mod}\ k)} \left(\frac{y}{k}\right) e\left(\frac{h^3\bar{y}+ly}{k^2}\right) \sum_{z \,(\mathrm{mod}\ k)} e\left(\frac{z(-h^3\bar{y}+ly)}{k}\right) \\ &= \frac{P}{k}\sideset{}{'}\sum_h \sum_{\substack{l \\ ly^2 \equiv h^3 \,(\mathrm{mod}\ k)}} \sum_{y \,(\mathrm{mod}\ k)} \left(\frac{y}{k}\right) e\left(\frac{h^3\bar{y}+ly}{k^2}\right) w\left(\frac{h}{H}, \frac{\widehat{lP}}{k^2}\right). \end{aligned}$$

Write $h = h_0 + h_1 k$ where $h_0 \asymp H$, $(h_0, k) = 1$, $h_1 \asymp H/k$, h_0 takes values in an interval of length k, and h_1 takes values in an interval of length $\asymp H/k$. Now extend the summation over h_0 to an interval of length $\asymp H$, so the sum is repeated $\asymp H/k$ times. We obtain

$$S \ll \frac{P}{k}\frac{k}{H}\sideset{}{'}\sum_{h_0} \sum_{\substack{l \\ ly^2 \equiv {h_0}^3 \,(\mathrm{mod}\ k)}} \sum_{y \,(\mathrm{mod}\ k)} \sum_{h_1} \left(\frac{y}{k}\right) e\left(\frac{h_0^3\bar{y}+3h_0^2h_1k\bar{y}}{k^2}\right) e\left(\frac{ly}{k^2}\right) w\left(\frac{h_0+h_1k}{H}, \frac{\widehat{lP}}{k^2}\right).$$

Applying the change of variables $y \to h_0^2\bar{y}$ gives

$$S \ll \frac{P}{k}\frac{k}{H}\sideset{}{'}\sum_{h_0} \sum_{\substack{l \\ y^2 \equiv lh_0 \,(\mathrm{mod}\ k)}} \sum_{y \,(\mathrm{mod}\ k)} \sum_{h_1} \left(\frac{y}{k}\right) e\left(\frac{h_0^2l\bar{y}}{k^2}\right) e\left(\frac{(h_0+3h_1k)y}{k^2}\right) w\left(\frac{h_0+h_1k}{H}, \frac{\widehat{lP}}{k^2}\right).$$

There will be virtually no oscillation in $e((h_0 + 3h_1k)y/k^2)$ if $y \ll P^\varepsilon k^2/H \ll P^{1/3+2\delta+\varepsilon}$. On the other hand, if $y \gg P^{1/3+2\delta+\varepsilon}$, then it is easily shown that the summation over h_1 is $\ll_{\varepsilon,M} P^{-M}$. Therefore we have fixed $0 < y \ll P^\varepsilon K^2/H$. Thus the sum is reduced to

$$S \ll \frac{P}{H} \sum_{|h_1| \ll H/k} \sideset{}{'}\sum_{h_0} \sum_{\substack{l \\ y^2 \equiv lh_0 \,(\mathrm{mod}\ k)}} \sum_{0 < y \ll P^\varepsilon K^2/H} \left(\frac{y}{k}\right) e\left(\frac{h_0^2l\bar{y}}{k^2}\right) w_1(h_0, h_1, k, l, y),$$

where w_1 is the new test function obtained by absorbing the nonoscillatory exponential factor into w (any process of differentiation of w_1 with respect to y introduces only factors of size P^ε). Now we apply the elementary reciprocity law (16), obtaining

$$S \ll \frac{P}{H} \sum_{|h_1| \ll H/k} \sum_{h_0} \sum_{\substack{l \\ y^2 \equiv l h_0 \,(\mathrm{mod}\ k)}} \sum_{0<y \ll P^\varepsilon K^2/H} \left(\frac{y}{k}\right) e\left(-\frac{h_0^2 \bar{k}^2 l}{y}\right) e\left(\frac{h_0^2 l}{y k^2}\right) w_1(h_0, h_1, k, l, y).$$

The equality $y^2 = lh_0 + sk$ means $|s| \ll (P^{2/3+4\delta}/k)^{1+\varepsilon} \ll P^{1/6+5\delta/2+\varepsilon}$. Then the sum is reduced to

$$\begin{aligned} S &\ll \frac{P}{H} \sum_{|h_1| \ll \frac{H}{k}} \sum_{h_0} \sum_{\substack{l \\ y^2 = l h_0 + sk}} \sum_{0<y \ll P^\varepsilon \frac{K^2}{H}} \left(\frac{y}{k}\right) e\left(-\frac{s^2 \bar{l}}{y}\right) e\left(\frac{(y^2 - sk)^2}{lyk^2}\right) w_1(h_0, h_1, k, l, y) \\ &= \frac{P}{H} \sum_{|h_1| \ll H/k} \sum_{s} \sum_{\substack{l \\ y^2 \equiv sk \,(\mathrm{mod}\ l)}} \sum_{0<y \ll P^\varepsilon K^2/H} \left(\frac{y}{k}\right) e\left(\frac{s^2 \bar{y}}{l}\right) e\left(-\frac{s^2}{ly} + \frac{(y^2 - sk)^2}{lyk^2}\right) w_2, \end{aligned}$$

where $w_2 = w_2(s, h_1, k, l, y)$ is the replacement of w_1 after the change of variables which eliminates h_0 and introduces s. Now we break the summation over y into progressions (mod l) and apply the Pólya-Vinogradov bound of

$$\sum_{\substack{y \ll Y \\ y \equiv \lambda \ (\mathrm{mod}\ l)}} \left(\frac{y}{k}\right) \ll (lY)^{1/2} \log lY$$

to S (via partial summation). We thus obtain the bound

$$\begin{aligned} S &\ll P^\varepsilon \frac{P}{H} \frac{H}{k} P^{1/6+5\delta/2} \left(\frac{k^2}{P}\right)^{3/2} \frac{k}{H^{1/2}} \\ &\ll P^\varepsilon P^{1+1/6+5\delta/2+9\delta/2-1/3-\delta/2} \\ &= P^{5/6+13\delta/2+\varepsilon}, \end{aligned}$$

which completes the proof. □

8. Curves with prescribed torsion

In this section we study in detail the family of elliptic curves with prescribed torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. There are a variety of other families with different torsion groups that exhibit similar behavior; we merely summarize some results and refer to either [Y1] or [Y2] for further details.

Each torsion family has its own interesting features. One common feature is that the square divisors of the conductor are generally rather easy to control. The source of this ease is that the discriminants factor into polynomials of smaller degree. In addition, the conductors are often much smaller than the discriminant because of high multiplicity in one or more of these polynomial factors. This fact causes these torsion families to have a rather large number of curves with conductor $N \le X$.

We refer to the paper of Kubert [Ku] as a reference for these torsion families. In particular Table 3 contains essentially all the information we use.

8.1. **Torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.** In this section we investigate a particularly interesting family of elliptic curves, given in Weierstrass form by

$$E : y^2 = x(x-a)(x+b).$$

E has discriminant

$$\Delta = 16a^2b^2(a+b)^2.$$

The torsion group is generated by the points $(0,0)$ and $(-a,0)$ and

$$\lambda(p) = -\sum_{x \,(\mathrm{mod}\ p)} \left(\frac{x(x-a)(x+b)}{p}\right).$$

Helfgott has shown that the root number in this family is equidistributed [He2].

We have the following.

Theorem 8.1. *Let $\mathcal{F}$ be the family of elliptic curves given by the Weierstrass equations $E_{a,b} : y^2 = x(x-a)(x+b)$ with a and b positive integers. Set $A = B = X^{1/3}$, let w be a smooth compactly supported function on $\mathbb{R}^+ \times \mathbb{R}^+$, and set $w_X(E_{a,b}) = w\left(\frac{a}{A}, \frac{b}{B}\right)$. Then*

$$\mathcal{D}(\mathcal{F}; \phi, w_X) \sim [\widehat{\phi}(0) + \tfrac{1}{2}\phi(0)]W_X(\mathcal{F}) \ \text{ as } X \to \infty,$$

for ϕ with supp $\widehat{\phi} \subset (-\frac{2}{3}, \frac{2}{3})$.

This family has particular interest because we can sum primes up to the size of the family (we are taking $\asymp AB = X^{2/3}$ curves), a natural barrier for any family (since square-root cancellation coming solely from averaging over the family gives us this support; to go further requires additional cancellation in the $\lambda(p)$'s as p varies, at least on average). To prove Theorem 8.1 we need two lemmas. For the conductor condition we have

Lemma 8.2. *Let $\mathcal{F}$ be the family given in Theorem* 8.1*. Then*

$$\sum_a \sum_b \frac{\log N}{\log X} w\left(\frac{a}{A}, \frac{b}{B}\right) = W_X(\mathcal{F}) + O\left(\frac{AB}{\log X}\right).$$

Proof. We will apply Lemma 4.1. We take $R(d) = ab(a+b)$. Then it is clear that $R(d) \asymp X$ and that the irreducible factors of $R(d)$ all divide $\Delta(d)$. We first consider

$$\sum_a \sum_b \sum_{\substack{p || ab(a+b) \\ p^2 | N,\ p>3}} w\left(\frac{a}{A}, \frac{b}{B}\right) \log p.$$

This sum is empty because $p^2|N$ implies $p|(a,b)$ (since $x(x-a)(x+b)$ has a triple root (mod p)). To estimate the sum

$$\sum_a \sum_b \sum_{p^\alpha || ab(a+b)} w\left(\frac{a}{A}, \frac{b}{B}\right) \log p^{\alpha-1}$$

we suppose $p^\gamma || a$ and $p^\delta || b$. Thus $p^{\alpha-\gamma-\delta} || a+b$. We first suppose $\gamma \neq \delta$. By symmetry we may assume $\gamma < \delta$ (which implies $p^\gamma || a+b$ and $\gamma < \alpha/3$). Since $a \asymp A = B = X^{1/3}$ we always have $p \ll X^{1/3}$. Then we get the bound

$$\sum_{\substack{p^\alpha \ll X \\ \alpha > 0 \\ p \ll X^{1/3}}} \sum_{\gamma \leq \alpha/3} \left(1 + \frac{A}{p^\gamma}\right)\left(1 + \frac{B}{p^{\alpha-2\gamma}}\right) \log p^{\alpha-1} \ll X^{2/3}.$$

In case $\gamma = \delta$ we apply the change of variables $a \to a'p^\gamma, b \to b'p^\gamma$ and get the bound

$$\sum_{\substack{p^\alpha \ll X \\ \alpha>0 \\ p \ll X^{1/3}}} \sum_{\gamma \le \alpha/3} \sum_{\substack{a' \\ p^{\alpha-3\gamma} || a'+b'}} \sum_{b'} w\left(\frac{a'p^\gamma}{A}, \frac{b'p^\gamma}{B}\right) \log p^{\alpha-1}.$$

For fixed a', b' is determined (mod $p^{\alpha-3\gamma}$), so we get the bound

$$\sum_{\substack{p^\alpha \ll X \\ \alpha>0 \\ p \ll X^{1/3}}} \sum_{\gamma \le \alpha/3} \left(1 + \frac{A}{p^\gamma}\right)\left(1 + \frac{B}{p^{\alpha-2\gamma}}\right) \log p^{\alpha-1},$$

which is the same bound we have for $\gamma \neq \delta$, so the proof is complete. □

The sum over the Fourier coefficients is handled with

Lemma 8.3. *Let $\mathcal{F}$ be the family given in Theorem* 8.1. *Then*

$$\sum_a \sum_b P(E;\phi) w\left(\frac{a}{A}, \frac{b}{B}\right) \ll \frac{X^{2/3}}{\log X}$$

provided supp $\widehat{\phi} \subset (-\frac{2}{3}, \frac{2}{3})$.

Proof. Set

$$S(p) = \sum_a \sum_b \lambda(p) w\left(\frac{a}{A}, \frac{b}{B}\right)$$

so that

$$\sum_a \sum_b P(E;\phi) w\left(\frac{a}{A}, \frac{b}{B}\right) = \sum_{p>3} S(p) \frac{2\log p}{p \log X} \widehat{\phi}\left(\frac{\log p}{\log X}\right).$$

Then

$$\begin{aligned} S(p) &= -\sum_{x \,(\mathrm{mod}\ p)} \sum_a \sum_b \left(\frac{x(x-a)(x+b)}{p}\right) w\left(\frac{a}{A}, \frac{b}{B}\right) \\ &= -\frac{AB}{p^2} \sum_h \sum_k \sum_{x,\rho,\sigma \,(\mathrm{mod}\ p)} \left(\frac{x(x-\rho)(x+\sigma)}{p}\right) e\left(\frac{\rho h + \sigma k}{p}\right) \widehat{w}\left(\frac{hA}{p}, \frac{kB}{p}\right) \\ &= -\frac{AB}{p^2} \sum_h \sum_k \sum_{x,\rho,\sigma \,(\mathrm{mod}\ p)} \left(\frac{x\rho\sigma}{p}\right) e\left(\frac{-\rho h + \sigma k + x(h-k)}{p}\right) \widehat{w}\left(\frac{hA}{p}, \frac{kB}{p}\right) \\ &= -\frac{AB}{p^{1/2}} \varepsilon_p \sum_h \sum_k \left(\frac{hk(h-k)}{p}\right) \widehat{w}\left(\frac{hA}{p}, \frac{kB}{p}\right). \end{aligned}$$

To get further cancellation we sum over p. To handle the variation of ε_p we introduce a character ψ_4 (mod 4) evaluated at p. For those terms with $(hk(h-k)/\cdot)\psi_4$ nontrivial we appeal to the Riemann Hypothesis for Dirichlet L-functions to obtain the bound (summing $p \le P$)

$$\frac{AB}{P} P^\varepsilon \frac{P^2}{AB} = P^{1+\varepsilon},$$

which is $\ll X^{2/3-\varepsilon}$ when $P \ll X^{2/3-\varepsilon}$, i.e. the restriction on the support of $\widehat{\phi}$ is 2/3.

When $(hk(h-k)/\cdot)\psi_4$ is trivial we do not obtain any savings in the summation over p. The character is trivial only if $hk(h-k) = \pm\square$, so the problem amounts to estimating the number of such solutions. This is carried out by the following.

Lemma 8.4. *Let*

$$C(Y) = \{(h,k) \in \mathbb{Z}^2 : |h| + |k| \le Y,\ hk(h-k) = \pm\square\}.$$

Then $|C(Y)| \ll_\varepsilon Y^{1+\varepsilon}$.

Before proving the lemma we apply it to our sum. By the rapid decay of the Fourier transform we may assume $|h|, |k| \ll (PA^{-1})^{1+\varepsilon}$. Using the value $Y = (PA^{-1})^{1+\varepsilon}$ in the lemma we obtain the bound

$$\frac{AB}{P^{1/2}} \sum_{p \le P} |C(Y)| \ll BP^{1/2+\varepsilon}$$

on the contribution of the terms with trivial character $(hk(h-k)/\cdot)\psi_4$. The contribution is $\ll X^{2/3-\varepsilon}$ when $P \ll X^{2/3-\varepsilon}$, as desired. This will complete the proof of Lemma 8.3 (and hence Theorem 8.1) once we prove Lemma 8.4. □

Proof of Lemma 8.4. Suppose we have a solution $hk(h-k) = \pm\square$ where $|h|+|k| \le Y$. By possibly changing the signs of h and k and switching the values of h and k we may assume $h > 0$, $k > 0$, and $h > k$ (the cases where $hk(h-k) = 0$ are trivial). Set $g = (h,k)$ and let $g = d^2 l$ where l is squarefree. Set $h = gh'$ and $k = gk'$. Then we have $lh'k'(h'-k') = \square$. Since $(h',k') = 1$ and l is squarefree we must have $l = l_1 l_2 l_3$ where $l_1 | h'$, $l_2 | k'$, $l_3 | (h'-k')$ and hence each of $l_1 h'$, $l_2 k'$, and $l_3(h'-k')$ must be a square. Thus $h' = l_1 \cdot \square$, $k' = l_2 \cdot \square$, and $h' - k' = l_3 \cdot \square$. Thus every solution to $hk(h-k) = \square$ is given by

$$h = d^2 l_1^2 l_2 l_3 x^2, \quad k = d^2 l_1 l_2^2 l_3 y^2,$$

where

$$l_1 x^2 = l_2 y^2 + l_3 z^2, \tag{28}$$

with the restrictions $(x,y) = (x,z) = (y,z) = 1$, $l = l_1 l_2 l_3$ is squarefree, and each l_i is positive. But now notice that the solution (28) gives rise to the factorization

$$l_1 l_2 x^2 = (l_2 y + \sqrt{-l_2 l_3}\, z)(l_2 y - \sqrt{-l_2 l_3}\, z).$$

The number of such factorizations is clearly bounded by $d_{\mathbb{Q}(\sqrt{-l_1 l_2})}(lx^2)$, the divisor function in the ring of integers of the field $\mathbb{Q}(\sqrt{-l_2 l_3})$. It is well known that $d_K(n) \le c(\varepsilon)(|N_K(n)|)^\varepsilon$ where $N_K(n)$ is the norm in the number field K and $c(\varepsilon)$ does not depend on the field K. Using $h = d^2 l_1 l x^2 \ge d^2 l x^2$ we easily get the bound $|C(Y)| \ll Y^{1+\varepsilon}$. □

8.2. **Curves with three-torsion.** Consider the elliptic curve $E_{a,b}$ given by

$$E_{a,b} : y^2 + axy - by = x^3.$$

E has discriminant

$$\Delta = -(a^3 + 27b)b^3.$$

The point $(0,0)$ is nonsingular and has order three. In fact, all curves over $\mathbb{Q}$ with three-torsion are $\mathbb{Q}$-isomorphic to one in our family [Ku].

We have the following density theorem for this family.

Theorem 8.5. *Let $\mathcal{F}$ be the family of elliptic curves given by the Weierstrass equations $E_{a,b} : y^2 + axy - by = x^3$ and set $A = X^{1/6}$ and $B = X^{1/2}$. Then the analogue of Theorem* 8.1 *holds for this family provided* supp $\widehat{\phi} \subset (-\frac{1}{2}, \frac{1}{2})$.

Notice that $W_X(\mathcal{F}) = \widehat{w}(0,0)AB + o(AB)$, so we are taking $\asymp AB = X^{2/3}$ curves from our family.

8.3. **Curves with two-torsion.** In this section we investigate the family given by

$$E_{a,b} : y^2 = x(x^2 + ax - b).$$

E has discriminant

$$\Delta = 16b^2(a^2 + 4b).$$

We have the following.

Theorem 8.6. *Let $\mathcal{F}$ be the family of elliptic curves given by the Weierstrass equations $E_{a,b} : y^2 = x(x^2 + ax - b)$ and set $A = X^{1/4}$ and $B = X^{1/2}$. Then the analogue of Theorem* 8.1 *holds for this family provided* supp $\widehat{\phi} \subset (-\frac{1}{2}, \frac{1}{2})$.

8.4. **Curves with four-torsion.** In this section we consider the family of curves $E = E(b)$ given by

$$E : y^2 + xy - by = x^3 - bx^2.$$

This curve has discriminant $\Delta = \Delta(b)$ given by

$$\Delta = b^4(1 + 16b).$$

The parameter c_4 is

$$c_4 = 16b^2 + 16b + 1.$$

The torsion group is cyclic of order 4 and is generated by the point $(0, 0)$.

We have the following density theorem.

Theorem 8.7. *Let $\mathcal{F}$ be the family of elliptic curves given by the Weierstrass equations $E_b : y^2 + xy - by = x^3 - bx^2$ and set $B = X^{1/2}$. Then the analogue of Theorem* 8.1 *holds for this family provided* supp $\widehat{\phi} \subset (-\frac{1}{2}, \frac{1}{2})$.

Note that we can sum primes as large as the size of the family here.

9. A positive rank family of quadratic twists

Many people have studied families of quadratic twists, especially the aspect of rank frequencies amongst these families. For instance, Stewart and Top [ST] and Rubin and Silverberg [RS] have produced examples of infinite families of twists with ranks as large as 3. In this section we investigate families composed of quadratic twists of a given fixed curve.

We consider a fixed elliptic curve

$$E : y^2 = x^3 + ax + b$$

and twist it by an integer d, giving the curve

$$E_d : dy^2 = x^3 + ax + b.$$

Let N be the conductor of E and N_d be the conductor of E_d. If d is squarefree and $(d, N) = 1$ the twisted conductor is given by

$$N_d = d^2N.$$

Provided $d \equiv 1 \pmod 4$ and $(d, N) = 1$ the root number w_d of E_d satisfies

$$w_d = \left(\frac{d}{-N}\right) w,$$

where w is the root number of E.

Now let $\mathcal{A}$ be a set of integers. We set

$$\mathcal{D}(\mathcal{A}; \phi, w_X) = \sum_{d \in \mathcal{A}} D(E_d; \phi) w_X(d).$$

We measure this sum against

$$W_X(\mathcal{A}) = \sum_{d \in \mathcal{A}} w_X(d).$$

Before specializing the family $\mathcal{A}$ we set up our machinery. As always, we will employ the explicit formula (7). To obtain a density we need the conductor condition

$$\sum_{d \in \mathcal{A}} \frac{\log N_d}{\log X} w_X(d) \sim \sum_{d \in \mathcal{A}} w_X(d) \text{ as } X \to \infty \tag{29}$$

and an evaluation of the sum of the Fourier coefficients

$$\sum_{d \in \mathcal{A}} P(E_d; \phi) w_X(d). \tag{30}$$

The sum of the Fourier coefficients may reveal extra zeros, depending on the family $\mathcal{A}$. It is particularly simple to calculate $\lambda(p)$ for quadratic twists since $\lambda_{E_d}(p) = \left(\frac{d}{p}\right) \lambda_E(p)$. Thus

$$\sum_{d \in \mathcal{A}} P(E_d; \phi) w_X(d) = \sum_p \lambda_E(p) \frac{2 \log p}{p \log X} \widehat{\phi}\left(\frac{\log p}{\log X}\right) \sum_{d \in \mathcal{A}} \left(\frac{d}{p}\right) w_X(d). \tag{31}$$

We consider a lacunary family of quadratic twists. Instead of twisting by all squarefree integers we twist by integers d of the form $d = u^3 + au + b$. When we do so the twisted curve E_d always has the point $(u, 1)$, so in general we expect the curve to have positive rank. For this family we have the density theorem.

Theorem 9.1. *Let $E : y^2 = x^3 + ax + b$ be a fixed elliptic curve. Let $\mathcal{A}$ be the set of all integers of the form $u^3 + au + b$ for u an integer. Let w be a smooth compactly supported function on $\mathbb{R}^+$, set $U = X^{1/6}$, and take $w_X(d) = w\left(\frac{u}{U}\right)$. Then we have*

$$\mathcal{D}(\mathcal{A}; \phi, w_X) \sim [\widehat{\phi}(0) + \tfrac{3}{2}\phi(0)] W_X(\mathcal{A}) \text{ as } X \to \infty,$$

for ϕ with supp $\widehat{\phi} \subset (-\frac{1}{6}, \frac{1}{6})$.

Notice that we can sum primes up to the size of the family here.

For notational simplicity we sum over u and take $w\left(\frac{u}{U}\right)$ as our test function.

9.1. **The conductor condition.** We first treat the conductor condition (29). The result is

Lemma 9.2. *With notation as in Theorem* 9.1*,*

$$\sum_u \frac{\log N_{u^3+au+b}}{\log X} w\left(\frac{u}{U}\right) = X^{1/6} \widehat{w}(0) + O\left(\frac{X^{1/6}}{\log^{1/4} X}\right).$$

Proof. It suffices to consider

$$\frac{1}{\log U}\sum_{u}\log\left(\frac{N_{u^3+au+b}}{(u^3+au+b)^2}\right)=\frac{1}{\log U}\sum_{u}\sum_{\substack{p^\beta||N_{u^3+au+b}\\ p^{2\alpha}||(u^3+au+b)^2}}\log p^{\beta-2\alpha}w\left(\frac{u}{U}\right).$$

We may trivially sum over the terms with $\alpha=0$, so we may assume $p|u^3+au+b$ and therefore $\beta=2$. Thus we obtain the sum

$$\frac{1}{\log U}\sum_{u}\sum_{\substack{p^\alpha||u^3+au+b\\ \alpha>0}}2\log p^{\alpha-1}w\left(\frac{u}{U}\right).$$

By splitting the summation over u into progressions (mod p^α) we get the bound

$$\frac{1}{\log U}\sum_{\substack{p^\alpha\ll U^3\\ \alpha\geq 3}}\log p^{\alpha-1}\left(1+U/p^\alpha\right)\ll\frac{U}{\log U},$$

so we may assume $\alpha=2$. Using the same technique we can sum $p\ll U$ when $\alpha=2$. In case u^3+au+b is reducible (over $\mathbb{Z}$) we immediately get $p\ll U$, so we may assume u^3+au+b is irreducible. To handle large p we use the same method as Lemma 6.3 to obtain

$$\sum_{p\geq P}\sum_{u^3+au+b\equiv 0\,(\mathrm{mod}\ p^2)}\frac{\log p}{\log U}\,w\left(\frac{u}{U}\right)\ll\sum_{d\geq P}\sum_{u^3+au+b=d^2l}\left|w\left(\frac{u}{U}\right)\right|.$$

We may bound $|w|$ by a smooth nonnegative function with slightly larger support. Abusing notation we rename w to be this new function. Setting

$$S(l)=\sum_{u^3+au+b=d^2l}w\left(\frac{u}{U}\right)$$

we get

$$S(l)\left(1-\frac{\log^2 U}{|\mathcal{Q}|^2\log^2 Q}\right)$$
$$\leq\frac{1}{|\mathcal{Q}|^2}\sum_{q_1}\sum_{q_2}\sum_{u^3+au+b\equiv 0\,(\mathrm{mod}\ l)}\left(\frac{l}{q_1q_2}\right)\left(\frac{u^3+au+b}{q_1q_2}\right)w\left(\frac{u}{U}\right),$$

where $\mathcal{Q}$ and Q are defined as in Lemma 6.3. We have compressed a number of steps because the calculations are identical to those used in the proof of Lemma 6.3. Let S_1 be the inner sum over u, set $r=q_1q_2$, and apply Poisson summation in $u\ (\mathrm{mod}\ lr)$ to obtain

$$S_1=\frac{U}{lr}\sum_{h}\sum_{\substack{x\,(\mathrm{mod}\ lr)\\ x^3+ax+b\equiv 0\,(\mathrm{mod}\ l)}}\left(\frac{l}{r}\right)\left(\frac{x^3+ax+b}{r}\right)e\left(\frac{xh}{lr}\right)\widehat{w}\left(\frac{hU}{lr}\right).$$

Write $x=x_1r+x_2l$ where x_1 is given (mod l) and x_2 is given (mod r) and get

$$S_1=\frac{U}{lr}\left(\frac{l}{r}\right)\sum_{h}\widehat{w}\left(\frac{hU}{lr}\right)Y(h,l,r),$$

where

$$Y(h,l,r) = \sum_{x_2 \,(\mathrm{mod}\ r)} \left(\frac{x_2^3 + ax_2 + b}{r}\right) e\left(\frac{x_2 h\bar{l}}{r}\right) \sum_{\substack{x_1 \,(\mathrm{mod}\ l) \\ x_1^3 r^3 + ax_1 r + b \equiv 0 \,(\mathrm{mod}\ l)}} e\left(\frac{x_1 h}{l}\right).$$

If $q_1 \neq q_2$, the summation over x_2 is $O(r^{1/2})$ by the Riemann Hypothesis for curves (Weil's bound). If $q_1 = q_2$, then the summation over x_2 is $r\delta_r(h) + O(1)$ (here $\delta_r(y)$ is the characteristic function of the arithmetic progression $y \equiv 0 \pmod r$). The summation over x_1 is bounded by $\rho(l)$, where $\rho(l)$ is the number of solutions to $x^3 + ax + b \equiv 0 \pmod l$ (since we may assume $(l, r) = 1$). Therefore we have the bound

$$S_1 \ll \rho(l)\left(r^{1/2} + \frac{U}{lr^{1/2}} + \frac{U}{l}\delta_{q_1=q_2}\right)$$

and hence

$$S(l)\left(1 - \frac{\log^2 U}{|\mathcal{Q}|^2 \log^2 Q}\right) \ll \frac{U}{|\mathcal{Q}|}\frac{\rho(l)}{l} + Q\rho(l).$$

Using the Prime Ideal Theorem we get the bounds $\sum_{l \leq L} \rho(l) \ll L$ and $\sum_{l \leq L} \rho(l) l^{-1} \ll 1$ (since we may assume $u^3 + au + b$ is irreducible), so

$$\sum_{l \leq L} S(l)\left(1 - \frac{\log^2 U}{|\mathcal{Q}|^2 \log^2 Q}\right) \ll \frac{U}{|\mathcal{Q}|} + LQ.$$

Now we take $Q \asymp \log U \log\log U$, $|\mathcal{Q}| \gg \log U$, and $L = U/\log^{3/2} U$ to obtain

$$\sum_{l \leq L} S(l) \ll \frac{U}{\sqrt{\log U}}.$$

Converting L to P via $LP^2 \asymp U^3$ means we can sum over $p \geq U \log^{3/4} U$. To close the gap we exploit the rarity of primes; for any $U_1 \geq U$ we have

$$\begin{aligned}\sum_{U \leq p \leq U_1} \sum_{u^3 + au + b \equiv 0 \,(\mathrm{mod}\ p^2)} w\left(\frac{u}{U}\right) &\ll \sum_{U \leq p \leq U_1} \left(1 + \frac{U}{p}\right) \\ &\ll \frac{U_1}{\log U_1} \ll \frac{U}{\log^{1/4} U},\end{aligned}$$

for the choice $U_1 = U \log^{3/4} U$. The proof is now complete. □

9.2. **The sum of Fourier coefficients.** As for condition (31), we calculate

$$-\sum_u \left(\frac{u^3 + au + b}{p}\right) w\left(\frac{u}{U}\right) = \frac{U}{p}\lambda_E(p)\widehat{w}(0) + O(p^{1/2}).$$

Therefore we obtain

$$\begin{aligned}
&\sum_{p\le P}\lambda_E(p)\frac{2\log p}{p\log X}\widehat{\phi}\left(\frac{\log p}{\log X}\right)\left(\frac{U}{p}\lambda_E(p)\widehat{w}(0)+O(p^{1/2})\right)\\
=\;& U\widehat{w}(0)\sum_{p\le P}\lambda_E^2(p)\frac{2\log p}{p^2\log X}\widehat{\phi}\left(\frac{\log p}{\log X}\right)+O\left(\frac{P}{\log X}\right)\\
=\;& U\widehat{w}(0)\sum_{p\le P}\chi_0(p)\frac{2\log p}{p\log X}\widehat{\phi}\left(\frac{\log p}{\log X}\right)\\
+\;& U\widehat{w}(0)\sum_{p\le P}\left[\frac{\lambda_f^2(p)}{p}-\chi_0(p)\right]\frac{2\log p}{p\log X}\widehat{\phi}\left(\frac{\log p}{\log X}\right)+O\left(\frac{P}{\log X}\right)\\
=\;& U\widehat{w}(0)\phi(0)+O\left(\frac{U\log\log X}{\log X}\right)+O\left(\frac{P}{\log X}\right),
\end{aligned}$$

by the Prime Number Theorem and the Riemann Hypothesis for the symmetric-square L-function associated to E. This bound is sufficient provided $P\ll U$, i.e., supp $\widehat{\phi}\subset\left(-\frac{1}{6},\frac{1}{6}\right)$.

Appendix A. A technical character sum

Recall our goal is to obtain the bound

$$H(s_1,s_2)\ll\frac{U^{\sigma_1}V^{\sigma_2}}{|(s_1/c+s_2)(s_1/c+s_2+1)||s_2|^{1+\varepsilon}}\left(1+\frac{U^c}{V|q|}\right)^{1/2},$$

where

$$H(s_1,s_2)=\int_0^\infty\int_0^\infty e\left(\frac{u^c}{vq}\right)F(u,v)u^{s_1}v^{s_2}\frac{dudv}{uv}.$$

This will complete the proof of Lemma 5.7.

We note first that the trivial bound on $H(s_1,s_2)$ is $U^{\sigma_1}V^{\sigma_2}$. We begin with the change of variables $t=u^c/(vq)$, obtaining

$$\begin{aligned}
H(s_1,s_2)&=\int\int e(t)F((tvq)^{1/c},v)(tvq)^{s_1/c}v^{s_2}\frac{dtdv}{ctv}\\
&=\int e(t)(tq)^{s_1/c}\left(\int G(t,v)v^{s_1/c+s_2-1}dv\right)\frac{dt}{ct},
\end{aligned}$$

where $G(t,v)=F((tvq)^{1/c},v)$.

At this point it is helpful to discuss the condition (23) in further detail. Suppose we have a function F satisfying (23) and change variables to x and y, where $u=u(x,y)$ and $v=v(x,y)$. Set $G(x,y)=F(u(x,y),v(x,y))$. On the supposition that

$$(*)\qquad |u^{(\alpha_1,\alpha_2)}(x,y)x^{\alpha_1}y^{\alpha_2}|\le C'(\alpha_1,\alpha_2)$$

and likewise for v, then we claim G also satisfies (23) with respect to x and y (with perhaps new constants $C(\alpha_1,\alpha_2)$ of course). This claim is easily proved by using the chain rule.

Notice that if $u=c_1x^{a_1}y^{b_1}$ and $v=c_2x^{a_2}y^{b_2}$ for some $a_i,b_i\ge 0$, $c_i\in\mathbb{R}$, then u and v satisfy (*).

Now we continue with our treatment of $H(s_1, s_2)$. In the inner integral we apply integration by parts twice, obtaining

$$\int G(t,v)v^{s_1/c+s_2}\frac{dv}{v} = \frac{1}{(s_1/c+s_2)(s_1/c+s_2+1)}\int G_1(t,v)v^{s_1/c+s_2}\frac{dv}{v},$$

where

$$G_1(t,v) = v^2\frac{\partial^2 G}{\partial v^2}(t,v).$$

Notice that G_1 satisfies (23). Therefore, at the expense of differentiating twice we have obtained the convergence factor $((s_1/c+s_2)(s_1/c+s_2+1))^{-1}$; i.e., we have the bound

$$H(s_1,s_2) \ll |(s_1/c+s_2)(s_1/c+s_2+1)|^{-1}\left|\int\int e(t)G((tvq)^{1/c},v)(tvq)^{s_1/c}v^{s_2}\frac{dtdv}{tv}\right|.$$

Now we concentrate on the t-variable aspect, specifically the integral

$$\int_0^\infty e(t)G_1(t,v)t^{s_1/c-1}dt = \int_0^\infty e^{il(t)}G_1(t,v)t^{-1+\sigma_1/c}dt,$$

where $s_1 = \sigma_1 + ir_1$ and $l(t) = 2\pi t + (r_1\log t)/c$. We expect that there should be a lot of cancellation in this integral as long as $l(t)$ has some variation, i.e. away from points where $l'(t) = 0$. Note $l'(t)$ has its only zero at $t_0 = -r_1/(2c\pi)$. Suppose $t_0 > 0$. Let $f_1 + f_2 + f_3$ be a partition of unity such that

$$f_1(t) = \begin{cases} 1 & \text{for } t < 1/2 \\ 0 & \text{for } t > 3/4 \end{cases}, \qquad f_2(t) = \begin{cases} 0 & \text{for } |t-1| > 1/2 \\ 1 & \text{for } |t-1| < 1/4 \end{cases},$$

$$f_3(t) = \begin{cases} 0 & \text{for } t < 5/4 \\ 1 & \text{for } t > 3/2 \end{cases}.$$

Using the partition (with arguments scaled by t_0) break up the integral into three pieces:

$$\int_0^{3t_0/4} + \int_{t_0/2}^{3t_0/2} + \int_{5t_0/4}^\infty.$$

For the first integral, we compute

$$\begin{aligned}
&\int_0^{3t_0/4} e^{il(t)}G_1(t,v)t^{-1+\sigma_1/c}f_1(t/t_0)dt \\
&\qquad = \int_0^{3t_0/4} il'(t)e^{il(t)}\frac{G_1(t,v)t^{-1+\sigma_1/c}f_1(t/t_0)}{il'(t)}dt \\
&\qquad = -\int_0^{3t_0/4} e^{il(t)}\left[\frac{G_1(t,v)t^{-1+\sigma_1/c}f_1(t/t_0)}{il'(t)}\right]'dt \\
&\qquad = -i\int_0^{3t_0/4} e^{il(t)}\frac{G_2(t,v)t^{-2+\sigma_1/c}l'(t) + G_3(t,v)t^{-1+\sigma_1/c}l''(t)}{l'(t)^2}dt,
\end{aligned}$$

where G_2 and G_3 satisfy (23). The boundary term for $t = 0$ is nonexistent because $l'(t) \asymp t^{-1}$ as $t \to 0$. The integral simplifies to

$$\int_0^{3t_0/4} e^{il(t)}G_4(t,v)t^{-1+\sigma_1/c}R(t)dt,$$

where G_4 satisfies (23) and $R(t) = \frac{d_0 t + d_1 r_1}{(t-t_0)^2}$ for d_0 and d_1 absolute constants. Apply integration by parts one more time in this integral and obtain

$$-\int_0^{3t_0/4} e^{il(t)} \left[\frac{G_4(t,v)t^{-1+\sigma_1/c}R(t)}{il'(t)}\right]' dt.$$

The boundary term at $3t_0/4$ is zero because $f_1 \equiv 0$ for $t \geq 3/4$. The boundary term at 0 is zero because $R(t) \asymp 1$ as $t \to 0$. Now

$$\begin{aligned}\left[\frac{G_4(t,v)t^{-1+\sigma_1/c}R(t)}{il'(t)}\right]' &= \left[\frac{G_4(t,v)t^{-1+\sigma_1/c}}{il'(t)}\right]' R(t) + \left[\frac{G_4(t,v)t^{-1+\sigma_1/c}}{il'(t)}\right] R'(t) \\ &= G_5(t,v)t^{-1+\sigma_1/c}\widetilde{R}(t),\end{aligned}$$

where G_5 again satisfies (23) and

$$\widetilde{R}(t) = \frac{d_2 t^2 + d_3 t_0 t + d_4 {t_0}^2}{(t-t_0)^4}$$

for absolute constants d_2, d_3, and d_4. The conclusion is that at the expense of differentiating twice more we have gained the convergence factor $\widetilde{R}(t)$.

Estimating the integral trivially gives the bound

$$\frac{|q|^{\sigma_1/c}}{t_0^2}\int_0^\infty \int_0^{3t_0/4} \left(1 + \frac{(tv|q|)^{1/c}}{U}\right)^{-2} \left(1+\frac{v}{V}\right)^{-2} t^{-1+\sigma_1/c} v^{\sigma_1/c+\sigma_2-1} dt dv,$$

using the bound $|\widetilde{R}(t)| \ll t_0^{-2}$. Simplifying, it is

$$\begin{aligned}&\ll \frac{|q|^{\sigma_1/c}}{t_0^2}\int_0^\infty \left(\min\left\{t_0, \frac{U^c}{v|q|}\right\}\right)^{\sigma_1/c} \left(1+\frac{v}{V}\right)^{-2} v^{\sigma_1/c+\sigma_2-1} dv \\ &\ll t_0^{-2} U^{\sigma_1} V^{\sigma_2}.\end{aligned}$$

Therefore we get the bound

$$\int_0^\infty \int_0^{3t_0/4} \ll \frac{U^{\sigma_1}V^{\sigma_2}}{|s_1/c+s_2||s_1/c+s_2+1||s_1|^2}.$$

We obtain the same bound for the integration over $t \geq 5t_0/4$. The reason is that the integration by parts gives the same convergence factor $\widetilde{R}(t)$. The only change is that we apply the bound $\widetilde{R}(t) \ll t^{-2}$ to get convergence at infinity. The bound is the same.

In the case that $t_0 < 0$ there is no need to break up the integral at all and we gain the convergence factor $\widetilde{R}(t)$, which immediately saves us $|t_0|^{-2}$.

It remains to bound the integral

$$\begin{aligned}&\int_{t_0/2}^{3t_0/2} e^{il(t)} G(t,v) t^{-1+\sigma_1/c} f_2(t/t_0) dt \\ &\quad = t_0^{\sigma_1/c} e^{il(t_0)} \int_{-1/2}^{1/2} e^{i[l(t_0(1+t))-l(t_0)]} G(t_0(1+t),v)(1+t)^{-1+\sigma_1/c} f_2(1+t) dt.\end{aligned}$$

Set $t_0\Phi(t) = l(t_0(1+t)) - l(t_0) = 2\pi t_0(t - \log(1+t))$ and define

$$a(t,t_0) = G((t_0(1+t),v)\left(1+\frac{v}{V}\right)^2 \left(1+\frac{(t_0 vq)^{1/c}}{U}\right)^2 (1+t)^{-1+\sigma_1/c} f_2(1+t).$$

With these changes in notation the integral is

$$t_0^{\sigma_1/c} e^{il(t_0)} \left(1+\frac{v}{V}\right)^{-2} \left(1+\frac{(t_0 vq)^{1/c}}{U}\right)^{-2} \int_{-\infty}^{\infty} e^{it_0\Phi(t)} a(t,t_0)dt.$$

Then it is clear from (23) that $a(t,t_0)$ satisfies (for $t_0>1$, which we may assume since the case where $r_1 \ll 1$ has already been implicitly treated above)

$$\left|\left(\frac{\partial}{\partial t}\right)^{\alpha}\left(\frac{\partial}{\partial t_0}\right)^{\gamma} a(t,t_0)\right| \ll (1+t_0)^{-\gamma}$$

uniformly in v. Since $\Phi(0)=\Phi'(0)=0$ and $\Phi'(t)\neq 0$ for $t\neq 0$ we may apply the Van der Corput bound of $O\left(t_0^{-1/2}\right)$ to the integration over t (cf. [So], Lemma 1.1.2). Continuing, we integrate over v and get

$$\begin{aligned}&\ll t_0^{-1/2+\sigma_1/c}|q|^{\sigma_1/c}\int_0^{\infty}\left(1+\frac{v}{V}\right)^{-2}\left(1+\frac{(t_0vq)^{1/c}}{U}\right)^{-2} v^{\sigma_1/c+\sigma_2-1}dv\\ &\ll t_0^{-1-\varepsilon}U^{\sigma_1}V^{\sigma_2}\left(1+\left(\frac{U^c}{V|q|}\right)^{1/2+\varepsilon}\right).\end{aligned}$$

Therefore

$$H(s_1,s_2) \ll \frac{U^{\sigma_1}V^{\sigma_2}}{|(s_1/c+s_2)(s_1/c+s_2+1)||s_1|^{1+\varepsilon}}\left(1+\left(\frac{U^c}{V|q|}\right)^{1/2+\varepsilon}\right)$$

and the proof of the main statement is complete.

Appendix B. A technical exponential sum

This appendix is dedicated to stating and proving the following general result.

Lemma B.1. *Let f and g be smooth real-valued functions defined on an open interval I containing $[1,2]$. Suppose $f(x)\asymp 1\asymp f'(x)$ and $g^{(k)}(x)\asymp 1$ on I for $k=0,1,2,3$. Let c_n, $n=1,2,\dots$ be arbitrary complex numbers satisfying $|c_n|\leq 1$, and let $M\geq 1, N\geq 1$, and Y be real numbers. Consider the sum*

$$S=\sum_{M\leq m<2M}\left|\sum_{N\leq n<2N} c_n e\left(Yf(n/N)g(m/M)\right)\right|.$$

If $M\geq C|Y|$ (C a positive real number), then the bound

$$S\ll N^{1/2}M+\frac{NM}{1+|Y|^{1/2}}\log N$$

holds. In case $M<C|Y|$, the bound

$$S\ll N^{1/2}M+\frac{NM}{1+|Y|^{1/4}}$$

holds. The implied constants in these bounds depend only on f, g, and C.

This lemma is used to prove Lemma 5.4.

Proof. Let $F_\varepsilon(x)$ be a smooth, nonnegative function which takes the value 1 for $1 \le x \le 2$ and has support in the interval $(1-\varepsilon, 2+\varepsilon)$. Suppose $\varepsilon > 0$ is small enough so that f and g are defined on the interval $(1-\varepsilon, 2+\varepsilon)$. Then

$$S \le \sum_{m\in\mathbb{Z}} F_\varepsilon\left(\frac{m}{M}\right) \left| \sum_{N\le n<2N} c_n e\left(Yf(n/N)g(m/M)\right)\right|.$$

Applying Cauchy's inequality, we obtain

$$S^2 \ll M \sum_{N\le n_1<2N} \sum_{N\le n_2<2N} c_{n_1}\overline{c_{n_2}} \sum_m F_\varepsilon\left(\frac{m}{M}\right) e\left(Y(f(n_1/N)-f(n_2/N))g(m/M)\right).$$

The diagonal terms contribute $O(NM^2)$.

Let T be any real number and consider the sum

$$S_1(T) = \sum_{m\in\mathbb{Z}} F_\varepsilon\left(\frac{m}{M}\right) e\left(Tg(m/M)\right). \tag{32}$$

Our goal is to obtain the bound

$$S_1(T) \ll \begin{cases} M(1+|T|)^{-1} & \text{when } M \gg |T| \\ M(1+|T|^{1/2})^{-1} & \text{when } M \ll |T|, \end{cases} \tag{33}$$

with implied constants depending on f, g, F_ε, and C. Applying this bound to S using $T = Y(f(n_1/N)-f(n_2/N)) \asymp Y(n_1-n_2)N^{-1}$ will prove Lemma B.1 by noting that since $|T| \ll Y$ we can use the better bound for all pairs $n_1 \ne n_2$ if $M \gg Y$. □

Proof of (33). By Poisson summation,

$$S_1(T) = \sum_{r=-\infty}^{\infty} \int_{-\infty}^{\infty} F_\varepsilon\left(\frac{u}{M}\right) e(Tg(u/M) - ru)du. \tag{34}$$

Apply the change of variables $u \to Mu$ and set $G(u) = G_{r,M,T}(u) = 2\pi(Tg(u) - ruM)$ to obtain

$$S_1(T) = \sum_{r=-\infty}^{\infty} M \int_{1-\varepsilon}^{2+\varepsilon} F_\varepsilon(u)\, e^{iG_{r,M,T}(u)}du. \tag{35}$$

Let J_r be the above integral (with the factor M included). Then by integration by parts we have

$$J_r = iM \int e^{iG(u)} \frac{F_\varepsilon'(u)G'(u) - F_\varepsilon(u)G''(u)}{G'(u)^2}du. \tag{36}$$

Integrate by parts again to obtain

$$J_r = -M \int e^{iG(u)} \left(\frac{F_\varepsilon''(u)G'(u) - F_\varepsilon(u)G'''(u)}{G'(u)^3} - 3\frac{(F_\varepsilon'(u)G'(u) - F_\varepsilon(u)G''(u))G''(u)}{G'(u)^4} \right) du.$$

Setting $l = l_{r,T} = \min_u\{|TM^{-1}g'(u) - r|\}$ and estimating this integral trivially (using the estimates $|G'(u)| \ge Ml$, $G''(u) \ll T$, and $G'''(u) \ll T$) gives the bound (provided $l \ne 0$)

$$|J_r| \ll M^{-1}l^{-2} + |T|M^{-2}l^{-3} + |T|^2M^{-3}l^{-4}, \tag{37}$$

the implied constant depending on f, g, and F_ε only. If $|T| \leq \varepsilon M$ for ε small enough with respect to the implied constant in $g'(x) \asymp 1$, then $l \gg |r|$ and we can sum over all $r \neq 0$ in (35) and get the bound $O(1)$ depending on f, g, and F_ε only (but from now on ε and F_ε are fixed, so in fact all implied constants depend on f and g only). The case $r = 0$ gives $l \asymp |T|/M$ and hence

$$|J_0| \ll \frac{M}{1+|T|}.$$

In case $|T| \geq \varepsilon M$ we can sum over all r except those of size $|r| \asymp |T|M^{-1}$ (using $l \gg |r|$ and (37)) to get the bound $O(1)$.

Now assume we are in the range $|r| \asymp |T|M^{-1}$. The contribution from those r such that

$$lM|T|^{-1} \geq \delta > 0 \tag{38}$$

is at most $O_\delta(M(1+|T|^2)^{-1})$. Thus we may take δ small enough (with respect to the implied constant in $g'(x) \asymp 1$) so that either (38) holds or $l = 0$ (since $g'(u) \asymp 1$ and $|r|M|T|^{-1} \asymp 1$). There are a bounded number (bounded in terms of the various implied constants already mentioned) of possible values of r such that $l = 0$. For each such r there is one value of u, say u_0, such that $Tg'(u_0) - rM = 0$. By taking $\Phi(u) = g(u) - g(u_0) + rMT^{-1}(u - u_0)$ it suffices to bound the integral

$$M \int_{-\infty}^{\infty} F_\varepsilon(u) e\left(T\Phi(u)\right) du,$$

where $\Phi(0) = \Phi'(0) = 0$, $\Phi'(u) \neq 0$ for $u \neq 0$, and $\Phi''(0) \neq 0$. Using stationary phase estimates (cf. [So], Theorem 1.1.1.) we get the bound

$$\ll \frac{M}{1+|T|^{1/2}}$$

for this integral, the implied constant depending on f and g only. Now the proof is complete. □

Acknowledgements

This work constitutes a large portion of my Ph.D. thesis. I thank my advisor, Henryk Iwaniec, for suggesting this problem and for his support and encouragement while doing this work.

I also thank Harald Helfgott and Steven J. Miller for some useful conversations and the referee for a careful reading of this paper.

References

[BCDT] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc. **14**(4), 843-939 (2001). MR1839918 (2002d:11058)

[B] A. Brumer, *The average rank of elliptic curves. I*, Invent. Math. **109**(3), 445–472 (1992). MR1176198 (93g:11057)

[BS] A. Brumer, J. Silverman, *The number of elliptic curves over $\mathbb{Q}$ with conductor N*, Manuscripta Math. **91**, 95-102 (1996). MR1404420 (97e:11062)

[C] J. B. Conrey, *L-functions and random matrices*, Mathematics unlimited—2001 and beyond, Springer, Berlin, 331–352 (2001). MR1852163 (2002g:11134)

[DK] W. Duke and E. Kowalski, *A problem of Linnik for elliptic curves and mean-value estimates for automorphic representations*, with an appendix by Dinakar Ramakrishnan. Invent. Math. **139**(1), 1-39 (2000). MR1728875 (2001b:11034)

[FNT] E. Fouvry, M. Nair, and G. Tenenbaum, *L'ensemble exceptionnel dans la conjecture de Szpiro*, Bull. Soc. Math. France **120**(4), 485-506 (1992). MR1194273 (94a:11076)

[GZ] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*. Invent. Math. 84 (1986), no. 2, 225–320. MR0833192 (87j:11057)

[H-B] D. R. Heath-Brown, *The average analytic rank of elliptic curves*, Duke Math J. 122 (2004), no. 3, 591–623. MR2057019 (2004m:11084)

[H-BP] D.R. Heath-Brown and S.J. Patterson, *The distribution of Kummer sums at prime arguments*, J. Reine und Angew. Math., **310**, 111-136 (1979). MR0546667 (81e:10033)

[He1] H. Helfgott, *On the behavior of root numbers in families of elliptic curves*, http://www.arxiv.org/abs/math.NT/0408141.

[He2] H. Helfgott, *The parity problem for reducible cubic forms*, http://www.arxiv.org/abs/math.NT/0408142.

[IK] H. Iwaniec and E. Kowalski, *Analytic Number Theory*. American Mathematical Society Colloquium Publications, 53. American Mathematical Society, Providence, RI, 2004. MR2061214 (2005h:11005)

[ILS] H. Iwaniec, W. Luo and P. Sarnak, *Low lying zeros of families of L-functions*, Inst. Hautes Études Sci. Publ. Math. no. 91, 55-131 (2001). MR1828743 (2002h:11081)

[KS1] N. Katz and P. Sarnak, *Random Matrices, Frobenius Eigenvalues, and Monodromy*. American Mathematical Society Colloquium Publications, 45. American Mathematical Society, Providence, RI, 1999. MR1659828 (2000b:11070)

[KS2] N. Katz and P. Sarnak, *Zeroes of zeta functions and symmetry*, Bull. Amer. Math. Soc., **36**, 1-26 (1999). MR1640151 (2000f:11114)

[Ko] V. Kolyvagin, *The Mordell-Weil and Shafarevich-Tate groups for Weil elliptic curves* (Russian) Izv. Akad. Nauk SSSR Ser. Mat. 52 (1988), no. 6, 1154–1180, 1327; translation in Math. USSR-Izv. 33 (1989), no. 3, 473–499. MR0984214 (90f:11035)

[KM1] E. Kowalski and P. Michel, *The analytic rank of $J_0(q)$ and zeros of automorphic L-functions*, Duke Math. J. 100 (1999), no. 3, 503–542. MR1719730 (2001b:11060)

[KM2] E. Kowalski and P. Michel, *Explicit upper bound for the (analytic) rank of $J_0(q)$*, Israel J. Math. 120 (2000), part A, 179–204. MR1815375 (2002e:11065)

[Ku] D. Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. (3) 33 (1976), no. 2, 193–237. MR0434947 (55:7910)

[Mic] P. Michel, *Rang moyen de familles de courbes elliptiques et lois de Sato-Tate*, Monatsh. Math. **120**(2), 127-136 (1995). MR1348365 (96j:11077)

[Mil] S. J. Miller, 1- *and* 2*-level densities for families of elliptic curves: evidence for underlying group symmetries*, Compositio Mathematics **104**, 952-992 (2004). MR2059225 (2005c:11085)

[RS] K. Rubin and Alice Silverberg, *Rank frequencies for quadratic twists of elliptic curves*, Experiment. Math. **10**(4), 559-569 (2001). MR1881757 (2002k:11081)

[R] M. Rubinstein, *Low-lying zeros of L-functions and random matrix theory*, Duke Math. J. **109**(1), 147–181 (2001). MR1844208 (2002f:11114)

[Sch] W. Schmidt, *Equations over Finite Fields, an Elementary Approach*, Springer-Verlag, Berlin, 1976. MR0429733 (55:2744)

[Si1] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986. MR0817210 (87g:11070)

[Si2] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1994. MR1312368 (96b:11074)

[Si3] J. Silverman, *The average rank of an algebraic family of elliptic curves*, J. Reine Angew. Math. **504**, 227-236 (1998). MR1656771 (99m:11066)

[So] C. Sogge, *Fourier Integrals in Classical Analysis*, Cambridge University Press, Cambridge, 1993. MR1205579 (94c:35178)

[ST] C. L. Stewart and J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms*, J. Amer. Math. Soc. **8**(4), 943-973 (1995). MR1290234 (95m:11055)

[TW] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. Math. (2) **141**(3), 553-572 (1995). MR1333036 (96d:11072)

[W] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. Math (2) **141**(3), 443-551 (1995). MR1333035 (96d:11071)

[Y1] M. Young, *Low-lying zeros of families of elliptic curves*, http://arxiv.org/abs/math.NT/0406330.

[Y2] M. Young, *Random matrix theory and families of elliptic curves*, Ph.D. thesis, Rutgers University, 2004.

American Institute of Mathematics, 360 Portage Avenue, Palo Alto, California 94306-2244

E-mail address: myoung@aimath.org