Canad. J. Math. Vol. **62** (5), 2010 pp. 1155–1181
doi:10.4153/CJM-2010-049-5

# Moments of the Critical Values of Families of Elliptic Curves, with Applications

Matthew P. Young

*Abstract.* We make conjectures on the moments of the central values of the family of all elliptic curves and on the moments of the first derivative of the central values of a large family of positive rank curves. In both cases the order of magnitude is the same as that of the moments of the central values of an orthogonal family of $L$-functions. Notably, we predict that the critical values of all rank 1 elliptic curves is logarithmically larger than the rank 1 curves in the positive rank family.

Furthermore, as arithmetical applications, we make a conjecture on the distribution of $a_p$'s amongst all rank 2 elliptic curves and show how the Riemann hypothesis can be deduced from sufficient knowledge of the first moment of the positive rank family (based on an idea of Iwaniec).

## 1 Introduction

Recently there have been many advances in the study of ranks of elliptic curves arising from random matrix theory. For instance, Conrey *et al.* [CKRS] have studied many interesting statistics of the family of quadratic twists of a fixed elliptic curve. In particular, they make a precise conjecture on the relative frequency of quadratic twists of rank two where the comparison is between the sets of curves twisted by integers that are quadratic residues $\pmod p$ and those that are quadratic nonresidues $\pmod p$. This conjecture is deduced from a general moment conjecture on the central values of the families of interest [CFKRS] combined with random matrix theory heuristics developed by Keating and Snaith [KS].

In this paper we study the analogous problems for the family of all rational elliptic curves. That is, we make a conjecture on the moments of the central values of this family, using the general recipe presented in [CFKRS].

In general such a conjecture for a family of $L$-functions has its gross order of magnitude determined only by the symmetry type of the family. For example, for an orthogonal family $\mathcal{F}$ the general conjecture [KS] is

$$\frac{1}{|\mathcal{F}(X)|}\sum_{f\in\mathcal{F}(X)} L(\tfrac{1}{2}, f)^k \sim a_k g_k (\log X)^{\frac{k(k-1)}{2}},$$

where it is understood that $\mathcal{F}(X)$ is a subset of $\mathcal{F}$ with conductors $\ll X$ and the asymptotic holds as $X \to \infty$. Here $a_k$ is called the arithmetical factor and $g_k$ is a constant arising from random matrix theory.

Received by the editors November 29, 2007; revised March 28, 2008.

Published electronically June 18, 2010.

This research was supported by an NSF Mathematical Sciences Post-Doctoral Fellowship and by the American Institute of Mathematics.

AMS subject classification: **11M41**, 11G40, 11M26.

We also study the moments of the first derivative of the $L$-functions at the central point for a positive rank family $\mathcal{F}'$. It is perhaps not obvious what to expect for a family $\mathcal{F}'$ where the central values should typically vanish to order one or two (depending on the sign in the functional equation). We predict that the order of magnitude of the $k$-th moment of $L'(\frac{1}{2}, E)$ where $E$ ranges over $\mathcal{F}'$ is the same as that given above for an orthogonal family. This conjecture lends evidence to the idea that the family $\mathcal{F}'$ should be modeled by an orthogonal family with the caveat that one should "add" one zero to the central point (the "independent" model; see [M, Conjecture 1.1] and [F]).

As an application of the moment conjecture we predict the relative proportion of rank 2 elliptic curves whose coefficients $a$ and $b$ of the Weierstrass equation $y^2 = x^3 + ax + b$ lie in prescribed arithmetic progressions $(\bmod q)$, similarly to the work of [CKRS]. This gives a large number of conjectures that have the attractive feature of potentially being tested numerically, based on the strikingly good agreement that was seen with the quadratic twist families considered by [CKRS].

The families of elliptic curves investigated in this paper (especially the positive rank family) can be thought of as somewhat exotic tests of the general moment conjectures of [CFKRS].

The arithmetical constant for the family of all elliptic curves is more subtle than for other families previously considered as it depends on the traces of the Hecke operators acting on the space of weight $k$ cusp forms for the full modular group. In previous examples (Riemann zeta, families of Dirichlet $L$-functions, weight $k$ level $N$ newforms, to name a few), the arithmetical factor was essentially given in terms of rational functions in $p$. A large part of this paper is the computation of the arithmetical factor for our family. The key to this computation is a useful formula for the orthogonality relation for the family of all elliptic curves, which we compute with Proposition 4.2. The arithmetical factor is essentially the Dirichlet series constructed from the orthogonality relation. In the case of the positive rank family there does not appear to be as nice a formula for the arithmetical factor as there is for the family of all elliptic curves.

The methods of this paper can be easily modified to obtain similar moment conjectures for other families of elliptic curves. However, the computation of the arithmetical factor in terms of easily computable "extrinsic" (non-tautological) quantities is not easily generalized to other families (see the remarks after Conjecture 1.4 for a more precise discussion of what is meant here).

There are a variety of ways to order elliptic curves: by conductor, by minimal discriminant (in absolute value), or by taking coefficients in the Weierstrass equation to lie in a box. Furthermore, there is the question of whether to count by isomorphism class or by isogeny class. (Put another way: is the family composed of curves or by $L$-functions?) However, there is reason to believe that almost every isogeny class contains only one isomorphism class; Watkins briefly touches on this issue [Wa, §5].

We have ordered our curves by taking the coefficients to lie in a box for a practical reason: it is possible to do explicit computations with this ordering. It may be most natural to order curves by conductor, but it is difficult to work with this ordering. Recently, Watkins [Wa] has developed various heuristics that, amongst other things, allow one to get some handle on the ordering by conductor by way of the ordering

https://doi.org/10.4153/CJM-2010-049-5 Published online by Cambridge University Press

in boxes. It would be interesting to compute the orthogonality relation for the family of elliptic curves ordered by conductor. Ordering by boxes is particularly pleasant because of periodicity of the Dirichlet series coefficients.

### 1.1 Notation and Definitions

Let $E_{a,b}$ be the elliptic curve over $\mathbb{Q}$ given by the Weierstrass equation

$$E_{a,b} : y^2 = x^3 + ax + b, \tag{1.1}$$

with discriminant $\Delta = \Delta_{a,b} = -16(4a^3 + 27b^2) \neq 0$ and conductor $N$.

For integers $r$, $t$, and squarefree $q$ coprime with 6, and parameter $X > 0$, we take the family $\mathcal{F}(X) = \mathcal{F}_{r,t;q}(X)$ defined by

$$\mathcal{F}(X) = \{E_{a,b} : a \equiv r (\text{mod } 6q),\ b \equiv t (\text{mod } 6q),\ |a| \leq X^{1/3}, \\ |b| \leq X^{1/2},\ p^4 | a \Rightarrow p^6 \nmid b\}.$$

We also suppose $(4r^3 + 27t^2, 6q) = 1$, so in particular $(3, r) = (2, t) = 1$, and $(\Delta_{a,b}, 3q) = 1$ for $E_{a,b} \in \mathcal{F}(X)$. In Section 2 we review some basic facts about elliptic curves and develop some of the properties of the curves in the family $\mathcal{F}(X)$. Occasionally we write $\mathcal{F}^+$ to denote the set of $E \in \mathcal{F}$ with root number $w_E = +1$.

Our positive rank family $\mathcal{F}'$ is defined by

$$\mathcal{F}'(X) = \{E_{a,b^2} : a \equiv r (\text{mod } 6),\ b \equiv t (\text{mod } 6),\ |a| \leq X^{1/3},\ |b| \leq X^{1/4}, \\ p^4 | a \Rightarrow p^3 \nmid b\}.$$

We could also take $q$, $r$, and $t$ as in the definition of $\mathcal{F}$ to analyze the behavior of $a$ and $b$ in arithmetic progressions, but have taken $q = 1$ for simplicity.

Each curve $E_{a,b^2}$ has the point $(0, b)$ which is almost always of infinite order (see Theorem 2.3 and subsequent remarks). The Birch and Swinnerton-Dyer conjecture therefore predicts that $L(\frac{1}{2}, E_{a,b^2}) = 0$ for almost all $a$ and $b$. In addition, the sign in the functional equation for this family is expected to be evenly distributed between ±1 (see Proposition 2.2 below).

Let $G(s)$ be the Barnes $G$-function, which satisfies $G(1) = 1$ and $G(s + 1) = \Gamma(s)G(s)$. The $k$-th Chebyshev polynomial of the second kind is denoted by $U_k$ and $Tr_l(p)$ is the trace of the Hecke operator $T_p$ acting on the space of weight $l$ cusp forms on the full modular group. We let $Tr_l^*(p)$ be the "scaled" trace determined by $Tr_l(p) = p^{\frac{l-1}{2}} Tr_l^*(p)$. We let $d\mu_{ST}$ be the Sato–Tate measure, *i.e.*,

$$\int f \, d\mu_{ST} := \frac{2}{\pi} \int_0^{\pi} f(\theta) \sin^2 \theta d\theta.$$

https://doi.org/10.4153/CJM-2010-049-5 Published online by Cambridge University Press

## 1.2 Moment Conjectures for the Family of all Elliptic Curves

We now state the following conjecture.

***Conjecture 1.1*** **(Keating-Snaith)** *For any $k \in \mathbb{C}$ such that* Re *$k > -\frac{1}{2}$,*

$$\frac{1}{|\mathcal{F}(X)|} \sum_{E \in \mathcal{F}(X)} L(\tfrac{1}{2}, E)^k \sim \tfrac{1}{2} a_k g_k (\log X)^{\frac{k(k-1)}{2}}$$

*holds as $X \to \infty$, where*

$$g_k = 2^{k/2} \frac{G(1+k)\sqrt{\Gamma(1+2k)}}{\sqrt{G(1+2k)\Gamma(1+k)}}$$

*is a certain constant familiar from random matrix theory, and $a_k$ is an arithmetical factor given by an explicit absolutely convergent Euler product* (*see* (4.6)).

***Remarks*** We use the convention that $0^k = 0$ for any $k$ (alternatively, one could only sum over nonzero central values). The restriction to Re $k > -\frac{1}{2}$ arises because the Barnes $G$-function has its rightmost pole at $k = -\frac{1}{2}$.

Conjecture 1.1 is the conjecture of Keating and Snaith for an orthogonal family [KS]. Our contribution is the explicit calculation of $a_k$ (which we have delayed due to its size).

For integral $k \geq 1$ this conjecture is a special case of the more precise Conjecture 1.3. Conjecture 1.1 is somewhat simpler and also provides an analytic continuation of $a_k$ to complex $k$ which is a necessary ingredient for deriving Conjecture 1.6. By taking $k = 0$ and computing that $a_0 = g_0 = 1$, we obtain the following conjecture.

***Corollary 1.2*** *Conjecture* 1.1 *implies that the average rank of the family of all elliptic curves $\mathcal{F}$ is $\frac{1}{2}$.*

We present this corollary simply to illustrate the strength of Conjecture 1.1 and the usefulness of extending the formulas to more general $k$ than positive integers. This result also indicates that it will be difficult to check Conjecture 1.1 numerically, because of the well-known disparity between the expected proportion of rank 2 elliptic curves and the numerical evidence; see [BMSW] for a recent survey on this fascinating problem. It may be that the large value distribution converges more quickly, so that there may be better numerical agreement for (slightly) larger $k$; this deserves investigation. In any case, one should include all lower-order terms in the conjectured asymptotic.

A more precise moment conjecture is as follows.

***Conjecture 1.3*** ([CFKRS]) *Let $k$ be a nonnegative integer. Then for some $\delta > 0$,*

$$\sum_{E \in \mathcal{F}(X)} L(\tfrac{1}{2}, E)^k = \frac{1}{2} \sum_{E \in \mathcal{F}(X)} P_k(N_E)(1 + O(N_E^{-\delta})),$$

https://doi.org/10.4153/CJM-2010-049-5 Published online by Cambridge University Press

*where*

$$(1.2)\quad P_k(N) = \frac{(-1)^{\frac{k(k-1)}{2}}2^k}{k!}\frac{1}{(2\pi i)^k}$$

$$\times \oint \cdots \oint H(z_1,\dots,z_k)\frac{\Delta(z_1^2,\dots,z_k^2)^2}{\prod_{i=1}^{k} z_i^{2k-1}}\prod_{i=1}^{k} X_N^{-\frac{1}{2}}(\tfrac{1}{2}+z_i)dz_1\cdots dz_k,$$

*and* $X_N(s) = X_E(s)$ *is such that* $L(s,E) = w_E X_E(s) L(1-s,E)$ *(see* (2.4)*). Here*

$$H(z_1,\dots,z_k) = A_k(z_1,\dots,z_k)\prod_{1\le i<j\le k}\zeta(1+z_i+z_j),$$

*where the arithmetical factor* $A_k$ *is holomorphic and nonzero in a neighborhood of* $(0,\dots,0)$*. Here* $P_k(N)$ *is a polynomial in* $\log N$ *of degree* $k(k-1)/2$*.*

Here Conjecture 1.3 is the specialization of [CFKRS, Conj. 1.5.3 and 1.5.5] to the elliptic curve family $\mathcal{F}(X)$. Due to the size of the formulas, we have delayed the precise formulation of the arithmetical factors; see Proposition 4.4.

The factor $\frac{1}{2}$ appears because roughly half of the $L$-functions vanish since the root number is $-1$.

The five authors boldly predict that any $\delta < \frac{1}{2}$ holds here [CFKRS].

### 1.3 Moment Conjectures for the Positive Rank Family

***Conjecture 1.4*** *For any* $k \in \mathbb{C}$ *such that* $\operatorname{Re} k > -\frac{1}{2}$ *there exists* $a'_k \neq 0$ *such that*

$$\frac{1}{|\mathcal{F}'(X)|}\sum_{E\in\mathcal{F}'(X)}(L'(1/2,E))^k \sim \tfrac{1}{2}a'_k g_k(\log X)^{\frac{k(k-1)}{2}}$$

*holds as* $X \to \infty$*.*

It is possible to write a formula for $a'_k$ as an Euler product, but it involves the sums $Q^*_{\square}(p^{e_1},\dots,p^{e_k})$ discussed in Section 5. This is in contrast to the family $\mathcal{F}$ where we have evaluated similar sums in terms of Chebyshev polynomials and the traces of the Hecke operators on $\Gamma(1)$.

As before, we have the following.

***Conjecture 1.5*** **([CFKRS])** *Let k be a nonnegative integer. Then for some* $\delta > 0$,

$$\sum_{E\in\mathcal{F}'(X)}(L'(1/2,E))^k = \frac{1}{2}\sum_{E\in\mathcal{F}'(X)}Q_k(N_E)(1+O(N_E^{-\delta})),$$

*where* $Q_k$ *has the form*

$$(1.3)\quad Q_k(N) = \frac{(-1)^{\frac{k(k-1)}{2}}2^k}{k!}\frac{1}{(2\pi i)^k}$$

$$\times \oint \cdots \oint H(z_1,\dots,z_k)\frac{\Delta(z_1^2,\dots,z_k^2)^2}{\prod_{i=1}^{k} z_i^{2k}}\prod_{i=1}^{k} X_N^{-\frac{1}{2}}(\tfrac{1}{2}+z_i)dz_1\cdots dz_k$$

https://doi.org/10.4153/CJM-2010-049-5 Published online by Cambridge University Press

*and*

$$H(z_1,\dots,z_k)=A_k'(z_1,\dots,z_k)\frac{\prod_{1\le i<j\le k}\zeta(1+z_i+z_j)}{\prod_{1\le i\le k}\zeta(1+z_i)},$$

*where the arithmetical factor $A_k'$ is given by an Euler product that is absolutely convergent in a neighborhood of $(0,\dots,0)$.*

In terms of the behavior near the origin there are two essential differences between Conjectures 1.3 and 1.5. Namely, in (1.3) there is the extra factor $\prod_i z_i^{-1}$ and the function $H(z_1,\dots,z_k)$ has the additional factor $\prod_i \zeta^{-1}(1+z_i)$. Thus $Q_k(N)$ and $P_k(N)$ have the same degree, because the polar behavior near the origin in their integral representations are the same. The factor $\prod_i z_i^{-1}$ arises from the differentiation; the extra zeta function factors arise from the positive rank of the family $\mathcal{F}'$.

## 1.4 The Relative Frequency of Rank 2 and Higher Curves

In this section we consider the question of the distribution of the $a_p$'s amongst all rank 2 elliptic curves. As a concrete example, we want to predict the ratio of the number of rank 2 elliptic curves with $a_5=-1$ to the number of rank 2 curves with $a_5=1$.

This distribution of $a_p$'s amongst all elliptic curves is known from [B]; (see also [Sch]). It is expected that rank 2 curves have $a_p$'s that are biased towards being negative. The conjecture in this section gives a precise prediction of this bias.

Given $r$ and $t(\mathrm{mod}\, p)$, $\lambda_{a,b}(p)$ is fixed for $a\equiv r$, $b\equiv t(\mathrm{mod}\, p)$. The number of residue classes $r$ and $t$ such that $\lambda_{r,t}(p)\sqrt{p}=T$ as a function of $p$ and $T$ is known exactly and involves the Hurwitz class number $H(4p-T^2)$ [B].

Thus, to understand the distribution of the $a_p$'s amongst all rank 2 curves it suffices to understand the frequency of occurences of rank 2 curves as a function of the residue class $r,t$ (since we can use Birch's computation to provide the number of such $r$ and $t$ with given $a_p$). Precisely, we consider the following ratio

$$R_q(X)=\Bigg(\sum_{\substack{E\in\mathcal{F}^+_{r,t}(X)\\ L(1/2,E)=0}}1\Bigg)\Bigg/\Bigg(\sum_{\substack{E\in\mathcal{F}^+_{r',t'}(X)\\ L(1/2,E)=0}}1\Bigg).$$

Technically, $R_q$ counts curves of even positive rank, but it is expected that the number of rank 4 and higher curves is of a lower order of magnitude than the number of rank 2 curves (and the numerical evidence apparently supports this).

***Conjecture 1.6*** *Let $R_q=\lim_{X\to\infty}R_q(X)$. Then*

$$R_q=\prod_{p\mid q}\left(\frac{1-\frac{\lambda_{r,t}(p)}{p^{1/2}}+\frac{1}{p}}{1-\frac{\lambda_{r',t'}(p)}{p^{1/2}}+\frac{1}{p}}\right)^{1/2}=\prod_{p\mid q}\left(\frac{N_p(r,t)}{N_p(r',t')}\right)^{1/2}, \tag{1.4}$$

*where $N_p(r,t)$ is the number of points on the elliptic curve $E_{r,t}$ over $\mathbb{F}_p$.*

https://doi.org/10.4153/CJM-2010-049-5 Published online by Cambridge University Press

This formula is similar to that given in Conjecture 2 of [CKRS]. A new feature of the above formula is that $\lambda_{r,t}(p)\sqrt{p}$ and $\lambda_{r',t'}(p)\sqrt{p}$ can attain any integer values between $-2\sqrt{p}$ and $2\sqrt{p}$.

An analogous conjecture may be easily formulated for the relative frequency of rank 3 curves in arithmetic progressions in $\mathcal{F}'$ with minor modifications: if $R_q(X)$ is given as above but with $L'(\frac{1}{2}, E)$ replacing $L(\frac{1}{2}, E)$, then we predict that (1.4) holds with $N_p(r,t)$ defined to be the number of points on $E_{r,t^2}$.

The idea of using moments to study the value distribution of $L$-functions is due to Keating and Snaith [KS], and the idea of considering the ratio $R_q(X)$ (which sidesteps the difficult issue of counting precisely the number of rank 2 curves) is due to [CKRS]. We note that Watkins [Wa] has given a heuristic which predicts an asymptotic for the number of rank 2 elliptic curves, but he does not explicitly give the proportionality constant in the asymptotic.

### 1.5 Organization of the Paper

In Section 2 we recall some necessary material on elliptic curves and $L$-functions. We derive the shifted moment conjectures in Section 3, modulo the precise form of the arithmetical factors, which are calculated in Sections 4 and 5. We briefly derive Conjecture 1.6 in Section 6 and explain the connection with the Riemann Hypothesis in Section 7.

## 2 Background and Basic Properties of the Families

In this section we summarize some of the relevant background material on elliptic curves. Our intended audience contains both random matrix theorists and number theorists who are not specialists in elliptic curves, so we have attempted to provide sufficient details and references.

### 2.1 Invariants

We first describe some of the algebraic invariants associated to an elliptic curve. Silverman's book is a standard reference [Si].

The general Weierstrass equation of an elliptic curve takes the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2.1}$$

where $a_i \in \mathbb{Z}$. We are primarily concerned with elliptic curves over $\mathbb{Q}$, but understanding the $L$-function associated with such an elliptic curve involves studying the curve over $\mathbb{F}_p$ (*i.e.*, reducing the coefficients modulo $p$) for all primes $p$. Completing the square via $y \longrightarrow \frac{1}{2}(y - a_1x - a_3)$ gives

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

where

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6.$$

https://doi.org/10.4153/CJM-2010-049-5 Published online by Cambridge University Press

The change of variables $x \longrightarrow x - b_2/12$ gets rid of the quadratic factor, and then scaling by $x \longrightarrow x/36$, $y \longrightarrow y/108$ gives

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

where

$$c_4 = b_2^2 - 24b_4, \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

These changes of variable are well defined provided the characteristic of the field is not 2 or 3. Clearly the Weierstrass equation for an elliptic curve is not unique. Table 1.2 of [Si] records the effect of the admissible change of variables $x = u^2x' + r$, $y = u^3y' + u^2sx' + t$ on the various quantities $\{a_i\}$, $\{b_i\}$, $\{c_i\}$, and $\Delta$. We record

$$u^4c_4' = c_4, \quad u^6c_6' = c_6, \quad u^{12}\Delta' = \Delta. \tag{2.2}$$

Notice that no two curves in $\mathcal{F}$ are isomorphic over $\mathbb{Q}$ because the curves $E_{a,b}$ and $E_{a',b'}$ are isomorphic if and only if there exists $d \in \mathbb{Q}$ such that $a' = d^4a$ and $b' = d^6b$.

In order to choose a "good" Weierstrass equation, we want one that, when reduced modulo various primes, has as good a reduction as possible. To make this precise, we say that the Weierstrass equation (2.1) is *minimal* at $p$ if the largest power of $p$ dividing $\Delta$ cannot be reduced by an admissible change of variables. Furthermore, we say that (2.1) is a global minimal Weierstrass equation if it is minimal for all primes $p$. Chapter 10 of [Kn] is a good reference for a down-to-earth discussion on global minimal Weierstrass equations. We quote the following result of Néron that appears as Theorem 10.3 of [Kn].

***Theorem 2.1*** **(Néron)** *If $E$ is an elliptic curve over $\mathbb{Q}$, then there exists an admissible change of variables over $\mathbb{Q}$ such that the resulting equation is a global minimal Weierstrass equation. Two such resulting global minimal Weierstrass equations are related by an admissible change of variables with $u = \pm 1$ and with $r, s, t \in \mathbb{Z}$.*

Now we claim that the Weierstrass equation (1.1) for each $E_{a,b} \in \mathcal{F}$ is a global minimal equation. We use the condition that if $p^{12} \nmid \Delta$ or $p^4 \nmid c_4$ or $p^6 \nmid c_6$, then the Weierstrass equation is minimal at $p$, where here $c_4 = -2^43a$, $c_6 = -2^53^3b$. This condition is Lemma 10.1 of [Kn] and is essentially Remark 1.1 of Section VII.1 of [Si], but is easily seen from inspection of (2.2). It is immediate from this test that (1.1) is minimal at all $p > 3$, using the condition that if $p^4 | a$ then $p^6 \nmid b$. We have $2^4 || \Delta$ and $3 \nmid \Delta$ since $(4r^3 + 27t^2, 6) = 1$, so the equation is minimal at $p \leq 3$. A point to take from this discussion is that it is easy to specify light conditions that ensure minimality of a given Weierstrass equation.

## 2.2 The $L$-Function

The *conductor* $N$ associated to $E$ is a certain divisor of the minimal discriminant (which is the discriminant of the global minimal Weierstrass equation). The conductor and the minimal discriminant have the same prime factors, and for $p > 3$

https://doi.org/10.4153/CJM-2010-049-5 Published online by Cambridge University Press

we have $p \| N$ if $E$ has a node (a double root) modulo $p$, and $p^2 \| N$ if $E$ has a cusp (a triple root) modulo $p$. For $p \leq 3$, it is not so simple to give a characterization of the power of $p$ dividing $N$, but it can be found using Tate's algorithm, which is described in [Si2, pp. 363–368].

Given a global minimal Weierstrass equation of the form (1.1), the $L$-function attached to $E_{a,b}$ is given by

$$L(s, E_{a,b}) = \sum_{n=1}^{\infty} \frac{\lambda_{a,b}(n)}{n^s} = \prod_p \Big(1 - \frac{\lambda_{a,b}(p)}{p^s} + \frac{\psi_N(p)}{p^{2s}}\Big)^{-1}, \tag{2.3}$$

where for $p \neq 2$,

$$\lambda_{a,b}(p) = \frac{1}{\sqrt{p}}(p + 1 - \#E(\mathbb{F}_p)) = -\frac{1}{\sqrt{p}} \sum_{x (\mathrm{mod}\ p)} \Big(\frac{x^3 + ax + b}{p}\Big),$$

and $\psi_N$ is the principal Dirichlet character of modulus the conductor $N$ of $E$. If $p = 2$, then (1.1) has a cusp and $\lambda_{a,b}(2^k) = 0$ for all $k$. The sum and product converge absolutely provided $\mathrm{Re}(s) > 1$, using Hasse's bound $|\lambda_{a,b}(n)| \leq d(n)$. The famous modularity theorem [Wi, TW, BCDT] shows that the completed $L$-function

$$\Lambda(s, E) = \Big(\frac{\sqrt{N}}{2\pi}\Big)^{s+\frac{1}{2}} \Gamma(s + \tfrac{1}{2}) L(s, E)$$

is entire and satisfies the functional equation $\Lambda(s, E) = w_E \Lambda(1-s, E)$ where $w_E = \pm 1$ is called the root number. We set

$$X_E(s) = \frac{\Gamma(\frac{3}{2} - s)}{\Gamma(\frac{1}{2} + s)} \Big(\frac{\sqrt{N}}{2\pi}\Big)^{1-2s}, \tag{2.4}$$

so that $L(s, E) = w_E X_E(s) L(1 - s, E)$. Note that $X_E(s)$ only depends on the conductor $N$. We have normalized the $L$-function to have central point $s = \frac{1}{2}$.

The root number can be effectively computed; it is given by a product of local root numbers. We state the following result that appears as Proposition 3.1 of [Y2].

***Proposition 2.2*** *Suppose* $4a^3 + 27b^2$ *is squarefree. Then the root number of* $E_{a,b} : y^2 = x^3 + ax + b$ *is given by*

$$w_{E_{a,b}} = \mu(4a^3 + 27b^2) \Big(\frac{a}{3b}\Big) \chi_4(b)(-1)^{a+1} \epsilon_2,$$

*where* $(\frac{\cdot}{\cdot})$ *is the Jacobi symbol,* $\chi_4$ *is the primitive Dirichlet character of conductor* 4, *and* $\epsilon_2$ *is the local root number at* $p = 2$.

The local root number at 2 is difficult to state explicitly because there are many possible cases. The point is that $\mu(4a^3 + 27b^2)$ is expected to oscillate independently of the other factors, so that the root number is evenly distributed between ±1.

https://doi.org/10.4153/CJM-2010-049-5 Published online by Cambridge University Press

An exercise with Möbius inversion shows that $|\mathcal{F}(X)| \sim X^{5/6}/(9q^2\zeta_{6q}(10))$, where $\zeta_{6q}$ is given by the same Euler product as $\zeta$ but with the local factors at $p|6q$ removed. A proof of this is contained in the proof of Lemma 3.2 (take $n_1 = 1, k = 1$). Similarly, $|\mathcal{F}'(X)| \sim X^{7/12}/9\zeta_6(7)$.

Each curve $E_{a,b^2} \in \mathcal{F}'$ has the obvious point $(0, b)$. The Lutz–Nagell criterion easily shows that this point is torsion (has finite order) very rarely. We paraphrase Corollary 7.2 of [Si].

***Theorem 2.3*** **(Lutz-Nagell)** *Let E be an elliptic curve given by* (1.1)*. Suppose* $(x, y)$ *is a non-zero torsion point. Then* $x, y \in \mathbb{Z}$ *and either* $y = 0$ *or* $y^2|4a^3 + 27b^2$*.*

Thus if $(0, b)$ is a torsion point, then $b^2|4a^3$. Clearly the number of $E_{a,b} \in \mathcal{F}'(X)$ such that $b^2|4a^3$ is $O(X^{\frac{1}{3}+\varepsilon})$ (which should be compared to $X^{7/12}$, the total number of curves).

## 2.3 Chebyshev Polynomials

We take a brief detour to summarize some relevant facts needed about Chebyshev polynomials (of the second kind) $U_k$. A reference for the necessary formulas is Section 8.94 of [GR]. By definition,

$$U_n(\cos\theta) = \frac{\sin(n+1)\theta}{\sin\theta}.$$

These satisfy the recursion formula ([GR, 8.941.2])

$$U_{n+2}(x) - 2xU_{n+1}(x) + U_n(x) = 0$$

which is equivalent to the formal identity

$$\sum_n U_n(x)t^n = \frac{1}{1 - 2xt + t^2}, \tag{2.5}$$

the sum being absolutely convergent for $|x|, |t| < 1$. Since the Hecke operators satisfy essentially the same recurrence relation, we have

$$\lambda_E(p^j) = \begin{cases} U_j\left(\frac{\lambda_E(p)}{2}\right), & \text{if } (p, N) = 1, \\ \lambda_E^j(p), & \text{if } p|N. \end{cases} \tag{2.6}$$

The Chebyshev polynomials $U_n(\cos\theta)$ form an orthonormal system with respect to the Sato–Tate measure $\frac{2}{\pi}\sin^2\theta d\theta := d\mu_{ST}$, where the integration is over the interval $[0, \pi]$.

It will be useful to represent a product of Chebyshev polynomials in terms of Chebyshev polynomials. Let $c_l = c_l(e_1, \dots, e_k)$ be defined by

$$U_{e_1}(x)\cdots U_{e_k}(x) = \sum_l c_l U_l(x), \tag{2.7}$$

https://doi.org/10.4153/CJM-2010-049-5 Published online by Cambridge University Press

and set $f = e_1 + \cdots + e_k$. Note that by parity considerations (namely, the parity of $U_k(x)$ as a function of $x$ is the same as the parity of $k$), $c_l = 0$ if $l \not\equiv f \pmod 2$. Furthermore, by degree considerations $c_l = 0$ if $l > f$. The orthogonality relation gives

$$c_l = \int U_l(\cos\theta) \prod_{j=1}^{k} U_{e_j}(\cos\theta) d\mu_{ST}. \tag{2.8}$$

# 3 Deriving the Conjectures

## 3.1 Central Values of the Family of all Elliptic Curves

We begin by deriving Conjecture 1.3, however we delay the computation of the exact form of the arithmetical factor until Section 4. Actually, we find a conjectural formula for a product of $k$ $L$-functions at points shifted slightly away from the central point. Conjecture 1.3 is a limiting form of this more general conjecture. This generality also allows us to compute the central values of the derivatives by differentiation with respect to the shift parameters.

We want the moment

$$\frac{1}{|\mathcal{F}(X)|} \sum_{E \in \mathcal{F}(X)} L(\tfrac{1}{2} + \alpha_1, E) \cdots L(\tfrac{1}{2} + \alpha_k, E),$$

which is analogous to 4.1.4 of [CFKRS]. Actually we will write a conjecture for the more symmetric expression

$$\frac{1}{|\mathcal{F}(X)|} \sum_{E \in \mathcal{F}(X)} \mathcal{Z}(E), \tag{3.1}$$

where

$$\mathcal{Z}(E) = X_E^{-\frac{1}{2}}(\tfrac{1}{2} + \alpha_1) \cdots X_E^{-\frac{1}{2}}(\tfrac{1}{2} + \alpha_k) L(\tfrac{1}{2} + \alpha_1, E) \cdots L(\tfrac{1}{2} + \alpha_k, E)$$

and where recall $X_E$ satisfies

$$X_E^{-\frac{1}{2}}(\tfrac{1}{2} + \alpha) L(\tfrac{1}{2} + \alpha, E) = w_E X_E^{-\frac{1}{2}}(\tfrac{1}{2} - \alpha) L(\tfrac{1}{2} - \alpha, E).$$

For now we just work with the $L$-functions.

For each $L$ function we write a kind of approximate functional equation as follows

$$L(\tfrac{1}{2} + \alpha, E) = \sum_n \frac{\lambda_E(n)}{n^{\frac{1}{2}+\alpha}} + w_E X_E(\tfrac{1}{2} + \alpha) \sum_n \frac{\lambda_E(n)}{n^{\frac{1}{2}-\alpha}}.$$

Consider the term obtained by taking the first part of each approximate functional equation:

$$\frac{1}{|\mathcal{F}(X)|} \sum_{E \in \mathcal{F}(X)} \sum_{n_1, \dots, n_k} \frac{\lambda_E(n_1) \cdots \lambda_E(n_k)}{n_1^{\frac{1}{2}+\alpha_1} \cdots n_k^{\frac{1}{2}+\alpha_k}}.$$

https://doi.org/10.4153/CJM-2010-049-5 Published online by Cambridge University Press

Now replace each summand and replace it with its average, say

$$\sum_{n_1,\dots,n_k} \frac{R_{r,t}(n_1,\dots,n_k)}{n_1^{\frac{1}{2}+\alpha_1}\cdots n_k^{\frac{1}{2}+\alpha_k}}, \tag{3.2}$$

where

$$R_{r,t}(n_1,\dots,n_k) = \lim_{X\to\infty} \frac{1}{|\mathcal{F}_{r,t}(X)|} \sum_{E\in\mathcal{F}_{r,t}(X)} \lambda_E(n_1)\cdots\lambda_E(n_k).$$

We now derive the necessary expected value. To this end, we define the following.

***Definition 3.1*** Let $n_1,\dots,n_k$ be positive integers, set $n = [n_1,\dots,n_k]$ (the least common multiple), and let $n^*$ be the product of primes dividing $n$. Define $Q^*$ by

$$Q^*(n_1,\dots,n_k) = \frac{1}{n^{*2}} \sum_{a,b \pmod{n^*}} \lambda_{a,b}(n_1)\cdots\lambda_{a,b}(n_k).$$

Furthermore, set $n_i = m_i l_i$, where $(m_i, 6q) = 1$ and every prime dividing $l_i$ also divides $6q$. Then set

$$Q^*_{r,t}(n_1,\dots,n_k) = \lambda_{r,t}(l_1)\cdots\lambda_{r,t}(l_k)Q^*(m_1,\dots,m_k)\prod_{\substack{p|n\\ p\nmid 6q}}(1-p^{-10})^{-1}.$$

The desired expected value is given by the following

***Lemma 3.2*** *We have $R_{r,t}(n_1,\dots,n_k) = Q^*_{r,t}(n_1,\dots,n_k)$. Moreover, $Q^*(n_1,\dots,n_k)$ is multiplicative. That is, if $n_i = n_i' n_i''$ for $1 \le i \le k$ with $(n_1'\cdots n_k', n_1''\cdots n_k'') = 1$, then*

$$Q^*(n_1,\dots,n_k) = Q^*(n_1',\dots,n_k')Q^*(n_1'',\dots,n_k'').$$

**Proof** Recall

$$R_{r,t}(n_1,\dots,n_k) = \lim \frac{1}{|\mathcal{F}(X)|} \sum\sum_{\substack{|a|\le X^{1/3}, |b|\le X^{1/2}\\ p^4|a \Rightarrow p^6\nmid b\\ a\equiv r \pmod{6q}\\ b\equiv t \pmod{6q}}} \lambda_{a,b}(n_1)\cdots\lambda_{a,b}(n_k),$$

where we originally defined $\lambda_{a,b}(n)$ to be the $n$-th coefficient in the Dirichlet series expansion of $L(s, E_{a,b})$. If (1.1) is a global minimal Weierstrass equation for $E_{a,b}$ (a condition that is met for all curves in $\mathcal{F}$), then

$$\lambda_{a,b}(p) = -\frac{1}{\sqrt{p}} \sum_{x \pmod p} \Big(\frac{x^3+ax+b}{p}\Big). \tag{3.3}$$

https://doi.org/10.4153/CJM-2010-049-5 Published online by Cambridge University Press

We extend the definition of $\lambda_{a,b}(p)$ to arbitrary integers $a$ and $b$ and primes $p$ by using (3.3) for $p > 2$, and setting $\lambda_{a,b}(2) = 0$. We then extend to prime powers using (2.6), replacing the condition $(p, N) = 1$ with $(p, 16(4a^3 + 27b^2)) = 1$, and we extend to composite integers by multiplicativity. This formulation will allow us to easily sum over $a$ and $b$ where (1.1) is not necessarily a global minimal Weierstrass equation.

A slight generalization of the Möbius inversion formula gives that

$$\sum_{\substack{d^4|a\\ d^6|b}} \mu(d) = \begin{cases} 1 & \text{if there does not exist a } p \text{ such that } p^4|a \text{ and } p^6|b,\\ 0 & \text{otherwise.}\end{cases}$$

Thus

$$R_{r,t}(n_1, \dots, n_k) = \lim \frac{1}{|\mathcal{F}(X)|} \sum_{\substack{d \le X^{\frac{1}{12}}\\ (d,6q)=1}} \mu(d) \sum\sum_{\substack{|a| \le d^{-4}X^{1/3}\\ |b| \le d^{-6}X^{1/2}\\ a \equiv \overline{d}^4 r \pmod{6q}\\ b \equiv \overline{d}^6 t \pmod{6q}}} \lambda_{ad^4,bd^6}(n_1) \cdots \lambda_{ad^4,bd^6}(n_k).$$

The condition $(d, 6q) = 1$ follows from the fact that $(4r^3 + 27t^2, 6q) = 1$. Now we claim that $\lambda_{ad^4,bd^6}(m) = \lambda_{a,b}(m)$ when $(m, d) = 1$, and $\lambda_{ad^4,bd^6}(m) = 0$ when $(m, d) > 1$. By multipicativity and the fact that prime powers are determined by primes, it suffices to check for $m$ prime. Notice that in case $p|(a, b)$ then the sum (3.3) vanishes. Thus if $p|d$, then $\lambda_{ad^4,bd^6}(p) = 0$. On the other hand, if $(p, d) = 1$, then the change of variables $x \longrightarrow d^2x$ modulo $p$ gives

$$\sum_{x \pmod p} \left(\frac{x^3 + ad^4x + bd^6}{p}\right) = \left(\frac{d^6}{p}\right) \sum_{x \pmod p} \left(\frac{x^3 + ax + b}{p}\right),$$

so $\lambda_{ad^4,bd^6}(p) = \lambda_{a,b}(p)$ as claimed. Thus for $(d, n) = 1$ we have

$$\lambda_{ad^4,bd^6}(n_1) \cdots \lambda_{a,b}(n_k) = \lambda_{r,t}(l_1) \cdots \lambda_{r,t}(l_k)\lambda_{a,b}(m_1) \cdots \lambda_{a,b}(m_k),$$

by multiplicativity and since $\lambda_{ad^4,bd^6}(l_i) = \lambda_{r,t}(l_i)$.

Hence we have

$$R_{r,t}(n_1, \dots, n_k) =$$
$$\lim \frac{1}{|\mathcal{F}(X)|}\lambda_{r,t}(l_1) \cdots \lambda_{r,t}(l_k) \sum_{\substack{d \le X^{\frac{1}{12}}\\ (d,6nq)=1}} \mu(d) \sum\sum_{\substack{|a| \le d^{-4}X^{1/3}\\ |b| \le d^{-6}X^{1/2}\\ a \equiv \overline{d}^4 r \pmod{6q}\\ b \equiv \overline{d}^6 t \pmod{6q}}} \lambda_{a,b}(m_1) \cdots \lambda_{a,b}(m_k).$$

Now $\lambda_{a,b}(m_1)\cdots\lambda_{a,b}(m_k)$ is periodic in $a$ and $b$ with period equal to the product of primes dividing the least common multiple of $m_1,\dots,m_k$, say $m^*$. Breaking up the sum over $a$ and $b$ into arithmetic progressions modulo $6qm^*$ gives

$$R_{r,t}(n_1,\dots,n_k)=\lim\frac{1}{|\mathcal{F}(X)|}\lambda_{r,t}(l_1)\cdots\lambda_{r,t}(l_k)\frac{4X^{5/6}}{36q^2}\\ \times\sum_{\substack{d\leq X^{\frac{1}{12}}\\(d,6mq)=1}}\frac{\mu(d)}{d^{10}}\frac{1}{{m^*}^2}\sum_{\substack{\alpha(\operatorname{mod} m^*)\\ \beta(\operatorname{mod} m^*)}}\lambda_{\alpha,\beta}(m_1)\cdots\lambda_{\alpha,\beta}(m_k),$$

which simplifies to

$$R_{r,t}(n_1,\dots,n_k)=\lim\frac{1}{|\mathcal{F}(X)|}\lambda_{r,t}(l_1)\cdots\lambda_{r,t}(l_k)\frac{X^{5/6}}{9q^2\zeta_{6mq}(10)}Q^*(m_1,\dots,m_k).$$

Taking $k=1$, $n_1=1$ gives

$$|\mathcal{F}(X)|\sim\frac{X^{5/6}}{9q^2\zeta_{6q}(10)},$$

so

$$R_{r,t}(n_1,\dots,n_k)=\lambda_{r,t}(l_1)\cdots\lambda_{r,t}(l_k)Q^*(m_1,\dots,m_k)\frac{\zeta_{6q}(10)}{\zeta_{6mq}(10)}.$$

Using that

$$\frac{\zeta_{6q}(10)}{\zeta_{6mq}(10)}=\prod_{\substack{p\mid m\\ p\nmid 6q}}(1-p^{-10})^{-1}=\prod_{\substack{p\mid n\\ p\nmid 6q}}(1-p^{-10})^{-1},$$

completes the proof that $R_{r,t}=Q^*_{r,t}$.

Now we show that $Q^*(n_1,\dots,n_k)$ is multiplicative. To simplify notation only, we take $k=1$ and show $Q^*(mn)=Q^*(m)Q^*(n)$ provided $(m,n)=1$, where $m$ and $n$ are squarefree. Extending to the general case is straightforward. By the Chinese remainder theorem we may write all representatives $a(\operatorname{mod} mn)$ uniquely in the form $a_1m\overline{m}+a_2n\overline{n}$, where $a_1$ runs modulo $n$, $a_2$ runs modulo $m$, $m\overline{m}\equiv1(\operatorname{mod} n)$, and $n\overline{n}\equiv1(\operatorname{mod} m)$, and similarly for $b$. Then we get, using $\lambda(mn)=\lambda(m)\lambda(n)$,

$$\begin{aligned}Q^*(mn)&=\frac{1}{m^2n^2}\sum_{a_1,b_1(\operatorname{mod} n)}\sum_{a_2,b_2(\operatorname{mod} m)}\lambda_{a_1m\overline{m}+a_2n\overline{n},b_1m\overline{m}+b_2n\overline{n}}(mn)\\&=\frac{1}{m^2n^2}\sum_{a_1,b_1(\operatorname{mod} n)}\sum_{a_2,b_2(\operatorname{mod} m)}\lambda_{a_1,b_1}(n)\lambda_{a_2,b_2}(m)=Q^*(m)Q^*(n).\qquad\blacksquare\end{aligned}$$

https://doi.org/10.4153/CJM-2010-049-5 Published online by Cambridge University Press

Now we continue with our derivation of the moment conjecture, picking up with (3.2). We extend the summation over the $n_i$ to all positive integers and set

$$N_E(\alpha_1,\dots,\alpha_k) = X_E^{-\frac{1}{2}}(\tfrac{1}{2}+\alpha_1)\cdots X_E^{-\frac{1}{2}}(\tfrac{1}{2}+\alpha_k)\sum_{n_1}\cdots\sum_{n_k}\frac{Q^*_{r,t}(n_1,\dots,n_k)}{n_1^{\frac{1}{2}+\alpha_1}\cdots n_k^{\frac{1}{2}+\alpha_k}}.$$

We will obtain a meromorphic continuation of $N_E(\alpha_1,\dots,\alpha_k)$ to a neighborhood of $(0,\dots,0)$. Let

$$M_E(\alpha_1,\dots,\alpha_k) = \sum_{\substack{\epsilon_1,\dots,\epsilon_k\in\{-1,1\}\\ \epsilon_1\cdots\epsilon_k=1}} N_E(\epsilon_1\alpha_1,\dots,\epsilon_k\alpha_k).$$

Here $M_E$ is obtained by summing $N_E$ over all possible ways of swapping an even number of $\alpha_i$'s with their negatives. The moment (3.1) is clearly invariant under these symmetries, so in effect this is the simplest way to manipulate $N_E(\alpha_1,\dots,\alpha_k)$ to obtain an expression with these symmetries. This procedure is different from that stated in [CFKRS], but is essentially equivalent.

The general conjecture is then [CFKRS, 4.1.6]

$$\sum_{E\in\mathcal{F}(X)}\mathcal{Z}(E) = \sum_{E\in\mathcal{F}(X)} M_E(\alpha_1,\dots,\alpha_k)\bigl(1+O(N_E^{-\delta})\bigr)$$

for some $\delta>0$.

The next step is to express this answer in a more usable form. We write

$$M_E(\alpha_1,\dots,\alpha_k) = \sum_{\epsilon_1\cdots\epsilon_k=1}\!\!\cdots\sum X_E^{-\frac{1}{2}}(\tfrac{1}{2}+\epsilon_1\alpha_1)\cdots X_E^{-\frac{1}{2}}(\tfrac{1}{2}+\epsilon_k\alpha_k)H(\epsilon_1\alpha_1,\dots,\epsilon_k\alpha_k),$$

where

$$H(z_1,\dots,z_k) = \sum_{n_1}\cdots\sum_{n_k}\frac{Q^*_{r,t}(n_1,\dots,n_k)}{n_1^{\frac{1}{2}+z_1}\cdots n_k^{\frac{1}{2}+z_k}}. \tag{3.4}$$

Using the multiplicativity of $Q^*$ we write

$$\begin{aligned} H(z_1,\dots,z_k) &= \prod_p\sum_{e_1}\cdots\sum_{e_k}\frac{Q^*_{r,t}(p^{e_1},\dots,p^{e_k})}{p^{e_1(\frac{1}{2}+z_1)+\cdots+e_k(\frac{1}{2}+z_k)}} \\ &= \Bigl(\prod_{p\mid 6q}\sum_{e_1}\cdots\sum_{e_k}\frac{\lambda_{r,t}(p^{e_1})\cdots\lambda_{r,t}(p^{e_k})}{p^{e_1(\frac{1}{2}+z_1)+\cdots+e_k(\frac{1}{2}+z_k)}}\Bigr) \\ &\qquad\Bigl(\prod_{p\nmid 6q}\sum_{e_1}\cdots\sum_{e_k}\frac{\delta(p)Q^*(p^{e_1},\dots,p^{e_k})}{p^{e_1(\frac{1}{2}+z_1)+\cdots+e_k(\frac{1}{2}+z_k)}}\Bigr), \end{aligned} \tag{3.5}$$

where $\delta(p) = (1 - p^{-10})^{-1}$ if $e_1 + \cdots + e_k > 0$ and $\delta(p) = 1$ otherwise. Note that for $p|3q$

$$\sum_{e=0}^{\infty} \frac{\lambda_{r,t}(p^e)}{p^{e(\frac{1}{2}+z)}} = \Big(1 - \frac{\lambda_{r,t}(p)}{p^{\frac{1}{2}+z}} + \frac{1}{p^{1+2z}}\Big)^{-1},$$

using (2.3) and the fact that $(6q, 4r^3 + 27t^2) = 1$.

We wish to determine the polar behavior of $H(z_1, \dots, z_k)$ for $z_i$ near 0. Since $Q^*(m_1, \dots, m_k) \ll (m_1 \cdots m_k)^{\varepsilon}$, it suffices to consider the contribution from $e_1 + \cdots + e_k \leq 2$. We compute $H$ precisely in Section 4 with Proposition 4.1. For now we simply state that $Q^*(p^j, 1, \dots, 1) = 0$ for $j = 1, 2$ (actually it vanishes for $j < 10$) and that $Q^*(p, p, 1, \dots, 1) = 1 - p^{-1}$ (see Corollary 4.3 for this identity). By factoring out the appropriate zeta functions we have

$$H(z_1, \dots, z_k) = \Big(\prod_{1 \leq i < j \leq k} \zeta(1 + z_i + z_j)\Big) A_k(z_1, \dots, z_k),$$

where $A_k$ is the arithmetical factor which is holomorphic and nonzero in a neighborhood of 0.

The next step in the recipe is to use Lemma 2.5.2 of [CFKRS] to express the permutation sum in terms of a multiple contour integral. To this end, set

$$f(s) = \zeta(1+s), \quad F(a_1, \dots, a_k) = A_k(a_1, \dots, a_k) X_E^{-\frac{1}{2}}(\tfrac{1}{2} + a_1) \cdots X_E^{-\frac{1}{2}}(\tfrac{1}{2} + a_k),$$

and

$$K(a_1, \dots, a_k) = F(a_1, \dots, a_k) \prod_{1 \leq i < j \leq k} f(a_i + a_j).$$

Then $f$, $F$, and $K$ satisfy the conditions of Lemma 2.5.2, namely $F$ is a symmetric function, holomorphic near the origin, and $f$ has a simple pole of residue 1 at $s = 0$ but is otherwise holomorphic near $s = 0$. With this setup we see that

$$M_E(\alpha_1, \dots, \alpha_k) = \sum_{\epsilon_j = \pm 1} \tfrac{1}{2}\Big(1 + \prod_{j=1}^{k} \epsilon_j\Big) K(\epsilon_1 \alpha_1, \dots, \epsilon_k \alpha_k).$$

So by Lemma 2.5.2,

$$M_E(\alpha_1, \dots, \alpha_k) = \frac{(-1)^{k(k-1)/2}}{(2\pi i)^k} \frac{2^{k-1}}{k!} \oint \cdots \oint K(z_1, \dots, z_k) \frac{\Delta(z_1^2, \dots, z_k^2)^2 (\prod_{j=1}^{k} z_j + \prod_{j=1}^{k} \alpha_j)}{\prod_{i=1}^{k} \prod_{j=1}^{k} (z_i - \alpha_j)(z_i + \alpha_j)} dz_1 \cdots dz_k, \tag{3.6}$$

where $\Delta$ is the Vandermonde determinant

$$\Delta(z_1, \dots, z_k) = \prod_{1 \leq i < j \leq k} (z_j - z_i),$$

and where the paths of integrations enclose the $\pm\alpha_j$'s. Taking the $\alpha_i$'s to be zero, we obtain Corollary 1.3.

The precise form of the arithmetical factor is given in Proposition 4.4. The computation of the arithmetical factor relies on further knowledge of $Q^*$, which is discussed in Section 4.

## 3.2 The Positive Rank Family

We now turn to the derivation of Conjectures 1.4 and 1.5. We follow the same procedure as in the previous section to obtain a conjecture on the shifted product

$$\frac{1}{|\mathcal{F}'(X)|}\sum_{E\in\mathcal{F}'(X)} X_E^{-\frac12}(\tfrac12+\alpha_1)\cdots X_E^{-\frac12}(\tfrac12+\alpha_k)L(\tfrac12+\alpha_1,E)\cdots L(\tfrac12+\alpha_k,E).$$

In this case, since the central values almost always vanish, this quantity will average to zero, at least if one of the shift parameters is zero. However, we can differentiate the moment conjecture (3.6) with respect to each $\alpha_i$ and set $\alpha_i = 0$ to obtain a conjecture for the moments of the first derivatives of the $L$-functions at the central point. The derivation of the shifted moment conjecture goes through essentially unchanged.

Before stating the conjecture, we first set some new notation for this family. Set

$$Q^*_\square(n_1,\dots,n_k) = \frac{1}{n^{*2}}\sum_{a,b (\operatorname{mod} n^*)}\lambda_{a,b^2}(n_1)\cdots\lambda_{a,b^2}(n_k),$$

and

$$Q'(n_1,\dots,n_k) = Q^*_\square(n_1,\dots,n_k)\prod_{p|n}(1-p^{-7})^{-1}.$$

The Dirichlet series formed from $Q'$ is given by

$$H'(z_1,\dots,z_k) = \prod_p\sum_{e_1}\cdots\sum_{e_k}\frac{Q'(p^{e_1},\dots,p^{e_k})}{p^{e_1(\frac12+z_1)+\cdots+e_k(\frac12+z_k)}}.$$

As shorthand we write

$$Y_E(z_1,\dots,z_k) = X_E^{-\frac12}(\tfrac12+z_1)\cdots X_E^{-\frac12}(\tfrac12+z_k).$$

The general shifted moment conjecture then reads

$$\sum_{E\in\mathcal{F}'(X)}\mathcal{Z}(E) = \sum_{E\in\mathcal{F}'(X)} M_E(\alpha_1,\dots,\alpha_k)\bigl(1+O(N_E^{-\delta})\bigr),$$

where

$$(3.7)\quad M_E(\alpha_1,\dots,\alpha_k) = c_k\oint\cdots\oint H'(z_1,\dots,z_k)$$
$$\times\frac{\Delta(z_1^2,\dots,z_k^2)^2\Bigl(\prod_{j=1}^k z_j+\prod_{j=1}^k\alpha_j\Bigr)}{\prod_{i=1}^k\prod_{j=1}^k(z_i-\alpha_j)(z_i+\alpha_j)}Y_E(z_1,\dots,z_k)\,dz_1\cdots dz_k,$$

https://doi.org/10.4153/CJM-2010-049-5 Published online by Cambridge University Press

and where

$$c_k = \frac{(-1)^{k(k-1)/2}}{(2\pi i)^k} \frac{2^{k-1}}{k!}.$$

The behavior of $M_E$ for the positive rank family is drastically different from the family of all elliptic curves because the polar behavior of $H'$ is different than that of $H$. A thorough study of $Q'$ is undertaken in Section 5. For now we use that $Q'(p, 1, \dots, 1) = -p^{-1/2} + O(p^{-3/2})$, $Q'(p, p, 1, \dots, 1) = 1 + O(p^{-1})$, and $Q'(p^2, 1, \dots, 1) = 0$ to deduce the polar behavior of $H'$. Precisely,

$$H'(z_1, \dots, z_k) = \frac{\prod_{1 \leq i < j \leq k} \zeta(1 + z_i + z_j)}{\prod_{1 \leq i \leq k} \zeta(1 + z_i)} A'_k(z_1, \dots, z_k), \tag{3.8}$$

where $A'_k$ is given by an absolutely and uniformly convergent Euler product in a neighborhood of $(0, \dots, 0)$.

We now check that the moment conjecture is consistent with the Birch and Swinnerton–Dyer conjecture, that is that $M_E(\alpha_1, \dots, \alpha_k) = 0$ if some $\alpha_i = 0$.

***Proposition 3.3*** *The function $M_E(\alpha_1, \dots, \alpha_k)$ given by* (3.7) *vanishes at $\alpha_i = 0$, for any $i$.*

**Proof** We go back to the original representation of $M$ as a permutation sum of the form

$$S = \sum_{\epsilon_1, \dots, \epsilon_k \in \{-1,1\}} \tfrac{1}{2}(1 + \prod_{1 \leq l \leq k} \epsilon_l) f(\epsilon_1\alpha_1, \dots, \epsilon_k\alpha_k) \prod_{1 \leq i < j \leq k} \zeta(1 + \epsilon_i\alpha_i + \epsilon_j\alpha_j),$$

where $f$ is a symmetric, regular function near the origin. We know from Lemma 2.5.2 of [CFKRS] that these conditions ensure that such a sum is holomorphic in terms of the shift parameters near the origin. In the case of $M$ given by (3.7), we furthermore know that $(z_1 \cdots z_k)^{-1} f(z_1, \dots, z_k) = g(z_1, \dots, z_k)$, say, is regular at the origin. Thus

$$S = \alpha_1 \cdots \alpha_k \sum_{\epsilon_1, \dots, \epsilon_k \in \{-1,1\}} \tfrac{1}{2}(1 + \prod_{1 \leq l \leq k} \epsilon_l) g(\epsilon_1\alpha_1, \dots, \epsilon_k\alpha_k) \prod_{1 \leq i < j \leq k} \zeta(1 + \epsilon_i\alpha_i + \epsilon_j\alpha_j),$$

so $(\alpha_1 \cdots \alpha_k)^{-1} S$ is regular at the origin, and hence $S$ vanishes when any shift parameter is set to zero. ■

Let $M'_E$ be the derivative of $M_E(\alpha_1, \dots, \alpha_k)$ with respect to all $\alpha_i$ evaluated at $\alpha_1 = \cdots = \alpha_k = 0$. Now we derive Conjecture 1.5 by computing $M'_E$ using (3.7). Again we consider the terms with $\prod z_j$ and $\prod \alpha_j$ separately. It is obvious that the former term is even with respect to each $\alpha_i$ so that differentiating at $\alpha_i = 0$ yields zero. By parity considerations it follows quickly that

$$\frac{\partial}{\partial \alpha_1} \cdots \frac{\partial}{\partial \alpha_k} \Big( \prod_{1 \leq j \leq k} \alpha_j \prod_{i=1}^{k} \prod_{j=1}^{k} (z_i^2 - \alpha_j^2)^{-1} \Big) \Big|_{\alpha_1 = \cdots = \alpha_k = 0} = \prod_{i=1}^{k} z_i^{-2k}.$$

https://doi.org/10.4153/CJM-2010-049-5 Published online by Cambridge University Press

We now see that

$$M_E' = c_k' \oint \cdots \oint A_k'(z_1, \dots, z_k) \prod_{1 \le i < j \le k} \zeta(1 + z_i + z_j) \\ \times \frac{\Delta(z_1^2, \dots, z_k^2)^2}{\prod_{i=1}^k z_i^{2k} \zeta(1 + z_i)} Y_E(z_1, \dots, z_k) dz_1 \cdots dz_k.$$

By comparison with (1.2) we see that $M_E'$ has the same order of magnitude as $P_k(N)$. This completes the derivation of Conjecture 1.5.

# 4 The Arithmetical Factor for the Family of all Elliptic Curves

In order to understand the arithmetical factor it is necessary to understand the behavior of $Q^*(n_1, \dots, n_k)$. Because of the multiplicativity of $Q^*$, it suffices to understand

$$Q^*(p^{e_1}, \dots, p^{e_k}) = \frac{1}{p^2} \sum_{a,b (\mathrm{mod}\ p)} \lambda_{a,b}(p^{e_1}) \cdots \lambda_{a,b}(p^{e_k}). \tag{4.1}$$

We desire a usable formula for this expression. Such a derivation is the purpose of this section.

## 4.1 The Case $k = 1$

We first derive a formula for $Q^*(p^j)$. To this end, we state

***Proposition 4.1*** *Set*

$$Q(p^j) = \sum_{a,b (\mathrm{mod}\ p)} p^{j/2} \lambda_{a,b}(p^j) \tag{4.2}$$

*and let $Tr_j(p)$ be the trace of the Hecke operator $T_p$ acting on the space of weight $j$ holomorphic cusp forms on the full modular group. Then for $j \neq 0$ and $p > 3$,*

$$-\frac{1}{p-1} Q(p^j) = Tr_{j+2}(p).$$

***Remarks*** Here $p^{j/2}\lambda_{a,b}(p^j)$ is an integer. The scaling factor $(p-1)^{-1}$ naturally arises because $|\lambda(p)|$ is fixed under quadratic twists (of which there are typically $p-1$). If we define the normalized trace $Tr_j^*(n)$ via $Tr_j(n) = n^{(j-1)/2} Tr_j^*(n)$, then the proposition reads

$$Q^*(p^j) = -\frac{p-1}{p^{3/2}} Tr_{j+2}^*(p)$$

for $j > 0$. Of course $Q^*(1) = 1$.

https://doi.org/10.4153/CJM-2010-049-5 Published online by Cambridge University Press

**Proof** The proof of this result is implicitly contained in [B]. Birch computes the related sum

$$p^{j/2}\Big(\sum_a \sum_b \lambda_{a,b}(p)\Big)^j.$$

It is actually simpler to work with (4.2). By modifying Birch's arguments we easily arrive at

$$\frac{1}{p-1}Q(p^j) = 1 + \frac{1}{2}\sum_{t^2<4p} U_j\Big(\frac{t}{2\sqrt{p}}\Big) V_w(t^2-4p),$$

where $V_w(D)$ is the number of classes of binary quadratic forms with discriminant $D < 0$, divided by 3 if $D = -3$ and divided by 2 if $D = -4$. This should be compared with [B, (3)]. The proof is completed by comparing the above equation with the Eichler–Selberg Trace Formula [Se, 4.5]. ■

### 4.2 The General Case

Now we may easily prove the following.

***Proposition 4.2*** *Let $Q^*$ be given by* (4.1). *Then for $p > 3$ and even $f = \sum e_i \neq 0$*

$$(4.3)\quad Q^*(p^{e_1},\dots,p^{e_k}) = \\ c_0\frac{p-1}{p} - \sum_{l\geq 1} c_l\Big(\frac{p-1}{p^{3/2}}Tr^*_{l+2}(p) + \frac{p-1}{p^2}p^{-l/2}\Big) + \frac{p-1}{p^2}p^{-f/2}$$

*holds. In addition, the left hand side above is zero if $f$ is odd or $p = 2$, and the right hand side is $1 - p^{-2}$ if $f = 0$.*

Recall that the $c_l = c_l(e_1,\dots,e_k)$ are defined by (2.7) and satisfy (2.8).

**Proof** To see that the left hand side is zero when $f$ is odd, simply apply the change of variables $a = d^2a'$, $b = d^3b'$ where $d$ is a quadratic nonresidue (mod $p$), and notice that the same sum is obtained except multiplied by $-1$.

The right hand side is easily seen to be $1 - p^{-2}$ when $f = 0$, since $c_l = 0$ for $l > 0$, and $c_0 = 1$.

We may now assume $f \neq 0$ is even. To begin, split the summation into two pieces as follows

$$Q^*(p^{e_1},\dots,p^{e_k}) = \\ \frac{1}{p^2}\sum_{\substack{a,b (\mathrm{mod}\ p)\\ (p,\Delta)=1}} \lambda_{a,b}(p^{e_1})\cdots\lambda_{a,b}(p^{e_k}) + \frac{1}{p^2}\sum_{\substack{a,b (\mathrm{mod}\ p)\\ p\mid\Delta}} \lambda_{a,b}(p^{e_1})\cdots\lambda_{a,b}(p^{e_k}),$$

where $\Delta = -16(4a^3 + 27b^2)$ of course. Using the Hecke relations and the definition of the $c_l$ given by (2.7), we have

$$Q^*(p^{e_1}, \dots, p^{e_k}) = \frac{1}{p^2} \sum_l c_l \sum_{\substack{a,b (\mathrm{mod}\, p) \\ (p,\Delta)=1}} \lambda_{a,b}(p^l) + \frac{1}{p^2} \sum_{\substack{a,b (\mathrm{mod}\, p) \\ p|\Delta}} \lambda^f_{a,b}(p).$$

In the first sum we separate the term $l = 0$ and remove the condition $(p, \Delta) = 1$ to obtain

$$\frac{1}{p^2} \sum_{\substack{a,b (\mathrm{mod}\, p) \\ (p,\Delta)=1}} 1 + \sum_{l \ge 1} c_l Q^*(p^l) - \sum_{l \ge 1} c_l \frac{1}{p^2} \sum_{\substack{a,b (\mathrm{mod}\, p) \\ p|\Delta}} \lambda_{a,b}(p^l) + \frac{1}{p^2} \sum_{\substack{a,b (\mathrm{mod}\, p) \\ p|\Delta}} \lambda^f_{a,b}(p).$$

One can parameterize all pairs $(a, b) \in \mathbb{F}_p^2$ such that $\Delta \equiv 0 (\mathrm{mod}\, p)$ by $a = -3c^2$, $b = 2c^3$, where $c$ runs modulo $p$. In particular, there are $p$ such pairs, and hence there are $p(p-1)$ pairs such that $(p, \Delta) = 1$. If $p|\Delta$ and $l$ is even then we claim that $\lambda_{a,b}(p^l) = p^{-l/2}$ unless $p|(a, b)$ or $p = 3$, in which case $\lambda_{a,b}(p^l) = 0$. To see this, note that $\lambda_{a,b}(p^l) = \lambda^l_{a,b}(p)$ for $p|\Delta$, and if $a = -3c^2$, $b = 2c^3$, then

$$\lambda_{a,b}(p) = -\frac{1}{\sqrt{p}} \sum_{x (\mathrm{mod}\, p)} \left( \frac{x^3 - 3c^2 x + 2c^3}{p} \right) = -\frac{1}{\sqrt{p}} \sum_{x (\mathrm{mod}\, p)} \left( \frac{(x-c)^2 (x+2c)}{p} \right)$$
$$= -\frac{1}{\sqrt{p}} \sum_{x \neq c} \left( \frac{x+2c}{p} \right) = \frac{1}{\sqrt{p}} \left( \frac{3c}{p} \right).$$

Hence we obtain

$$Q^*(p^{e_1}, \dots, p^{e_k}) = \frac{p-1}{p} c_0 + \sum_{l \ge 1} c_l Q^*(p^l) - \frac{(p-1)}{p^2} \sum_{l \ge 1} c_l p^{-l/2} + \frac{(p-1)}{p^2} p^{-f/2},$$

for $p > 3$. Applying Proposition 4.1 completes the proof. ■

***Corollary 4.3*** *We have $Q^*(p, 1, \dots, 1) = 0$ and $Q^*(p, p, \dots, 1) = 1 - p^{-1}$.*

**Proof** The former assertion was already stated in Proposition 4.2. As for the latter, we compute that $c_0(1, 1, 0, \dots, 0) = c_2(1, 1, 0, \dots, 0) = 1$ since $U_1(x)^2 = 4x^2 = 1 + (4x^2 - 1) = U_0(x) + U_2(x)$. ■

Now we can compute the arithmetical factor.

https://doi.org/10.4153/CJM-2010-049-5 Published online by Cambridge University Press

***Proposition 4.4*** *Let $H$ be given by* (3.4). *Then*

(4.4)

$$H(z_1,\dots,z_k)$$

$$= \prod_{p|3q}\prod_{j=1}^{k}\Big(1-\frac{\lambda_{r,t}(p)}{p^{\frac{1}{2}+z_j}}+\frac{1}{p^{1+2z_j}}\Big)^{-1}\prod_{p\nmid 6q}\Big\{1+\Big(1-\frac{1}{p}\Big)\Big(1-\frac{1}{p^{10}}\Big)^{-1}$$

$$\Big[\Big(-1+\int\prod_{j=1}^{k}\Big(1-\frac{2\cos\theta}{p^{\frac{1}{2}+z_j}}+\frac{1}{p^{1+2z_j}}\Big)^{-1}d\mu_{ST}\Big)$$

$$-\frac{1}{p^{1/2}}\sum_{l}Tr^{*}_{l+2}(p)\int U_l(\cos\theta)\prod_{j=1}^{k}\Big(1-\frac{2\cos\theta}{p^{\frac{1}{2}+z_j}}+\frac{1}{p^{1+2z_j}}\Big)^{-1}d\mu_{ST}$$

$$-\frac{p+1}{p^2}\int\Big(-1+\Big(1-\frac{2\cos 2\theta}{p}+\frac{1}{p^2}\Big)^{-1}\Big)\prod_{j=1}^{k}\Big(1-\frac{2\cos\theta}{p^{\frac{1}{2}+z_j}}+\frac{1}{p^{1+2z_j}}\Big)^{-1}d\mu_{ST}$$

$$+\frac{1}{p}\Big(-1+\frac{1}{2}\Big(\prod_{i=1}^{k}\big(1-p^{-1-z_i}\big)^{-1}+\prod_{i=1}^{k}\big(1+p^{-1-z_i}\big)^{-1}\Big)\Big)\Big]\Big\}.$$

*Furthermore, $H$ has the form*

$$H(z_1,\dots,z_k)=\Big(\prod_{1\le i<j\le k}\zeta(1+z_i+z_j)\Big)A_k(z_1,\dots,z_k), \tag{4.5}$$

*where $A_k$ is given by an Euler product that is uniformly convergent in the region $Re(z_i)\ge -\delta$, $1\le i\le k$, for some $\delta>0$.*

**Proof** Recall $H$ satisfies (3.5), so

$$H(z_1,\dots,z_k)=\prod_{p|3q}\prod_{i=1}^{k}\Big(1-\frac{\lambda_{r,t}(p)}{p^{\frac{1}{2}+z_i}}+\frac{1}{p^{1+2z_i}}\Big)^{-1}$$
$$\prod_{p\nmid 6q}\Big(1+(1-p^{-10})^{-1}\sum_{\substack{e_1,\dots,e_k\\ e_1+\dots+e_k>0}}\frac{Q^{*}(p^{e_1},\dots,p^{e_k})}{p^{e_1(\frac{1}{2}+z_1)+\dots+e_k(\frac{1}{2}+z_k)}}\Big).$$

We apply Proposition 4.2 and sum over the four terms given by (4.3) separately. We compute, using $c_0 = 0$ if $f$ is odd,

$$\begin{aligned}\sum_{\substack{e_1,\dots,e_k\\ 2\mid f\neq 0}} \frac{c_0(e_1,\dots,e_k)}{p^{e_1(\frac12+z_1)+\cdots+e_k(\frac12+z_k)}} &= -1 + \sum_{e_1,\dots,e_k} \int \frac{U_{e_1}(\cos\theta)\cdots U_{e_k}(\cos\theta)}{p^{e_1(\frac12+z_1)+\cdots+e_k(\frac12+z_k)}} d\mu_{ST}\\ &= -1 + \int \prod_{j=1}^{k} \Big(1 - \frac{2\cos\theta}{p^{\frac12+z_j}} + \frac{1}{p^{1+2z_j}}\Big)^{-1} d\mu_{ST}\\ &= \sum_{1\le i<j\le k} p^{-1-z_i-z_j} + (\text{higher degree terms}),\end{aligned}$$

this final estimation being easily seen using that $c_0(1,1,0,\dots,0) = 1$. This term accounts for the Riemann zeta factors.

The term involving traces requires a computation as follows

$$\begin{aligned}&\sum_{l\ge 1} Tr^*_{l+2}(p) \sum_{\substack{e_1,\dots,e_k\\ 2\mid f\neq 0}} \frac{c_l(e_1,\dots,e_k)}{p^{e_1(\frac12+z_1)+\cdots+e_k(\frac12+z_k)}}\\ &\quad= \sum_{l\ge 1} Tr^*_{l+2}(p) \sum_{e_1,\dots,e_k} \int \frac{U_{e_1}(\cos\theta)\cdots U_{e_k}(\cos\theta)}{p^{e_1(\frac12+z_1)+\cdots+e_k(\frac12+z_k)}} U_l(\cos\theta) d\mu_{ST}\\ &\quad= \sum_{l} Tr^*_{l+2}(p) \int U_l(\cos\theta) \prod_{j=1}^{k} \Big(1 - \frac{2\cos\theta}{p^{\frac12+z_j}} + \frac{1}{p^{1+2z_j}}\Big)^{-1} d\mu_{ST}.\end{aligned}$$

Since the traces are zero for $l+2 < 12$, this sum is uniformly convergent in a product of half-planes containing the origin.

The other term involving $c_l$ involves

$$\begin{aligned}&\sum_{l\ge 1} p^{-l/2} \sum_{\substack{e_1,\dots,e_k\\ 2\mid f\neq 0}} \frac{c_l(e_1,\dots,e_k)}{p^{e_1(\frac12+z_1)+\cdots+e_k(\frac12+z_k)}}\\ &\quad= \sum_{l\ge 1} p^{-l} \sum_{e_1,\dots,e_k} \int \frac{U_{e_1}(\cos\theta)\cdots U_{e_k}(\cos\theta)}{p^{e_1(\frac12+z_1)+\cdots+e_k(\frac12+z_k)}} U_{2l}(\cos\theta) d\mu_{ST}\\ &\quad= \sum_{l\ge 1} p^{-l} \int U_{2l}(\cos\theta) \prod_{j=1}^{k} \Big(1 - \frac{2\cos\theta}{p^{\frac12+z_j}} + \frac{1}{p^{1+2z_j}}\Big)^{-1} d\mu_{ST}\\ &\quad= \int \Bigg(-1 + \Bigg(\frac{1+\frac1p}{1 - \frac{2\cos 2\theta}{p} + \frac{1}{p^2}}\Bigg)\Bigg) \prod_{j=1}^{k} \Big(1 - \frac{2\cos\theta}{p^{\frac12+z_j}} + \frac{1}{p^{1+2z_j}}\Big)^{-1} d\mu_{ST},\end{aligned}$$

where the summation over $l$ is executed using the identity

$$\sum_{n=0}^{\infty} U_{2n}(x) t^{2n} = \frac{1+t^2}{1 + 2t^2(1-2x^2) + t^4},$$

which is easily derived from (2.5) by replacing $t$ with $-t$ and adding.

https://doi.org/10.4153/CJM-2010-049-5 Published online by Cambridge University Press

The final term is

$$\sum_{\substack{e_1,\dots,e_k\\ 2|f\neq 0}} \frac{1}{p^{e_1(1+z_1)+\cdots+e_k(1+z_k)}} = -1 + \frac{1}{2}\sum_{e_1,\dots,e_k} \frac{1+(-1)^{e_1+\cdots+e_k}}{p^{e_1(1+z_1)+\cdots+e_k(1+z_k)}}$$

$$= -1 + \frac{1}{2}\Big[\prod_{i=1}^{k}\Big(1-p^{-1-z_i}\Big)^{-1} + \prod_{i=1}^{k}\Big(1+p^{-1-z_i}\Big)^{-1}\Big]$$

The proposition follows by appropriately summing the four terms above. ■

To obtain a formula for $a_k$, we use that the leading coefficient of $P_k(N)$ is

$$A_k(0,\dots,0)2^k\prod_{j=1}^{k-1}\frac{j!}{2j!} = A_k(0,\dots,0)2^{k/2}\frac{G(1+k)\sqrt{\Gamma(1+2k)}}{\sqrt{G(1+2k)\Gamma(1+k)}} =: a_k g_k,$$

where $a_k = A_k(0,\dots,0)$. This computation can be found in [CFKRS]. Then we compute

$$\begin{aligned}(4.6)\qquad a_k = {}& \Big(\frac{\phi(6q)}{6q}\Big)^{k(k-1)/2}\prod_{p|3q}\Big(1-\frac{\lambda_{r,t}(p)}{p^{\frac{1}{2}}}+\frac{1}{p}\Big)^{-k}\prod_{p\nmid 6q}\Big(1-\frac{1}{p}\Big)^{k(k-1)/2}\\ &\times\Big\{1+\Big(1-\frac{1}{p}\Big)\Big(1-\frac{1}{p^{10}}\Big)^{-1}\Big[\Big(-1+\int V_p(\theta)^k d\mu_{ST}\Big)\\ &-\frac{1}{p^{1/2}}\sum_l Tr^*_{l+2}(p)\int U_l(\cos\theta)V_p(\theta)^k d\mu_{ST}\\ &-\frac{p+1}{p^2}\int\Big(-1+\Big(1-\frac{2\cos 2\theta}{p}+\frac{1}{p^2}\Big)^{-1}\Big)V_p(\theta)^k d\mu_{ST}\\ &+\frac{1}{p}\Big(-1+\frac{1}{2}\Big(\Big(1-\frac{1}{p}\Big)^{-k}+\Big(1+\frac{1}{p}\Big)^{-k}\Big)\Big)\Big]\Big\},\end{aligned}$$

where

$$V_p(\theta) = \Big(1-\frac{2\cos\theta}{p^{1/2}}+\frac{1}{p}\Big)^{-1}.$$

## 5 The Arithmetical Factor for the Positive Rank Family $\mathcal{F}'$

The computation of the arithmetical factor for the family $\mathcal{F}'$ is more difficult than that for the family of all elliptic curves $\mathcal{F}$. This author does not know an explicit formula similar to (4.4). Nevertheless, we can compute $Q^*_\square(p^{e_1},\dots,p^{e_k})$ when $e_1+\cdots+e_k$ is even. The reason for this is that the change of variables $x \to rx$, $a \to r^2a$ gives

$$\sum_{a(\operatorname{mod} p)}\lambda_{a,c}(p^l) = \Big(\frac{r}{p}\Big)^l\sum_{a(\operatorname{mod} p)}\lambda_{a,r^{-3}c}(p^l),$$

https://doi.org/10.4153/CJM-2010-049-5 Published online by Cambridge University Press

so applying $b \longrightarrow r^2 b$ for $l$ even gives that

$$\sum_a \sum_b \lambda_{a,b^2}(p^l) = \sum_a \sum_b \lambda_{a,rb^2}(p^l).$$

We conclude that

$$\sum_a \sum_b \lambda_{a,b^2}(p^l) = \sum_a \sum_b \lambda_{a,b}(p^l),$$

Using the same arguments as in the proof of Proposition 4.2 shows that

$$Q^*_\square(p^{e_1},\dots,p^{e_k}) = Q^*(p^{e_1},\dots,p^{e_k})$$

for $e_1 + \cdots + e_k$ even.

On the other hand, $Q^*_\square(p^l)$ is not so easily analysed for $l$ odd. For $l = 1$ we compute directly

$$Q^*_\square(p) = -p^{-5/2} \sum_a \sum_b \sum_x \Big(\frac{x^3+ax+b^2}{p}\Big).$$

The summation over $a$ clearly vanishes unless $x = 0$, in which case the summation over $a$ is $p$. The summation over $b$ is $p - 1$. Hence

$$Q^*_\square(p) = -p^{-1/2} + p^{-3/2}.$$

We now have enough information to deduce that (3.8) holds, as desired. Obtaining a formula for $A'_k$ similar to the analogous formula (4.4)–(4.5) for $A_k$ requires a formula for $Q^*_\square(p^l)$ for $l$ odd.

For the application to the Riemann Hypothesis described in Section 7, it is relevant to know the region of convergence of $A'_1(\alpha)$. We compute

$$\begin{aligned}\sum_{e=0}^{\infty} \frac{Q^*_\square(p^e)}{p^{e(\frac12+\alpha)}} &= 1 - \frac{1}{p^{1+\alpha}} + O(p^{-3(\frac12+\alpha)}) + O(p^{-2-\alpha}) \\ &= (1-p^{-1-\alpha})(1 + O(p^{-2(1+\alpha)}) + O(p^{-3(\frac12+\alpha)})),\end{aligned}$$

so $A'_1(\alpha)$ is given by an absolutely and uniformly convergent Euler product in the region $\operatorname{Re}(\alpha) > -\frac16$. This region could be improved with better bounds on $Q^*_\square(p^e)$ for $e \geq 3$. We have made no such attempt.

## 6 Conjecture 1.6

Our arguments follow those of [CKRS], so we shall be brief. For further elaboration of the method see their paper. The idea is to consider the following ratio

$$R_{q,k} = \lim_{X\to\infty} \Big(\sum_{E\in\mathcal{F}^+_{r,t}(X)} L(1/2,E)^k\Big) \Big/ \Big(\sum_{E\in\mathcal{F}^+_{r',t'}(X)} L(1/2,E)^k\Big).$$

Arguments as in [CKRS] lead to the conjecture that $R_q(X) \sim R_{q,-\frac{1}{2}}$. Our Conjecture 1.1 gives the asymptotic behavior of $R_{q,k}$ for general $k$.

The expectation is that

$$R_{q,k} = \frac{\prod_{p|q}\left(1 - \frac{\lambda_{r,t}(p)}{p^{1/2}} + \frac{1}{p}\right)^{-k}}{\prod_{p|q}\left(1 - \frac{\lambda_{r',t'}(p)}{p^{1/2}} + \frac{1}{p}\right)^{-k}},$$

since all other factors are independent of the choice or $r$ and $t \pmod{6q}$. By random matrix theory considerations, taking $k = -1/2$ above gives the prediction.

## 7 The Riemann Hypothesis

At the Riemann Hypothesis conference in 2002 at Courant sponsored by AIM, Iwaniec described an approach to RH using positive rank families of elliptic curves, such as the family $\mathcal{F}'$ considered in this paper. Conrey [C] has given a brief summary of the approach. Here we show how to use the moment conjectures to frame the method.

The identity

$$\lim \frac{1}{|\mathcal{F}'(X)|} \sum_{E \in \mathcal{F}'(X)} \lambda_E(p) = -\frac{1}{\sqrt{p}} + O(p^{-3/2})$$

and multiplicativity suggests

$$\lim \frac{1}{|\mathcal{F}'(X)|} \sum_{E \in \mathcal{F}'(X)} \lambda_E(n) \approx \frac{\mu(n)}{\sqrt{n}},$$

for $n$ squarefree. The point is that the Möbius function can be obtained by averaging Dirichlet series coefficients of these positive rank elliptic curves.

Consider (3.7) with $k = 1$. A quick calculation gives that

$$M(\alpha) = \frac{A'(\alpha)}{\zeta(1+\alpha)} X_E^{-\frac{1}{2}}(\tfrac{1}{2} + \alpha),$$

where $A'(\alpha)$ is the arithmetical factor that converges uniformly on compact subsets of the region $\mathrm{Re}(\alpha) > -\frac{1}{6}$, using the computation at the end of Section 5.

Thus we obtain the following conjecture.

***Conjecture 7.1*** *Let $|Re(\alpha)| < \frac{1}{6}$. Then*

$$\sum_{E \in \mathcal{F}'(X)} L(\tfrac{1}{2} + \alpha, E) = \frac{A'(\alpha)}{\zeta(1+\alpha)} \sum_{E \in \mathcal{F}'(X)} (1 + O(N_E^{-\delta})).$$

To deduce a quasi-Riemann Hypothesis, let $1+\alpha$ be a nontrivial zero with $\mathrm{Re}(\alpha) > -\frac{1}{6}$. The left hand side is obviously holomorphic at $\alpha$, but the right hand side is not.

***Corollary 7.2*** *Conjecture* 7.1 *implies that the Riemann zeta function $\zeta(s)$ has no zeros for $Re(s) > \frac{5}{6}$.*

**Acknowledgments** I thank Brian Conrey and David Farmer for suggesting this line of research and for many helpful discussions. I also thank Duc Khiem Huynh and Nina Snaith for useful feedback.

## References

[BMSW] B. Bektemirov, B. Mazur, W. Stein, and M. Watkins, *Average ranks of elliptic curves: tension between data and conjecture.* Bull. Amer. Math. Soc. (N.S.) **44**(2007), no. 2, 233–254. doi:10.1090/S0273-0979-07-01138-X

[B] B. Birch, *How the number of points of an elliptic curve over a fixed prime field varies.* J. London Math. Soc. **43**(1968), 57-60. doi:10.1112/jlms/s1-43.1.57

[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**(2001), no. 4, 843–939. doi:10.1090/S0894-0347-01-00370-8

[C] J. Conrey, *The Riemann hypothesis.* Notices Amer. Math. Soc. **50**(2003), no. 3, 341–353.

[CFKRS] J. Conrey, D. Farmer, J. Keating, M. Rubinstein, and N. Snaith, *Integral moments of L-functions.* Proc. London Math. Soc. (3) **91**(2005), no. 1, 33–104. doi:10.1112/S0024611504015175

[CKRS] J. B. Conrey, J. Keating, M. Rubinstein, and N. Snaith, *On the frequency of vanishing of quadratic twists of modular L-functions.* In: Number theory for the millennium, I (Urbana, IL, 2000), A K Peters, Natick, MA, 2002, pp. 301–315.

[F] D. W. Farmer, *Modeling families of L-functions.* In: Ranks of elliptic curves and random matrix theory, London Mathematical Society Lecture Note Series, 341, Cambridge University Press, Cambridge, 2007.

[GR] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products.* Fourth edition, Academic Press, New York, 1965.

[KS] J. P. Keating and N. Snaith, *Random matrix theory and L-functions at $s = 1/2$.* Comm. Math. Phys. **214**(2000), no. 1, 91–110. doi:10.1007/s002200000262

[Kn] A. W. Knapp, *Elliptic curves.* Mathematical Notes, 40, Princeton University Press, Princeton, NJ, 1992.

[M] S. J. Miller, *Investigations of zeros near the central point of elliptic curve L-functions.* With an appendix by Eduardo Dueñez. Experiment. Math. **15**(2006), no. 3, 257–279.

[Sch] R. Schoof, *Nonsingular plane cubic curves over finite fields.* J. Combin. Theory Ser. A **46**(1987), no. 2, 183–211. doi:10.1016/0097-3165(87)90003-3

[Se] A. Selberg, *Harmonic analysis and discontinuous groups in weakly symmetric Riemannian spaces with applications to Dirichlet series.* J. Indian Math. Soc. **20**(1956), 47–87.

[Si] J. H. Silverman, *The arithmetic of elliptic curves.* Graduate Texts in Mathematics, 106, Springer-Verlag, New York, 1986.

[Si2] ———, *Advanced topics in the arithmetic of elliptic curves.* Graduate Texts in Mathematics, 151, Springer-Verlag, New York, 1994.

[TW] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras.* Ann. of Math. (2) **141**(1995), no. 3, 553–572. doi:10.2307/2118560

[Wa] M. Watkins, *Some heuristics about elliptic curves.* Experiment Math. **17**(2008), no. 1, 105–125.

[Wi] A. Wiles, *Modular elliptic curves and Fermat's last theorem.* Ann. of Math. (2) **141**(1995), no. 3, 443–551. doi:10.2307/2118559

[Y2] M. Young, *On the non-vanishing of elliptic curve L-functions at the central point.* Proc. London Math. Soc. (3) **93**(2006), no. 1, 1–42. doi:10.1017/S0024611506015760

*American Institute of Mathematics, Palo Alto, CA 94306-2244, U.S.A.*

and

*Department of Mathematics, Texas A&M University, College Station, TX 77843-3368, U.S.A.*
*e-mail*: myoung@math.tamu.edu

https://doi.org/10.4153/CJM-2010-049-5 Published online by Cambridge University Press