Low-lying zeros in families of elliptic curve L-functions over function fields

Downloaded from: https://research.chalmers.se, 2025-12-08 23:24 UTC

Citation for the original published paper (version of record):
Meisner, P., Södergren, A. (2022). Low-lying zeros in families of elliptic curve L-functions over function fields. Finite Fields and their Applications, 84. http://dx.doi.org/10.1016/j.ffa.2022.102096

N.B. When citing this work, cite the original published paper.

research.chalmers.se offers the possibility of retrieving research publications produced at Chalmers University of Technology. It covers all kind of research output: articles, dissertations, conference papers, reports etc. since 2004. research.chalmers.se is administrated and maintained by Chalmers Library

(article starts on next page)

Finite Fields and Their Applications 84 (2022) 102096

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Low-lying zeros in families of elliptic curve L-functions over function fields

Patrick Meisner [a], Anders Södergren [b,*]

[a] *Department of Mathematics, KTH, SE-100 44 Stockholm, Sweden*
[b] *Department of Mathematical Sciences, Chalmers University of Technology and the University of Gothenburg, SE-412 96 Gothenburg, Sweden*

ARTICLE INFO

Article history:
Received 14 October 2021
Received in revised form 7 May 2022
Accepted 27 July 2022
Available online xxxx
Communicated by Sergey Rybakov

MSC:
primary 11G40, 11R59
secondary 11M50

Keywords:
Elliptic curves
Quadratic and cubic twists
Function fields over finite fields
L-functions
Frobenius class
One-level density

ABSTRACT

We investigate the low-lying zeros in families of L-functions attached to quadratic and cubic twists of elliptic curves defined over $\mathbb{F}_q(T)$. In particular, we present precise expressions for the expected values of traces of high powers of the Frobenius class in these families with a focus on the lower order behavior. As an application we obtain results on one-level densities and we verify that these elliptic curve families have orthogonal symmetry type. In the quadratic twist families our results refine previous work of Comeau-Lapointe. Moreover, in this case we find a lower order term in the one-level density reminiscent of the deviation term found by Rudnick in the hyperelliptic ensemble. On the other hand, our investigation is the first to treat these questions in families of cubic twists of elliptic curves and in this case it turns out to be more complicated to isolate lower order terms due to a larger degree of cancellation among lower order contributions.
© 2022 The Author(s). Published by Elsevier Inc. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

* Corresponding author.
E-mail addresses: pfmeisner@gmail.com (P. Meisner), andesod@chalmers.se (A. Södergren).

https://doi.org/10.1016/j.ffa.2022.102096
1071-5797/© 2022 The Author(s). Published by Elsevier Inc. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

1. Introduction

The Katz–Sarnak heuristics [25] is concerned with the distribution of low-lying zeros in families of L-functions and predicts that this distribution is determined by a certain random matrix model called the symmetry type of the family (see also [32] and the references therein). In this paper we are interested in families of L-functions attached to elliptic curves, where quantities related to low-lying zeros have been studied for a comparatively long time due to their close relation to the average rank of the elliptic curves in the family via the Birch and Swinnerton-Dyer conjecture; see, e.g., [3,18,20,21]. For families of elliptic curves defined over the rationals, the systematic investigation of low-lying zeros and the Katz–Sarnak heuristic started with papers by Miller [30] and Young [35,36] in the early 2000's. More recent contributions include [14,19,22,23] that focus on lower order terms in the one-level density and the corresponding predictions of the L-functions ratios conjecture.

In the present paper we investigate families of L-functions attached to elliptic curves defined over the function field $\mathbb{F}_q(t)$. Recall that additional tools are available in the function field setting since, for example, the Riemann Hypothesis is a celebrated theorem due to Deligne [15]. Already the pioneering work by Katz and Sarnak [25] studied low-lying zeros in families of quadratic twists of elliptic curves defined over $\mathbb{F}_q(t)$ in the limit where both q and the degree of the twists, i.e. the degree of the polynomials that parameterize the family, tend to infinity. However, it is expected that keeping q fixed while the degree of the twists tend to infinity is a closer analogue of quadratic twist families in the number field setting. Important results in this direction were proved by Rudnick [31] and Bui–Florea [4] who investigated the low-lying zeros of quadratic Dirichlet L-functions in the hyperelliptic ensemble. More recently, Comeau-Lapointe [9] investigated expected values of traces of high powers of the Frobenius class and the one-level density of families of quadratic twists of elliptic curves in this context and used the results to give upper bounds on the average rank in these families. In this paper, we refine results in [9] to isolate lower order terms and compare the structure of our results with the results of Rudnick [31] for quadratic Dirichlet L-functions.

In recent years, there has been an increased interest in a variety of different aspects of higher order characters and twists; see, e.g., [1,7–13,28,29]. Motivated by this development, we investigate expected values of traces of high powers of the Frobenius class and the one-level density of families of cubic twists of elliptic curves of the form $y^2 = x^3 + B$ defined over $\mathbb{F}_q(t)$. In this case we are not able to isolate lower order terms and we discuss what is needed in order to obtain refined results also in this situation.

We now turn to a precise description of our results.

1.1. Setup

Fix a prime $p \neq 2, 3$ and let $q = p^m$ for some power $m \in \mathbb{Z}_{\geq 1}$. For simplicity, assume $q \equiv 1 \bmod 6$. Let E be an elliptic curve defined over $\mathbb{F}_q(T)$ given by the minimal

Weierstrass equation $y^2 = x^3 + Ax + B$, where $A, B \in \mathbb{F}_q[T]$, and such that the prime at infinity has additive reduction.[1] Then the L-function attached to E is (cf., e.g., [34, Lecture 1])

$$L(u, E) := \prod_{P|\Delta_E} \left(1 - a_P(E)u^{\deg(P)}\right)^{-1} \prod_{P\nmid\Delta_E} \left(1 - a_P(E)u^{\deg(P)} + u^{2\deg(P)}\right)^{-1}, \tag{1.1}$$

where $\Delta_E = 4A^3 + 27B^2$ is the discriminant of E and

$$\#E(P) = q^{\deg(P)} + 1 - a_P(E)q^{\deg(P)/2}.$$

Here $E(P)$ is the curve[2] obtained from reducing E modulo a prime polynomial P and $\#E(P)$ denotes the number of $\mathbb{F}_{q^{\deg(P)}}$-rational points on the non-singular locus of $E(P)$. If it is clear which elliptic curve we are referring to, we will simply write a_P instead of $a_P(E)$. Recall, in particular, that with the above normalization the Hasse–Weil bound states that $|a_P| \leq 2$. Recall also that $L(u, E)$ is a polynomial of degree

$$\mathfrak{n}_E := \deg(M_E) + 2(\deg(A_E) + 1) - 4$$

all of whose zeros lie on the "critical line" $|u| = q^{-1/2}$, where M_E is the product of prime polynomials with multiplicative reduction and A_E is the product of prime polynomials with additive reduction (see [34, Lecture 1]). Furthermore, $L(u, E)$ satisfies the functional equation

$$L(u, E) = \epsilon(E)(\sqrt{q}u)^{\mathfrak{n}_E} L\left(\frac{1}{qu}, E\right),$$

where $\epsilon(E) \in \{\pm 1\}$ is the root number of the elliptic curve E.

We are interested in investigating the one-level density of the zeros of these L-functions. That is, for an even Schwartz test function f, we define the one-level density of E as

$$\mathcal{D}(E, f) := \sum_{\theta} f\left(\mathfrak{n}_E \frac{\theta}{2\pi}\right),$$

where the sum is over all $\theta \in \mathbb{R}$ such that $q^{-1/2}e^{i\theta}$ is a zero of $L(u, E)$, counted with multiplicity. Since $L(u, E)$ is a polynomial with all its zeros on the critical line, we can find a unitary $\mathfrak{n}_E \times \mathfrak{n}_E$ matrix Θ_E (in fact a conjugacy class of unitary matrices), called the Frobenius, such that

[1] That the prime at infinity has additive reduction is a simplifying assumption that makes the corresponding Euler factor of the L-function $L(u, E)$ trivial. This assumption can be removed with some work. See [34, Lecture 1] and Appendix A.1 for details.

[2] If P is a prime of good reduction, then $E(P)$ is in fact an elliptic curve.

$$L(u, E) = \det(1 - \sqrt{q}u\Theta_E). \tag{1.2}$$

Defining the one-level density of a unitary $\mathfrak{n}_E \times \mathfrak{n}_E$ matrix U as

$$\mathcal{D}(U, f) = \sum_{j=1}^{\mathfrak{n}_E} \sum_{n \in \mathbb{Z}} f\left(\mathfrak{n}_E\left(\frac{\theta_j}{2\pi} - n\right)\right),$$

where θ_j $(1 \leq j \leq \mathfrak{n}_E)$ are the eigenangles of U, we immediately get the relation[3]

$$\mathcal{D}(E, f) = \mathcal{D}(\Theta_E, f).$$

Finally, we may apply Poisson summation to obtain, for any unitary $\mathfrak{n}_E \times \mathfrak{n}_E$ matrix,

$$\mathcal{D}(U, f) = \frac{1}{\mathfrak{n}_E} \sum_{n \in \mathbb{Z}} \widehat{f}\left(\frac{n}{\mathfrak{n}_E}\right) \mathrm{Tr}(U^n). \tag{1.3}$$

Hence, for Schwartz test functions f whose Fourier transforms are supported in $(-\alpha, \alpha)$, to determine the expected value of $\mathcal{D}(E, f)$ as E ranges over some family of elliptic curves, it is enough to determine the expected value of $\mathrm{Tr}(\Theta_E^n)$ for $n < \alpha\mathfrak{n}_E$.

1.2. Quadratic twists

The first family we will be interested in is the family of quadratic twists of a given elliptic curve E. That is, if $E : y^2 = x^3 + Ax + B$ and D is a polynomial, then we define the quadratic twist of E by D as the curve with affine model

$$E_D : y^2 = x^3 + AD^2x + BD^3.$$

As D varies, these equations will give distinct elliptic curves if and only if the polynomials D are square-free and coprime to the discriminant Δ_E of E. Moreover, we see that all the primes that divide D will have additive reduction and that if D is monic and of even degree then the prime at infinity will have the same reduction type on E_D as it did on E (see Appendix A). Therefore, the degree of $L(u, E_D)$ will be

$$\mathfrak{n}_{E_D} = \mathfrak{n}_E + 2\deg(D).$$

From now on, and throughout the parts of this paper dealing with quadratic twists, we will assume that $N \in \mathbb{Z}^+$ is even. Hence, if we consider the family of twists coming from the set

[3] Recall that we define the one-level density of the elliptic curve E as a sum over *all* $\theta \in \mathbb{R}$ such that $L(q^{-1/2}e^{i\theta}, E) = 0$.

$$\mathcal{H}_N(\Delta_E) := \big\{D \in \mathbb{F}_q[T] : D \text{ monic, square-free, coprime to } \Delta_E \text{ and } \deg(D) = N\big\},$$

then we see that this will form a family of distinct elliptic curves all of whose Frobenius elements have the same size.

For any $D \in \mathcal{H}_N(\Delta_E)$ let $\epsilon(E_D)$ denote the root number of the L-function attached to E_D. Then (by [2, Proposition 4.3])

$$\epsilon(E_D) = \epsilon_N \epsilon(E) \chi_D(M_E),$$

where $\chi_D = \left(\frac{D}{\cdot}\right)$ is the Kronecker symbol and $\epsilon_N = \pm 1$, depending only on the value of $\deg(D) = N$. Therefore we define the sets

$$\mathcal{H}_N^+(\Delta_E) := \big\{D \in \mathcal{H}_N(\Delta_E) : \chi_D(M_E) = \epsilon_N \epsilon(E)\big\}$$

and

$$\mathcal{H}_N^-(\Delta_E) := \big\{D \in \mathcal{H}_N(\Delta_E) : \chi_D(M_E) = -\epsilon_N \epsilon(E)\big\}.$$

We will typically, however, just write $\mathcal{H}_N^{\pm}(\Delta_E)$ to mean either the set $\mathcal{H}_N^+(\Delta_E)$ or the set $\mathcal{H}_N^-(\Delta_E)$.

It was recently proven by Comeau-Lapointe [9] that, for $\epsilon > 0$, $n \in \mathbb{Z}_{\geq 1}$ and $N > 4\mathfrak{n}_E + 16$, the averages of traces of powers of Θ_{E_D} satisfy[4,5]

$$\big\langle \mathrm{Tr}(\Theta_{E_D}^n)\big\rangle_{\mathcal{H}_N^{\pm}(\Delta_E)} = \eta_2(n) + O_\epsilon\left((n+N)N^{2\mathfrak{n}_E+11}\left(\frac{1}{q^{N/8}} + \frac{1}{q^{\epsilon N}} + \frac{q^{n/2}}{q^{(1-\epsilon)N}}\right) + \frac{n^2}{q^{n/4}}\right), \tag{1.4}$$

where (see [17, Theorem 4])

$$\eta_2(n) := \int\limits_{\mathrm{O}(\mathfrak{n}_E+2N)} \mathrm{Tr}(U^n)\, dU = \begin{cases} 1 & 2|n, \\ 0 & 2 \nmid n. \end{cases}$$

This is then enough to deduce that if $\mathrm{supp}(\widehat{f}) \subset (-1, 1)$, then

$$\big\langle \mathcal{D}(E_D, f)\big\rangle_{\mathcal{H}_N^{\pm}(\Delta_E)} = \int\limits_{\mathrm{O}(\mathfrak{n}_E+2N)} \mathcal{D}(U, f)\, dU + O\left(\frac{1}{N}\right). \tag{1.5}$$

[4] Here, and throughout this paper, we use the convention that for any finite and non-empty set S and any function ϕ on S, $\langle \phi \rangle_S = \frac{1}{|S|}\sum_{s \in S} \phi(s)$.

[5] Note that the family considered in [9] is not the same as the one stated here. However, one may easily deduce this result from that of [9].

Remark 1.1. For every sufficiently nice family of elliptic curves $\mathcal{F}$, the Katz–Sarnak heuristic predicts that

$$\big\langle \mathcal{D}(E,f)\big\rangle_{\mathcal{F}} = \int_G \mathcal{D}(U,f)\,dU,$$

where G is a compact Lie group indicating the symmetry type of the family and dU is the Haar measure on G. Recall that the one-level densities of the three orthogonal symmetry types O, SO(*even*) and SO(*odd*) agree for test functions whose Fourier transforms are supported in $(-1,1)$. Therefore, for the sake of tidiness, we have chosen to state all results in terms of the symmetry type O.

Remark 1.2. In (1.4) and (1.5) the implied constants depend on E. All implied constants in the rest of this paper are similarly allowed to depend on the base elliptic curve. Moreover, throughout this paper we implicitly restrict our attention to non-empty families $\mathcal{H}_N^{\pm}(\Delta_E)$. Note that a family of this type is empty only if $M_E = 1$ so that the root number is constant (see Lemma 3.4).

In this paper, we are interested in determining lower order terms in the estimate (1.4). Specifically, to deduce the exact form of the error term $O(\frac{n^2}{q^{n/4}})$.

Theorem 1.3. *Let E be an elliptic curve defined over $\mathbb{F}_q(T)$ and given by the minimal Weierstrass equation $y^2 = x^3 + Ax + B$, where $A, B \in \mathbb{F}_q[T]$. Let $n \in \mathbb{Z}_{\geq 1}$ and assume that M_E is not a prime of odd degree dividing n. Then, for any $\epsilon > 0$ and $N > 4\mathfrak{n}_E + 16$, we have*

$$\big\langle \operatorname{Tr}(\Theta_{E_D}^n)\big\rangle_{\mathcal{H}_N^{\pm}(\Delta_E)} = \eta_2(n)\left(1 + \frac{\operatorname{Tr}\left(\Theta_{sym^2 E}^{n/2}\right)}{q^{n/4}} + \frac{\mathcal{D}(n)}{q^{n/2}}\right) + O_\epsilon\left((n+N)N^{2\mathfrak{n}_E+11}\left(\frac{1}{q^{N/8}} + \frac{1}{q^{\epsilon N}} + \frac{q^{n/2}}{q^{(1-\epsilon)N}}\right)\right),$$

where $\Theta_{sym^2 E}$ is the Frobenius element attached to the symmetric square L-function $L(u, sym^2 E)$ and $\mathcal{D}(n)$ is given by (3.4); in particular, $\mathcal{D}(n) \ll \tau(n) + \deg(\Delta_E)$.

Remark 1.4. In the case where M_E is a prime of odd degree dividing n, then the result still holds with the only difference that there is an additional contribution to $\mathcal{D}(n)$. See (3.6) and the brief discussion thereafter for further details.

While we are able to improve the error term slightly by finding some secondary terms, we retain the error term containing the expression $\frac{q^{n/2}}{q^{(1-\epsilon)N}}$ and so we are not able to extend the range of $\operatorname{supp}(\widehat{f})$ in (1.5). However, we are able to write down a term in the one-level density that is reminiscent of the deviation term that Rudnick found for the hyperelliptic ensemble (cf. [31, Corollary 3]).

Corollary 1.5. *Let E be an elliptic curve defined over $\mathbb{F}_q(T)$ as in Theorem 1.3 and let f be an even Schwartz test function. If $supp(\widehat{f}) \subset (-1,1)$, then*

$$\left\langle \mathcal{D}(E_D, f) \right\rangle_{\mathcal{H}_N^{\pm}(\Delta_E)} = \int\limits_{\mathrm{O}(\mathfrak{n}_E+2N)} \mathcal{D}(U,f)\, dU + \frac{dev_E(f)}{N} + O_\epsilon\left(\frac{1}{N^{2-\epsilon}}\right),$$

where

$$dev_E(f) = \widehat{f}(0)\Bigg(-\frac{1}{q}\frac{L'(q^{-1}, sym^2 E)}{L(q^{-1}, sym^2 E)} + \sum_{P \nmid \Delta_E} \frac{\deg(P)}{|P|+1} \sum_{d=1}^{\infty} \frac{a^*_{1,P^{2d}}}{|P|^d} - \sum_{P \mid \Delta_E} \deg(P) \sum_{d=1}^{\infty} \frac{a^*_{1,P^{2d}} - a^*_{2,P^d} + 1}{|P|^d} \Bigg),$$

a^*_{1,P^d} is the P^d-th coefficient of $\frac{L'(u,E)}{L(u,E)}$, a^*_{2,P^d} is the P^d-th coefficient of $\frac{L'(u,sym^2 E)}{L(u,sym^2 E)}$ and $|P| = q^{\deg(P)}$.

In the family of L-functions $L(u, \chi_D)$ attached to quadratic characters, Rudnick [31, Corollary 3] showed that the one-level density is asymptotically the same as for the unitary symplectic matrices with a deviation term of the form

$$dev(f) = \widehat{f}(0) \sum_P \frac{\deg(P)}{|P|^2 - 1} - \widehat{f}(1)\frac{1}{q-1}.$$

For f of small support, the main terms in the one-level density come from the prime squares. We note that $\chi_D(P^2) = \chi_D^2(P)$ and thus the contribution of the prime squares to the explicit formula is determined by the logarithmic derivative of

$$L(u, \chi_D^2) = R_D(u)\zeta_q(u),$$

where R_D is a finite Euler product. Taking logarithmic derivatives, there is a simple pole at $u = q^{-1}$. The residue of ζ_q'/ζ_q corresponds to the matrix integral whereas one can show that

$$\left\langle \frac{R_D'(q^{-1})}{R_D(q^{-1})} \right\rangle_{\mathcal{H}_{2g+1}(1)} = \sum_P \frac{\deg(P)}{|P|^2 - 1} + O(q^{-g}).$$

To see the term containing $\widehat{f}(1)$ in $dev(f)$, one needs to analyze also the contribution from the primes to the explicit formula. As we need to restrict to functions that have $\widehat{f}(1) = 0$, we do not see such a term in Corollary 1.5.

Now, for the quadratic twists of an elliptic curve, we again need to look at the contribution of the prime squares to the explicit formula. Here we obtain terms that contribute to the main term matrix integral, whereas the logarithmic derivative of

$$L(u, sym^2 E_D) = S_D(u) L(u, sym^2 E),$$

where S_D is a finite product of Euler factors, contributes the deviation terms in $dev_E(f)$ (see Section 3.6). Note in particular that, similar to the quadratic character case, $L(u, sym^2 E_D)$ is essentially constant as we vary D, changing only by a finite Euler product.

Finally, we note the close connection between the formulas in the quadratic character and quadratic twist cases. Indeed, by substituting 1 for all the $a^*_{1,P^{2d}}$ in the sum over primes of good reduction in $dev_E(f)$, we get exactly the part of $dev(f)$ corresponding to the same set of primes.[6]

1.3. Cubic twists

Performing a quadratic twist of an elliptic curve has the nice property that if $L(u, E) = \sum_F a_F u^{\deg(F)}$, then $L(u, E_D) = \sum_F a_F \chi_D(F) u^{\deg(F)}$. Therefore, one natural extension is to consider twists of the L-function $L(u, E)$ by other characters, that is, to consider L-functions of the form

$$L(u, E, \chi) := \sum_F a_F \chi(F) u^{\deg(F)}.$$

Comeau-Lapointe [9, Theorem 12.1] considered the families where χ runs over characters of fixed order $\ell \neq 2$, and proved that these families have unitary symmetry type. This change of symmetry type is to be expected as when you twist by non-quadratic characters the L-functions $L(u, E, \chi)$ fail to be L-functions of elliptic curves and therefore loses the orthogonal symmetry inherent in families of elliptic curve L-functions.

However, in this paper we choose to twist at the level of elliptic curves instead of at the level of L-functions. That is, if the elliptic curve has the special form

$$\widetilde{E} : y^2 = x^3 + B,$$

with $B \in \mathbb{F}_q[T]$, then, for any polynomial $D \in \mathbb{F}_q[T]$ coprime to B, we define the cubic twist of $\widetilde{E}$ as the curve with affine model

$$\widetilde{E}_D : y^2 = x^3 + BD^2.$$

Similar to the case of quadratic twists, as long as D is chosen to be cube-free and coprime to B, these will be distinct elliptic curves and all the primes that divide D will have additive reduction. Furthermore, if we consider only the case $3 | \deg(D)$, then the prime

[6] Note that R_D and $\zeta_q(u)$ are related to the constant coefficients 1 in exactly the same way as S_D and $L(u, sym^2 E)$ are related to the coefficients $a^*_{1,P^{2d}}$.

at infinity will have the same reduction type on $\widetilde{E}_D$ as it did on $\widetilde{E}$ (see Appendix A) and hence the degree of $L(u, \widetilde{E}_D)$ will be[7]

$$\mathfrak{n}_{\widetilde{E}_D} = \mathfrak{n}_{\widetilde{E}} + 2\deg(\mathrm{rad}(D)).$$

Therefore, if we define the set

$$\mathcal{F}_N(B) := \big\{D \in \mathbb{F}_q[T] : D \text{ monic, cube-free, } (D, B) = 1, \\ \deg(\mathrm{rad}(D)) = N, \deg(D) \equiv 0 \bmod 3\big\},$$

then the cubic twists by this family will form a family of distinct elliptic curves all of whose Frobenius elements have the same size.

Theorem 1.6. *Let $\widetilde{E}$ be an elliptic curve defined over $\mathbb{F}_q(T)$ and given by the minimal Weierstrass equation $y^2 = x^3 + B$, where $B \in \mathbb{F}_q[T]$. Then, for any $\epsilon > 0$ and $n \in \mathbb{Z}_{\geq 1}$, we have*

$$\big\langle \mathrm{Tr}(\Theta^n_{\widetilde{E}_D})\big\rangle_{\mathcal{F}_N(B)} = \eta_2(n) + O_\epsilon\left(\frac{q^{n/2}e^{2n}}{Nq^{(\frac{1}{2}-\epsilon)N}} + \frac{\eta_2(n)n}{q^{n/4}} + \frac{1}{q^{n/3}} + \frac{n(\deg(\Delta_{\widetilde{E}}) + \tau(n))}{q^{n/2}}\right),$$

where τ is the number of divisors function. Moreover, for any Schwartz test function satisfying $\mathrm{supp}(\widehat{f}) \subset (-\alpha, \alpha)$ for some $\alpha < \frac{1}{2} - \frac{2}{4+\log q}$, we get

$$\big\langle \mathcal{D}(\widetilde{E}_D, f)\big\rangle_{\mathcal{F}_N(B)} = \int\limits_{\mathrm{O}(\mathfrak{n}_{\widetilde{E}}+2N)} \mathcal{D}(U, f)\, dU + O\left(\frac{1}{N}\right). \tag{1.6}$$

Similar to Corollary 1.5, the main term in (1.6) comes from considering the prime squares whose contribution is the sum of the matrix integral and a term determined by the logarithmic derivative of $L(u, sym^2\widetilde{E}_D)$. However, unlike the quadratic twist family, $L(u, sym^2\widetilde{E}_D)$ is not essentially constant as D varies (see Section 4) and thus we get some cancellation that prevents us from obtaining a deviation term.

The next obvious thing to consider is the contribution from the prime cubes. Using Lemma 2.3, we find that the contribution from the prime cubes is determined by the logarithmic derivative of $L(u, sym^3\widetilde{E}_D)L(u, \widetilde{E}_D)^{-1}$. However, since the coefficients of $L(u, \widetilde{E}_D)$ are not obtained by a simple twist of a character (as in the quadratic twist case), we get that $L(u, sym^3\widetilde{E}_D)$ is still not essentially constant as D varies. Although, $L(u, sym^2\widetilde{E}_D)$ and $L(u, sym^3\widetilde{E}_D)$ will have parts that are essentially constant.

In order to describe these essentially constant parts, we need to introduce some notation. For any prime P and any $\widetilde{E}$, define

[7] Note that here we have to use the radical of D. This was not necessary for the quadratic twists since we were assuming D to be square-free in that case and hence equal to its radical.

$$\lambda_P = \lambda_P(\widetilde{E}) := \frac{1}{q^{\deg(P)/2}} \sum_{F \bmod P} \left(\frac{F^2 - B}{P}\right)_3,$$

where $\left(\frac{\cdot}{P}\right)_3$ is the cubic residue symbol modulo P.[8] The quantity λ_P behaves nicely with respect to cubic twists. Namely,

$$\lambda_P(\widetilde{E}_D) = \left(\frac{D}{P}\right)_3^2 \lambda_P(\widetilde{E}) \tag{1.7}$$

(cf. Lemma 4.1). Moreover, we get that $\lambda_P + \overline{\lambda}_P = -a_P$, where as usual a_P denotes the P-th coefficient of $L(u, \widetilde{E})$. Therefore, it is possible to write a^*_{1,P^d} in terms of the λ_P and then determine how these vary with D. However, we can show that approximately half of the time $|\lambda_P| \neq 1$ (see Corollary 1.9), and hence λ_P can typically not be a root of $1 - a_P u + u^2$. Therefore, while possible, writing a^*_{1,P^d} in terms of λ_P is in general not so nice. Using Lemma 4.2 and (1.7) to identify parts of $a^*_{1,P^2}(\widetilde{E}_D)$ and $a^*_{1,P^3}(\widetilde{E}_D)$ that are essentially constant as we vary D, we get the following theorem.

Theorem 1.7. *Let $\widetilde{E}$ be an elliptic curve defined over $\mathbb{F}_q(T)$ and given by the minimal Weierstrass equation $y^2 = x^3 + B$, where $B \in \mathbb{F}_q[T]$. Then, for any $\epsilon > 0$ and $n \in \mathbb{Z}_{\geq 1}$, we have*

$$\begin{aligned}\left\langle \operatorname{Tr}(\Theta^n_{\widetilde{E}_D}) \right\rangle_{\mathcal{F}_N(B)} &= -\frac{n/2}{q^{n/2}} \sum_{\deg(P)=\frac{n}{2}} 2(|\lambda_P|^2 - 1) + \frac{n/3}{q^{n/2}} \sum_{\deg(P)=\frac{n}{3}} (\lambda_P^3 + \overline{\lambda}_P^3) \\ &+ \frac{\widetilde{\mathcal{D}}_1(n) + \widetilde{\mathcal{D}}_2(n)}{q^{n/2}} + O_\epsilon\left(\frac{q^{n/2} e^{2n}}{N q^{(\frac{1}{2}-\epsilon)N}} + \frac{1}{q^{3n/8}} + \frac{n(\deg(\Delta_{\widetilde{E}}) + \tau(n))}{q^{n/2}} + \frac{1}{N q^{n/2}}\right),\end{aligned}$$

where τ is the number of divisors function and $\widetilde{\mathcal{D}}_1(n)$ and $\widetilde{\mathcal{D}}_2(n)$ are defined in (4.10) and (4.11); in particular, $\widetilde{\mathcal{D}}_1(n), \widetilde{\mathcal{D}}_2(n) \ll 1$.

Remark 1.8. Note that the presence of the terms $q^{-3n/8}$ and $n\tau(n)q^{-n/2}$ in the error term means that we could absorb the tertiary main term $(\widetilde{\mathcal{D}}_1(n) + \widetilde{\mathcal{D}}_2(n))q^{-n/2}$ into the error term. However, these error terms come from trivially bounding primes of degree at most $\frac{n}{4}$ and the primes of bad reduction, respectively, while $\widetilde{\mathcal{D}}_1(n)$ is written as a sum over primes of degree $\frac{n}{2}$ and $\widetilde{\mathcal{D}}_2(n)$ is written as a sum over primes of degree $\frac{n}{3}$. Therefore, if one is careful, one would (at least for small n) be able to remove these error terms and make the tertiary main term a sum over all primes of degree dividing n and a real main term. This process would involve extending Lemma 4.2. While not difficult, it would result in a less clean statement of Theorem 1.7. Note also that this new tertiary main term may no longer be bounded by $q^{-n/2}$.

[8] We assume $q \equiv 1 \bmod 6$ so that the cubic residue symbol is well defined.

It is not clear that Theorem 1.7 gives us what we were hoping for. That is, a term of size $q^{-n/3}$ that is related to the Frobenius of $L(u, sym^3 \widetilde{E})$ in some way which would lead to a deviation term for the one-level density that involves the logarithmic derivative of $L(u, sym^3 \widetilde{E})$. However, using some heuristic arguments, we can see a way that this appears.

1.4. Heuristics and conjectures

Using the Weil bound and comparing Theorems 1.6 and 1.7, we get the following immediate corollary:

Corollary 1.9. *For any $m \in \mathbb{Z}_{\geq 1}$, we have*

$$\frac{m}{q^m} \sum_{\deg(P)=m} |\lambda_P|^2 = \frac{1}{2} + O\left(\frac{1}{q^{m/3}}\right).$$

Heuristically, replacing $|\lambda_P|^2$ with its average of $\frac{1}{2}$, we can show that

$$\frac{n/3}{q^{n/2}} \sum_{\deg(P)=\frac{n}{3}} \left(\lambda_P^3 + \overline{\lambda}_P^3\right) \approx \frac{\eta_3(n)}{q^{n/3}} \left(\mathrm{Tr}\big(\Theta^{n/3}_{sym^3 \widetilde{E}}\big) + \frac{1}{2}\mathrm{Tr}\big(\Theta^{n/3}_{\widetilde{E}}\big)\right)$$

(see Section 5), where

$$\eta_3(n) := \begin{cases} 1 & 3|n, \\ 0 & 3 \nmid n. \end{cases}$$

This naturally leads to the following conjecture:

Conjecture 1.10. *Let $\widetilde{E}$ be an elliptic curve defined over $\mathbb{F}_q(T)$ and given by the minimal Weierstrass equation $y^2 = x^3 + B$, where $B \in \mathbb{F}_q[T]$. Then, for any $n \in \mathbb{Z}_{\geq 1}$, we have*

$$\left\langle \mathrm{Tr}(\Theta^n_{\widetilde{E}_D}) \right\rangle_{\mathcal{F}_N(B)} = \eta_2(n) + \frac{\eta_3(n)}{q^{n/3}} \left(\mathrm{Tr}\left(\Theta^{n/3}_{sym^3 \widetilde{E}}\right) + \frac{1}{2}\,\mathrm{Tr}\left(\Theta^{n/3}_{\widetilde{E}}\right)\right) + \frac{\widetilde{\mathcal{D}}(n)}{q^{n/2}}\big(1 + o(1)\big),$$

where $\widetilde{\mathcal{D}}(n)$ can be written as a sum over primes of degree dividing n and is bounded by (and might be considerably smaller than) $q^{n/8}$.

Therefore, passing to the one-level density, we get an idea of what kind of deviation term we could expect in cubic twist families. As this relies on the conjecture and the proof would be essentially the same as the one of Corollary 1.5, we state only that the deviation term should contain the two terms

$$-\widehat{f}(0)\frac{L'(q^{-3/2}, sym^3\widetilde{E})}{q^{3/2}L(q^{-3/2}, sym^3\widetilde{E})} \qquad \text{and} \qquad -\widehat{f}(0)\frac{L'(q^{-3/2}, \widetilde{E})}{2q^{3/2}L(q^{-3/2}, \widetilde{E})},$$

as well as a third term which can be expressed as a sum over primes and will depend on $\widetilde{\mathcal{D}}(n)$.

Outline of the paper

In Section 2, we define the symmetric power L-functions and prove several relations that will be needed throughout the later sections. In Section 3, we briefly discuss the quadratic twist family as the majority of the work in getting a reasonable error term is already done in [9]. In Section 4, we consider the cubic twist family and prove Theorems 1.6 and 1.7. In Section 5, we give a heuristic argument for Conjecture 1.10. Finally, in Appendix A we discuss the choices we made in choosing our families and indicate how one could extend our work to "fuller" families.

Acknowledgments

We thank the referees for reading our paper carefully and giving detailed comments and important suggestions. We thank Daniel Fiorilli and Zeév Rudnick for helpful comments on an early version of this paper. We also thank Lucile Devin for pointing our attention to Lumley's paper [26]. The first author was supported by the Verg foundation. The second author was supported by a grant from the Swedish Research Council (grant 2016-03759).

2. Symmetric power L-functions

Let E be any elliptic curve defined over $\mathbb{F}_q(T)$. Recall the definition of the L-function attached to E

$$L(u, E) := \prod_{P|\Delta_E}\left(1 - a_P(E)u^{\deg(P)}\right)^{-1}\prod_{P\nmid\Delta_E}\left(1 - a_P(E)u^{\deg(P)} + u^{2\deg(P)}\right)^{-1},$$

which converge for $|u| < q^{-1}$. If $P \nmid \Delta_E$, then we define α_P and β_P such that

$$1 - a_P u + u^2 = (1 - \alpha_P u)(1 - \beta_P u). \tag{2.1}$$

In addition, when $P|\Delta_E$, we set $\alpha_P = a_P$ and $\beta_P = 0$. In other words, we define α_P and β_P such that the inverse of the Euler factor at P equals

$$L_P(u, E) = \left(1 - \alpha_P u^{\deg(P)}\right)\left(1 - \beta_P u^{\deg(P)}\right),$$

where $\beta_P = 0$ if E has bad reduction at P.

For m a positive integer, we define

$$L(u, sym^m E) := \prod_{P \nmid \Delta_E} \prod_{i=0}^{m} \left(1 - \alpha_P^i \beta_P^{m-i} u^{\deg(P)}\right)^{-1} \prod_{P \mid \Delta_E} L_P\left(u^{\deg(P)}, sym^m E\right)^{-1} \quad (2.2)$$

where $L_P(u, sym^m E)$ is a polynomial of degree at most $m+1$ with bounded coefficients.[9] We refer the reader to [6, Section 1.2] for more information on symmetric power L-functions, and the references therein (specifically [16] and [33]) for more general statements and proofs. See also [27] for symmetric power L-functions of elliptic curves defined over $\mathbb{Q}$.

Proposition 2.1 *(Parts of Theorem 1.1 of [6]). For any elliptic curve E defined over $\mathbb{F}_q(T)$ and any positive integer m, $L(u, sym^m E)$ is a polynomial of degree $\mathfrak{n}_{sym^m E}$ all of whose roots have norm $q^{-1/2}$. Hence, we can find a matrix $\Theta_{sym^m E} \in \mathrm{U}(\mathfrak{n}_{sym^m E})$ such that*

$$L(u, sym^m E) = \det\left(1 - \sqrt{q} u \Theta_{sym^m E}\right).$$

Remark 2.2. It follows from [5, Lemma 2.1] that $\mathfrak{n}_{sym^m E} \ll m$ for all positive integers m, where the implied constant depends on E.

It will be useful to have notation for $L(u, sym^m E)$ also when $m = 0$ and -1. Therefore, we define

$$L(u, sym^0 E) := \zeta_q(u) \qquad \text{and} \qquad L(u, sym^{-1} E) := 1,$$

where $\zeta_q(u)$ is the usual zeta function of $\mathbb{F}_q[T]$ defined as

$$\zeta_q(u) := \sum_{F \text{ monic}} u^{\deg(F)} = \frac{1}{1 - qu}.$$

2.1. A symmetric power trace formula

We define $a^*_{m,P^k} = a^*_{m,P^k}(E)$ such that

$$\frac{L'(u, sym^m E)}{L(u, sym^m E)} = \frac{1}{u} \sum_P \deg(P) \sum_{k=1}^{\infty} a^*_{m,P^k} u^{k \deg(P)}. \quad (2.3)$$

If m is a positive integer, then we can use (2.3) together with Proposition 2.1 to get a formula for the trace of the Frobenius element:

[9] In fact, if P has multiplicative reduction, then $L_P(u, sym^m E) = (1 - \alpha_P^m u)$. However, if P has additive reduction, then the situation is more complicated.

$$-q^{n/2}\mathrm{Tr}(\Theta^n_{sym^m E}) = \sum_{d|n} \frac{n}{d} \sum_{\deg(P)=\frac{n}{d}} a^*_{m,P^d}. \tag{2.4}$$

If m is not a positive integer, then we see that

$$a^*_{0,P^k} = 1 \text{ and } a^*_{-1,P^k} = 0 \tag{2.5}$$

for all P and k. Thus, even though there is no Frobenius matrix associated with $m = 0, -1$, we can still determine their respective sums in the right-hand side of (2.4):

$$\sum_{d|n} \frac{n}{d} \sum_{\deg(P)=\frac{n}{d}} a^*_{m,P^d} = \begin{cases} q^n & m = 0, \\ 0 & m = -1. \end{cases} \tag{2.6}$$

2.2. Useful lemmas

Combining equations (2.1), (2.2) and (2.3), we see that if m is a positive integer and P is a prime of good reduction, then

$$a^*_{m,P^k} = \eta_2(m) + \sum_{j=0}^{\lfloor \frac{m-1}{2} \rfloor} \left(\alpha_P^{k(m-2j)} + \beta_P^{k(m-2j)} \right). \tag{2.7}$$

Further, for any prime P, we have the bound

$$|a^*_{m,P^k}| \leq 2(m+1). \tag{2.8}$$

Note that by (2.5), we see that (2.7) and (2.8) also hold for $m = 0, -1$.

We can now use (2.7) to relate the coefficients of the logarithmic derivatives of different symmetric power L-functions.

Lemma 2.3. *If P is a prime of good reduction and m is a positive integer, then*

$$a^*_{1,P^{md}} = a^*_{m,P^d} - a^*_{m-2,P^d}.$$

Proof. Applying (2.7), we get

$$\begin{aligned} a^*_{m,P^d} - a^*_{m-2,P^d} &= \sum_{j=0}^{\lfloor \frac{m-1}{2} \rfloor} \left(\alpha_P^{d(m-2j)} + \beta_P^{d(m-2j)} \right) - \sum_{j=0}^{\lfloor \frac{m-3}{2} \rfloor} \left(\alpha_P^{d(m-2-2j)} + \beta_P^{d(m-2-2j)} \right) \\ &= \alpha_P^{dm} + \beta_P^{dm} \\ &= a^*_{1,P^{md}}, \end{aligned}$$

which is the desired result. □

Next, we are able to use Lemma 2.3 to obtain a nice formula that relates traces of different symmetric powers. But first, we need to introduce some notation that will be useful in order to optimize the contribution of the primes of bad reduction to our error terms. For any $D \in \mathbb{F}_q[T]$, and any $n > 0$, we denote

$$D_n = \prod_{\substack{P|D \\ \deg(P)=n}} P. \tag{2.9}$$

Lemma 2.4. *Let E be any elliptic curve defined over $\mathbb{F}_q(T)$.*

(1) Let $m|n$. Then, if $m \geq 3$, we have

$$\sum_{\substack{d|n \\ m|d}} \frac{n}{d} \sum_{\deg(P)=\frac{n}{d}} a^*_{1,P^d} = -q^{\frac{n}{2m}} \left(\mathrm{Tr}\left(\Theta^{n/m}_{sym^m E}\right) - \mathrm{Tr}\left(\Theta^{n/m}_{sym^{m-2} E}\right)\right) + O\left(m \sum_{d|\frac{n}{m}} \deg(\Delta_{E,n/dm})\right).$$

(2) If $2|n$, then

$$\sum_{\substack{d|n \\ 2|d}} \frac{n}{d} \sum_{\deg(P)=\frac{n}{d}} a^*_{1,P^d} = -q^{n/2} - q^{n/4}\,\mathrm{Tr}\left(\Theta^{n/2}_{sym^2 E}\right) + \sum_{\substack{d|n \\ 2|d}} \frac{n}{d} \sum_{\substack{\deg(P)=\frac{n}{d} \\ P|\Delta_E}} \left(a^*_{1,P^d} - a^*_{2,P^{d/2}} + 1\right).$$

Proof. To prove (1), we first observe that

$$\sum_{\substack{d|n \\ m|d}} \frac{n}{d} \sum_{\deg(P)=\frac{n}{d}} a^*_{1,P^d} = \sum_{d|\frac{n}{m}} \frac{n}{dm} \sum_{\deg(P)=\frac{n}{dm}} a^*_{1,P^{md}}.$$

Splitting the sum over primes into primes of good and bad reduction, we find that the primes of bad reduction contribute

$$\sum_{d|\frac{n}{m}} \frac{n}{dm} \sum_{\substack{\deg(P)=\frac{n}{dm} \\ P|\Delta_E}} a^*_{1,P^{md}} \ll \sum_{d|\frac{n}{m}} \deg(\Delta_{E,n/dm}).$$

Now, when $m \geq 3$, for the primes of good reduction, we use Lemma 2.3 as well as (2.4) to get

$$\sum_{d|\frac{n}{m}} \frac{n}{dm} \sum_{\substack{\deg(P)=\frac{n}{dm} \\ P\nmid\Delta_E}} a^*_{1,P^{md}} = \sum_{d|\frac{n}{m}} \frac{n}{dm} \sum_{\substack{\deg(P)=\frac{n}{dm} \\ P\nmid\Delta_E}} \left(a^*_{m,P^d} - a^*_{m-2,P^d}\right)$$
$$= -q^{\frac{n}{2m}} \left(\mathrm{Tr}\left(\Theta^{n/m}_{sym^m E}\right) - \mathrm{Tr}\left(\Theta^{n/m}_{sym^{m-2} E}\right)\right) + O\left(m \sum_{d|\frac{n}{m}} \deg(\Delta_{E,n/dm})\right),$$

where the error term again comes from the primes of bad reduction.

Finally, to prove (2) we can still use Lemma 2.3 on the primes of good reduction. However, we also have to use (2.5) and (2.6) in conjunction with (2.4) to get

$$\sum_{d|\frac{n}{2}} \frac{n}{2d} \sum_{\substack{\deg(P)=\frac{n}{2d} \\ P\nmid\Delta_E}} a^*_{1,P^{2d}} = \sum_{d|\frac{n}{2}} \frac{n}{2d} \sum_{\substack{\deg(P)=\frac{n}{2d} \\ P\nmid\Delta_E}} \left(a^*_{2,P^d} - 1\right)$$

$$= -q^{n/2} - q^{n/4}\mathrm{Tr}\left(\Theta^{n/2}_{sym^2 E}\right) - \sum_{\substack{d|n \\ 2|d}} \frac{n}{d} \sum_{\substack{\deg(P)=\frac{n}{d} \\ P|\Delta_E}} \left(a^*_{2,P^{d/2}} - 1\right),$$

and the result follows. □

We can now use these relations to bound sums of a^*_{m,P^k} over primes P of a fixed degree for various combinations of m and k.

Lemma 2.5. *Let E be any elliptic curve defined over $\mathbb{F}_q(T)$.*

(1) If m is any positive integer, then

$$\sum_{\deg(P)=n} a^*_{m,P} \ll \frac{m}{n} q^{n/2}.$$

(2) If $m \geq 3$, then

$$\sum_{\deg(P)=n} a^*_{1,P^m} \ll \frac{m}{n}\left(q^{n/2} + \deg(\Delta_{E,n})\right).$$

(3) For prime squares, we have

$$\sum_{\deg(P)=n} a^*_{1,P^2} = -\frac{q^n}{n} + O\left(q^{n/2} + \frac{\deg(\Delta_{E,n})}{n}\right).$$

Proof. To prove (1), we see from (2.4) that

$$\sum_{\deg(P)=n} a^*_{m,P} = -\frac{q^{n/2}}{n}\mathrm{Tr}\left(\Theta^n_{sym^m E}\right) - \sum_{\substack{d|n \\ d>1}} \frac{1}{d} \sum_{\deg(P)=\frac{n}{d}} a^*_{m,P^d}.$$

Since $\Theta_{sym^m E}$ is a unitary matrix of size $\mathfrak{n}_{sym^m E} \times \mathfrak{n}_{sym^m E}$, we get $|\mathrm{Tr}(\Theta^n_{sym^m E})| \leq \mathfrak{n}_{sym^m E} \ll m$ by Remark 2.2. Moreover, for the prime sum, we use the bound in (2.8) and bound the number of primes of degree $\frac{n}{d}$ by $\frac{q^{n/d}}{n/d}$ to obtain the result.

Now, for (2), we apply Lemma 2.3 and (1) to get

$$\sum_{\deg(P)=n} a^*_{1,P^m} = \sum_{\deg(P)=n} \left(a^*_{m,P} - a^*_{m-2,P}\right) + O\Big(\frac{m}{n}\deg(\Delta_{E,n})\Big)$$
$$\ll \frac{m}{n}\big(q^{n/2} + \deg(\Delta_{E,n})\big),$$

where the error term $O\left(\frac{m}{n}\deg(\Delta_{E,n})\right)$ comes from using (2.8) for the primes of degree n that divide Δ_E.

Finally, for (3), we still apply Lemma 2.3 but now we can only apply (1) on the sum of $a^*_{2,P}$ and need to use (2.6) on the sum of $a^*_{0,P} = 1$. That is, we get

$$\sum_{\deg(P)=n} a^*_{1,P^2} = \sum_{\deg(P)=n} \left(a^*_{2,P} - a^*_{0,P}\right) + O\left(\frac{\deg(\Delta_{E,n})}{n}\right)$$
$$= -\frac{q^n}{n} + O\left(q^{n/2} + \frac{\deg(\Delta_{E,n})}{n}\right),$$

which completes the proof. □

These first few lemmas are crucial in picking out the lower order terms in the family of quadratic twists. However, they are a little less useful for the family of cubic twists. In that case, we will need the following two lemmas.

Lemma 2.6. *Let E be any elliptic curve defined over $\mathbb{F}_q(T)$. For any $m \geq 2$, we have*

$$-q^{n/2}\operatorname{Tr}(\Theta_E^n) = \sum_{\substack{d|n\\ d\leq m}} \frac{n}{d} \sum_{\deg(P)=\frac{n}{d}} a^*_{1,P^d} + O\left(mq^{\frac{n}{2(m+1)}} + n\sum_{\substack{d|n\\ d>m}} \deg(\Delta_{E,n/d})\right).$$

Proof. We see from (2.4) that it suffices to bound

$$\sum_{\substack{d|n\\ d>m}} \frac{n}{d} \sum_{\deg(P)=\frac{n}{d}} a^*_{1,P^d}.$$

Applying Lemma 2.5, we bound this sum by

$$\sum_{\substack{d|n\\ d>m}} \left(dq^{\frac{n}{2d}} + d\deg(\Delta_{E,n/d})\right) \ll mq^{\frac{n}{2(m+1)}} + n\sum_{\substack{d|n\\ d>m}} \deg(\Delta_{E,n/d}),$$

and the claimed estimate follows. □

Finally, we note that if we fix an elliptic curve $\widetilde{E} : y^2 = x^3 + B$ and perform a cubic twist by D for some $D \in \mathcal{F}_N(B)$, then we get that

$$\deg\left(\Delta_{\widetilde{E}_D,n/d}\right) \ll \deg\left(\Delta_{\widetilde{E},n/d}\right) + \deg(D_{n/d}).$$

Thus, in Section 4, we will need a bound of a modified expected value of $\deg(D_{n/d})$ as D ranges over $\mathcal{F}_N(B)$.

Lemma 2.7. *We have*

$$\frac{1}{|\mathcal{F}_N(B)|}\sum_{D\in\mathcal{F}_N(B)} n\sum_{d|n}\deg(D_{n/d}) \ll n\tau(n),$$

where τ is the number of divisors function.

Proof. We have that

$$\begin{aligned}\frac{1}{|\mathcal{F}_N(B)|}\sum_{D\in\mathcal{F}_N(B)} n\sum_{d|n}\deg(D_{n/d}) &= \frac{1}{|\mathcal{F}_N(B)|}\sum_{D\in\mathcal{F}_N(B)} n\sum_{d|n}\sum_{\substack{P|D\\ \deg(P)=\frac{n}{d}}}\deg(P)\\ &= n\sum_{d|n}\sum_{\deg(P)=\frac{n}{d}}\deg(P)\left(\frac{\left|\{D\in\mathcal{F}_N(B): P|D\}\right|}{|\mathcal{F}_N(B)|}\right)\\ &\ll n\sum_{d|n}\sum_{\deg(P)=\frac{n}{d}}\frac{\deg(P)}{q^{\deg(P)}} \ll n\sum_{\substack{d|n\\ d\geq\frac{n}{N}}} 1 \ll n\tau(n),\end{aligned}$$

where we have used Remark 4.8 to bound $\frac{|\{D\in\mathcal{F}_N(B):P|D\}|}{|\mathcal{F}_N(B)|}$. □

3. Quadratic twists

In this section, we prove Theorem 1.3 and Corollary 1.5.

3.1. A formula for $a^*_{1,P^k}(E_D)$

Recall that we are considering an elliptic curve given by the equation

$$E: y^2 = x^3 + Ax + B,$$

where $A, B \in \mathbb{F}_q[T]$, and that for every $D \in \mathcal{H}_N^{\pm}(\Delta_E)$, we have the quadratic twist

$$E_D: y^2 = x^3 + AD^2x + BD^3. \tag{3.1}$$

While it is well known how $a^*_{1,P^k}(E_D)$ behaves as we vary D, we will prove it here to illustrate the differences between the quadratic twists and the cubic twists (cf. Section 4.1).

Lemma 3.1. *For any elliptic curve E with discriminant Δ_E, prime P and $D \in \mathcal{H}_N^{\pm}(\Delta_E)$, we have*

$$a_P(E_D) = \left(\frac{D}{P}\right) a_P(E),$$

where for any $F, G \in \mathbb{F}_q[T]$, $\left(\frac{F}{G}\right)$ is the quadratic residue symbol.

Proof. Recall that $a_P(E_D)$ is defined such that the relation

$$\#E_D(P) = q^{\deg(P)} + 1 - a_P(E_D) q^{\deg(P)/2} \tag{3.2}$$

holds. Let us compute $\#E_D(P)$. Since $E_D(P)$ is a curve given by the cubic equation (3.1), reduced modulo P, we get that there is exactly one point lying above the point at infinity. For the finite points $F \in \mathbb{F}_q[T]/(P)$, the number of points lying above F on $E_D(P)$ is

$$\begin{cases} 2 & \text{if } F^3 + AD^2F + BD^3 \text{ is a non-zero square mod } P, \\ 1 & \text{if } F^3 + AD^2F + BD^3 \equiv 0 \text{ mod } P, \\ 0 & \text{if } F^3 + AD^2F + BD^3 \text{ is a non-square mod } P. \end{cases}$$

Therefore, we may capture the number of points on $E_D(P)$ as a character sum:

$$\#E_D(P) = 1 + \sum_{F \bmod P} \left(1 + \left(\frac{F^3 + AD^2F + BD^3}{P}\right)\right), \tag{3.3}$$

where the first term in the right-hand side is the contribution from the point lying over the point at infinity.

Now, if $P \nmid D$, then for every $F \bmod P$, we can find a unique $G \bmod P$ such that $F = GD$. Hence

$$\begin{aligned} \#E_D(P) &= 1 + \sum_{G \bmod P} \left(1 + \left(\frac{(GD)^3 + AD^2(GD) + BD^3}{P}\right)\right) \\ &= q^{\deg(P)} + 1 + \left(\frac{D}{P}\right) \sum_{G \bmod P} \left(\frac{G^3 + AG + B}{P}\right) \\ &= q^{\deg(P)} + 1 - \left(\frac{D}{P}\right) a_P(E) q^{\deg(P)/2}. \end{aligned}$$

Comparing this to (3.2) completes the proof for all primes $P \nmid D$.

On the other hand, if $P | D$, then we see that (3.3) becomes

$$\#E_D(P) = 1 + \sum_{F \bmod P} \left(1 + \left(\frac{F}{P}\right)\right) = q^{\deg(P)} + 1.$$

It follows that $a_P(E_D) = 0 = \left(\frac{D}{P}\right) a_P(E)$, which concludes the proof. □

Lemma 3.1 has the following immediate consequence.

Corollary 3.2. *With $\alpha_P(E_D)$ and $\beta_P(E_D)$ defined as in (2.1), we have*

$$\alpha_P(E_D) = \left(\frac{D}{P}\right)\alpha_P(E) \quad \text{and} \quad \beta_P(E_D) = \left(\frac{D}{P}\right)\beta_P(E).$$

Consequently,

$$a^*_{1,P^k}(E_D) = \left(\frac{D}{P}\right)^k a^*_{1,P^k}(E).$$

Proof. If $P \nmid D\Delta_E$, then we get by Lemma 3.1 that

$$1 - a_P(E_D)u + u^2 = \left(1 - \alpha_P(E)\left(\frac{D}{P}\right)u\right)\left(1 - \beta_P(E)\left(\frac{D}{P}\right)u\right),$$

so that

$$\alpha_P(E_D) = \left(\frac{D}{P}\right)\alpha_P(E) \quad \text{and} \quad \beta_P(E_D) = \left(\frac{D}{P}\right)\beta_P(E).$$

Hence, by (2.7) we obtain

$$a^*_{1,P^k}(E_D) = \alpha^k_P(E_D) + \beta^k_P(E_D) = \left(\frac{D}{P}\right)^k a^*_{1,P^k}(E).$$

Moreover, for $P|D\Delta_E$, we get by (2.3) and Lemma 3.1 that

$$a^*_{1,P^k}(E_D) = (a_P(E_D))^k = \left(\frac{D}{P}\right)^k (a_P(E))^k = \left(\frac{D}{P}\right)^k a^*_{1,P^k}(E),$$

which completes the proof. □

3.2. A trace formula

The starting point for our proof of Theorem 1.3 is the following trace formula. Combining Corollary 3.2 with (2.4), we get

$$\left\langle \mathrm{Tr}\left(\Theta^n_{E_D}\right)\right\rangle_{\mathcal{H}^{\pm}_N(\Delta_E)} = -\frac{q^{-n/2}}{|\mathcal{H}^{\pm}_N(\Delta_E)|}\sum_{d|n}\frac{n}{d}\sum_{\deg(P)=\frac{n}{d}} a^*_{1,P^d}\sum_{D\in\mathcal{H}^{\pm}_N(\Delta_E)}\left(\frac{D}{P}\right)^d.$$

For convenience, we define

$$MT^{\pm}(n,N) := -q^{-n/2}\sum_{\substack{d|n\\ 2|d}}\frac{n}{d}\sum_{\deg(P)=\frac{n}{d}}a^*_{1,P^d}\frac{|\mathcal{H}_N^{\pm}(P\Delta_E)|}{|\mathcal{H}_N^{\pm}(\Delta_E)|}$$

and

$$ET^{\pm}(n,N) := -\frac{q^{-n/2}}{|\mathcal{H}_N^{\pm}(\Delta_E)|}\sum_{\substack{d|n\\ 2\nmid d}}\frac{n}{d}\sum_{\deg(P)=\frac{n}{d}}a^*_{1,P^d}\sum_{D\in\mathcal{H}_N^{\pm}(\Delta_E)}\left(\frac{D}{P}\right).$$

3.3. Estimating $M^{\pm}(n,N)$

We see that in order to compute $MT^{\pm}(n,N)$ it is enough to prove the following proposition.

Proposition 3.3. *For any prime P, we have*

$$\frac{|\mathcal{H}_N^{\pm}(P\Delta_E)|}{|\mathcal{H}_N^{\pm}(\Delta_E)|} = \begin{cases} \frac{|P|}{|P|+1}+O(q^{-N/2}) & P\nmid\Delta_E,\\ 1 & P|\Delta_E. \end{cases}$$

We first note that the case where $P|\Delta_E$ is trivial as in this case $\mathcal{H}_N^{\pm}(P\Delta_E)=\mathcal{H}_N^{\pm}(\Delta_E)$. The proof of the remaining part of the proposition, i.e. the case where $P\nmid\Delta_E$, follows immediately from the following two lemmas.

Lemma 3.4. *Let E be an elliptic curve defined over $\mathbb{F}_q[T]$. If $M_E\neq 1$, then, for any $\Delta\in\mathbb{F}_q[T]$ (not necessarily the discriminant of E), we have*

$$|\mathcal{H}_N^{\pm}(\Delta)| = \frac{1}{2}|\mathcal{H}_N(\Delta)|+O_\Delta(q^{N/2}).$$

Moreover, if $M_E=1$, then either $\mathcal{H}_N^{+}(\Delta)=\mathcal{H}_N(\Delta)$ or $\mathcal{H}_N^{-}(\Delta)=\mathcal{H}_N(\Delta)$.

Proof. The second part of the lemma follows immediately from the formula for the root number $\epsilon(E_D)$. For the first part, we have

$$|\mathcal{H}_N^{\pm}(\Delta)| = \sum_{D\in\mathcal{H}_N(\Delta)}\frac{1}{2}\big(1\pm\epsilon_N\epsilon(E)\chi_D(M_E)\big) = \frac{1}{2}|\mathcal{H}_N(\Delta)|\pm\frac{\epsilon_N\epsilon(E)}{2}\sum_{D\in\mathcal{H}_N(\Delta)}\chi_D(M_E).$$

Now, by quadratic reciprocity, we have that

$$\chi_D(M_E) = (-1)^{\frac{q-1}{2}\deg(M_E)N}\chi_{M_E}(D).$$

Furthermore, we observe that

$$\mathcal{G}_\Delta(u,\chi_{M_E}) := \sum_{(D,\Delta)=1} \mu^2(D)\chi_{M_E}(D)u^{\deg(D)} = \prod_{P\nmid\Delta}\left(1+\chi_{M_E}(P)u^{\deg(P)}\right)$$
$$= \prod_{P|\Delta}\left(1+\chi_{M_E}(P)u^{\deg(P)}\right)^{-1}\prod_{P|M_E}\left(1-u^{2\deg(P)}\right)^{-1}\frac{L(u,\chi_{M_E})}{\zeta_q(u^2)}.$$

Hence, the above generating series can be analytically extended to the region $|u| \le q^{-1/2}$ and we conclude that

$$\sum_{D\in\mathcal{H}_N(\Delta)}\chi_D(M_E) = \frac{(-1)^{\frac{q-1}{2}\deg(M_E)N}}{2\pi i}\oint_\Gamma \frac{\mathcal{G}_\Delta(u,\chi_{M_E})}{u^{N+1}}\,du \ll q^{N/2}\max_{u\in\Gamma}|\mathcal{G}_\Delta(u,\chi_{M_E})|,$$

where $\Gamma = \{u : |u| = q^{-1/2}\}$. We also note that

$$\max_{u\in\Gamma}\left|\prod_{P|\Delta}\left(1+\chi_{M_E}(P)u^{\deg(P)}\right)^{-1}\prod_{P|M_E}\left(1-u^{2\deg(P)}\right)^{-1}\right| = O_\Delta(1).$$

Finally, we use the fact that the Riemann Hypothesis is known for the L-function $L(u,\chi_{M_E})$ to get that there exists a unitary matrix Θ_{M_E} of size $\mathcal{M}\times\mathcal{M}$, where $\mathcal{M} \le \deg(M_E)-1$, such that $L(u,\chi_{M_E}) = \det(1-\sqrt{q}u\Theta_{M_E})$. Thus

$$\max_{u\in\Gamma}|L(u,\chi_{M_E})| = \max_{|u|=1}\det(1-u\Theta_{M_E}) \ll 2^{\deg(M_E)} = O(1),$$

and the result follows. □

Next, we estimate the size of $\mathcal{H}_N(\Delta)$.

Lemma 3.5. *For any $\Delta\in\mathbb{F}_q[T]$, we have*

$$|\mathcal{H}_N(\Delta)| = q^{N-1}(q-1)\prod_{Q|\Delta}\frac{|Q|}{|Q|+1} + O_\Delta(1),$$

where the product is over all prime divisors of Δ.

Proof. For any $\Delta\in\mathbb{F}_q[T]$, let

$$\mathcal{G}_\Delta(u) := \sum_{(D,\Delta)=1}\mu^2(D)u^{\deg(D)} = \sum_{k=0}^{\infty}|\mathcal{H}_k(\Delta)|u^k.$$

We can then write $\mathcal{G}_\Delta(u)$ as an Euler product:

$$\mathcal{G}_\Delta(u) = \prod_{Q\nmid\Delta}\left(1+u^{\deg(Q)}\right) = \prod_{Q|\Delta}\left(1+u^{\deg(Q)}\right)^{-1}\frac{\zeta_q(u)}{\zeta_q(u^2)}.$$

Hence, we get that $\mathcal{G}_\Delta(u)$ can be meromorphically extended to the region $|u| < 1$ with a simple pole at $u = q^{-1}$. Therefore, if $\Gamma = \{u : |u| = \frac{1}{2}\}$, then

$$\begin{aligned}|\mathcal{H}_N(\Delta)| &= -\mathrm{Res}_{u=q^{-1}}\left(\frac{\mathcal{G}_\Delta(u)}{u^{N+1}}\right) + \frac{1}{2\pi i}\oint_\Gamma \frac{\mathcal{G}_\Delta(u)}{u^{N+1}}\,du \\ &= q^{N-1}(q-1)\prod_{Q|\Delta}\frac{|Q|}{|Q|+1} + O_\Delta(1),\end{aligned}$$

which is the desired result. □

Remark 3.6. Note that the error terms in Lemmas 3.4 and 3.5 only depend on the number of prime divisors of Δ. Thus, it follows that the error term in Proposition 3.3 can be made independent of the prime P.

Using Proposition 3.3, together with the fact that

$$\frac{|P|}{|P|+1} = 1 - \frac{1}{|P|+1},$$

we get that every prime in the inner sum of $MT^{\pm}(n,N)$ contributes a term of a^*_{1,P^d} while the primes such that $P \nmid \Delta_E$ also contribute a term of

$$-a^*_{1,P^d}\left(\frac{1}{|P|+1} + O\left(q^{-N/2}\right)\right).$$

Combining this with Lemma 2.4, we get

$$\begin{aligned}MT^{\pm}(n,N) &:= -q^{-n/2}\sum_{\substack{d|n\\ 2|d}}\frac{n}{d}\sum_{\deg(P)=\frac{n}{d}} a^*_{1,P^d}\frac{|\mathcal{H}^{\pm}_N(P\Delta_E)|}{|\mathcal{H}^{\pm}_N(\Delta_E)|} \\ &= -q^{-n/2}\sum_{\substack{d|n\\ 2|d}}\frac{n}{d}\sum_{\deg(P)=\frac{n}{d}} a^*_{1,P^d} + q^{-n/2}\sum_{\substack{d|n\\ 2|d}}\frac{n}{d}\sum_{\substack{\deg(P)=\frac{n}{d}\\ P\nmid\Delta_E}} a^*_{1,P^d}\left(\frac{1}{|P|+1} + O\left(\frac{1}{q^{N/2}}\right)\right) \\ &= \eta_2(n)\left(1 + \frac{\mathrm{Tr}\left(\Theta^{n/2}_{sym^2 E}\right)}{q^{n/4}} + \frac{\mathcal{D}(n)}{q^{n/2}}\right) + O\left(\frac{1}{q^{N/2}}\right),\end{aligned}$$

where

$$\mathcal{D}(n) := \sum_{\substack{d|n\\ 2|d}}\frac{n}{d}\sum_{\substack{\deg(P)=\frac{n}{d}\\ P\nmid\Delta_E}}\frac{a^*_{1,P^d}}{|P|+1}$$

$$-\sum_{\substack{d|n\\2|d}}\frac{n}{d}\sum_{\substack{\deg(P)=\frac{n}{d}\\P|\Delta_E}}\left(a^*_{1,P^d}-a^*_{2,P^{d/2}}+1\right)\ll\tau(n)+\deg(\Delta_E). \quad (3.4)$$

3.4. Bounding $ET^{\pm}(n,N)$

To bound $ET^{\pm}(n,N)$, we refer to the work of Comeau-Lapointe [9]. To align with the notation from [9], we define

$$\mathcal{H}_{N,C}=\{D\in\mathcal{H}_N(\Delta_E):D\equiv C \bmod N_E\},$$

where N_E is the conductor of the elliptic curve E as defined in, e.g., [34, Lecture 1] (see also [9, Section 2.1]). In particular, with our notation, we have $\mathfrak{n}_E=\deg(N_E)-4$.

Next, we define

$$S_C(n,N):=-\frac{n}{q^{n/2}|\mathcal{H}_{N,C}|}\sum_{\deg(P)=n}a^*_{1,P}\sum_{D\in\mathcal{H}_{N,C}}\left(\frac{D}{P}\right).$$

Then, [9, Proposition 7.2] shows that for any $\epsilon>0$, $N>4\mathfrak{n}_E+16$ and C coprime to N_E, we have

$$S_C(n,N)\ll_\epsilon(n+N)N^{2\mathfrak{n}_E+11}\left(\frac{1}{q^{N/8}}+\frac{1}{q^{\epsilon N}}+\frac{q^{n/2}}{q^{(1-\epsilon)N}}\right).$$

Moreover, as we saw in the proof of Lemma 3.4, as long as $P\neq M_E$,

$$\sum_{D\in\mathcal{H}_N^{\pm}(\Delta_E)}\left(\frac{D}{P}\right)=\frac{1}{2}\sum_{D\in\mathcal{H}_N(\Delta_E)}\left(1\pm\epsilon_N\epsilon(E)\left(\frac{D}{M_E}\right)\right)\left(\frac{D}{P}\right)\ll q^{N/2}, \quad (3.5)$$

and so as long as M_E is not a prime of degree dividing n,

$$\begin{aligned}
&ET^{\pm}(n,N)\\
&=-\frac{q^{-n/2}}{|\mathcal{H}_N^{\pm}(\Delta_E)|}\sum_{\substack{d|n\\2\nmid d}}\frac{n}{d}\sum_{\deg(P)=\frac{n}{d}}a^*_{1,P^d}\sum_{D\in\mathcal{H}_N^{\pm}(\Delta_E)}\left(\frac{D}{P}\right)\\
&=\sum_{\substack{C \bmod N_E\\(C,N_E)=1\\\chi_C(M_E)=\pm\epsilon_N\epsilon(E)}}\frac{|\mathcal{H}_{N,C}|}{|\mathcal{H}_N^{\pm}(\Delta_E)|}S_C(n,N)+O\left(\frac{1}{q^{(n+N)/2}}\sum_{\substack{d|n\\d\geq 3}}\frac{n}{d}\sum_{\deg(P)=\frac{n}{d}}|a^*_{1,P^d}|\right)\\
&=O_\epsilon\left((n+N)N^{2\mathfrak{n}_E+11}\left(\frac{1}{q^{N/8}}+\frac{1}{q^{\epsilon N}}+\frac{q^{n/2}}{q^{(1-\epsilon)N}}\right)+\frac{1}{q^{N/2+n/6}}\right).
\end{aligned}$$

Finally, in the case that $M_E = P$, then by using (3.5), we see that

$$\sum_{D \in \mathcal{H}_N^{\pm}(\Delta_E)} \left(\frac{D}{P}\right) = \pm \epsilon_N \epsilon(E) |\mathcal{H}_N^{\pm}(\Delta_E)| + O\big(q^{N/2}\big). \tag{3.6}$$

Therefore, if additionally $\deg(P) = \frac{n}{d}$ for some odd $d|n$, then this prime would contribute a term

$$\mp \epsilon_N \epsilon(E) \frac{n}{d} \frac{a^*_{1,P^d}}{q^{n/2}}$$

to $ET^{\pm}(n,N)$, which we could incorporate into the term $\mathcal{D}(n)q^{-n/2}$ from the previous subsection.

3.5. Proof of Theorem 1.3

We are now in position to complete the proof of Theorem 1.3.

Proof of Theorem 1.3. Combining the results from the previous subsections, for any $\epsilon > 0$ and $N > 4\mathfrak{n}_E + 16$, we have

$$\begin{aligned}\left\langle \mathrm{Tr}\left(\Theta_{E_D}^n\right)\right\rangle_{\mathcal{H}_N^{\pm}(\Delta_E)} &= MT^{\pm}(n,N) + ET^{\pm}(n,N) \\ &= \eta_2(n)\left(1 + \frac{\mathrm{Tr}\big(\Theta_{sym^2 E}^{n/2}\big)}{q^{n/4}} + \frac{\mathcal{D}(n)}{q^{n/2}}\right) \\ &\quad + O_\epsilon\left((n+N)N^{2\mathfrak{n}_E+11}\left(\frac{1}{q^{N/8}} + \frac{1}{q^{\epsilon N}} + \frac{q^{n/2}}{q^{(1-\epsilon)N}}\right) + \frac{1}{q^{N/2+n/6}}\right).\end{aligned}$$

We may then absorb the term $q^{-N/2-n/6}$ into the other error terms which gives the desired result. □

3.6. Proof of Corollary 1.5

Recall that we have, for any unitary $N \times N$ matrix U,

$$\mathcal{D}(U,f) := \sum_{j=1}^{N} \sum_{n \in \mathbb{Z}} f\left(N\left(\frac{\theta_j}{2\pi} - n\right)\right) = \frac{1}{N} \sum_{n \in \mathbb{Z}} \widehat{f}\left(\frac{n}{N}\right) \mathrm{Tr}(U^n),$$

where the θ_j run over the eigenangles of the matrix U. In particular, since we know that

$$\int_{\mathrm{O}(N)} \mathrm{Tr}(U^n)\, dU = \begin{cases} N & \text{if } n = 0, \\ \eta_2(n) & \text{if } n \neq 0, \end{cases}$$

we get that

$$\int_{\mathrm{O}(\mathfrak{n}_E+2N)} \mathcal{D}(U,f)\,dU = \frac{1}{\mathfrak{n}_E+2N}\sum_{n\in\mathbb{Z}} \widehat{f}\left(\frac{n}{\mathfrak{n}_E+2N}\right) \int_{\mathrm{O}(\mathfrak{n}_E+2N)} \mathrm{Tr}(U^n)\,dU$$
$$= \widehat{f}(0) + \frac{2}{\mathfrak{n}_E+2N}\sum_{n=1}^{\infty} \widehat{f}\left(\frac{2n}{\mathfrak{n}_E+2N}\right).$$

Now, we note that since $\mathrm{Tr}(U^{-n}) = \overline{\mathrm{Tr}(U^n)} = \mathrm{Tr}(U^n)$ for orthogonal matrices, we may trivially extend the results of Theorem 1.3 to negative integers n as well. Hence, using Theorem 1.3 to average over the quadratic twist family, we find that if $\mathrm{supp}(\widehat{f}) \subset (-1+\delta, 1-\delta)$ for some $\delta > 0$, then

$$\left\langle \mathcal{D}(\Theta_{E_D}, f)\right\rangle_{\mathcal{H}_N^{\pm}(\Delta_E)} = \frac{1}{\mathfrak{n}_{E_D}}\sum_{n\in\mathbb{Z}} \widehat{f}\left(\frac{n}{\mathfrak{n}_{E_D}}\right)\left\langle \mathrm{Tr}(\Theta_{E_D}^n)\right\rangle_{\mathcal{H}_N^{\pm}(\Delta_E)}$$
$$= \widehat{f}(0) + \frac{2}{\mathfrak{n}_E+2N}\sum_{n=1}^{(1-\delta)(\frac{\mathfrak{n}_E}{2}+N)} \widehat{f}\left(\frac{2n}{\mathfrak{n}_E+2N}\right)\left(1 + \frac{\mathrm{Tr}\left(\Theta_{sym^2 E}^n\right)}{q^{n/2}} + \frac{\mathcal{D}(2n)}{q^n}\right) \tag{3.7}$$
$$+ O_\epsilon\left(\sum_{n=1}^{(1-\delta)(\mathfrak{n}_E+2N)} (n+N)N^{2\mathfrak{n}_E+10}\left(\frac{1}{q^{N/8}} + \frac{1}{q^{\epsilon N}} + \frac{q^{n/2}}{q^{(1-\epsilon)N}}\right)\right).$$

We divide the right-hand side above into pieces that we analyze separately.

Firstly, we note that the error term in (3.7) is bounded by

$$O_\epsilon\left(N^{2\mathfrak{n}_E+12}\left(\frac{1}{q^{N/8}} + \frac{1}{q^{\epsilon N}} + q^{(\epsilon-\delta)N}\right)\right) = O_\epsilon\left(\frac{1}{q^{\epsilon' N}}\right)$$

for some $\epsilon' > 0$ as long as $\epsilon < \delta$. Next, we use the assumption that $\mathrm{supp}(\widehat{f}) \subset (-1+\delta, 1-\delta)$ to extend the sum to be over all positive n. Hence, we can write the main term in (3.7) as

$$\widehat{f}(0) + \frac{2}{\mathfrak{n}_E+2N}\sum_{n=1}^{(1-\delta)(\frac{\mathfrak{n}_E}{2}+N)} \widehat{f}\left(\frac{2n}{\mathfrak{n}_E+2N}\right)$$
$$= \widehat{f}(0) + \frac{2}{\mathfrak{n}_E+2N}\sum_{n=1}^{\infty} \widehat{f}\left(\frac{2n}{\mathfrak{n}_E+2N}\right) = \int_{\mathrm{O}(\mathfrak{n}_E+2N)} \mathcal{D}(U,f)\,dU. \tag{3.8}$$

For the secondary terms in (3.7), we split the sum over n into two parts. Let $\phi(N)$ be any function (to be determined later). Then, we use the fact that f is a Schwartz function to get that $\widehat{f}(x+y) = \widehat{f}(x) + O(y)$ and so

$$\sum_{n=1}^{\phi(N)} \widehat{f}\left(\frac{2n}{\mathfrak{n}_E+2N}\right)\frac{\mathrm{Tr}\left(\Theta^n_{sym^2E}\right)}{q^{n/2}} = \sum_{n=1}^{\phi(N)}\left(\widehat{f}(0)+O\left(\frac{n}{N}\right)\right)\frac{\mathrm{Tr}\left(\Theta^n_{sym^2E}\right)}{q^{n/2}}$$
$$= \widehat{f}(0)\sum_{n=1}^{\phi(N)}\frac{\mathrm{Tr}\left(\Theta^n_{sym^2E}\right)}{q^{n/2}} + O\left(\frac{\phi(N)}{N}\right). \quad (3.9)$$

Next, combining (2.3) and (2.4), we get that

$$\frac{L'(u,sym^2E)}{L(u,sym^2E)} = -\frac{1}{u}\sum_{n=1}^{\infty}\mathrm{Tr}\left(\Theta^n_{sym^2E}\right)(\sqrt{q}u)^n.$$

Therefore, extending the sum in (3.9) to be over all positive n, while gaining an additional error term of order $q^{-\phi(N)/2}$, we find that the main contribution from (3.9) equals

$$-\frac{\widehat{f}(0)}{q}\frac{L'(q^{-1},sym^2E)}{L(q^{-1},sym^2E)}.$$

For the remaining terms with $n>\phi(N)$, we use the fact that $\widehat{f}$ is bounded to get

$$\sum_{\phi(N)<n\le(1-\delta)(\frac{\mathfrak{n}_E}{2}+N)}\widehat{f}\left(\frac{2n}{\mathfrak{n}_E+2N}\right)\frac{\mathrm{Tr}\left(\Theta^n_{sym^2E}\right)}{q^{n/2}} \ll q^{-\phi(N)/2}.$$

Combining the above observations, we set $\phi(N)=N^\epsilon$ and conclude that

$$\frac{2}{\mathfrak{n}_E+2N}\sum_{n=1}^{(1-\delta)(\frac{\mathfrak{n}_E}{2}+N)}\widehat{f}\left(\frac{2n}{\mathfrak{n}_E+2N}\right)\frac{\mathrm{Tr}\left(\Theta^n_{sym^2E}\right)}{q^{n/2}} = -\frac{\widehat{f}(0)}{N}\frac{L'(q^{-1},sym^2E)}{qL(q^{-1},sym^2E)}$$
$$+O_\epsilon\left(\frac{1}{N^{2-\epsilon}}\right).$$

Finally, we consider also the remaining secondary term in (3.7). Similarly as in the treatment of the first secondary term above, we get that

$$\frac{2}{\mathfrak{n}_E+2N}\sum_{n=1}^{(1-\delta)(\frac{\mathfrak{n}_E}{2}+N)}\widehat{f}\left(\frac{2n}{\mathfrak{n}_E+2N}\right)\frac{\mathcal{D}(2n)}{q^n}$$
$$=\frac{\widehat{f}(0)}{N}\sum_{n=1}^{\infty}\sum_{\substack{d\mid 2n\\ 2\mid d}}\left(\sum_{\substack{\deg(P)=\frac{2n}{d}\\ P\nmid\Delta_E}}\frac{\deg(P)a^*_{1,P^d}}{q^n(|P|+1)}\right.$$
$$\left.-\sum_{\substack{\deg(P)=\frac{2n}{d}\\ P\mid\Delta_E}}\frac{\deg(P)\left(a^*_{1,P^d}-a^*_{2,P^{d/2}}+1\right)}{q^n}\right)+O_\epsilon\left(\frac{1}{N^{2-\epsilon}}\right)$$

$$= \frac{\widehat{f}(0)}{N}\left(\sum_{P\nmid\Delta_E}\frac{\deg(P)}{|P|+1}\sum_{d=1}^{\infty}\frac{a^*_{1,P^{2d}}}{|P|^d} - \sum_{P\mid\Delta_E}\deg(P)\sum_{d=1}^{\infty}\frac{a^*_{1,P^{2d}}-a^*_{2,P^d}+1}{|P|^d}\right) + O_\epsilon\left(\frac{1}{N^{2-\epsilon}}\right).$$

This concludes the proof of Corollary 1.5.

4. Cubic twists

In this section, we prove Theorems 1.6 and 1.7.

4.1. A formula for $a_P(\widetilde{E})$

Recall that we denote by $\widetilde{E}$ an elliptic curve given by the equation

$$\widetilde{E} : y^2 = x^3 + B, \tag{4.1}$$

where $B \in \mathbb{F}_q[T]$, and that for every $D \in \mathcal{F}_N(B)$, we consider the cubic twist

$$\widetilde{E}_D : y^2 = x^3 + BD^2.$$

For any elliptic curve $\widetilde{E}$ of the above form, and any prime P, we define

$$\lambda_P = \lambda_P(\widetilde{E}) := \frac{1}{q^{\deg(P)/2}}\sum_{F \bmod P}\left(\frac{F^2-B}{P}\right)_3,$$

where $\left(\frac{\cdot}{P}\right)_3$ is the cubic residue symbol on $\mathbb{F}_q[T]/(P) \cong \mathbb{F}_{q^{\deg(P)}}$. Note in particular that the Weil bound implies that $|\lambda_P| \leq 1$.

Similar to the case of quadratic twists, we will use the fact that $a_P(\widetilde{E}_D)$ can be expressed in terms of the number of points of $\widetilde{E}_D(P)$ (as a character sum) and then use this information to understand how these coefficients change as we vary D. See [24, Chapter 18] for related explicit formulas in the number field setting.

Lemma 4.1. *For any elliptic curve $\widetilde{E}$ given by an equation of the form (4.1), prime P and $D \in \mathcal{F}_N(B)$, we have*

$$a_P(\widetilde{E}) = -(\lambda_P + \overline{\lambda}_P) \tag{4.2}$$

and

$$\lambda_P(\widetilde{E}_D) = \left(\frac{D}{P}\right)_3^2 \lambda_P(\widetilde{E}). \tag{4.3}$$

Proof. Recall that

$$\#\widetilde{E}(P) = q^{\deg(P)} + 1 - a_P(\widetilde{E})q^{\deg(P)/2}.$$

We also know from our discussion in Section 3 that there will always be exactly one point lying above ∞ on $\widetilde{E}(P)$. Moreover, since our curves have the form (4.1), we observe that for a prime P and a finite point $F \in \mathbb{F}_q[T]/(P)$, the number of points lying over F on $\widetilde{E}(P)$ is

$$\begin{cases} 3 & \text{if } F^2 - B \text{ is a non-zero perfect cube mod } P, \\ 1 & \text{if } F^2 - B \equiv 0 \text{ mod } P, \\ 0 & \text{if } F^2 - B \text{ is not a perfect cube mod } P. \end{cases}$$

We capture this information in the character sum

$$\begin{aligned} \#\widetilde{E}(P) &= 1 + \sum_{F \text{ mod } P} \left(1 + \left(\frac{F^2 - B}{P}\right)_3 + \left(\frac{F^2 - B}{P}\right)_3^2\right) \\ &= q^{\deg(P)} + 1 + \sum_{F \text{ mod } P} \left(\left(\frac{F^2 - B}{P}\right)_3 + \left(\frac{F^2 - B}{P}\right)_3^2\right) \\ &= q^{\deg(P)} + 1 + (\lambda_P + \overline{\lambda}_P) q^{\deg(P)/2}, \end{aligned}$$

which proves (4.2).

To prove (4.3), we first consider the case when $P \nmid D$. Then D is invertible modulo P and so

$$\begin{aligned} \lambda_P(\widetilde{E}_D) &= \frac{1}{q^{\deg(P)/2}} \sum_{F \text{ mod } P} \left(\frac{F^2 - BD^2}{P}\right)_3 \\ &= \left(\frac{D^2}{P}\right)_3 \frac{1}{q^{\deg(P)/2}} \sum_{F \text{ mod } P} \left(\frac{(FD^{-1})^2 - B}{P}\right)_3 \\ &= \left(\frac{D}{P}\right)_3^2 \lambda_P(\widetilde{E}), \end{aligned}$$

where the last equality comes from the fact that as F runs over all the elements mod P so does FD^{-1}. Finally, if $P|D$, then we get

$$\lambda_P(\widetilde{E}_D) = \frac{1}{q^{\deg(P)/2}} \sum_{F \text{ mod } P} \left(\frac{F}{P}\right)_3^2 = 0,$$

which clearly equals $\left(\frac{D}{P}\right)_3^2 \lambda_P(\widetilde{E})$ in this case. □

It is tempting to try to conclude from (4.2) that $\lambda_P = -\alpha_P$. This is true if and only if $|\lambda_P| = 1$. However, we will see that the expected value of $|\lambda_P|^2$, for primes P of large degree, is $\frac{1}{2}$ (cf. Corollary 1.9) and so λ_P is in general not equal to $-\alpha_P$. Therefore, it is not necessarily true that $\alpha_P(\widetilde{E}_D) = \left(\frac{D}{P}\right)_3^2 \alpha_P(\widetilde{E})$. This causes some minor issues when

we calculate the expected values of traces of the Frobenius, as we need to first write everything in terms of λ_P instead of the more natural α_P. The following lemma presents the essential parts of this reformulation.

Lemma 4.2. *If P is a prime of good reduction for $\widetilde{E}$, then we have the following:*

(1) $a^*_{1,P} = -(\lambda_P + \overline{\lambda}_P)$,
(2) $a^*_{1,P^2} = \lambda_P^2 + \overline{\lambda}_P^2 + 2(|\lambda_P|^2 - 1)$,
(3) $a^*_{1,P^3} = -(\lambda_P^3 + \overline{\lambda}_P^3) - 3(|\lambda_P|^2 - 1)(\lambda_P + \overline{\lambda}_P)$.

Proof. For (1), we have that

$$a^*_{1,P} = a_P = -(\lambda_P + \overline{\lambda}_P).$$

To prove (2), we note that

$$a^*_{1,P^2} = \alpha_P^2 + \beta_P^2 = (\alpha_P + \beta_P)^2 - 2 = (\lambda_P + \overline{\lambda}_P)^2 - 2 = \lambda_P^2 + \overline{\lambda}_P^2 + 2(|\lambda_P|^2 - 1).$$

Finally, for (3), we have that

$$\begin{aligned} a^*_{1,P^3} &= \alpha_P^3 + \beta_P^3 = (\alpha_P + \beta_P)^3 - 3(\alpha_P + \beta_P) = -(\lambda_P + \overline{\lambda}_P)^3 + 3(\lambda_P + \overline{\lambda}_P) \\ &= -(\lambda_P^3 + \overline{\lambda}_P^3) - 3(|\lambda_P|^2 - 1)(\lambda_P + \overline{\lambda}_P), \end{aligned}$$

which concludes the proof. □

4.2. Trace formulas

Applying Lemma 2.6 with $m = 2$ and using Lemmas 2.5 and 4.2, we obtain

$$\begin{aligned} -q^{n/2}\mathrm{Tr}(\Theta^n_{\widetilde{E}}) &= n \sum_{\deg(P)=n} a^*_{1,P} + \frac{n}{2} \sum_{\deg(P)=\frac{n}{2}} a^*_{1,P^2} + O\left(q^{n/6} + n \sum_{\substack{d|n \\ d>2}} \deg(\Delta_{\widetilde{E},n/d})\right) \\ &= -\eta_2(n) q^{n/2} - n \sum_{\deg(P)=n} (\lambda_P + \overline{\lambda}_P) + O\left(\eta_2(n) n q^{n/4} + q^{n/6} + n \sum_{d|n} \deg(\Delta_{\widetilde{E},n/d})\right). \end{aligned}$$

Therefore, if for every prime P, we define

$$E_P = E_P(N) := \frac{1}{|\mathcal{F}_N(B)|} \sum_{D \in \mathcal{F}_N(B)} \left(\frac{D}{P}\right)_3, \tag{4.4}$$

then we get

$$\left\langle \mathrm{Tr}(\Theta^n_{\widetilde{E}_D})\right\rangle_{\mathcal{F}_N(B)} = \eta_2(n) + \frac{n}{q^{n/2}} \sum_{\deg(P)=n} \left(\lambda_P \overline{E}_P + \overline{\lambda}_P E_P\right) + O\left(\frac{\eta_2(n)n}{q^{n/4}} + \frac{1}{q^{n/3}} + \frac{n(\deg(\Delta_{\widetilde{E}}) + \tau(n))}{q^{n/2}}\right), \quad (4.5)$$

where we have used Lemma 2.7 to bound the contribution from the primes of bad reduction dividing elements in $\mathcal{F}_N(B)$.

On the other hand, if we apply Lemma 2.6 with $m = 3$ instead of $m = 2$, together with Lemma 4.2, then we get a different trace formula:

$$-q^{n/2}\mathrm{Tr}(\Theta^n_{\widetilde{E}}) = -n \sum_{\deg(P)=n} \left(\lambda_P + \overline{\lambda}_P\right) + \frac{n}{2} \sum_{\deg(P)=\frac{n}{2}} \left(\lambda_P^2 + \overline{\lambda}_P^2 + 2(|\lambda_P|^2 - 1)\right) - \frac{n}{3} \sum_{\deg(P)=\frac{n}{3}} \left(\lambda_P^3 + \overline{\lambda}_P^3 + 3(|\lambda_P|^2 - 1)(\lambda_P + \overline{\lambda}_P)\right) + O\left(q^{n/8} + n\sum_{d|n} \deg(\Delta_{\widetilde{E},n/d})\right).$$

Now, we note that as long as $P \nmid D$, we have $|\lambda_P(\widetilde{E}_D)|^2 = |\lambda_P(\widetilde{E})|^2$ and $\lambda_P^3(\widetilde{E}_D) = \lambda_P^3(\widetilde{E})$. Therefore, if we define

$$M(n,N) := -\frac{n/2}{q^{n/2}} \sum_{\deg(P)=\frac{n}{2}} 2(|\lambda_P|^2 - 1)\frac{|\mathcal{F}_N(PB)|}{|\mathcal{F}_N(B)|}, \quad (4.6)$$

$$S(n,N) := \frac{n/3}{q^{n/2}} \sum_{\deg(P)=\frac{n}{3}} \left(\lambda_P^3 + \overline{\lambda}_P^3\right)\frac{|\mathcal{F}_N(PB)|}{|\mathcal{F}_N(B)|}, \quad (4.7)$$

$$E(n,N) := \frac{n}{q^{n/2}} \sum_{\deg(P)=n} \left(\lambda_P \overline{E}_P + \overline{\lambda}_P E_P\right) - \frac{n/2}{q^{n/2}} \sum_{\deg(P)=\frac{n}{2}} \left(\lambda_P^2 E_P + \overline{\lambda}_P^2 \overline{E}_P\right) + \frac{n/3}{q^{n/2}} \sum_{\deg(P)=\frac{n}{3}} 3(|\lambda_P|^2 - 1)\left(\lambda_P \overline{E}_P + \overline{\lambda}_P E_P\right), \quad (4.8)$$

with each $\lambda_P = \lambda_P(\widetilde{E})$, then we have

$$\left\langle \mathrm{Tr}(\Theta^n_{\widetilde{E}_D})\right\rangle_{\mathcal{F}_N(B)} = M(n,N) + S(n,N) + E(n,N) + O\left(\frac{1}{q^{3n/8}} + \frac{n(\deg(\Delta_{\widetilde{E}}) + \tau(n))}{q^{n/2}}\right), \quad (4.9)$$

where we use the same bounds as in (4.5), together with Remark 4.8, to handle the primes of bad reduction.

Hence, in order to prove Theorems 1.6 and 1.7, we need to bound E_P and compute $\frac{|\mathcal{F}_N(PB)|}{|\mathcal{F}_N(B)|}$, which we can view as the probability that a random $D \in \mathcal{F}_N(B)$ is coprime to P.

4.3. Bounding $E_P(N)$

In this short subsection, we prove the following bound on $E_P(N)$.

Proposition 4.3. *For any $\epsilon > 0$ and any prime P, we have*

$$E_P(N) \ll_\epsilon \frac{e^{2\deg(P)}}{Nq^{(\frac{1}{2}-\epsilon)N}}.$$

Proof. We denote the cubic residue symbol modulo P by

$$\psi_P = \Big(\frac{\cdot}{P}\Big)_3$$

and consider the generating series

$$\mathcal{G}(u, \psi_P) := \sum_{N=0}^{\infty} \sum_{D \in \mathcal{F}_N(B)} \psi_P(D) u^N.$$

Every $D \in \mathcal{F}_N(B)$ can be written as $D = D_1 D_2^2$, where $\deg(D_1 D_2) = N$, $3 | \deg(D_1 D_2^2)$ and D_1, D_2 are monic, square-free, coprime to each other and coprime to B. Using this, we obtain that

$$\begin{aligned}\mathcal{G}(u, \psi_P) &= \frac{1}{3} \sum_{\substack{D_1, D_2 \\ (D_1 D_2, B)=1}} \mu^2(D_1 D_2) \psi_P(D_1 D_2^2) \left(1 + \xi_3^{\deg(D_1 D_2^2)} + \xi_3^{2\deg(D_1 D_2^2)}\right) u^{\deg(D_1 D_2)} \\ &= \frac{1}{3}\big(H_0(u, \psi_P) + H_1(u, \psi_P) + H_2(u, \psi_P)\big),\end{aligned}$$

where ξ_3 is a primitive cube root of unity and

$$H_j(u, \psi_P) := \sum_{\substack{D_1, D_2 \\ (D_1 D_2, B)=1}} \mu^2(D_1 D_2) \psi_P(D_1 D_2^2) \xi_3^{j\deg(D_1 D_2^2)} u^{\deg(D_1 D_2)}.$$

Writing $H_j(u, \psi_P)$ as a product over primes, we get

$$\begin{aligned}H_j(u, \psi_P) &= \prod_{Q \nmid B} \left(1 + \psi_P(Q)(\xi_3^j u)^{\deg(Q)} + \psi_P^2(Q)(\xi_3^{2j} u)^{\deg(Q)}\right) \\ &= L(\xi_3^j u, \psi_P) L(\xi_3^{2j} u, \psi_P^2) \widetilde{H}_j(u, \psi_P),\end{aligned}$$

where $L(u, \psi_P)$ is the L-function attached to the Dirichlet character ψ_P and $\widetilde{H}_j(u, \psi_P)$ is a function that has an Euler product with factors of the form $\big(1 + O(u^{2\deg(Q)})\big)$ for all $Q \nmid B$ (respectively, $\big(1 + O(u^{\deg(Q)})\big)$ for $Q \mid B$), and so is analytic in the region $|u| < q^{-1/2}$.

Now, since ψ_P and ψ_P^2 are both non-trivial Dirichlet characters modulo P, we get that $H_j(u,\psi_P)$ is analytic in the region $|u| < q^{-1/2}$ and hence so is $\mathcal{G}(u,\psi_P)$. Therefore, if $\Gamma := \{u : |u| = q^{-1/2-\epsilon}\}$, then we use [26, Proposition 1.2][10] to get

$$\sum_{D\in\mathcal{F}_N(B)} \left(\frac{D}{P}\right)_3 = \frac{1}{2\pi i}\oint_\Gamma \frac{\mathcal{G}(u,\psi_P)}{u^{N+1}}du \ll \max_{u\in\Gamma}\left(\frac{|\mathcal{G}(u,\psi_P)|}{|u|^N}\right) \ll_\epsilon e^{2\deg(P)}q^{(\frac{1}{2}+\epsilon)N}.$$

To conclude, we refer to Corollary 4.6 below which implies that $|\mathcal{F}_N(B)| \sim cNq^N$ for some non-zero constant c. □

4.4. Proof of Theorem 1.6

Using the results from the previous subsections, we are now ready to complete the proof of Theorem 1.6.

Proof of Theorem 1.6. Applying Proposition 4.3 to (4.5), we get

$$\begin{aligned}\left\langle \mathrm{Tr}(\Theta^n_{\widetilde{E}_D})\right\rangle_{\mathcal{F}_N(B)} &= \eta_2(n) + \frac{n}{q^{n/2}}\sum_{\deg(P)=n}\left(\lambda_P\overline{E}_P + \overline{\lambda}_P E_P\right)\\ &\qquad + O\left(\frac{\eta_2(n)n}{q^{n/4}} + \frac{1}{q^{n/3}} + \frac{n(\deg(\Delta_{\widetilde{E}})+\tau(n))}{q^{n/2}}\right)\\ &= \eta_2(n) + O_\epsilon\left(\frac{q^{n/2}e^{2n}}{Nq^{(\frac{1}{2}-\epsilon)N}} + \frac{\eta_2(n)n}{q^{n/4}} + \frac{1}{q^{n/3}} + \frac{n(\deg(\Delta_{\widetilde{E}})+\tau(n))}{q^{n/2}}\right).\end{aligned}$$

Hence, if $\mathrm{supp}(\widehat{f}) \subset (-\alpha,\alpha)$ for some $\alpha < \frac{1}{2} - \frac{2}{4+\log q}$, we use (1.3) to get

$$\begin{aligned}\left\langle \mathcal{D}(\Theta_{\widetilde{E}_D}, f)\right\rangle_{\mathcal{F}_N(B)} &= \frac{1}{\mathfrak{n}_{\widetilde{E}}+2N}\sum_{n\in\mathbb{Z}}\widehat{f}\left(\frac{n}{\mathfrak{n}_{\widetilde{E}}+2N}\right)\left\langle \mathrm{Tr}(\Theta^n_{\widetilde{E}_D})\right\rangle_{\mathcal{F}_N(B)}\\ &= \widehat{f}(0) + \frac{2}{\mathfrak{n}_{\widetilde{E}}+2N}\sum_{n=1}^{\alpha(\mathfrak{n}_{\widetilde{E}}+2N)}\widehat{f}\left(\frac{n}{\mathfrak{n}_{\widetilde{E}}+2N}\right)\left\langle \mathrm{Tr}(\Theta^n_{\widetilde{E}_D})\right\rangle_{\mathcal{F}_N(B)}\\ &= \widehat{f}(0) + \frac{2}{\mathfrak{n}_{\widetilde{E}}+2N}\sum_{n=1}^{\alpha(\frac{\mathfrak{n}_{\widetilde{E}}}{2}+N)}\widehat{f}\left(\frac{2n}{\mathfrak{n}_{\widetilde{E}}+2N}\right)\\ &\quad + O_\epsilon\left(\frac{1}{N}\sum_{n=1}^{\alpha(\mathfrak{n}_{\widetilde{E}}+2N)}\left(\frac{q^{n/2}e^{2n}}{Nq^{(\frac{1}{2}-\epsilon)N}} + \frac{\eta_2(n)n}{q^{n/4}} + \frac{1}{q^{n/3}} + \frac{n(\deg(\Delta_{\widetilde{E}})+\tau(n))}{q^{n/2}}\right)\right)\end{aligned}$$

[10] Note that Lumley [26] is assuming that $q \equiv 1 \bmod 4$. However, this assumption is not important for the proof of [26, Proposition 1.2] and the same result holds also in the case $q \equiv 3 \bmod 4$.

$$= \int\limits_{\mathrm{O}(\mathfrak{n}_{\widetilde{E}}+2N)} \mathcal{D}(U,f)\,dU + O\left(\frac{1}{N}\right),$$

where we fix a sufficiently small ϵ and use (3.8) in the last step. □

4.5. The probability of being coprime to P

Recall that for the quadratic twists, we proved in Proposition 3.3 that

$$\frac{|\mathcal{H}_N^{\pm}(P\Delta_E)|}{|\mathcal{H}_N^{\pm}(\Delta_E)|} = \frac{|P|}{|P|+1} + O\big(q^{-N/2}\big)$$

for all $P \nmid \Delta_E$. To pick out the lower order terms in Theorem 1.7, we need a similar result for $\mathcal{F}_N(B)$ with an error term that decays as N tends to infinity. Proving such a result is a little more delicate due to the fact that the generating series for $\mathcal{H}_N(\Delta_E)$ has a simple pole at q^{-1}, whereas the generating series for $\mathcal{F}_N(B)$ has a double pole at q^{-1}. That being said, the rest of this subsection will be devoted to proving the following proposition.

Proposition 4.4. *Let P be a prime of degree m. If $P \nmid B$, then*

$$\frac{|\mathcal{F}_N(PB)|}{|\mathcal{F}_N(B)|} = 1 + \sum_{a=1}^{\lfloor \frac{N}{m} \rfloor} \left(\frac{-2}{q^m}\right)^a \left(1 - \frac{am}{N}\right) + O\left(\frac{1}{Nq^m}\right),$$

whereas if $P|B$, then

$$\frac{|\mathcal{F}_N(PB)|}{|\mathcal{F}_N(B)|} = 1.$$

The case where $P|B$ is trivial since in this case $\mathcal{F}_N(B) = \mathcal{F}_N(PB)$. Thus, we will consider only the case $P \nmid B$. Towards this goal, we define the generating series

$$\mathcal{G}(u;B) := \sum_{N=0}^{\infty} |\mathcal{F}_N(B)| u^N.$$

For any analytic function $K(u)$ defined in an open neighborhood of the origin, we define $[u^d]K(u)$ as the dth coefficient in the Taylor expansion of $K(u)$ around 0. Therefore,

$$\frac{|\mathcal{F}_N(PB)|}{|\mathcal{F}_N(B)|} = \frac{[u^N]\mathcal{G}(u;PB)}{[u^N]\mathcal{G}(u;B)}.$$

Similar to when we bounded E_P (see Proposition 4.3), we note that every element in $\mathcal{F}_N(B)$ can be written as $D_1 D_2^2$ where $\deg(D_1 D_2) = N$, $3|\deg(D_1 D_2^2)$ and the D_i are monic, square-free, coprime to each other and coprime to B. Hence, we obtain that

$$\mathcal{G}(u;B) = \frac{1}{3} \sum_{\substack{D_1,D_2 \\ (D_1D_2,B)=1}} \mu^2(D_1D_2) \left(1 + \xi_3^{\deg(D_1D_2^2)} + \xi_3^{2\deg(D_1D_2^2)}\right) u^{\deg(D_1D_2)}$$
$$= \frac{1}{3}\big(H_0(u;B) + H_1(u;B) + H_2(u;B)\big),$$

where ξ_3 is a primitive cube root of unity and

$$H_j(u;B) := \sum_{\substack{D_1,D_2 \\ (D_1D_2,B)=1}} \mu^2(D_1D_2)\xi_3^{j\deg(D_1D_2^2)} u^{\deg(D_1D_2)}$$
$$= \prod_{Q \nmid B} \left(1 + (\xi_3^j u)^{\deg(Q)} + (\xi_3^{2j} u)^{\deg(Q)}\right).$$

It is clear that $H_1(u;B) = H_2(u;B)$ and so we can write

$$\mathcal{G}(u;B) = \frac{1}{3}\big(H_0(u;B) + 2H_1(u;B)\big).$$

Lemma 4.5. *Let $\epsilon > 0$ and $d \in \mathbb{Z}_{\geq 0}$. Then there exists a linear polynomial L such that*

$$[u^d]H_0(u;B) = L(d)q^d + O_\epsilon\big(q^{(\frac{1}{2}+\epsilon)d}\big).$$

Furthermore, there exists a constant C such that

$$[u^d]H_1(u;B) = Cq^d + O_\epsilon\big(q^{(\frac{1}{2}+\epsilon)d}\big).$$

Proof. We have

$$H_j(u;B) = \prod_{Q \nmid B} \left(1 + (\xi_3^j u)^{\deg(Q)} + (\xi_3^{2j} u)^{\deg(Q)}\right)$$
$$= \prod_{Q} \left(1 - (\xi_3^j u)^{\deg(Q)}\right)^{-1} \prod_{Q} \left(1 - (\xi_3^{2j} u)^{\deg(Q)}\right)^{-1} \widetilde{H}_j(u;B)$$
$$= \frac{1}{\big(1 - \xi_3^j qu\big)\big(1 - \xi_3^{2j} qu\big)} \widetilde{H}_j(u;B),$$

where

$$\widetilde{H}_j(u;B) = \prod_{Q \mid B} \left(1 + O\big(u^{\deg(Q)}\big)\right) \prod_{Q \nmid B} \left(1 + O\big(u^{2\deg(Q)}\big)\right)$$

is absolutely convergent in the region $|u| < q^{-1/2}$. Let $\epsilon > 0$ and $\Gamma = \{u : |u| = q^{-1/2-\epsilon}\}$. Then $\frac{H_j(u;B)}{u^{d+1}}$ is meromorphic in the region bounded by Γ with poles at $u = 0$ and $u = q^{-1}$ if $j = 0$, and with poles at $u = 0$, $u = \xi_3 q^{-1}$ and $u = \xi_3^2 q^{-1}$ if $j = 1, 2$. Hence,

$$\frac{1}{2\pi i}\oint_{\Gamma}\frac{H_j(u;B)}{u^{d+1}}\,du \ll \max_{u\in\Gamma}\left(\frac{|H_j(u;B)|}{|u|^d}\right) \ll_\epsilon q^{(\frac{1}{2}+\epsilon)d}.$$

On the other hand, if $j=0$, then

$$\frac{1}{2\pi i}\oint_{\Gamma}\frac{H_0(u;B)}{u^{d+1}}\,du = \mathrm{Res}_{u=0}\left(\frac{H_0(u;B)}{u^{d+1}}\right) + \mathrm{Res}_{u=q^{-1}}\left(\frac{H_0(u;B)}{u^{d+1}}\right).$$

Moreover, we note that

$$\mathrm{Res}_{u=0}\left(\frac{H_0(u;B)}{u^{d+1}}\right) = [u^d]H_0(u;B)$$

and

$$\begin{aligned}\mathrm{Res}_{u=q^{-1}}\left(\frac{H_0(u;B)}{u^{d+1}}\right) &= \lim_{u\to q^{-1}}\frac{d}{du}\left(\frac{(u-q^{-1})^2}{(1-qu)^2}\frac{\widetilde{H}_0(u;B)}{u^{d+1}}\right)\\ &= -\big((d+1)\widetilde{H}_0(q^{-1};B) - q^{-1}\widetilde{H}_0'(q^{-1};B)\big)q^d,\end{aligned}$$

which proves the result for $j=0$. Finally, if $j=1$, then we have

$$\begin{aligned}\frac{1}{2\pi i}\oint_{\Gamma}\frac{H_1(u;B)}{u^{d+1}}\,du &= \mathrm{Res}_{u=0}\left(\frac{H_1(u;B)}{u^{d+1}}\right)\\ &\quad + \mathrm{Res}_{u=\xi_3 q^{-1}}\left(\frac{H_1(u;B)}{u^{d+1}}\right) + \mathrm{Res}_{u=\xi_3^2 q^{-1}}\left(\frac{H_1(u;B)}{u^{d+1}}\right),\end{aligned}$$

where

$$\mathrm{Res}_{u=0}\left(\frac{H_1(u;B)}{u^{d+1}}\right) = [u^d]H_1(u;B)$$

and

$$\begin{aligned}\mathrm{Res}_{u=\xi_3 q^{-1}}\left(\frac{H_1(u;B)}{u^{d+1}}\right) &= \lim_{u\to\xi_3 q^{-1}}\frac{(u-\xi_3 q^{-1})\widetilde{H}_1(u;B)}{(1-\xi_3 qu)(1-\xi_3^2 qu)u^{d+1}}\\ &= -\left(\frac{\widetilde{H}_1(\xi_3 q^{-1};B)}{(1-\xi_3^2)\xi_3^d}\right)q^d = -C_1 q^d.\end{aligned}$$

By a similar calculation, we find that the residue at $\xi_3^2 q^{-1}$ equals $-C_2 q^d$ for a suitable constant C_2. Setting $C = C_1 + C_2$ completes the proof. □

Lemma 4.5 has the following immediate consequence.

Corollary 4.6. *Let L and C be as in Lemma 4.5. Then, we have*

$$|\mathcal{F}_N(B)| = \frac{1}{3}\big(L(N) + 2C\big)q^N + O_\epsilon\big(q^{(\frac{1}{2}+\epsilon)N}\big).$$

Proof. Using Lemma 4.5, we obtain

$$\begin{aligned}|\mathcal{F}_N(B)| = [u^N]\mathcal{G}(u;B) &= \frac{1}{3}[u^N]\big(H_0(u;B) + 2H_1(u;B)\big)\\ &= \frac{1}{3}\big(L(N) + 2C\big)q^N + O_\epsilon\big(q^{(\frac{1}{2}+\epsilon)N}\big),\end{aligned}$$

as desired. □

In order to prove Proposition 4.4, we need to know how to pass from $[u^d]\mathcal{G}(u;B)$ to $[u^d]\mathcal{G}(u;PB)$. Fortunately, using the fact that $H_j(u;PB)$ has an Euler product, it is straightforward to pass from $[u^d]H_j(u;B)$ to $[u^d]H_j(u;PB)$.

Lemma 4.7. *Let $d \in \mathbb{Z}_{\geq 0}$ and let P be a prime of degree m such that $P \nmid B$. Then*

$$[u^d]H_j(u;PB) = \sum_{a=0}^{\lfloor \frac{d}{m} \rfloor}(-1)^a \left(\xi_3^{jm} + \xi_3^{2jm}\right)^a [u^{d-am}]H_j(u;B).$$

Proof. From the definition of $H_j(u;B)$, we see that

$$H_j(u;B) = \left(1 + (\xi_3^j u)^m + (\xi_3^{2j}u)^m\right) H_j(u;PB)$$

and it follows that

$$[u^d]H_j(u;B) = [u^d]H_j(u;PB) + \left(\xi_3^{jm} + \xi_3^{2jm}\right)[u^{d-m}]H_j(u;PB).$$

Rearranging, we then get

$$\begin{aligned}[u^d]H_j(u;PB) &= [u^d]H_j(u;B) - \left(\xi_3^{jm} + \xi_3^{2jm}\right)[u^{d-m}]H_j(u;PB)\\ &= [u^d]H_j(u;B) - \left(\xi_3^{jm} + \xi_3^{2jm}\right)[u^{d-m}]H_j(u;B) + \left(\xi_3^{jm} + \xi_3^{2jm}\right)^2[u^{d-2m}]H_j(u;PB),\end{aligned}$$

and iterating this procedure, we obtain

$$[u^d]H_j(u;PB) = \sum_{a=0}^{\lfloor \frac{d}{m} \rfloor}(-1)^a \left(\xi_3^{jm} + \xi_3^{2jm}\right)^a [u^{d-am}]H_j(u;B).$$

This concludes the proof of the lemma. □

Using Lemmas 4.5 and 4.7, we now complete the proof of Proposition 4.4.

Proof of Proposition 4.4. It follows from Lemmas 4.5 and 4.7 that if $P \nmid B$, then

$$\begin{aligned}|\mathcal{F}_N(PB)| &= [u^N]\mathcal{G}(u;PB) = \frac{1}{3}[u^N]\big(H_0(u;PB) + 2H_1(u;PB)\big)\\ &= \frac{1}{3}\sum_{a=0}^{\lfloor \frac{N}{m}\rfloor}(-1)^a[u^{N-am}]\left(2^a H_0(u;B) + 2\left(\xi_3^m + \xi_3^{2m}\right)^a H_1(u;B)\right)\\ &= |\mathcal{F}_N(B)| + \frac{1}{3}\sum_{a=1}^{\lfloor \frac{N}{m}\rfloor}(-1)^a\left(2^a L(N-am) + 2C\left(\xi_3^m + \xi_3^{2m}\right)^a\right)q^{N-am}\\ &\qquad + O_\epsilon\big(q^{(\frac{1}{2}+\epsilon)(N-m)}\big).\end{aligned}$$

Hence, by Corollary 4.6, we find that $\frac{|\mathcal{F}_N(PB)|}{|\mathcal{F}_N(B)|}$ equals

$$\begin{aligned}&1 + \frac{\frac{1}{3}\sum_{a=1}^{\lfloor \frac{N}{m}\rfloor}(-1)^a\left(2^a L(N-am) + 2C\left(\xi_3^m + \xi_3^{2m}\right)^a\right)q^{N-am} + O_\epsilon\big(q^{(\frac{1}{2}+\epsilon)(N-m)}\big)}{\frac{1}{3}\big(L(N)+2C\big)q^N + O_\epsilon\big(q^{(\frac{1}{2}+\epsilon)N}\big)}\\ &= 1 + \sum_{a=1}^{\lfloor \frac{N}{m}\rfloor}\left(\frac{-2}{q^m}\right)^a\left(1 - \frac{am}{N}\right) + O\left(\frac{1}{Nq^m}\right),\end{aligned}$$

which is the desired result. □

We conclude this subsection with an observation that is useful in the proof of Lemma 2.7.

Remark 4.8. We can use the same ideas as above to prove that for any prime P, we have

$$\begin{aligned}&|\{D \in \mathcal{F}_N(B) : P|D\}|\\ &\quad \le 2\left|\left\{D \in \mathbb{F}_q[T] : D \text{ monic, cube-free and } \deg(\mathrm{rad}(D)) = N - \deg(P)\right\}\right|\\ &\quad \ll (N-\deg(P))q^{N-\deg(P)} \ll \frac{|\mathcal{F}_N(B)|}{q^{\deg(P)}}.\end{aligned}$$

Indeed, the first inequality is obvious as we have removed the conditions of being coprime to B and $\deg(D) \equiv 0 \bmod 3$, and the factor 2 accounts for the two cases $P\|D$ and $P^2\|D$. The second bound follows by the same proof as that of Corollary 4.6 with the minor change that here we only need to consider $H_0(u;1)$ as we have removed the conditions $(D,B) = 1$ and $\deg(D) \equiv 0 \bmod 3$.

4.6. Proof of Theorem 1.7

We now have everything we need to complete the proof of Theorem 1.7.

Proof of Theorem 1.7. Recall from (4.9) that

$$\left\langle \mathrm{Tr}(\Theta^n_{\widetilde{E}_D}) \right\rangle_{\mathcal{F}_N(B)} = M(n,N) + S(n,N) + E(n,N) + O\left(\frac{1}{q^{3n/8}} + \frac{n(\deg(\Delta_{\widetilde{E}}) + \tau(n))}{q^{n/2}} \right).$$

Using Proposition 4.3 to bound $E(n,N)$, we get

$$E(n,N) = \frac{n}{q^{n/2}} \sum_{\deg(P)=n} \left(\lambda_P \overline{E}_P + \overline{\lambda}_P E_P \right) - \frac{n/2}{q^{n/2}} \sum_{\deg(P)=\frac{n}{2}} \left(\lambda_P^2 E_P + \overline{\lambda}_P^2 \overline{E}_P \right)$$
$$+ \frac{n/3}{q^{n/2}} \sum_{\deg(P)=\frac{n}{3}} 3(|\lambda_P|^2 - 1)\left(\lambda_P \overline{E}_P + \overline{\lambda}_P E_P \right) \ll_\epsilon \frac{q^{n/2} e^{2n}}{N q^{(\frac{1}{2}-\epsilon)N}}.$$

Finally, we use Proposition 4.4 to estimate $M(n,N)$ and $S(n,N)$. We obtain

$$M(n,N) = -\frac{n/2}{q^{n/2}} \sum_{\deg(P)=\frac{n}{2}} 2(|\lambda_P|^2 - 1) \frac{|\mathcal{F}_N(PB)|}{|\mathcal{F}_N(B)|}$$
$$= -\frac{n/2}{q^{n/2}} \sum_{\deg(P)=\frac{n}{2}} 2(|\lambda_P|^2 - 1) + \frac{\widetilde{\mathcal{D}}_1(n)}{q^{n/2}} + O\left(\frac{1}{N q^{n/2}} \right),$$

where

$$\widetilde{\mathcal{D}}_1(n) := -\frac{n}{2} \sum_{\substack{\deg(P)=\frac{n}{2} \\ P \nmid B}} 2(|\lambda_P|^2 - 1) \sum_{a=1}^{\lfloor \frac{2N}{n} \rfloor} \left(\frac{-2}{q^{n/2}} \right)^a \left(1 - \frac{an}{2N} \right) \ll 1, \tag{4.10}$$

and

$$S(n,N) = \frac{n/3}{q^{n/2}} \sum_{\deg(P)=\frac{n}{3}} \left(\lambda_P^3 + \overline{\lambda}_P^3 \right) \frac{|\mathcal{F}_N(PB)|}{|\mathcal{F}_N(B)|}$$
$$= \frac{n/3}{q^{n/2}} \sum_{\deg(P)=\frac{n}{3}} \left(\lambda_P^3 + \overline{\lambda}_P^3 \right) + \frac{\widetilde{\mathcal{D}}_2(n)}{q^{n/2}} + O\left(\frac{1}{N q^{n/2}} \right),$$

where

$$\widetilde{\mathcal{D}}_2(n) := \frac{n}{3} \sum_{\substack{\deg(P)=\frac{n}{3} \\ P \nmid B}} \left(\lambda_P^3 + \overline{\lambda}_P^3 \right) \sum_{a=1}^{\lfloor \frac{3N}{n} \rfloor} \left(\frac{-2}{q^{n/3}} \right)^a \left(1 - \frac{an}{3N} \right) \ll 1. \tag{4.11}$$

This completes the proof. □

5. Heuristics and conjectures

In this section, we return to the heuristic arguments in Section 1.4. We first prove Corollary 1.9.

Proof of Corollary 1.9. First, we note that

$$\frac{n/3}{q^{n/2}} \sum_{\deg(P)=\frac{n}{3}} \left(\lambda_P^3 + \overline{\lambda}_P^3\right) \ll \frac{1}{q^{n/6}}.$$

Hence, setting the right-hand sides of Theorems 1.6 and 1.7 equal to each other for $n = 2m$, we find that

$$\begin{aligned} -\frac{m}{q^m} \sum_{\deg(P)=m} 2(|\lambda_P|^2 - 1) &= 1 - \frac{2m/3}{q^m} \sum_{\deg(P)=\frac{2m}{3}} \left(\lambda_P^3 + \overline{\lambda}_P^3\right) + O\left(\frac{m}{q^{m/2}}\right) \\ &= 1 + O\left(\frac{1}{q^{m/3}}\right). \end{aligned} \tag{5.1}$$

Furthermore, by the Prime Polynomial Theorem, we get

$$-\frac{m}{q^m} \sum_{\deg(P)=m} 2(|\lambda_P|^2 - 1) = -\frac{2m}{q^m} \sum_{\deg(P)=m} |\lambda_P|^2 + 2 + O\left(\frac{m}{q^{m/2}}\right). \tag{5.2}$$

Finally, equating the right-hand sides of (5.1) and (5.2), we find that

$$\frac{m}{q^m} \sum_{\deg(P)=m} |\lambda_P|^2 = \frac{1}{2} + O\left(\frac{1}{q^{m/3}}\right),$$

as desired. □

Next, we turn our attention to Conjecture 1.10. For evidence of the conjecture, we first consider the term

$$\frac{n/3}{q^{n/2}} \sum_{\deg(P)=\frac{n}{3}} \left(\lambda_P^3 + \overline{\lambda}_P^3\right)$$

from the right-hand side of Theorem 1.7. For primes of good reduction, we use (2.7) and Lemma 4.2 to write

$$\begin{aligned} a^*_{3,P} &= \alpha_P^3 + \beta_P^3 + \alpha_P + \beta_P \\ &= a^*_{1,P^3} + a^*_{1,P} \\ &= -\big(\lambda_P^3 + \overline{\lambda}_P^3\big) - 3(|\lambda_P|^2 - 1)(\lambda_P + \overline{\lambda}_P) + a^*_{1,P} \\ &= -\big(\lambda_P^3 + \overline{\lambda}_P^3\big) + (3|\lambda_P|^2 - 2)a^*_{1,P}. \end{aligned}$$

Hence, if we replace $|\lambda_P|^2$ with its average value when averaging over $\deg(P) = \frac{n}{3}$ and assume that the contribution of the primes of bad reduction will be of lower order, then we get

$$\begin{aligned} \frac{n/3}{q^{n/2}} \sum_{\deg(P)=\frac{n}{3}} \big(\lambda_P^3 + \overline{\lambda}_P^3\big) &\approx -\frac{n/3}{q^{n/2}} \sum_{\deg(P)=\frac{n}{3}} a^*_{3,P} + \frac{n/3}{q^{n/2}} \sum_{\deg(P)=\frac{n}{3}} (3|\lambda_P|^2 - 2)a^*_{1,P} \\ &\approx -\frac{n/3}{q^{n/2}} \sum_{\deg(P)=\frac{n}{3}} a^*_{3,P} - \frac{1}{2}\frac{n/3}{q^{n/2}} \sum_{\deg(P)=\frac{n}{3}} a^*_{1,P} \\ &\sim \frac{\eta_3(n)}{q^{n/3}} \left(\mathrm{Tr}\big(\Theta^{n/3}_{sym^3 \widetilde{E}}\big) + \frac{1}{2}\mathrm{Tr}\big(\Theta^{n/3}_{\widetilde{E}}\big) \right). \end{aligned}$$

In the final step above, we applied (2.4) together with the assumption that the sums in the second line constitute the dominant contribution to the respective trace.

Finally, by a similar argument we find that

$$-\frac{n/2}{q^{n/2}} \sum_{\deg(P)=\frac{n}{2}} 2(|\lambda_P|^2 - 1) \approx \frac{n/2}{q^{n/2}} \sum_{\deg(P)=\frac{n}{2}} 1 \sim \eta_2(n).$$

Assuming that the tertiary main term is handled in the way described in Remark 1.8 and that all error terms are sufficiently small, we arrive at Conjecture 1.10.

Appendix A. Comments on families of twists

One criterion for a family of function field L-functions to be considered "nice" and thus have interesting symmetries is that all members of the family have the same degree of the conductor, or equivalently, that all L-functions in the family are polynomials of the same degree. Ideally, when considering a certain class of L-functions, one would like the family to contain all the L-functions in that class of a given degree.

For the cubic twists, we consider only the family $\mathcal{F}_N(B)$ and all L-functions of twists of $\widetilde{E}$ by a polynomial $D \in \mathcal{F}_N(B)$ have degree $\mathfrak{n}_{\widetilde{E}} + 2N$. However, since the condition $\deg(D) \equiv 0 \bmod 3$ is included in the definition of $\mathcal{F}_N(B)$, we clearly see that there are cubic twists of $\widetilde{E}$ that do not come from $\mathcal{F}_N(B)$ and, indeed, some of them will have L-functions of degree $\mathfrak{n}_{\widetilde{E}} + 2N$.

It is easy to check that every *finite* prime that divides D will have additive reduction on $\widetilde{E}_D$ (or E_D). Each of these primes will then contribute P^2 to the conductor of $\widetilde{E}_D$

and so the degree of $L(u, \widetilde{E}_D)$ will always be roughly $\mathfrak{n}_{\widetilde{E}} + 2\deg(\mathrm{rad}(D))$. It remains to check what happens to the prime at infinity.

A.1. Reduction at the prime at infinity

Let $E : y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{F}_q[T]$. Define $a := \deg(A)$ and $b := \deg(B)$. To analyze what happens at the point at infinity, we let $S := 1/T$ and write

$$A(T) = S^{-a}A^*(S), \qquad B(T) = S^{-b}B^*(S)$$

and analyze what happens at $S = 0$ for the curve given by the equation

$$y^2 = x^3 + S^{-a}A^*x + S^{-b}B^*.$$

Setting

$$\ell = \max\{\lceil a/4 \rceil, \lceil b/6 \rceil\}$$

and

$$Y = S^{3\ell}y, \qquad X = S^{2\ell}x,$$

we rewrite the equation as

$$Y^2 = X^3 + S^{4\ell-a}A^*X + S^{6\ell-b}B^*. \tag{A.1}$$

We now note that

$$A^*(0), B^*(0) \neq 0$$

unless $A = 0$ or $B = 0$. Moreover, by our choice of ℓ, we have

$$4\ell - a, 6\ell - b \geq 0$$

and either

$$4\ell - a < 4 \qquad \text{or} \qquad 6\ell - b < 6.$$

Hence, (A.1) is a minimal Weierstrass equation for $S = 0$. Therefore, if P_∞ is the prime at infinity, then we define

$$E(P_\infty) : Y^2 = X^3 + S^{4\ell-a}A^*X + S^{6\ell-b}B^* \mod S. \tag{A.2}$$

We are now ready to discuss the reduction type for the prime at infinity. We get several cases:

(1) If $a/2 < b/3$, then $4\ell - a > 0$. Hence, reducing mod S in (A.2), we get:

   (a) $6|b$: $Y^2 = X^3 + B^*(0)$, so P_∞ is a prime of **good reduction**;
   (b) $6 \nmid b$: $Y^2 = X^3$, so P_∞ is a prime of **additive reduction**.

(2) If $a/2 > b/3$, then $6\ell - b > 0$. Hence, reducing mod S in (A.2), we get:

   (a) $4|a$: $Y^2 = X^3 + A^*(0)X$, so P_∞ is a prime of **good reduction**;
   (b) $4 \nmid a$: $Y^2 = X^3$, so P_∞ is a prime of **additive reduction**.

(3) If $a/2 = b/3$, then it must be that $2|a$ and $3|b$. If $a/2 = b/3$ is an even integer, then reducing mod S in (A.2), we get $Y^2 = X^3 + A^*(0)X + B^*(0)$.

   (a) If $4A^*(0)^3 + 27B^*(0)^2 \neq 0$, then P_∞ is a prime of **good reduction**.
   (b) If $4A^*(0)^3 + 27B^*(0)^2 = 0$, then P_∞ is a prime of **multiplicative reduction**.

   On the other hand, if $a/2 = b/3$ is an odd integer, then we get that $4\ell - a = 2$ and $6\ell - b = 3$. Hence, reducing mod S in (A.2), we find:

   (c) $Y^2 = X^3$, so P_∞ is a prime of **additive reduction**.

A.2. The cubic twist family

We deal with the case of the cubic twists first as there are less cases to consider. In this case, we have

$$\widetilde{E} : y^2 = x^3 + B$$

and

$$\widetilde{E}_D : y^2 = x^3 + BD^2.$$

Therefore, we see that since $A = 0$ we always have $a/2 < b/3$ and hence are only ever in case (1) above. The following chart captures, for D cube-free and coprime to B, what happens to the prime at infinity and how this affects the degree of the conductor:

b mod 6	$2\deg(D)$ mod 6	Ram. for $\widetilde{E}$	Ram. for $\widetilde{E}_D$	$\mathfrak{n}_{\widetilde{E}_D} - \mathfrak{n}_{\widetilde{E}}$
0	0	good	good	$2\deg(\mathrm{rad}(D))$
0	$\not\equiv 0$	good	additive	$2(\deg(\mathrm{rad}(D)) + 1)$
$\not\equiv 0$	$-b$	additive	good	$2(\deg(\mathrm{rad}(D)) - 1)$
$\not\equiv 0$	$\not\equiv -b$	additive	additive	$2\deg(\mathrm{rad}(D))$

As a consequence, to create a family of cubic twists in which all curves have the same degree of the conductor, we define the set

$$\widehat{\mathcal{F}}_N(B) := \big\{D \in \mathbb{F}_q[T] : D \text{ monic, cube-free}, (D, B) = 1, \deg(\mathrm{rad}(D)) = N\big\}.$$

As we see above, the ramification at infinity depends only on the congruence of $\deg(D)$ mod 3. Hence, we define

$$\widehat{\mathcal{F}}_{N;k}(B) := \big\{D \in \widehat{\mathcal{F}}_N(B) : \deg(D) \equiv k \bmod 3\big\}$$

and, when b is even,

$$\mathcal{J}_N(B) := \widehat{\mathcal{F}}_{N;-b/2}(B) \cup \widehat{\mathcal{F}}_{N-1,-b/2+1}(B) \cup \widehat{\mathcal{F}}_{N-1,-b/2+2}(B).$$

In addition, we define

$$\mathcal{K}_N(B) := \begin{cases} \mathcal{J}_N(B) & 6|b, \\ \mathcal{J}_{N+1}(B) & b \text{ is even and } 6 \nmid b, \\ \widehat{\mathcal{F}}_N(B) & b \text{ is odd.} \end{cases}$$

From all this, we may now conclude that the family

$$\big\{\widetilde{E}_D : D \in \mathcal{K}_N(B)\big\}$$

consists of all cubic twists of $\widetilde{E}$ with L-functions of degree $\mathfrak{n}_{\widetilde{E}} + 2N$.

Finally, we note that $\widehat{\mathcal{F}}_{N;0}(B) = \mathcal{F}_N(B)$. It is relatively easy to see how one would adapt our methods in Section 4 to deal with the "full" family $\mathcal{K}_N(B)$. One would just have to split everything into the relevant cases and the same proofs would work. Hence, we leave this as a comment and end the discussion here.

A.3. The quadratic twist family

In the case of quadratic twists, we have

$$E : y^2 = x^3 + Ax + B$$

and

$$E_D : y^2 = x^3 + AD^2x + BD^3.$$

We observe that the conditions on the degrees (from the cases at the end of Appendix A.1) aren't changed by twisting by $D \in \mathcal{H}_{2N}^{\pm}(\Delta_E)$. Moreover, in the case that $a/2 = b/3$, we get

$$4\big((AD^2)^*(0)\big)^3 + 27\big((BD^3)^*(0)\big)^2 = 4A^*(0)^3 + 27B^*(0)^2$$

since $D^*(0) = 1$. Therefore, the reduction at the prime at infinity is not changed by quadratic twists by $D \in \mathcal{H}^{\pm}_{2N}(\Delta_E)$ and $\mathfrak{n}_{E_D} = \mathfrak{n}_E + 2\deg(D)$.

In the case of $D \in \mathcal{H}^{\pm}_{2N+1}(\Delta_E)$, one may enumerate all the cases that appear in Appendix A.1 as we did for the cubic twist family to develop a "full" family of quadratic twists consisting of all the twists that give a specific degree of the conductor. Doing so is a tedious process and not illuminating so we end here and just state that, as in the cubic case, one could use the same methods to extend our results to this "full" family.

References

[1] S. Baier, M.P. Young, Mean values with cubic characters, J. Number Theory 130 (4) (2010) 879–903.
[2] S. Baig, C. Hall, Experimental data for Goldfeld's conjecture over function fields, Exp. Math. 21 (4) (2012) 362–374.
[3] A. Brumer, The average rank of elliptic curves I, Invent. Math. 109 (3) (1992) 445–472.
[4] H.M. Bui, A. Florea, Zeros of quadratic Dirichlet L-functions in the hyperelliptic ensemble, Trans. Am. Math. Soc. 370 (11) (2018) 8013–8045.
[5] B. Cha, D. Fiorilli, F. Jouve, Prime number races for elliptic curves over function fields, Ann. Sci. Éc. Norm. Supér. (4) 49 (5) (2016) 1239–1277.
[6] B. Cha, D. Fiorilli, F. Jouve, Independence of the zeros of elliptic curve L-functions over function fields, Int. Math. Res. Not. (9) (2017) 2614–2661.
[7] P.J. Cho, J. Park, Low-lying zeros of cubic Dirichlet L-functions and the ratios conjecture, J. Math. Anal. Appl. 474 (2) (2019) 876–892.
[8] P.J. Cho, J. Park, Dirichlet characters and low-lying zeros of L-functions, J. Number Theory 212 (2020) 203–232.
[9] A. Comeau-Lapointe, One-level density of the family of twists of an elliptic curve over function fields, J. Number Theory (2022), https://doi.org/10.1016/j.jnt.2022.03.005.
[10] C. David, J. Fearnley, H. Kisilevsky, On the vanishing of twisted L-functions of elliptic curves, Exp. Math. 13 (2) (2004) 185–198.
[11] C. David, A. Florea, M. Lalin, The mean values of cubic L-functions over function fields, preprint, arXiv:1901.00817, 2019.
[12] C. David, A. Florea, M. Lalin, Nonvanishing for cubic L-functions, Forum Math. Sigma 9 (2021), Paper No. e69, 58 pp.
[13] C. David, A.M. Güloğlu, One-level density and non-vanishing for cubic L-functions over the Eisenstein field, Int. Math. Res. Not. (2021), https://doi.org/10.1093/imrn/rnab240.
[14] C. David, D.K. Huynh, J. Parks, One-level density of families of elliptic curves and the Ratios Conjecture, Res. Number Theory 1 (2015), Paper No. 6, 37 pp.
[15] P. Deligne, La conjecture de Weil. I, Publ. Math. IHÉS 43 (1974) 273–307.
[16] P. Deligne, La conjecture de Weil. II, Publ. Math. IHÉS 52 (1980) 137–252.
[17] P. Diaconis, M. Shahshahani, On the eigenvalues of random matrices, J. Appl. Probab. 31A (1994) 49–62.
[18] D. Fiorilli, A conditional determination of the average rank of elliptic curves, J. Lond. Math. Soc. (2) 94 (3) (2016) 767–792.
[19] D. Fiorilli, J. Parks, A. Södergren, Low-lying zeros of elliptic curve L-functions: beyond the ratios conjecture, Math. Proc. Camb. Philos. Soc. 160 (2) (2016) 315–351.
[20] D. Goldfeld, Conjectures on elliptic curves over quadratic fields, in: Number Theory, Carbondale 1979, Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979, in: Lecture Notes in Math., vol. 751, Springer, Berlin, 1979, pp. 108–118.
[21] D.R. Heath-Brown, The average analytic rank of elliptic curves, Duke Math. J. 122 (3) (2004) 591–623.
[22] D.K. Huynh, J.P. Keating, N.C. Snaith, Lower order terms for the one-level density of elliptic curve L-functions, J. Number Theory 129 (12) (2009) 2883–2902.
[23] D.K. Huynh, S.J. Miller, R. Morrison, An elliptic curve test of the L-functions ratios conjecture, J. Number Theory 131 (6) (2011) 1117–1147.
[24] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, second edition, Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990.

[25] N.M. Katz, P. Sarnak, Zeroes of zeta functions and symmetry, Bull. Am. Math. Soc. (N.S.) 36 (1) (1999) 1–26.
[26] A. Lumley, Moments and distribution of values of L-functions over function fields inside the critical strip, Acta Arith. 201 (4) (2021) 329–369.
[27] P. Martin, M. Watkins, Symmetric Powers of Elliptic Curve L-Functions, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 377–392.
[28] P. Meisner, One level density for cubic Galois number fields, Can. Math. Bull. 62 (1) (2019) 149–167.
[29] P. Meisner, Lower order terms for expected value of traces of Frobenius of a family of cyclic covers of $\mathbb{P}^1_{\mathbb{F}_q}$ and one-level densities, preprint, arXiv:2006.16886, 2020.
[30] S.J. Miller, One- and two-level densities for rational families of elliptic curves: evidence for the underlying group symmetries, Compos. Math. 140 (4) (2004) 952–992.
[31] Z. Rudnick, Traces of high powers of the Frobenius class in the hyperelliptic ensemble, Acta Arith. 143 (1) (2010) 81–99.
[32] P. Sarnak, S.W. Shin, N. Templier, Families of L-functions and their symmetry, in: Proceedings of Simons Symposia, Families of Automorphic Forms and the Trace Formula, Springer-Verlag, 2016, pp. 531–578.
[33] D. Ulmer, Geometric non-vanishing, Invent. Math. 159 (1) (2005) 133–186.
[34] D. Ulmer, Elliptic curves over function fields, in: Arithmetic of L-Functions, in: IAS/Park City Math. Ser., vol. 18, Amer. Math. Soc., Providence, RI, 2011, pp. 211–280.
[35] M.P. Young, Lower-order terms of the 1-level density of families of elliptic curves, Int. Math. Res. Not. (10) (2005) 587–633.
[36] M.P. Young, Low-lying zeros of families of elliptic curves, J. Am. Math. Soc. 19 (1) (2006) 205–250.