EXTREMAL PRIMES FOR ELLIPTIC CURVES
WITHOUT COMPLEX MULTIPLICATION

C. DAVID, A. GAFNI, A. MALIK, N. PRABHU, AND C. L. TURNAGE-BUTTERBAUGH

(Communicated by Amanda Folsom)

ABSTRACT. Fix an elliptic curve E over $\mathbb{Q}$. An *extremal prime* for E is a prime p of good reduction such that the number of rational points on E modulo p is maximal or minimal in relation to the Hasse bound, i.e., $a_p(E) = \pm [2\sqrt{p}]$. Assuming that all the symmetric power L-functions associated to E have analytic continuation for all $s \in \mathbb{C}$ and satisfy the expected functional equation and the Generalized Riemann Hypothesis, we provide upper bounds for the number of extremal primes when E is a curve without complex multiplication. In order to obtain this bound, we use explicit equidistribution for the Sato-Tate measure as in the work of Rouse and Thorner, and refine certain intermediate estimates taking advantage of the fact that extremal primes are less probable than primes where $a_p(E)$ is fixed because of the Sato-Tate distribution.

1. INTRODUCTION

Let E denote an elliptic curve over $\mathbb{Q}$. For a prime p of good reduction, E reduces to an elliptic curve over the finite field $\mathbb{F}_p$, and we denote by $a_p(E)$ the trace of the Frobenius automorphism acting on the points of E over $\overline{\mathbb{F}}_p$. Then $a_p(E) = p + 1 - \#E(\mathbb{F}_p)$, and $|a_p(E)| \leq 2\sqrt{p}$ (the Hasse bound). The following conjecture for the distribution of the normalized traces $a_p(E)/2\sqrt{p}$ in $[-1, 1]$ was formulated independently by Sato and Tate.

Theorem 1.1 (Sato-Tate conjecture). *Let E be an elliptic curve without complex multiplication over $\mathbb{Q}$. Let $\alpha, \beta \in \mathbb{R}$ with $0 \leq \alpha \leq \beta \leq 1$. Then, as $x \to \infty$,*

$$\frac{1}{\pi(x)} \# \left\{ p \leq x \ : \ \frac{a_p(E)}{2\sqrt{p}} \in (\alpha, \beta) \right\} \sim \frac{2}{\pi} \int_\alpha^\beta \sqrt{1 - t^2}\, dt.$$

If E has at least one prime of multiplicative reduction, the Sato-Tate conjecture was proven by Taylor [16], in collaboration with Clozel, Harris, and Shepherd-Barron [3, 7].

We study in this paper a refinement of the Sato-Tate conjecture concerning the distribution of the primes p which fall at the extremes of this distribution, i.e., the primes p such that $a_p(E) = \pm[2\sqrt{p}]$, where for any real number y, $[y]$ denotes the integer part of y. Then $\#E(\mathbb{F}_p)$ is maximal when $a_p(E) = -[2\sqrt{p}]$ and minimal when $a_p(E) = [2\sqrt{p}]$.

1

Extremal primes were first studied by James et al. [9], who conjectured (as refined by James and Pollack [8]) that, as $x \to \infty$,

$$\# \{p \leq x \ : \ a_p(E) = [2\sqrt{p}]\}$$

(1.1) $$\sim \begin{cases} \dfrac{8}{3\pi} \dfrac{x^{1/4}}{\log x} & \text{if } E \text{ does not have complex multiplication,} \\[3ex] \dfrac{2}{3\pi} \dfrac{x^{3/4}}{\log x} & \text{if } E \text{ has complex multiplication.} \end{cases}$$

By symmetry, an analogous conjecture has been stated for extremal primes with $a_p(E) = -[2\sqrt{p}]$. It is enlightening to compare this conjecture with another refinement of the Sato-Tate conjecture, namely, the Lang-Trotter conjecture. For any fixed value $h \in \mathbb{Z}$, the Lang-Trotter conjecture [10] predicts that

(1.2) $$\pi_{E,h}(x) = \# \{p \leq x \ : \ a_p(E) = h\} \sim C_{E,h} \frac{x^{1/2}}{\log x}$$

as $x \to \infty$, where $C_{E,h}$ is a specific constant.[1] Comparing (1.1) and (1.2), we notice that for non-CM curves, there are expected to be fewer extremal primes than primes with a fixed value of $a_p(E)$, since the extremal primes are at the edge of the Sato-Tate distribution of Theorem 1.1, where the measure is small. On the other hand, for CM curves, an excess of extremal primes is predicted, since in this case, the measure for the distribution of $a_p(E)/2\sqrt{p}$ in $[\alpha, \beta] \subseteq [-1, 1] \setminus \{0\}$ is given by

$$\mu_{\mathrm{CM}}([\alpha, \beta]) = \frac{1}{2\pi} \int_{\alpha}^{\beta} \frac{dt}{\sqrt{1 - t^2}}.$$

The asymptotic (1.1) for CM curves was proven by James and Pollack [8]. In a subsequent paper by Agwu et al. [1] the authors obtained asymptotics for a refined question for CM curves, namely, the primes where $a_p(E)$ falls within a small range of the end of the Hasse interval. In this article, we focus on the case of non-CM curves.

Like the Lang-Trotter conjecture, the asymptotic (1.1) for non-CM curves seems to be out of reach with current techniques. An asymptotic was proven to hold on average for non-CM elliptic curves $E/\mathbb{Q}$ in the Ph.D. thesis of Giberson [5] (see also [6]). However, no non-trivial upper bounds are known for a single curve $E/\mathbb{Q}$. The goal of this paper is to obtain such upper bounds.

Let N_E denote the conductor of the elliptic curve E, and define

(1.3) $$L(s, E) = \prod_{p \nmid N_E} \left(1 - \frac{\alpha_p(E)}{p^s}\right)^{-1} \left(1 - \frac{\overline{\alpha}_p(E)}{p^s}\right)^{-1} \prod_{p | N_E} \left(1 - \frac{a_p(E)}{p^s}\right)^{-1},$$

where we have normalized the L-function so that $\alpha_p(E), \overline{\alpha}_p(E)$ satisfy

$$\#E(\mathbb{F}_p) = p + 1 - \sqrt{p}(\alpha_p(E) + \overline{\alpha}_p(E)) \quad \text{for } p \nmid N_E.$$

For any integer $n \geq 0$, the symmetric power L-functions of E are given by

$$L(s, \mathrm{Sym}^n(E)) = \prod_{p | N_E} L_p(s, \mathrm{Sym}^n(E)) \prod_{p \nmid N_E} \prod_{j=0}^{n} \left(1 - \frac{\alpha_p(E)^j \overline{\alpha}_p(E)^{n-j}}{p^s}\right)^{-1},$$

---

[1] If $h = 0$, then it is additionally assumed that E does not have complex multiplication. The case $h = 0$ and E with complex multiplication was treated in [4].

where the Euler factors $L_p(s, \mathrm{Sym}^n(E))$ at the bad primes are described in Appendix A.3.

The aforementioned proof of the Sato-Tate conjecture was obtained by proving that if E has at least one prime of multiplicative reduction, then the functions $L(s, \mathrm{Sym}^n(E))$ have meromorphic continuation to the whole complex plane, satisfy the functional equation (A.1), and are analytic and non-zero for $\mathrm{Re}(s) \geq 1$. (See [16, Theorem B], with the difference there that the L-functions are not normalized.) To get an effective version of the Sato-Tate conjecture in [15], the authors need to assume each $L(s, \mathrm{Sym}^n(E))$ has analytic continuation to the whole complex plane and satisfies the Generalized Riemann Hypothesis (GRH). For convenience, we include the function $L(s, \mathrm{Sym}^0(E)) = \zeta(s)$, which is analytic except for a simple pole at $s = 1$.

Under the same hypotheses, one can also obtain upper bounds for the Lang-Trotter conjecture. This was carried out by K. Murty [13] and extended by Bucur and Kedlaya to arbitrary motives [2]. These results were improved recently by Rouse and Thorner [15], who proved (under the same hypotheses as in Theorem 1.2, stated below) that

$$\pi_{E,h}(x) \ll_{E,h} x^{3/4}(\log x)^{-1/2}.$$

In our case, taking advantage of the fact that extremal primes fall at the edge of the Sato-Tate interval, we refine the work of Rouse and Thorner to obtain a better upper bound for the number of extremal primes.

Theorem 1.2. *Let E be a non-CM elliptic curve over $\mathbb{Q}$. Assume that for any $n \geq 0$, the L-functions $L(s, \mathrm{Sym}^n(E))$ have analytic continuation to the entire complex plane (except for a simple pole at $s = 1$ when $n = 0$) and satisfy the functional equation* (A.1) *and the Generalized Riemann Hypothesis. Then*

$$\#\{x < p \leq 2x \ : \ a_p(E) = [2\sqrt{p}]\} \ll_E x^{1/2}.$$

2. Explicit equidistiribution for the Sato-Tate measure

In this section, we prove upper bounds on Fourier coefficients of certain trigonometric polynomials which approximate characteristic functions of intervals. By considering short intervals at the edge of the Sato-Tate distribution, we obtain upper bounds that are stronger than what one obtains for general intervals.

We first briefly review classical results on explicit equidistribution. We refer the reader to [12, Chapter 1] for a detailed exposition of trigonometric polynomials approximating the characteristic function on subintervals of $[0, 1]$ with respect to the uniform measure and for the notation in this section. By the change of variable $t = \cos \theta$, we can view the Sato-Tate measure for non-CM curves, stated in Theorem 1.1, as the measure on $[0, \pi]$ given by

$$\mu_{ST}([\alpha, \beta]) = \frac{2}{\pi} \int_\alpha^\beta \sin^2 \theta \ d\theta$$

for $[\alpha, \beta] \subseteq [0, \pi]$. To approximate the characteristic function of intervals in $[0, \pi]$ with respect to the Sato-Tate measure, one uses the Chebyshev polynomials of the

second kind, denoted by U_n and defined by the recurrence relation

$$U_0(x) = 1,$$
$$U_1(x) = 2x,$$
$$U_n(x) = 2xU_{n-1}(x) - U_{n-2}(x).$$

We remark that the polynomials form an orthonormal basis with respect to the Sato-Tate measure on $[0, \pi]$. We refer to [15] for the proof of the following lemma, which follows directly from explicit uniform equidistribution.

Lemma 2.1 ([15, Lemma 1.3]). *Let $I = [\alpha, \beta] \subseteq [0, \pi]$, and let M be a positive integer. There exist trigonometric polynomials*

$$F_{I,M}^\pm(\theta) = \sum_{n=0}^{M} \hat{F}_{I,M}^\pm(n) U_n(\cos \theta)$$

that satisfy the following properties:

- *For $0 \leq \theta \leq \pi$, we have*

$$F_{I,M}^-(\theta) \leq \chi_I(\theta) \leq F_{I,M}^+(\theta).$$

- *We have*

$$|\hat{F}_{I,M}^\pm(0) - \mu_{ST}(I)| \leq \frac{4}{M+1}.$$

- *For $1 \leq n \leq M$, we have*

$$|\hat{F}_{I,M}^\pm(n)| \leq 4 \left(\frac{1}{M+1} + \min \left\{ \frac{\beta - \alpha}{2\pi}, \frac{1}{\pi n} \right\} \right).$$

The above lemma is valid for any interval $[\alpha, \beta] \subseteq [0, \pi]$. In our case, however, we are interested in counting at the edge of the Sato-Tate interval, where the measure is very small. More precisely, we will consider intervals where $t = \cos \theta$ is close to 1, i.e., where θ is close to 0. In this way, we obtain the following sharper estimate for the Fourier coefficients $\hat{F}_{I,M}^+(n)$, which will be key inputs in the proof of Theorem 1.2.

Proposition 2.2. *Assume the setting and notation of Lemma 2.1. If $I = [0, \frac{1}{M}] \subseteq [0, \pi]$, then for $0 \leq n \leq M$,*

$$\hat{F}_{I,M}^+(n) \ll \frac{1}{M^2}.$$

Proof. Since the U_n are an orthonormal basis, for $0 \leq n \leq M$ we have

$$\hat{F}_{I,M}^+(n) = \int_0^\pi F_{I,M}^+(\theta) U_n(\cos \theta) \sin^2 \theta \, d\theta$$

(2.1)
$$= \int_0^\pi \chi_I(\theta) U_n(\cos \theta) \sin^2 \theta \, d\theta$$

$$+ \int_0^\pi \left(F_{I,M}^+(\theta) - \chi_I(\theta) \right) U_n(\cos \theta) \sin^2 \theta \, d\theta.$$

The first integral of (2.1) is easily bounded by using the fact that

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

yielding

$$\int_0^\pi \chi_I(\theta) \, U_n(\cos\theta) \sin^2\theta \, d\theta \;=\; \int_0^{1/M} \sin\left((n+1)\theta\right) \sin\theta \, d\theta \ll \frac{1}{M^2}.$$

For the second integral of (2.1), we must bound the distance between the approximation of length M and $\chi_I(\theta)$. We recall the definition of $F_{I,M}^+(\theta)$. For any $J = [0, \beta] \subseteq [0, 1]$, it is straightfoward to see that

$$\chi_J(x) = \beta + s(x - \beta) + s(-x),$$

where $s(x)$ denotes the saw-tooth function

$$s(x) = \begin{cases} \{x\} - 1/2 & \text{if } x \notin \mathbb{Z}, \\ 0 & \text{if } x \in \mathbb{Z}. \end{cases}$$

Next, recall that the Beurling polynomial, $B_M(x)$, is defined by

$$B_M(x) = V_M(x) + \frac{1}{2(M+1)} \Delta_{M+1}(x),$$

where $\Delta_M(x)$ is the Fejer kernel given by

$$\Delta_M(x) = \frac{1}{M} \left(\frac{\sin \pi M x}{\sin \pi x} \right)^2,$$

and $V_M(x)$ is the Vaaler polynomial given by

$$V_M(x) = \frac{1}{M+1} \sum_{k=1}^M \left(\frac{k}{M+1} - \frac{1}{2} \right) \Delta_{M+1} \left(x - \frac{k}{M+1} \right)$$

$$+ \frac{1}{2\pi(M+1)} \sin(2\pi(M+1)x) - \frac{1}{2\pi} \Delta_{M+1}(x) \sin 2\pi x.$$

We set

$$S_{J,M}^+(x) = \beta + B_M(x - \beta) + B_M(-x).$$

When $I = [0, 1/M]$, setting the interval $J = [0, 1/(2\pi M)] \subseteq [0, 1/2]$, we have that

$$F_{I,M}^+(\theta) = S_{J,M}^+ \left(\frac{\theta}{2\pi} \right) + S_{J,M}^+ \left(-\frac{\theta}{2\pi} \right).$$

With the change of variable $x = \theta/2\pi$ and $\beta = 1/(2\pi M)$, we find that

$$\begin{aligned} F_{I,M}^+(\theta) - \chi_I(\theta) &= S_{J,M}^+(x) + S_{J,M}^+(-x) - \chi_J(x) - \chi_J(-x) \\ &= B_M(x - \beta) - s(x - \beta) + B_M(-x) - s(-x) \\ &\quad + B_M(-x - \beta) - s(-x - \beta) + B_M(x) - s(x). \end{aligned}$$

The second integral of (2.1) then writes as

$$2\pi \int_{-1/2}^{1/2} (B_M(x) - s(x)) \, U_n(\cos 2\pi x) \, \sin^2(2\pi x) \, dx$$

$$+ 2\pi \int_{-1/2}^{1/2} (B_M(x - \beta) - s(x - \beta)) \, U_n(\cos 2\pi x) \, \sin^2(2\pi x) \, dx.$$

We now compute the second integral in the above expression, since upon taking $\beta = 0$ we will recover the first integral. From the definition of the polynomial B_M, we have

$$\int_{-1/2}^{1/2} (B_M(x - \beta) - s(x - \beta))\ U_n(\cos 2\pi x)\ \sin^2(2\pi x)\ dx$$

$$(2.2) \qquad = \int_{-1/2}^{1/2} (V_M(x - \beta) - s(x - \beta))\ U_n(\cos 2\pi x)\ \sin^2(2\pi x)\ dx$$

$$(2.3) \qquad + \frac{1}{2(M+1)} \int_{-1/2}^{1/2} \Delta_{M+1}(x - \beta)\ U_n(\cos 2\pi x)\ \sin^2(2\pi x)\ dx.$$

To estimate (2.2), we use the bound (for $|x| \le 1/2$)

$$V_M(x - \beta) - s(x - \beta) \quad \ll \quad \min\left(1, \frac{1}{M^3|x - \beta|^3}\right)$$

$$\ll \quad \begin{cases} 1 & \text{if } |x - \beta| < 1/M, \\ (M|x - \beta|)^{-3} & \text{if } 1/M \le |x - \beta| \le 1/2 \end{cases}$$

and find, for $\beta = 1/(2\pi M) \ll 1/M$, that

$$\int_{-1/2}^{1/2} (V_M(x - \beta) - s(x - \beta))\ U_n(\cos 2\pi x)\ \sin^2(2\pi x)\ dx$$

$$\ll \int_{\beta - 1/M}^{\beta + 1/M} |\sin((n+1)2\pi x)\ \sin(2\pi x)|\ dx$$

$$+ \frac{1}{M^3}\left(\int_{\beta + 1/M}^{1/2} + \int_{-1/2}^{\beta - 1/M}\right) |x - \beta|^{-3}\ |\sin((n+1)2\pi x)\ \sin(2\pi x)|\ dx$$

$$\ll \int_0^{\beta + 1/M} x\ dx + \frac{1}{M^3} \int_{\beta + 1/M}^{1/2} \frac{x}{(x - \beta)^3}\ dx$$

$$\ll \frac{1}{M^2} + \frac{1}{M^3} \int_{\beta + 1/M}^{1/2} \left(\frac{1}{(x - \beta)^2} + \frac{\beta}{(x - \beta)^3}\right)\ dx$$

$$\ll \frac{1}{M^2}.$$

It remains to show that the expression in (2.3) is also $\ll 1/M^2$. First note that we may write

$$(2.4) \qquad U_n(\cos(2\pi x)) = \frac{\sin((n+1)2\pi x)}{\sin(2\pi x)}.$$

Moreover, the Fejér kernel may alternatively be expressed as

$$\Delta_M(x) = \frac{1}{M} \sum_{k=0}^{M-1} D_k(x),$$

where $D_k(x)$ is the k-th order Dirichlet kernel that has a closed form expression given by

$$D_k(x) = 1 + 2\sum_{j=1}^{k} \cos(2\pi jx).$$

Thus, we may express $\Delta_{M+1}(x)$ as

$$(2.5) \qquad \Delta_{M+1}(x) = \frac{1}{M+1}\sum_{k=0}^{M}\left(1 + 2\sum_{j=1}^{k}\cos(2\pi jx)\right).$$

From (2.4), (2.5), and a trigonometric sum-difference formula, we have

$$(M+1)\int_{-1/2}^{1/2}\Delta_{M+1}(x-\beta)\,U_n(\cos 2\pi x)\,\sin^2(2\pi x)\,dx$$

$$= (M+1)\int_{-1/2}^{1/2}\Delta_{M+1}(x-\beta)\,\sin((n+1)2\pi x)\sin(2\pi x)\,dx$$

$$= \frac{1}{2}\int_{-1/2}^{1/2}\left((M+1)+2\sum_{k=1}^{M}\sum_{j=1}^{k}\cos(2\pi j(x-\beta))\right)(\cos(2\pi nx)$$

$$\qquad\qquad - \cos(2\pi(n+2)x))\,dx$$

$$= \sum_{k=1}^{M}\sum_{j=1}^{k}\int_{-1/2}^{1/2}\cos(2\pi j(x-\beta))\big(\cos(2\pi nx) - \cos(2\pi(n+2)x)\big)\,dx$$

$$(2.6) \qquad = \sum_{k=1}^{M}\sum_{j=1}^{k}\int_{-1/2}^{1/2}\cos(2\pi j(x-\beta))\cos(2\pi nx)\,dx$$

$$(2.7) \qquad - \sum_{k=1}^{M}\sum_{j=1}^{k}\int_{-1/2}^{1/2}\cos(2\pi j(x-\beta))\cos(2\pi(n+2)x)\,dx.$$

Using trigonometric identities, we can rewrite the sum in (2.6) as

$$(2.8) \quad \sum_{k=1}^{M}\sum_{j=1}^{k}\int_{-1/2}^{1/2}(\cos(2\pi j\beta)\cos(2\pi jx) + \sin(2\pi j\beta)\sin(2\pi jx))\cos(2\pi nx)\,dx.$$

Recall that

$$\int_{-1/2}^{1/2}\cos(m\pi x)\cos(n\pi x)\,dx = \begin{cases} \frac{1}{2} & \text{if } m = n, \\ 0 & \text{otherwise} \end{cases}$$

and that for any $m, n \in \mathbb{Z}$,

$$\int_{-1/2}^{1/2}\cos(m\pi x)\sin(n\pi x)\,dx = 0.$$

Therefore, the only term that survives in the inner sum over j in (2.8) is the term $j = n$. This gives

$$\sum_{k=1}^{M}\sum_{j=1}^{k}\int_{-1/2}^{1/2}\cos(2\pi j(x-\beta))\cos(2\pi nx)\,dx = \frac{M-n+1}{2}\cos(2\pi n\beta),$$

and a similar calculation gives that the sum in (2.7) is

$$\sum_{k=1}^{M}\sum_{j=1}^{k}\int_{-1/2}^{1/2}\cos(2\pi j(x-\beta))\cos(2\pi(n+2)x)\,dx = \frac{M-(n+2)+1}{2}\cos(2\pi(n+2)\beta)$$

if $1 \le n \le M-2$ and equal to 0 if $n = M-1, M$. Thus, for $1 \le n \le M-2$,

$$(M+1)\int_{-1/2}^{1/2}\Delta_{M+1}(x-\beta)\,U_n(\cos 2\pi x)\,\sin^2(2\pi x)\,dx$$

$$= \frac{M-n+1}{2}\cos(2\pi n\beta) - \frac{M-(n+2)+1}{2}\cos(2\pi(n+2)\beta)$$

(2.9) $$= (M-n+1)\sin(2\pi(n+1)\beta)\sin(2\pi\beta) + \cos(2\pi(n+2)\beta),$$

while for $n = M-1, M$ we have

$$(M+1)\int_{-1/2}^{1/2}\Delta_{M+1}(x-\beta)\,U_n(\cos 2\pi x)\,\sin^2(2\pi x)\,dx$$

(2.10) $$= \frac{M-n+1}{2}\cos(2\pi n\beta).$$

Dividing by $2(M+1)^2$, the integral in (2.3) is $\ll 1/M^2$ for $\beta = 1/(2\pi M)$. Setting $\beta = 0$ in (2.9) and (2.10), we find that for non-negative integers n, M with $M \ge 1$,

$$\int\limits_{-1/2}^{1/2}\left(\frac{\sin((M+1)\pi x)}{\sin(\pi x)}\right)^2 U_n(\cos 2\pi x)\sin^2(2\pi x)\,dx = \begin{cases} 1 & \text{if } 0 \le n < M, \\ \frac{1}{2} & \text{if } n = M. \end{cases}$$

We have thus shown that for $\beta = 1/(2\pi M)$,

$$\int_{-1/2}^{1/2}(B_M(x-\beta)-s(x-\beta))\,U_n(\cos 2\pi x)\,\sin^2(2\pi x)\,dx \ll \frac{1}{M^2},$$

and using $\beta = 0$ in the above formulas, we have

$$\int_{-1/2}^{1/2}(B_M(x)-s(x))\,U_n(\cos 2\pi x)\,\sin^2(2\pi x)\,dx \ll \frac{1}{M^2}.$$

This completes the proof of the proposition. □

Remark. The results of Proposition 2.2 also hold for the coefficients $\hat{F}_{I,M}^-(n)$, following appropriate minor changes, but this is not needed for our application.

3. Proof of Theorem 1.2

We adapt the arguments of [15] to prove Theorem 1.2, using the stronger bound on the size of the Fourier coefficients computed in Proposition 2.2. To estimate the prime counting function

$$\#\{x \le p < 2x : a_p(E) = [2\sqrt{p}]\},$$

we first perform the change of variable $a_p(E) = 2\sqrt{p}\cos\theta_p(E)$. Let I_ε be an interval of the form $[0, \varepsilon] \subseteq [0, \pi/2]$ and $I_\varepsilon' = [\cos(\varepsilon), 1]$ is such that

$$\cos\theta_p(E) \in I_\varepsilon' \iff \theta_p(E) \in I_\varepsilon.$$

If $\varepsilon = \varepsilon(x)$ is such that

$$\cos \varepsilon \le 1 - x^{-1/2}, \tag{3.1}$$

then using $x \le p < 2x$, we have

$$\cos \varepsilon \le 1 - \frac{1}{x^{1/2}} < 1 - \frac{1}{2\sqrt{p}} < 1 - \frac{\{2\sqrt{p}\}}{2\sqrt{p}} < 1.$$

Using this, we obtain the upper bound

$$\begin{aligned}
\#\{x \le p < 2x : a_p(E) = [2\sqrt{p}]\} &= \# \left\{ x \le p < 2x : \frac{a_p(E)}{2\sqrt{p}} = 1 - \frac{\{2\sqrt{p}\}}{2\sqrt{p}} \right\} \\
&\le \#\{x \le p < 2x : \cos \theta_p(E) \in I_\varepsilon'\} \\
&= \#\{x \le p < 2x : \theta_p(E) \in I_\varepsilon\} \\
&= \sum_{x \le p < 2x} \chi_{I_\varepsilon}(\theta_p(E)),
\end{aligned}$$

where for any interval I, χ_I is the characteristic function of the interval.

Let $\varepsilon = 1/M$ so that $I_\varepsilon = [0, 1/M]$, where M is chosen later. Using the first property in Lemma 2.1, we have

$$\begin{aligned}
\sum_{x \le p < 2x} \chi_{I_\varepsilon}(\theta_p) &\le \sum_{n=0}^{M} \hat{F}_{I_\varepsilon,M}^+(n) \sum_{x \le p < 2x} U_n(\cos \theta_p(E)) \\
&\le \sum_{n=0}^{M} |\hat{F}_{I_\varepsilon,M}^+(n)| \left| \sum_{x \le p < 2x} U_n(\cos \theta_p(E)) \right|.
\end{aligned} \tag{3.2}$$

To estimate the quantity $\sum_{x \le p < 2x} U_n(\cos \theta_p(E))$, as in [15], we get sharper estimates by weighting the contribution from primes using a test function which is a pointwise upper bound for the characteristic function on $[x, 2x]$. Let

$$g(y) = \begin{cases} \exp\left(\frac{4}{3} + \frac{1}{(y-\frac{1}{2})(y-\frac{5}{2})} \right) & \text{if } \frac{1}{2} < y < \frac{5}{2}, \\ 0 & \text{otherwise}, \end{cases} \tag{3.3}$$

and $g_x(y) = g(y/x)$. Using the bound $1 \le \frac{\log p}{\log x}$ for all $x \le p < 2x$, this allows us to write

$$\left| \sum_{x \le p < 2x} U_n(\cos \theta_p(E)) \right| \le \frac{1}{\log x} \left| \sum_p U_n(\cos \theta_p(E)) g_x(p) \log p \right|. \tag{3.4}$$

We next use a result of [15] stated in the following form.

Proposition 3.1 ([15, Proposition 3.5]). *For each $n \ge 0$, assume that the L-function $L(s, Sym^n(E))$ is entire (with the exception of a simple pole at $s = 1$ when $n = 0$), satisfies the functional equation (A.1) and the Generalized Riemann Hypothesis. Then, we have*

$$\sum_p U_n(\cos \theta_p(E)) g_x(p) \log p \ll_E \delta_{n,0} x + \sqrt{x} n \log n, \tag{3.5}$$

where $\delta_{n,0} = 1$ if $n = 0$ and 0 otherwise.

Remark. Proposition 3.5 of [15] has the additional hypothesis that N_E is square-free. We describe how to remove this hypothesis in Appendix A.

Using (3.4) and (3.5) in (3.2) we now have

$$\sum_{x \le p < 2x} \chi_{I_\varepsilon}(\theta_p(E)) \ll \frac{1}{\log x} \sum_{n=0}^{M} |\hat{F}^+_{I_\varepsilon, M}(n)| \left(\delta_{n,0}x + \sqrt{x}n \log n\right).$$

We now use Proposition 2.2 to bound the Fourier coefficients $\hat{F}^+_{I_\varepsilon, M}(n)$. Doing so, the right hand side of the above equation is

$$\ll \frac{1}{M^2 \log x} \left(x + \sqrt{x} \sum_{n=1}^{M} n \log n\right)$$

$$\ll \frac{x}{M^2 \log x} + \frac{x^{1/2} \log M}{\log x}.$$

Letting $M = \left\lceil \dfrac{x^{1/4}}{(\log x)^{1/2}} \right\rceil$, we see that (3.1) is satisfied, and we have

$$\#\left\{x \le p < 2x \ : \ a_p(E) = [2\sqrt{p}]\right\} \le \sum_{x \le p < 2x} \chi_{I_\varepsilon}(\theta_p(E)) \ll x^{1/2},$$

which completes the proof of Theorem 1.2.

APPENDIX A

A.1. **Proof of Proposition 3.1.** We now extend the proof of Proposition 3.5 of [15] to all non-CM elliptic curves over $\mathbb{Q}$, without assuming that N_E is square-free, i.e., that the bad primes are primes of multiplicative reduction. This necessitates a bound on the conductor of $\mathrm{Sym}^n(E)$ and computing the local factors at the bad primes of all reduction types. We summarize in subsections A.2 and A.3 the work of Martin and Watkins [11] which gives us these estimates.

Let $N_{E,n}$ be the conductor of $\mathrm{Sym}^n(E)$. Notice that in this notation, $N_{E,1} = N_E$ (and $N_{E,0} = 1$). It is conjectured that the $L(s, \mathrm{Sym}^n(E))$ satisfy the functional equation

(A.1) $$\Lambda(s, \mathrm{Sym}^n(E)) = \varepsilon_n \Lambda(1 - s, \mathrm{Sym}^n(E)),$$

where the root number $\varepsilon_n \in \mathbb{C}$ has absolute value 1 and the completed L-function is

$$\Lambda(s, \mathrm{Sym}^n(E)) = N_{E,n}^{s/2} \gamma(s, \mathrm{Sym}^n(E)) L(s, \mathrm{Sym}^n(E)),$$

with the gamma factor

$$\gamma(s, \mathrm{Sym}^n(E)) = \begin{cases} \left(2^{1-s}\pi^{-s}\right)^{(n+1)/2} \displaystyle\prod_{j=1}^{(n+1)/2} \Gamma\left(s + (j-1/2)(n-1)\right) & \text{if } n \text{ is odd} \\[2em] \pi^{-(s+n_2)/2}\Gamma((s+n_2)/2)\left(2^{1-s}\pi^{-s}\right)^{n/2} \displaystyle\prod_{j=1}^{n/2} \Gamma\left(s + j(n-1)\right) \\[1em] \hfill \text{if } n \text{ is even.} \end{cases}$$

In the above, $n_2 = n/2 \mod 2$.

As in [15], define the numbers $\Lambda_{\mathrm{Sym}^n(E)}(j)$ by

$$-\frac{L'}{L}(s, \mathrm{Sym}^n(E)) = \sum_{j=1}^{\infty} \frac{\Lambda_{\mathrm{Sym}^n(E)}(j)}{j^s}, \qquad \mathrm{Re}(s) > 1.$$

For primes p not dividing N_E and $m \geq 1$, it is a straightforward computation to show that

(A.2) $$\Lambda_{\mathrm{Sym}^n(E)}(p^m) = U_n(\cos(m\theta_p(E))) \log p.$$

Also, $\Lambda_{\mathrm{Sym}^n(E)}(j)$ is zero when j is not a power of a prime. Thus,

$$\sum_p U_n(\cos\theta_p(E)) g_x(p) \log p = \sum_{j=1}^{\infty} \Lambda_{\mathrm{Sym}^n(E)}(j) g_x(j) - \sum_{\substack{j \geq 1 \\ j = p^m, m \geq 2 \\ \text{or } j = p, p | N_E}} \Lambda_{\mathrm{Sym}^n(E)}(j) g_x(j)$$

$$+ \sum_{p | N_E} U_n(\cos\theta_p(E)) g_x(p) \log p.$$

We now show that for any integer j, we have

$$\Lambda_{\mathrm{Sym}^n(E)}(j) \ll (n+1)\Lambda(j),$$

where $\Lambda(j)$ is the usual von Mangoldt function. If $j = p^m$ and $p \nmid N_E$, the result is clear by (A.2). Suppose now that $j = p^m$, for $p \mid N_E$ and $m \geq 1$. Using the formulas (A.6), (A.7), and (A.8) which give the Euler products at the bad primes of $-\frac{L'}{L}(s, \mathrm{Sym}^n(E))$ for multiplicative, potentially multiplicative, and potentially good reduction, the result follows easily. Thus, we have

$$\sum_{\substack{j \geq 1 \\ j = p^m, m \geq 2 \\ \text{or } j = p, p | N_E}} \Lambda_{\mathrm{Sym}^n(E)}(j) g_x(j) - \sum_{p \nmid N_E} U_n(\cos\theta_p(E)) g_x(p) \log p$$

$$\ll (n+1) \left(\sum_{\substack{x/2 < p^m \leq 5x/2 \\ m \geq 2 \\ p \nmid N_E}} \log p + \sum_{\substack{x/2 \leq p^m < 5x/2 \\ p | N_E}} \log p + \sum_{p | N_E} \log p \right)$$

(A.3)

$$\ll (n+1) \left(\sum_{\substack{x/2 < p^m \leq 5x/2 \\ m \geq 2}} \log p + \log N_E \right) \ll_E n\sqrt{x}.$$

Then, as in [15], we have to estimate

$$\sum_{j=1}^{\infty} \Lambda_{\mathrm{Sym}^n(E)}(j) \, g_x(j).$$

This is done by first writing an explicit formula for the non-smoothed sum

$$\psi_{\mathrm{Sym}^n(E)}(x) = \sum_{j \leq x} \Lambda_{\mathrm{Sym}^n(E)}(j),$$

and evaluating the residues at the poles, coming from the zeroes of $L(s, \mathrm{Sym}^n(E))$ in the critical strips. In all those estimates, the authors use the fact that $N_{E,n} = N_E^n$, which leads to the bound $\log(N_{E,n}) \leq n \log N_E$. From (A.5) of subsection A.2, it follows that without any hypothesis on the reduction type of E at the bad primes, we have

$$\log N_{E,n} \ll n \log N_E,$$

where the implied constant is absolute. The argument of [15, Section 8] becomes

$$\sum_{j=1}^{\infty} \Lambda_{\mathrm{Sym}^n(E)}(j) g_x(j) \quad = \quad \delta_{n,0} x \int_0^{\infty} g(t)\, dt + O\left(\sqrt{x}\left(n \log n + \log N_{E,n}\right)\right)$$

$$\text{(A.4)} \qquad\qquad\qquad \ll_E \quad \delta_{n,0} x + \sqrt{x}\, n \log(n),$$

where we recall that g is defined by (3.3).

Comparing (A.4) and (A.3), we complete the proof of Proposition 3.1 without assumption on N_E.

A.2. **The conductors $N_{E,n}$.** We now summarize the results concerning the conductors $N_{E,n}$ from [11, Section 3]. For each prime $p \mid N$, fix $\ell \neq p$, and let $T_\ell(E)$ denote the Tate module at ℓ. Let $H_\ell(E) = \mathrm{Hom}(T_\ell(E) \otimes \mathbb{Q}_\ell, \mathbb{Q}_\ell)$ and let $I_p \leq \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ be the local inertia group at p. Define $\epsilon_n(I_p)$ to be the co-dimension of the subspace of $\mathrm{Sym}^n(H_\ell(E))$ fixed by I_p. Then, we have that

$$N_{E,n} = \prod_{p \mid N_E} p^{\epsilon_n(I_p) + \delta_n(p)},$$

where $\delta_n(p)$ is the wild part of the conductor. If p is a prime of multiplicative reduction, then $\epsilon_n(I_p) = n$ and $\delta_n(p) = 0$ for all n, and then $N_{E,n} = N_E^n$ when N_E is square-free as assumed in [15, Conjecture 1.1(a)].

For the other cases, we first remark that the wild conductor $\delta_n(p) = 0$ when $p \geq 5$ for all reduction types. For p a prime of potentially multiplicative reduction, we have that $\epsilon_n(I_p) = n + 1$ if n is odd and $\epsilon_n(I_p) = n$ if n is even. The wild conductors $\delta_n(p)$ are always 0, except for the case $p = 2$ and n odd, where we have $\delta_n(2) = \frac{n+1}{2}\delta_1(2)$.

For p a prime of potentially good reduction, the value of $\epsilon_n(p)$ depends on the inertia group of the local extension $G_p = \mathrm{Gal}(\mathbb{Q}_p(E_\ell)/\mathbb{Q}_p)$ and the congruence of n modulo 12. The values of $\epsilon_n(p)$ in all cases that arise are given in Table 1 of [11], and we always have $0 \leq \epsilon_n(p) \leq n + 1$. The wild conductors $\delta_n(2)$ and $\delta_n(3)$ are given in Tables 2 and 3 of [11], and we have that $\delta_n(2) \leq 2(n+1)$ and $\delta_n(3) \leq (n+1)/2$.

We then have the bound

$$\text{(A.5)} \qquad\qquad N_{E,n} \leq 2^{6(n+1)} 3^{(n+1)/2} \prod_{p \mid N_E} p^{(n+1)} \ll_E N_E^{6n}.$$

We also remark that the computation of the conductor $N_{E,n}$ in [11] is the idea presented in [14, Section 5] applied to the special case of elliptic curves.

A.3. **The local factors at the bad primes.** Next, we summarize the results concerning the Euler factors at primes of bad reduction from [11, Section 3]. Since we use the normalized L-function $L(s, E)$ defined by (1.3), and Martin and Watkins use the non-normalized L-function, we adjust their result accordingly using the fact that

$$L(s, \mathrm{Sym}^n(E)) = L_{\text{non-norm}}(s + n/2, \mathrm{Sym}^n(E)).$$

Let $L_p(s, \mathrm{Sym}^n(E))$ be the Euler factors at the bad primes p of $L(s, \mathrm{Sym}^n(E))$.

If p is a prime of multiplicative reduction or potentially multiplicative reduction, then

$$L_p(s, \mathrm{Sym}^n(E)) = \left(1 - \frac{a_{p,n}}{p^{s+n/2}}\right)^{-1},$$

where $a_{p,n} \in \{0, \pm 1\}$, and then

$$\text{(A.6)} \qquad \sum_{m=1}^{\infty} \frac{\Lambda_{\mathrm{Sym}^n(E)}(p^m)}{p^{ms}} = \sum_{m=1}^{\infty} \frac{\log p}{p^{sm}} \frac{a_{p,n}^m}{p^{nm/2}}.$$

In the case where p is a prime with potentially good reduction, there are 2 cases depending on whether or not the local decomposition group G_p is abelian. When G_p is abelian, the local inertia group is cyclic of order d, where $d = 2, 3, 4,$ or 6, and

$$L_p(s, \mathrm{Sym}^n(E)) = \prod_{\substack{0 \le k \le n \\ d|(2k-n)}} \left(1 - \frac{\beta_p(E)^{n-k}\overline{\beta}_p(E)^k}{p^{s+n/2}}\right)^{-1},$$

where $\beta_p(E)$ is obtained by counting points on a p^r-th quadratic twist of E (which is non-singular) where r depends on the p-valuation of the coefficients of E. It follows that $|\beta_p(E)| = p^{1/2}$. Then,

$$\text{(A.7)} \qquad \sum_{m=1}^{\infty} \frac{\Lambda_{\mathrm{Sym}^n(E)}(p^m)}{p^{ms}} = \sum_{m=1}^{\infty} \frac{\log p}{p^{sm}} \frac{1}{p^{nm/2}} \sum_{\substack{0 \le k \le n \\ d|(2k-n)}} \left(\beta_p(E)^{n-k}\overline{\beta}_p(E)^k\right)^m.$$

On the other hand, when G_p is non-abelian, we have

$$L_p(s, \mathrm{Sym}^n(E)) = \left(1 - \frac{(\pm 1)(-p)^{n/2}}{p^{s+n/2}}\right)^{-(n+1-\epsilon_n(I_p))}$$

and

$$\text{(A.8)} \qquad \sum_{m=1}^{\infty} \frac{\Lambda_{\mathrm{Sym}^n(E)}(p^m)}{p^{ms}} = \sum_{m=1}^{\infty} \frac{(\pm 1)^m(-1)^{mn/2}\log p}{p^{sm}}\left(n + 1 - \epsilon_n(I_p)\right).$$

References

[1] Anthony Agwu, Phillip Harris, Kevin James, Siddarth Kannan, and Huixi Li, *Frobenius distributions in short intervals for CM elliptic curves*, J. Number Theory **188** (2018), 263–280, DOI 10.1016/j.jnt.2018.01.007. MR3778634

[2] Alina Bucur and Kiran S. Kedlaya, *An application of the effective Sato-Tate conjecture*, Frobenius distributions: Lang-Trotter and Sato-Tate conjectures, Contemp. Math., vol. 663, Amer. Math. Soc., Providence, RI, 2016, pp. 45–56, DOI 10.1090/conm/663/13349. MR3502938

[3] Laurent Clozel, Michael Harris, and Richard Taylor, *Automorphy for some l-adic lifts of automorphic mod l Galois representations,* with Appendix A, summarizing unpublished work of Russ Mann, and Appendix B by Marie-France Vignéras, Publ. Math. Inst. Hautes Études Sci. **108** (2008), 1–181, DOI 10.1007/s10240-008-0016-1. MR2470687

[4] Max Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper* (German), Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272, DOI 10.1007/BF02940746. MR0005125

[5] Luke M. Giberson, *Average Frobenius Distributions for Elliptic Curves: Extremal Primes and Koblitz's Conjecture*, ProQuest LLC, Ann Arbor, MI. Thesis (Ph.D.)–Clemson University, 2017. MR3698846

[6] Luke Giberson and Kevin James, *An average asymptotic for the number of extremal primes of elliptic curves*, Acta Arith. **183** (2018), no. 2, 145–165, DOI 10.4064/aa170406-30-1. MR3798785

[7] Michael Harris, Nick Shepherd-Barron, and Richard Taylor, *A family of Calabi-Yau varieties and potential automorphy*, Ann. of Math. (2) **171** (2010), no. 2, 779–813, DOI 10.4007/annals.2010.171.779. MR2630056

[8] Kevin James and Paul Pollack, *Extremal primes for elliptic curves with complex multiplication*, J. Number Theory **172** (2017), 383–391, DOI 10.1016/j.jnt.2016.09.033. MR3573159

[9] Kevin James, Brandon Tran, Minh-Tam Trinh, Phil Wertheimer, and Dania Zantout, *Extremal primes for elliptic curves*, J. Number Theory **164** (2016), 282–298, DOI 10.1016/j.jnt.2016.01.009. MR3474389

[10] Serge Lang and Hale Trotter, *Frobenius distributions in* GL_2*-extensions*, Distribution of Frobenius automorphisms in GL_2-extensions of the rational numbers, Lecture Notes in Mathematics, Vol. 504, Springer-Verlag, Berlin-New York, 1976. MR0568299

[11] Phil Martin and Mark Watkins, *Symmetric powers of elliptic curve L-functions*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 377–392, DOI 10.1007/11792086_27. MR2282937

[12] Hugh L. Montgomery, *Ten lectures on the interface between analytic number theory and harmonic analysis*, CBMS Regional Conference Series in Mathematics, vol. 84, Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 1994. MR1297543

[13] V. Kumar Murty, *Explicit formulae and the Lang-Trotter conjecture*, Number theory (Winnipeg, Man., 1983), Rocky Mountain J. Math. **15** (1985), no. 2, 535–551, DOI 10.1216/RMJ-1985-15-2-535. MR823264

[14] Jeremy Rouse, *Atkin-Serre type conjectures for automorphic representations on* $GL(2)$, Math. Res. Lett. **14** (2007), no. 2, 189–204, DOI 10.4310/MRL.2007.v14.n2.a3. MR2318618

[15] Jeremy Rouse and Jesse Thorner, *The explicit Sato-Tate conjecture and densities pertaining to Lehmer-type questions*, Trans. Amer. Math. Soc. **369** (2017), no. 5, 3575–3604, DOI 10.1090/tran/6793. MR3605980

[16] Richard Taylor, *Automorphy for some l-adic lifts of automorphic mod l Galois representations. II*, Publ. Math. Inst. Hautes Études Sci. **108** (2008), 183–239, DOI 10.1007/s10240-008-0015-2. MR2470688

Department of Mathematics, Concordia University, 1455 de Maisonneuve West, Montreal, Quebec H3G 1M8, Canada
Email address: chantal.david@concordia.ca

Department of Mathematics, The University of Mississippi, Hume Hall 305, University, Mississippi 38677
Email address: ayla.gafni@gmail.com

Department of Mathematics, Rutgers University, 110 Frelinghuysen Road, Piscataway, New Jersey 08854
Email address: amita.malik@rutgers.edu

Department of Mathematics and Statistics, Queen's University, 48 University Avenue, Kingston, Ontario K7L 3N6, Canada
Email address: neha.prabhu@queensu.ca

Department of Mathematics and Statistics, Carleton College, 1 North College Street, Northfield, Minnesota 55057
Email address: cturnageb@carleton.edu