Contemporary Mathematics
Volume **663**, 2016
http://dx.doi.org/10.1090/conm/663/13354

Variants of the Sato-Tate and Lang-Trotter Conjectures

Kevin James

1. Introduction

In this paper, we survey some results related to the Sato-Tate and Lang-Trotter conjectures which naturally give rise to variations of these conjectures. Let $E_{A,B}$ denote the elliptic curve over $\mathbb{Q}$ with Weierstrass equation

$$E_{A,B} : y^2 = x^3 + Ax + B.$$

As usual, we will let

$$a_E(p) = p + 1 - \#E(\mathbb{F}_p).$$

Recall that Hasse's theorem guarantees us that $|a_E(p)| < 2\sqrt{p}$. The Lang-Trotter and Sato-Tate conjectures are concerned with the distribution of $a_E(p)$ for a fixed elliptic curve $E/\mathbb{Q}$ as p varies over the primes of $\mathbb{Z}$. Both of these conjectures can of course be considered in the setting of general number fields. We will restrict our attention for the moment to the rationals to ease notation.

The Sato-Tate conjecture, which was proved in 2006 by Clozel, Harris, Shepherd-Barron and Taylor (see [**Tay08**], [**CHT08**], [**HSBT10**]), states that

Theorem 1 (Clozel,Harris,Shepard-Baron,Taylor). *If E does not have complex multiplication and $-1 < \alpha < \beta < 1$, then*

$$\#\{p < X : \alpha \cdot 2\sqrt{p} < a_E(p) < \beta \cdot 2\sqrt{p}\} \sim \frac{2}{\pi}\left(\int_\alpha^\beta \sqrt{1-t^2}\,dt\right)\frac{X}{\log X}.$$

One may of course ask for more precise distribution information. The Cebotarev density theorem gives the following analogue of Dirichlet's theorem.

Theorem 2 (Cebotarev). *Suppose that $E/\mathbb{Q}$ is an elliptic curve and $a, m \in \mathbb{Z}$ with $m > 1$. Then there is an explicit constant $C_E(a,m)$ such that*

$$\#\{p < X \mid a_E(p) \equiv a \pmod{m}\} \sim C_E(a,m) \cdot \frac{X}{\log X}.$$

The more precise Lang-Trotter conjecture [**LT76**] states the following.

2010 *Mathematics Subject Classification.* Primary 11G05, 11N05; Secondary 11M50, 11P55, 11D85.

Conjecture 3 (Lang-Trotter). *Let $E/\mathbb{Q}$ be an elliptic curve and let $r \in \mathbb{Z}$. If E does not have complex multiplication or if $r \neq 0$ then*

$$\#\{p < X : a_E(p) = r\} \sim C_{E,r} \frac{\sqrt{X}}{\log X},$$

where $C_{E,r}$ is an explicit constant depending only on E and r (see Conjecture 10 below).

Although this conjecture has received much attention, it remains unproved.

2. Variations of the Sato-Tate conjecture

In this section we consider modifying the Sato-Tate Conjecture by asking that the trace $a_E(p)$ not only lie in a fixed interval but that it also reside in a particular arithmetic set. For example we first consider the set of perfect k-th powers and make the following definitions.

Definition 4. *For fixed $k \in \mathbb{Z}$, we define*

- $\pi_E(\alpha, \beta, k; X) := \# \left\{ p \leq X \;\middle|\; \begin{array}{l} a_E(p) \in (2\alpha\sqrt{p}, 2\beta\sqrt{p}); \\ \exists n \in \mathbb{Z}, a_E(p) = n^k \end{array} \right\}$,
- $\pi_k(X) = \int_2^X \frac{t^{\frac{1}{2k}-\frac{1}{2}}}{\log t} dt \sim \frac{2k}{(k+1)} \frac{X^{\frac{1}{2}+\frac{1}{2k}}}{\log X}$.

Gang Yu and the author [**JY06**] were able to prove the following theorem concerning the average value of $\pi_E(\alpha, \beta, k; X)$.

Theorem 5 (J.-Yu). *Let $0 < \beta < 1$ and $k > 1$ be fixed. For X sufficiently large, if $A, B > X \log X$, then we have*

$$\frac{1}{4AB} \sum_{\substack{|a| \leq A \\ |b| \leq B}} \pi_{E(a,b)}(0, \beta, k; X) \sim \frac{2kc_k(\beta)}{(k+1)} \frac{X^{\frac{1}{2}+\frac{1}{2k}}}{\log X},$$

where $c_k(\beta) = \frac{2^{\frac{1}{k}}}{3k\pi} \int_0^\beta |t|^{\frac{1}{k}-1}\sqrt{1-t^2}dt$.

The proof follows the ideas of Birch who proved that the Sato-Tate conjecture holds on average in [**Bir68**] by employing Deuring's theorem [**Deu41**] (see also Theorem 18) to relate the number of curves $E/\mathbb{F}_p$ to the Kronecker class number $H(r^2 - 4p)$. The novelty of our approach is to employ the Hardy-Littlewood circle method to estimate the number of representations of a negative integer $n \equiv 0, 1 \pmod 4$ as $r^2 - 4p$ where p is a prime and r is a perfect k-th power.

Given the above theorem it seems natural to conjecture the following.

Conjecture 6 (J-Yu). *Given an elliptic curve $E/\mathbb{Q}$, $0 < \beta < 1$ and $k > 1$,*

$$\pi_E(0, \beta, k; X) \sim \frac{2kc_k(\beta)}{(k+1)} \frac{X^{\frac{1}{2}+\frac{1}{2k}}}{\log X},$$

where $c_k(\beta) = \frac{2^{\frac{1}{k}}}{3k\pi} \int_0^\beta |t|^{\frac{1}{k}-1}\sqrt{1-t^2}dt$.

One may of course consider other arithmetic sets such as the set of primes.

Definition 7. *We consider the prime counting function,*

$$\pi_E(\alpha; X) := \#\{p < X \;:\; a_E(p) \leq 2\alpha\sqrt{p};\; a_E(p) \text{ is prime}\}$$

Using techniques similar to those in [**JY06**], Tran, Trinh, Werthiemer, Zantout and the author [**JTT$^+$14**] proved the following.

THEOREM 8 (J-Tran-Trinh-Wertheimer-Zantout). *Suppose $A, B > (X \log X)^2$. Then*

$$\frac{1}{AB} \sum_{\substack{a \in (U, U+A] \\ b \in (V, V+B]}} \pi_{E_{a,b}}(\alpha; X) \sim c(\alpha) \frac{X}{(\log X)^2},$$

where

$$c(\alpha) = \frac{16C}{3\pi} \int_0^\alpha \sqrt{1-t^2}\ \mathrm{dt}$$

and $C \approx 0.9226 \pm 10^{-4}$ is an explicit constant.

This of course suggests a conjecture analogous to Conjecture 6 above. It is almost certain that the range over which we average in the Theorem 8 can be shortened. It might also prove interesting to consider other arithmetic sets.

3. The Lang-Trotter Conjecture on Average

One may wish for more precise information than is given by Theorem 1 and Theorem 2.

DEFINITION 9. *For an elliptic curve $E/\mathbb{Q}$ and $r \in \mathbb{Z}$, put*

$$\pi_E^r(X) := \#\{p < X : a_E(p) = r\}.$$

Lang and Trotter [**LT76**] conjectured the following asymptotic for $\pi_E^r(X)$.

CONJECTURE 10 (Lang-Trotter). *Let $E/\mathbb{Q}$ be an elliptic curve and let $r \in \mathbb{Z}$. If E does not have complex multiplication or if $r \neq 0$ then*

$$\pi_E^r(X) \sim C_{E,r} \frac{\sqrt{X}}{\log X},$$

where $C_{E,r}$ is an explicit constant depending only on E and r and defined as follows. Let M_E be the Serre number for E. Then,

$$C_{E,r} \quad = \quad \frac{2}{\pi} M_E \frac{\#[\tilde{\rho}_{E,M_E}(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})]_r}{\#\tilde{\rho}_{E,M_E}(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})} \prod_{\substack{\ell \nmid M_E \\ \ell \nmid r}} \frac{\ell(\ell^2-\ell-1)}{(\ell+1)(\ell-1)^2} \prod_{\substack{\ell \nmid M_E \\ \ell | r}} \frac{\ell^2}{\ell^2-1},$$

where G_r in the above formula denotes the elements of G of trace r.

Unlike the Sato-Tate conjecture, the above conjecture seems far from proof at present. However we can glean further information and evidence for the conjecture by considering the average behavior of $\pi_E^r(X)$ as we vary E over families of curves. The theme of studying this conjecture "on average" following Birch's approach [**Bir68**] to the Sato-Tate conjecture was initiated by Fouvry and Murty in [**FM96**], who considered the case when $r = 0$. The density of complex multiplication curves is so small that they do not affect the asymptotic. Their work was generalized by David and Pappalardi [**DP99**], who considered the remaining cases.

Theorem 11 (David-Pappalardi). *Let $E(a,b) : y^2 = x^3 + ax + b$ and let $\epsilon > 0$. If $A, B > X^{1+\epsilon}$, then we have as $X \to \infty$,*

$$\frac{1}{4AB} \sum_{|a|\le A |b|\le B} \pi^r_{E(a,b)}(X) \sim D_r \pi_{1/2}(X),$$

where

$$D_r := \frac{2}{\pi} \prod_{q \nmid r} \frac{q(q^2-q-1)}{(q+1)(q-1)^2} \prod_{q \mid r} \frac{q^2}{q^2-1}.$$

This was later improved by Baier [**Bai07**], who showed that the average can be taken over a shorter range. In a complimentary direction, Jones [**Jon09**] verified that the average of the constants conjectured by Lang and Trotter matches the constant in the asymptotic of David and Pappalardi above.

Finer averages have also been considered. In [**Jam04**], the author considered the problem when the average was restricted to curves admitting a rational 3-torsion point. Averages over families of elliptic curves with various prescribed torsion structures were considered in [**BBIJ05**]. In particular, they prove the following.

Theorem 12 (Battista-Bayless-Ivanov-J). *Let $E(s)$ be the parameterization of elliptic curves having a point of order $M \in \{3,5,6,7,9,10\}$. Let $\epsilon > 0$ and $N > X^{1+\epsilon}$. Then,*

$$\frac{1}{2N} \sum_{|s|\le N} \pi^r_{E(s)}(X) \sim \frac{2}{\pi} C_{r,M} \frac{\sqrt{X}}{\log X}$$

where

$$C_{r,M} = C_r(M) \prod_{\substack{\ell \nmid M \\ \ell \mid r}} \frac{\ell^2}{\ell^2-1} \prod_{\substack{\ell \nmid M \\ \ell \nmid r}} \frac{\ell(\ell^2-\ell-1)}{(\ell+1)(\ell-1)^2},$$

and

$$C_r(M) = \begin{cases} 3/2 & \text{if } n = 5;\ r \equiv 1 \pmod 3, \\ 5/4, & \text{if } n = 5;\ r \equiv 0,3,4 \pmod 5, \\ 2, & \text{if } n = 6;\ r \equiv 0 \pmod 6, \\ 7/6, & \text{if } n = 7;\ r \equiv 0,3,4,5,6 \pmod 7, \\ 3/2, & \text{if } n = 9;\ r \equiv 0,3,6 \pmod 9, \\ 5/3, & \text{if } n = 10;\ r \equiv 0,4,8 \pmod{10}. \end{cases}$$

It is interesting to note that the constant accurately reflects the restriction on the associated Galois representations caused by the presence of rational torsion points. More general averages over 2-parameter families were considered by Shparlinski and Cojocaru [**CS08**] and Shparlinski [**Shp13**].

3.1. Extending the Lang-Trotter Conjecture to Number Fields. We now turn to the number field case. Suppose that K is a number field and E is an elliptic curve defined over K. Given a prime ideal $\mathfrak{p}$ of the ring of integers $\mathcal{O}_K$ where E has good reduction, we define the trace of Frobenius $a_E(\mathfrak{p})$ as before. In particular, we have $a_E(\mathfrak{p}) = \mathbb{N}\mathfrak{p} + 1 - \#E(\mathcal{O}_K/\mathfrak{p})$ and $|a_E(\mathfrak{p})| \le 2\sqrt{\mathbb{N}\mathfrak{p}} = 2p^{f/2}$. Here, $\mathbb{N}\mathfrak{p} := \#(\mathcal{O}_K/\mathfrak{p}) = p^f$ is the norm of $\mathfrak{p}$, p is the unique rational prime lying below $\mathfrak{p}$, and $f = \deg \mathfrak{p}$ is the absolute degree of $\mathfrak{p}$. For a fixed elliptic curve E and fixed integers r and f, we define the prime counting function

$$\pi_E^{r,f}(x) := \#\{\mathbb{N}\mathfrak{p} \le x : a_E(\mathfrak{p}) = r \text{ and } \deg \mathfrak{p} = f\}.$$

For elliptic curves defined over a number field K, the heuristics of Lang and Trotter [**LT76**] suggest the following more refined conjecture. See [**DP04**] also.

Conjecture 13 (Lang-Trotter for number fields). *Let E be a fixed elliptic curve defined over K, and let r be a fixed integer. In the case that E has complex multiplication, also assume that $r \neq 0$. Let f be a positive integer. There exists a constant $\mathfrak{C}_{E,r,f}$ such that*

$$\pi_E^{r,f}(x) \sim \mathfrak{C}_{E,r,f} \begin{cases} \frac{\sqrt{x}}{\log x} & \text{if } f = 1, \\ \log\log x & \text{if } f = 2, \\ 1 & \text{if } f \geq 3 \end{cases}$$

as $x \to \infty$. The constant $\mathfrak{C}_{E,r,f}$ may be zero, in which case the asymptotic is interpreted to mean that there are only finitely many such primes.

Remark 14. *For a fixed $f \geq 3$, we interpret the conjecture to say that there are only finitely many such primes. In this case, the constant $\mathfrak{C}_{E,r,f}$ would necessarily be a nonnegative integer.*

This conjecture too has been studied on average. David and Pappalardi [**DP04**] considered the case when $K = \mathbb{Q}(i)$ and $f = 2$. Calkin, Faulkner, King, Penniston and the author [**CFJ$^+$11**] extended this work to the setting of an arbitrary Abelian number field K. In fact, the authors of [**CFJ$^+$11**] considered any positive integer f and obtained asymptotics in accordance with the conjecture. The author along with Ethan Smith further generalized the above results to the setting of Galois number fields in the $f = 1$ case (see [**JS11**]) and to many additional number fields in the $f = 2$ case (see [**JS13**]).

In order to state these results, we adopt the following notation. We assume that K is a fixed Galois number field. We denote the degree of the extension by $n_K := [K : \mathbb{Q}]$, and let $\mathcal{B} = \{\gamma_j\}_{j=1}^{n_K}$ be a fixed integral basis for $\mathcal{O}_K$. We denote the coordinate map for the basis $\mathcal{B}$ by

$$[\cdot]_{\mathcal{B}} : \mathcal{O}_K \xrightarrow{\sim} \bigoplus_{j=1}^{n_K} \mathbb{Z} = \mathbb{Z}^{n_K}.$$

Given two vectors $\mathbf{a}, \mathbf{b} \in \mathbb{Z}^{n_K}$, if each entry of $\mathbf{a}$ is less than or equal to the corresponding entry of $\mathbf{b}$, then we write $\mathbf{a} \leq \mathbf{b}$. If $\mathbf{b} \geq \mathbf{0}$, then we define a "box" of algebraic integers by

$$\mathcal{B}(\mathbf{a}, \mathbf{b}) := \{\alpha \in \mathcal{O}_K : \mathbf{a} - \mathbf{b} \leq [\alpha]_{\mathcal{B}} \leq \mathbf{a} + \mathbf{b}\}.$$

For two algebraic integers $\alpha, \beta \in \mathcal{O}_K$, we write $E_{\alpha,\beta}$ for the elliptic curve given by the model

$$E_{\alpha,\beta} : Y^2 = X^3 + \alpha X + \beta.$$

Then for appropriate vectors, we define a "box" of elliptic curves by

$$\mathscr{B} := \mathscr{B}(\mathbf{a}_1, \mathbf{b}_1; \mathbf{a}_2, \mathbf{b}_2) = \{E_{\alpha,\beta} : \alpha \in \mathcal{B}(\mathbf{a}_1, \mathbf{b}_1) \text{ and } \beta \in \mathcal{B}(\mathbf{a}_2, \mathbf{b}_2)\}.$$

To be more precise, this box should be thought of as a box of equations or models since the same elliptic curve may appear multiple times in $\mathscr{B}$. For $i = 1, 2$, let $b_{i,j}$

denote the j-th entry of $\mathbf{b}_i$. Associated to box $\mathscr{B}$, we define the quantities

$$\mathscr{V}(\mathscr{B}) = 2^{2n_K}\prod_{j=1}^{n_K} b_{1,j} * b_{2,j}, \qquad \mathscr{V}_{\min}(\mathscr{B}) = 2\min_{1\le j\le n_K}\{b_{1,j}, b_{2,j}\},$$

$$\mathscr{V}_1(\mathscr{B}) = 2^{n_K}\prod_{j=1}^{n_K} b_{1,j}, \qquad \mathscr{V}_2(\mathscr{B}) = 2^{n_K}\prod_{j=1}^{n_K} b_{2,j},$$

which give a description of the size of this box. In particular,

$$\#\mathscr{B} = \mathscr{V}(\mathscr{B}) + O\left(\mathscr{V}(\mathscr{B})/\mathscr{V}_{\min}(\mathscr{B})\right).$$

Recall that

$$\pi_{1/2}(x) := \int_2^x \frac{dt}{2\sqrt{t}\log t} \sim \frac{\sqrt{x}}{\log x}.$$

Combining the results of [**CFJ$^+$11**], [**JS11**] and [**JS13**], we have the following theorem.

THEOREM 15 (Faulkner-J-Smith.). (1) *Let $\eta > 0$, and let r be a fixed integer. Then*

$$\frac{1}{\#\mathscr{B}}\sum_{E\in\mathscr{B}} \pi_E^{r,1}(x) \sim \mathfrak{C}_{K,r,1}\pi_{1/2}(x),$$

provided that the box $\mathscr{B}$ satisfies the growth conditions:

$$\mathscr{V}(\mathscr{B}) \gg x^{2n_K-1/2}(\log x)^{2n_K+1+\eta},$$
$$\mathscr{V}_1(\mathscr{B}), \mathscr{V}_2(\mathscr{B}) \gg x^{n_K-1/2}(\log x)^{n_K+1+\eta},$$
$$\mathscr{V}_{\min}(\mathscr{B}) \gg (\log x)^{\eta}.$$

(2) *Suppose that $K/\mathbb{Q}$ is a degree n number field which is Abelian, or which can be decomposed as $K = K_1K_2$ with K_1 totally non-Abelian and K_2 2-pretentious (-i.e. primes of $\mathbb{Q}$ which split into degree 2 primes in K_2 are precisely the primes belonging to some set of arithmetic progressions) and with $K_1 \cap K_2 = \emptyset$. If $2|n$, then provided that $\mathscr{V}_{min}(\mathscr{B}) \ge 2\sqrt{x}$,*

$$\frac{1}{\#\mathscr{B}}\sum_{E\in\mathscr{B}} \pi_E^{r,2}(x) \sim \mathfrak{C}_{K,r,2}\log\log x,$$

(3) *For $f \ge 3$ with $f|n$, if $\mathscr{V}_{min}(\mathscr{B})$ is sufficiently large, then*

$$\frac{1}{\#\mathscr{B}}\sum_{E\in\mathscr{B}} \pi_E^{r,2}(x) = \mathrm{O}(1),$$

where the $\mathfrak{C}_{r,f,K}$'s are explicit constants depending only on r, f and the field K.

The proofs of these theorems follow a similar line of reasoning as the proofs used by David and Pappalardi. The major difficulty was that we needed to prove a number field analogue of the Barban-Davenport-Halberstam Theorem [**Bar64, DH66, DH68**] which gives a surprisingly small error term for the average value of the prime counting function for primes in arithmetic progressions. The necessary analog was provided by Ethan Smith. We state a useful special case of Smith's results below. For more generality, the reader is referred to [**Smi10**] and [**Smi11**].

For $q \in \mathbb{Z}$ we denote by G_q the image of the natural map

$$\mathrm{Gal}\left(K(\zeta_q)/K\right) \hookrightarrow \mathrm{Gal}\left(\mathbb{Q}(\zeta_q)/\mathbb{Q}\right) \xrightarrow{\cong} \left(\mathbb{Z}/q\mathbb{Z}\right)^*,$$

and by $\phi_K(q)$ the size of G_q. Finally we define for $q \in \mathbb{Z}$ and $a \in G_q$ the prime counting function

$$\theta_K(X,1,q,a) := \sum_{\substack{N\mathfrak{p}<X \\ \deg\ \mathfrak{p}=1 \\ N\mathfrak{p}\equiv a \pmod q}} \log N\mathfrak{p}.$$

The Cebotarev Density Theorem yields

$$\theta_K(X,1,q,a) \sim \frac{X}{\phi_K(q)},$$

and we have the following bound on the average order of the error due to Smith (see [**JS11**, Theorem 6]).

THEOREM 16 (E. Smith). *Suppose that $K/\mathbb{Q}$ is Galois, $M > 0$ and $X(\log X)^{-M} \le Q \le X$. Then we have*

$$\sum_{q\le Q}\sum_{a\in G_q}\left(\theta_K(X,1,q,a) - \frac{X}{\phi_K(q)}\right)^2 \ll XQ\log X.$$

4. Champion Primes

In this section, we consider a variant of the Lang-Trotter conjecture.

DEFINITION 17. *Suppose that E is an elliptic curve over $\mathbb{Q}$. We say that a prime p is a champion prime for E if*

$$\#E(\mathbb{F}_p) = p + 1 + \lfloor 2\sqrt{p}\rfloor$$

that is, if

$$a_E(p) = -\lfloor 2\sqrt{p}\rfloor.$$

Similarly we say that a prime p is an extremal prime if

$$|a_E(p)| = \lfloor 2\sqrt{p}\rfloor.$$

We first note that the existence of champion primes for at least some elliptic curves is guaranteed by the following theorem of Deuring [**Deu41**].

THEOREM 18 (Deuring). *Given a prime $p > 4$, there are*

$$\frac{p-1}{2}H(4p - \lfloor 2\sqrt{p}\rfloor^2)$$

pairs $(a,b) \in \mathbb{F}_p^2$ such that if $(A,B) \equiv (a,b) \pmod p$ then p is a champion for $E_{A,B}$.

This immediately yields the following corollary.

COROLLARY 19. *Given a prime p, the density of elliptic curves E for which*

(1) *p is a prime of good reduction for E, and*
(2) *p is a champion prime for E*

is given by

$$\frac{1}{p} \ll \frac{H(4p - \lfloor 2\sqrt{p}\rfloor^2)}{2p} \ll \frac{\log^2(p)}{p^{3/4}}.$$

If we wish to have a more precise estimate of how many elliptic curves posses champion primes we might wish to consider the following density functions.

Definition 20. *We consider the following density functions.*

(1) $\delta(A,B,X) = \frac{1}{4AB}\# \left\{ (a,b) \;\middle|\; \begin{array}{l} |a|<A;\ |b|<B; \\ E_{a,b} \text{ has a champion} \\ \text{prime } p \text{ of good reduction} \\ \text{with } 4<p<X. \end{array} \right\}.$

(2) $\delta(X) = \lim_{A\to\infty} \delta(A,A,X)$.

(3) $\delta = \lim_{X\to\infty} \delta(e^{(5/8+\epsilon)X}, e^{(5/8+\epsilon)X}, X)$.

Using the above corollary along with an inclusion-exclusion argument and the Chinese remainder theorem Hedetniemi, Xue and the author [**HJX14**] proved the following theorem.

Theorem 21 (Hedetniemi, J-, Xue). *Let $A, B, X > 0$, and define the density $\delta(A,B,X)$ of elliptic curves $E_{a,b}$ with $|a| < A$ and $|b| < B$ which have a champion prime p of good reduction satisfying $4 < p < X$ as above (see Definition 20-1). Then we have*

$$\begin{aligned}\delta(A,B,X) &= \left[1 - \prod_{4<p<X}\left[1 - \frac{p-1}{2p^2}H\left(4p - \lfloor 2\sqrt{p}\rfloor^2\right)\right]\right] \\ &+ \mathrm{O}\left(\exp\left(\frac{1}{4}X + o(X)\right)\left(\frac{1}{A}+\frac{1}{B}\right) + \frac{\exp\left(\frac{5}{4}X + o(X)\right)}{AB}\right).\end{aligned}$$

One immediately obtains the following corollaries.

Corollary 22. *Let $X > 0$, and define the density $\delta(X)$ of elliptic curves with a champion prime of good reduction satisfying $4 < p < X$ as above (see Definition 20-2). Then we have*

$$\delta(X) = \left[1 - \prod_{4<p<X}\left[1 - \frac{p-1}{2p^2}H\left(4p - \lfloor 2\sqrt{p}\rfloor^2\right)\right]\right] + o(1).$$

Corollary 23. *Define the density δ of elliptic curves possessing a champion prime $p > 4$ of good reduction as above (see Definition 20-3). Then we have*

$$\delta = 1.$$

So, this phenomenon is not rare and we may wish to count the number of champion or extremal primes for a given curve $E/\mathbb{Q}$.

Definition 24. *Let $E/\mathbb{Q}$ be an elliptic curve. Then we define the following champion and extremal prime counting functions.*

(1) $\pi_E^{\text{Champ}}(X) = \#\left\{p < X \mid a_E(p) = -\lfloor 2\sqrt{p}\rfloor\right\}$, *and*

(2) $\pi_E^{\text{Extremal}}(X) = \#\left\{p < X \mid |a_E(p)| = \lfloor 2\sqrt{p}\rfloor\right\}$.

At this point, not much is known about these functions. In work which is still in preparation, Luke Giberson and the author have proved that for $A, B \gg X^{1+\epsilon}$ and for any $\eta > 0$,

$$\frac{X^{1/4-\eta}}{\log X} \ll \frac{1}{4AB}\sum_{|a|<A,|b|<B}\pi_E^{\text{Champ}}(X) \ll \frac{X^{1/4}}{\log X}.$$

Thus one is led to the following conjecture

Conjecture 25. *Given an elliptic curve $E/\mathbb{Q}$ without CM, there exists a constant C_E depending only on E such that*

$$\pi_E^{Champ}(X) \sim C_E \frac{X^{1/4}}{\log X}.$$

One of course expects that $\pi_E^{\text{Extremal}}(X) = 2\pi_E^{\text{Champ}}(X)$. Computations suggest that the value of $\pi_E^{\text{Extremal}}(X)$ could be much larger for elliptic curves possessing complex multiplication. The following theorem [**JTT$^+$15**] gives solid evidence that this is indeed the case.

Theorem 26 (J-,Tran, Trinh, Wertheimer, Zantout). *Suppose $End(E) = \mathcal{O}_K$ where $K/\mathbb{Q}$ is imaginary quadratic and $\Delta_K \neq -3, -4$. If RH holds for $L(s, \chi_K^n)$ for all n, then*

$$\pi_E^{Extremal}(X) = \frac{4X^{3/4}}{3\pi \log X} + \mathrm{O}\left(\frac{X^{3/4}}{\log^2 X}\right).$$

The technique of proof for this theorem is to use basic facts about complex multiplication theory to deduce that the extremal primes of a CM curve must factor in the CM order into primes one of which (say ω) must be contained in the region of the complex plane satisfying $\mathrm{Re}(\omega)^2 \geq \Im(\omega) \geq 0$. We then use a theorem of Rajan [**Raj98**] to count such primes under the Riemann Hypotheses mentioned in the theorem.

References

[Bai07] Stephan Baier, *The Lang-Trotter conjecture on average*, J. Ramanujan Math. Soc. **22** (2007), no. 4, 299–314. MR2376806 (2008j:11065)

[Bar64] M.B. Barban, *On the distribution of primes in arithmetic progressions "on average"*, Dokl. Akad. Nauk UzSSR **5** (1964), 5–7, (Russian).

[BBIJ05] Jonathan Battista, Jonathan Bayless, Dmitriy Ivanov, and Kevin James, *Average Frobenius distributions for elliptic curves with nontrivial rational torsion*, Acta Arith. **119** (2005), no. 1, 81–91, DOI 10.4064/aa119-1-6. MR2163519 (2006g:11106)

[Bir68] B. J. Birch, *How the number of points of an elliptic curve over a fixed prime field varies*, J. London Math. Soc. **43** (1968), 57–60. MR0230682 (37 #6242)

[CFJ$^+$11] Neil Calkin, Bryan Faulkner, Kevin James, Matt King, and David Penniston, *Average Frobenius distributions for elliptic curves over abelian extensions*, Acta Arith. **149** (2011), no. 3, 215–244, DOI 10.4064/aa149-3-2. MR2812425 (2012h:11083)

[CHT08] Laurent Clozel, Michael Harris, and Richard Taylor, *Automorphy for some l-adic lifts of automorphic mod l Galois representations*, Publ. Math. Inst. Hautes Études Sci. **108** (2008), 1–181, DOI 10.1007/s10240-008-0016-1. With Appendix A, summarizing unpublished work of Russ Mann, and Appendix B by Marie-France Vignéras. MR2470687 (2010j:11082)

[CS08] Alina Carmen Cojocaru and Igor E. Shparlinski, *Distribution of Farey fractions in residue classes and Lang-Trotter conjectures on average*, Proc. Amer. Math. Soc. **136** (2008), no. 6, 1977–1986, DOI 10.1090/S0002-9939-08-09324-6. MR2383504 (2009a:11035)

[Deu41] Max Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper* (German), Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272. MR0005125 (3,104f)

[DH66] H. Davenport and H. Halberstam, *Primes in arithmetic progressions*, Michigan Math. J. **13** (1966), 485–489. MR0200257 (34 #156)

[DH68] H. Davenport and H. Halberstam, *Corrigendum: "Primes in arithmetic progression"*, Michigan Math. J. **15** (1968), 505. MR0233778 (38 #2099)

[DP99] Chantal David and Francesco Pappalardi, *Average Frobenius distributions of elliptic curves*, Internat. Math. Res. Notices **4** (1999), 165–183, DOI 10.1155/S1073792899000082. MR1677267 (2000g:11045)

[DP04] Chantal David and Francesco Pappalardi, *Average Frobenius distribution for inerts in* $\mathbb{Q}(i)$, J. Ramanujan Math. Soc. **19** (2004), no. 3, 181–201. MR2139503 (2006i:11059)

[FM96] Etienne Fouvry and M. Ram Murty, *On the distribution of supersingular primes*, Canad. J. Math. **48** (1996), no. 1, 81–104, DOI 10.4153/CJM-1996-004-7. MR1382477 (97a:11084)

[HJX14] Jason Hedetniemi, Kevin James, and Hui Xue, *Champion primes for elliptic curves*, Integers **14** (2014), Paper No. A53, 8. MR3268583

[HSBT10] 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 (2011g:11106)

[Jam04] Kevin James, *Average Frobenius distributions for elliptic curves with 3-torsion*, J. Number Theory **109** (2004), no. 2, 278–298, DOI 10.1016/j.jnt.2004.06.012. MR2106483 (2005k:11110)

[Jon09] Nathan Jones, *Averages of elliptic curve constants*, Math. Ann. **345** (2009), no. 3, 685–710, DOI 10.1007/s00208-009-0373-1. MR2534114 (2010j:11090)

[JS11] Kevin James and Ethan Smith, *Average Frobenius distribution for elliptic curves defined over finite Galois extensions of the rationals*, Math. Proc. Cambridge Philos. Soc. **150** (2011), no. 3, 439–458, DOI 10.1017/S0305004111000041. MR2784769 (2012c:11123)

[JS13] Kevin James and Ethan Smith, *Average Frobenius distribution for the degree two primes of a number field*, Math. Proc. Cambridge Philos. Soc. **154** (2013), no. 3, 499–525, DOI 10.1017/S0305004112000631. MR3044212

[JTT$^+$14] K. James, B. Tran, M. Trinh, P. Wertheimer, and D. Zantout, *On the distribution of prime traces of frobenius for elliptic curves*, (preprint) (2014).

[JTT$^+$15] ———, *Extremal primes for elliptic curves*, (preprint) (2015).

[JY06] Kevin James and Gang Yu, *Average Frobenius distribution of elliptic curves*, Acta Arith. **124** (2006), no. 1, 79–100, DOI 10.4064/aa124-1-7. MR2262142 (2008a:11066)

[LT76] Serge Lang and Hale Trotter, *Frobenius distributions in* GL_2*-extensions*, Lecture Notes in Mathematics, Vol. 504, Springer-Verlag, Berlin-New York, 1976. Distribution of Frobenius automorphisms in GL_2-extensions of the rational numbers. MR0568299 (58 #27900)

[Raj98] C. S. Rajan, *Distribution of values of Hecke characters of infinite order*, Acta Arith. **85** (1998), no. 3, 279–291. MR1627843 (99e:11142)

[Shp13] Igor E. Shparlinski, *On the Lang-Trotter and Sato-Tate conjectures on average for polynomial families of elliptic curves*, Michigan Math. J. **62** (2013), no. 3, 491–505, DOI 10.1307/mmj/1378757885. MR3102527

[Smi10] Ethan Smith, *A Barban-Davenport-Halberstam asymptotic for number fields*, Proc. Amer. Math. Soc. **138** (2010), no. 7, 2301–2309, DOI 10.1090/S0002-9939-10-10303-7. MR2607859 (2011i:11162)

[Smi11] Ethan Smith, *A variant of the Barban-Davenport-Halberstam theorem*, Int. J. Number Theory **7** (2011), no. 8, 2203–2218, DOI 10.1142/S179304211100499X. MR2873149

[Tay08] 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 (2010j:11085)

Clemson University, Dept. Math. Sci., BOX 340975, Clemson, South Carolina 29634-0975

E-mail address: kevja@clemson.edu