Journal of Number Theory 164 (2016) 282–298

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Extremal primes for elliptic curves

Kevin James [a,*], Brandon Tran [c], Minh-Tam Trinh [d], Phil Wertheimer [b], Dania Zantout [a]

[a] *Department of Mathematical Sciences, Clemson University, Box 340975, Clemson, SC 29634, United States*
[b] *Department of Mathematics, University of Maryland, College Park, MD 20742, United States*
[c] *Department of Mathematics, MIT, Cambridge, MA 02142, United States*
[d] *Department of Mathematics, University of Chicago, Chicago, IL 60637, United States*

A R T I C L E   I N F O

Article history:
Received 26 June 2015
Received in revised form 25 December 2015
Accepted 2 January 2016
Available online 3 March 2016
Communicated by Steven J. Miller

Keywords:
Frobenius distributions
Trace of Frobenius
Distribution of primes
Elliptic curves
Lang–Trotter conjecture

A B S T R A C T

For an elliptic curve $E/\mathbb{Q}$, we define an extremal prime for E to be a prime p of good reduction such that the trace of Frobenius of E at p is $\pm\lfloor 2\sqrt{p}\rfloor$, i.e., maximal or minimal in the Hasse interval. Conditional on the Riemann Hypothesis for certain Hecke L-functions, we prove that if $\mathrm{End}(E) = \mathcal{O}_K$, where K is an imaginary quadratic field of discriminant $\neq -3, -4$, then the number of extremal primes $\leq X$ for E is asymptotic to $X^{3/4}/\log X$. We give heuristics for related conjectures.

1. Introduction

Let $E/\mathbb{Q}$ be an elliptic curve. Let p be a prime of good reduction for E, and let $\overline{E}/\mathbb{F}_p$ be the corresponding reduction. The *trace of Frobenius of E modulo p* can be defined

* Corresponding author.
E-mail addresses: kevja@clemson.edu (K. James), btran115@mit.edu (B. Tran), mqt@uchicago.edu (M.-T. Trinh), phil.wertheimer@gmail.com (P. Wertheimer), dzantou@g.clemson.edu (D. Zantout).

http://dx.doi.org/10.1016/j.jnt.2016.01.009

by $a_p(E) = p + 1 - \#\overline{E}(\mathbb{F}_p)$. Hasse's theorem [Si1, Theorem V.1.1] famously asserts that

$$-2\sqrt{p} \leq a_p(E) \leq +2\sqrt{p}. \tag{1.1}$$

We therefore say $[-2\sqrt{p}, +2\sqrt{p}]$ is the *Hasse interval* of p. By [De], every integer in the Hasse interval of a fixed prime p is the trace of Frobenius of some rational elliptic curve modulo p. However, if we instead fix $E/\mathbb{Q}$ and vary p, then the statistical distribution of the $a_p(E)$ is not completely understood.

Hereafter, if f, g denote functions of X, then the phrase "$f \sim g$ as $X \to \infty$" stands for $\lim_{X\to\infty} f/g = 1$. In comparison with the *unnormalized* traces $a_p(E)$, we know much more about the distribution of the *normalized* traces $b_p(E) = a_p(E)/2\sqrt{p}$. Specifically, the latter depends only on whether E has complex multiplication (CM). In the CM case, the distribution of the b_p is due to Hecke, cf. [He1,He2]:

Theorem 1.1 *(Hecke). If E has CM and $[a, b] \subseteq [-1, +1]$, then the distribution of the $b_p(E)$ has a spike at 0 of measure $1/2$ and*

$$\begin{aligned} &\#\{p \leq X \text{ of good reduction for } E : b_p(E) \in [a, b] \setminus \{0\}\} \\ &\sim \frac{1}{2\pi} \left(\int_a^b \frac{1}{\sqrt{1-t^2}} \, \mathrm{d}t \right) \frac{X}{\log X} \end{aligned} \tag{1.2}$$

as $X \to \infty$.

In the non-CM case, the analogous result was known as the Sato–Tate conjecture until its recent proof by Clozel, Harris, Shepherd-Barron and Taylor, cf. [CHT,T,HST], and [BGHT]:

Theorem 1.2 *(Clozel, Harris, Shepherd-Barron, Taylor). If E does not have CM and $[a, b] \subseteq [-1, +1]$, then*

$$\begin{aligned} &\#\{p \leq X \text{ of good reduction for } E : b_p(E) \in [a, b]\} \\ &\sim \frac{2}{\pi} \left(\int_\alpha^\beta \sqrt{1-t^2} \, \mathrm{d}t \right) \frac{X}{\log X} \end{aligned} \tag{1.3}$$

as $X \to \infty$.

Finally, the current hypothesis for the distribution of the unnormalized $a_p(E)$ is known as the Lang–Trotter conjecture [LT]:

Conjecture 1.3 *(Lang–Trotter). Let $E/\mathbb{Q}$ be an elliptic curve and let $r \in \mathbb{Z}$. If either $r \neq 0$ or E does not have CM, then*