CHAMPION PRIMES FOR ELLIPTIC CURVES

Jason Hedetniemi

Department of Mathematical Sciences, Clemson University, Clemson, South Carolina 29634, United States of America jhedetn@clemson.edu

Kevin James

Department of Mathematical Sciences, Clemson University, Clemson, South Carolina 29634, United States of America kevja@clemson.edu

Hui Xue

Department of Mathematical Sciences, Clemson University, Clemson, South Carolina 29634, United States of America huixue@clemson.edu

Received: , Revised: , Accepted: , Published:

Abstract

We show that the set of elliptic curves with trace of Frobenius at p a minimum has density one.

1. Introduction

Let $E_{a,b}$ be the elliptic curve $y^2 = x^3 + ax + b$ over \mathbb{F}_p . Suppose $E_{a,b}$ has good reduction at p. A famous result of Hasse (see [3, Theorem 7.3.1]) states that

$$|\#E_{a,b}(\mathbb{F}_p) - (p+1)| \le 2\sqrt{p}$$

or equivalently that

$$(p+1) - 2\sqrt{p} \le \#E_{a,b}(\mathbb{F}_p) \le (p+1) + 2\sqrt{p}.$$

Thus, a natural question to ask is how often the number of points on an elliptic curve hits its upper bound.

Definition 1. If p is such that $E_{a,b}$ is nonsingular over \mathbb{F}_p and $\#E_{a,b}(\mathbb{F}_p) = (p+1) + \lfloor 2\sqrt{p} \rfloor$, then we call p a champion prime for $E_{a,b}$.

By defining $a_p := p + 1 - \# E_{a,b}(\mathbb{F}_p)$, as a direct corollary to Hasse's Theorem we have that

$$|a_p| < 2\sqrt{p}.$$

Thus, we can equivalently say that p is a champion prime for $E_{a,b}$ if and only if $a_p = -\lfloor 2\sqrt{p} \rfloor$. We note that when $a_p = 0$, $E_{a,b}$ has a supersingular reduction at p. For more on supersingular primes see [4].

2. Champion Primes

We first show that champion primes do occur. This fact is a direct corollary of Deuring's Theorem.

Theorem 2 (Deuring). (see [2, 14.C]) Let p > 3 be prime, and let N = p + 1 - a be an integer, where $-2\sqrt{p} \le a \le 2\sqrt{p}$. Then the number of non-isomorphic elliptic curves E over \mathbb{F}_p which have $\#E(\mathbb{F}_p) = p + 1 - a$ is

$$\frac{(p-1)}{2}H(4p-a^2)$$

where H is the Hurwitz class number as defined in [1, Definition 5.3.6, p.234]. Please note the Hurwitz class number differs from the Kronecker class number, which has the same notation, and is sometimes used to state Deuring's Theorem as in [5].

Thus, if we are given a prime p, we can find an elliptic curve for which p is a champion. However, the alternative question is more difficult to answer. That is, does a given elliptic curve have a champion prime? To provide a partial answer to this question, we will consider a density argument. Namely, if we consider a box $\Omega_{AB} = [-A, A] \times [-B, B]$ in the plane for some $A, B > 0 \in \mathbb{R}$ and fix some bound X, we can calculate the density of curves in this box which have a champion prime less than X. Letting our box grow will then provide a density of all curves which have a champion prime less than X. If we then let X grow, we obtain the density of curves which have a champion prime. We will show this density is 1.

Throughout, we will assume X < A, B. We let

$$N(A, B, X) = \#\{(a, b) \in \Omega_{AB} : \exists \text{ prime } p, (4 s.t. p is a champion prime for $E_{a,b}$.}$$

Similarly, for fixed primes $4 < p_1 < p_2 < \cdots < p_k < X$ we let

$$N_{p_1p_2\cdots p_k}(A, B, X) = \#\{(a, b) \in \Omega_{AB} : E_{a, b} \text{ has champion prime } p_i, i = 1, 2, \dots, k\}$$

We define the density of curves in Ω_{AB} with a champion prime p, 4 to be

$$\delta(A, B, X) := \frac{N(A, B, X)}{4AB},$$

and if the limit exists, we define

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

to be the density of curves which have a champion prime p, 4 . Finally, if <math>A(X), B(X) are functions of X satisfying $A(X), B(X) \gg \exp((\frac{5}{8} + \epsilon)X)$ (see Theorem 3) we define

$$\delta := \lim_{X \to \infty} \delta(A(X), B(X), X)$$

to be the density of elliptic curves which have a champion prime. Using this notation, our first result is as follows.

Theorem 3. Suppose A, B and X < A, B are real numbers. We have the following formula for N(A, B, X), the number of curves $E_{a,b}$ with $(a, b) \in \Omega_{AB}$ for which there exists a prime p, 4 so that <math>p is a champion prime for $E_{a,b}$:

$$\begin{split} N(A,B,X) &= 4AB \bigg[1 - \prod_{4$$

Proof. Fix a prime 4 where <math>A, B > X. We first compute the number of integer pairs in Ω_{AB} for which the curve $E_{a,b}$ has good reduction at p and has p as a champion. Consider the region $[1, p] \times [1, p]$. Deuring's Theorem implies that the number of curves in this box which have good reduction at champion p is

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

Thus, by translating this $p \times p$ box within Ω_{AB} , we see that

$$N_p(A, B, X) = \left(\frac{2A}{p} + O(1)\right) \left(\frac{2B}{p} + O(1)\right) \frac{p-1}{2} H(4p - \lfloor 2\sqrt{p} \rfloor^2).$$
(1)

Let $\Delta = 4p - \lfloor 2\sqrt{p} \rfloor^2$, and note that $\Delta = O(\sqrt{p})$. Recall [2, p.319] that

$$H(\Delta) = 2 \sum_{\substack{f^2 \mid \Delta \\ \frac{-\Delta}{f^2} \equiv 0, 1 \pmod{4}}} \frac{h(-\Delta/f^2)}{w(-\Delta/f^2)}$$

INTEGERS: 13 (2013)

Also recall Dirichlet's class number formula [3, p.247]

$$h(-\Delta) = \frac{w(-\Delta)| - \Delta|^{1/2}}{2\pi} L(1, \chi_{-\Delta}).$$

Combining these two results with a result from [5, p.656], we get that

$$H(\Delta) \ll p^{1/4} (\log p)^2.$$

Thus, $H(4p - \lfloor 2\sqrt{p} \rfloor^2) = O(p^{1/4}(\log p)^2)$. If we apply this to equation (1) above, we find through expansion that

$$N_p(A, B, X) = \frac{4AB(p-1)}{2p^2} H(4p - \lfloor 2\sqrt{p} \rfloor^2) + O\left((A + B + p)p^{1/4}(\log p)^2\right).$$

By inclusion/exclusion

$$N(A, B, X) = \sum_{k=1}^{\pi(X)-2} (-1)^{k+1} \sum_{\substack{n=p_1\cdots p_k\\4 < p_i < X}} N_n(A, B, X).$$
(2)

By the Chinese Remainder Theorem, if $n = p_1 p_2 \cdots p_k$, then

$$N_n(A, B, X) = \left[\prod_{p|n} \frac{p-1}{2} H(4p - \lfloor 2\sqrt{p} \rfloor^2)\right] \left(\frac{2A}{n} + O(1)\right) \left(\frac{2B}{n} + O(1)\right)$$
$$= \frac{4AB}{n^2} \left[\prod_{p|n} \frac{p-1}{2} H(4p - \lfloor 2\sqrt{p} \rfloor^2)\right] + O\left(\frac{1}{2^k} (A + B + n)n^{1/4} \prod_{p|n} (\log p)^2\right).$$

where we have once again used the fact that $H(4p - \lfloor 2\sqrt{p} \rfloor^2) = O(p^{1/4}(\log p)^2)$. Thus, if we substitute this into (2) above, we find that

$$\begin{split} N(A,B,X) &= \sum_{k=1}^{\pi(X)-2} (-1)^{k+1} \sum_{\substack{n=p_1 \cdots p_k \\ 4 < p_i < X}} \left[\frac{4AB}{n^2} \Big[\prod_{p|n} \frac{p-1}{2} H(4p - \lfloor 2\sqrt{p} \rfloor^2) \Big] \right] \\ &+ O\left(\frac{1}{2^k} (A + B + n) n^{1/4} \prod_{p|n} (\log p)^2 \right) \Big] \\ &= 4AB \Big[1 - \prod_{4 < p < X} \Big[1 - \frac{p-1}{2p^2} H(4p - \lfloor 2\sqrt{p} \rfloor^2) \Big] \Big] \\ &+ O\Big(A \Big[\prod_{4 < p < X} \Big[1 + \frac{1}{2} p^{1/4} (\log p)^2 \Big] - 1 \Big] + B \Big[\prod_{4 < p < X} \Big[1 + \frac{1}{2} p^{1/4} (\log p)^2 \Big] - 1 \Big] \\ &+ \Big[\prod_{4 < p < X} \Big[1 + \frac{1}{2} p^{5/4} (\log p)^2 \Big] - 1 \Big] \Big). \end{split}$$

Note that

$$\begin{split} \prod_{4$$

We next note that

$$\sum_{4$$

and by partial summation,

$$\sum_{4$$

Since

$$\begin{split} \sum_{4$$

converges as $X \to \infty$, we see that

$$\exp\left(-\frac{X^{1/4}}{\log X} + O\left(\frac{X^{1/4}}{(\log X)^2}\right) + O(1)\right) \le \prod_{4
$$\le \exp\left(-\log(\log(X)) + O\left(\frac{1}{(\log X)^2}\right) + O(1)\right).$$$$

Now, since $\log(1+x) = \log(x) + O(\frac{1}{x})$, we see that

$$\prod_{4$$

The Prime Number Theorem then implies that

$$\prod_{4$$

Putting all of our results together, we find that

$$\begin{split} N(A, B, X) &= 4AB \bigg[1 - \prod_{4$$

This result gives us the following corollary, whose proof is immediate from Theorem 2.

Corollary 4. If A(X) and B(X) are chosen so that they satisfy

- $A(X) \gg \exp\left(\left(\frac{1}{4} + \epsilon_1\right)X\right)$
- $B(X) \gg \exp\left(\left(\frac{1}{4} + \epsilon_2\right)X\right)$
- $A(X)B(X) \gg \exp\left(\left(\frac{5}{4} + \epsilon_3\right)X\right)$

then

$$N(A(X), B(X), X) = 4A(X)B(X) \left[1 - \prod_{4$$

and

$$\delta(A(X), B(X), X) = \left[1 - \prod_{4$$

Furthermore, $\delta(A(X), B(X), X)$ equals the density of curves $E_{a,b}$ for which there exists a prime $4 such that <math>E_{a,b}$ has p as a champion prime.

Suppose we fix a box, centered at the origin, in the plane. Using our work above, we can now obtain the density of curves in this specific box which will have a champion prime less than a determined bound.

Corollary 5. Suppose A and B are fixed positive real numbers, and let

$$s = \left(\frac{8}{5} - \epsilon\right) \log(\min\{A, B\})$$

Then the density of curves $E_{a,b}$ with $|a| \leq A$, $|b| \leq B$ for which there exists a prime $4 such that <math>E_{a,b}$ has good reduction at p and p is a champion prime is given by

$$\left[1-\prod_{4$$

Our main density result, however, is as follows.

Theorem 6. Suppose A(X) and B(X) are chosen so that they satisfy the conditions of Corollary 4. Then the density of curves which have good reduction for some prime p and have p as a champion prime satisfies

$$\delta = \lim_{X \to \infty} \delta(A(X), B(X), X) = 1.$$

Proof. In the proof of Theorem 2 we showed that

$$\left[1 - \prod_{4$$

and that

$$\left[1 - \prod_{4$$

Given this, and Corollary 4, we now see that

$$\delta = \lim_{X \to \infty} \delta(A(X), B(X), X) = 1$$

which concludes the proof of Theorem 6.

We conclude with the following remarks.

- **Remark 7.** 1. If we wished to consider elliptic curves with trace of Frobenius at p a maximum, the results and proofs given above would still hold by the symmetry of $4p a^2$ in a. Such primes could be called "minimal primes," since the curve E would have the minimum possible number of points modulo p.
 - 2. In our proof, we chose Ω_{AB} to be centered at the origin. We could, in fact, center Ω_{AB} anywhere without altering our results.

References

- H. Cohen. A course in computational algebraic number theory. Graduate texts in mathematics. Springer-Verlag, 1993.
- [2] D.A. Cox. Primes of the Form X + Ny: Fermat, Class Field Theory, and Complex Multiplication. Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. John Wiley & Sons, 2011.
- [3] R.E. Crandall and C. Pomerance. *Prime numbers: a computational perspective*. Lecture notes in statistics. Springer, 2005.
- [4] N. Elkies. Distribution of supersingular primes. Astérisque, 198(200):127–132, 1991.
- [5] H. W. Lenstra, Jr. Factoring integers with elliptic curves. Ann. of Math. (2), 126(3):649-673, 1987.