CHAMPION PRIMES FOR ELLIPTIC CURVES

Jason Hedetniemi
Dept. of Mathematical Sciences, Clemson University, Clemson, South Carolina
jhedetn@clemson.edu

Kevin James
Dept. of Mathematical Sciences, Clemson University, Clemson, South Carolina
kevja@clemson.edu

Hui Xue
Dept. of Mathematical Sciences, Clemson University, Clemson, South Carolina
huixue@clemson.edu

Received: 11/10/12, Revised: 10/6/13, Accepted: 8/11/14, Published: 10/8/14

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

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

or equivalently that $(p+1) - 2\sqrt{p} \leq \#E_{a,b}(\mathbb{F}_p) \leq (p+1) + 2\sqrt{p}$. 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). ([2, Theorem 14.18]) *Let $p > 3$ be prime, and let $N = p+1-a$ be an integer, where $-2\sqrt{p} \leq a \leq 2\sqrt{p}$. 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

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

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

$$N_{p_1 p_2 \cdots p_k}(A, B, X) = \#\{(a, b) \in \Omega_{AB} : E_{a,b} \text{ has champion prime } p_i,\ i = 1, 2, \ldots, k\}.$$

We define the density of curves in Ω_{AB} with a champion prime p, $4 < p < X$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, $4 < p < X$. Finally, if $A(X), B(X)$ 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, $4 < p < X$ so that p is a champion prime for $E_{a,b}$:*

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

Proof. Fix a prime $4 < p < X$ where $A, B > X$. 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

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

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

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

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

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

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

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

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

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

Note that

$$\prod_{4<p<X}\left[1-\frac{p-1}{2p^2}H(4p-\lfloor 2\sqrt{p}\rfloor^2)\right] = \exp\Bigg(-\sum_{4<p<X}\frac{p-1}{2p^2}H(4p-\lfloor 2\sqrt{p}\rfloor^2) - \sum_{4<p<X}\sum_{k=2}^{\infty}\frac{(\frac{p-1}{2p^2}H(4p-\lfloor 2\sqrt{p}\rfloor^2))^k}{k}\Bigg).$$

We next note that

$$\sum_{4<p<X}\frac{p-1}{2p^2}H(4p-\lfloor 2\sqrt{p}\rfloor^2) \gg \sum_{4<p<X}\frac{1}{p} = \log(\log(X)) + O\left(\frac{1}{(\log X)^2}\right)$$

and by partial summation,

$$\sum_{4<p<X}\frac{p-1}{2p^2}H(4p-\lfloor 2\sqrt{p}\rfloor^2) \ll \frac{4X^{1/4}}{\log X} + O\left(\frac{X^{1/4}}{(\log X)^2}\right).$$

Since

$$\begin{aligned}
\sum_{4<p<X}\sum_{k=2}^{\infty}\frac{(\frac{p-1}{2p^2}H(4p-\lfloor 2\sqrt{p}\rfloor^2))^k}{k} &= \sum_{4<p<X}\sum_{k=2}^{\infty}\frac{(p-1)^k}{2^k k p^{2k}}H(4p-\lfloor 2\sqrt{p}\rfloor^2)^k \\
&\ll \sum_{4<p<X}\sum_{k=2}^{\infty}\frac{(p-1)^k}{2^k k p^{2k}}(p^{5k/16}) \\
&\le \sum_{4<p<X}\sum_{k=2}^{\infty}\frac{1}{(2p^{11/16})^k} \\
&= \sum_{4<p<X}\frac{1}{(2p^{11/16})^2}\cdot\frac{1}{1-\left(\frac{1}{2p^{11/16}}\right)} \\
&= \sum_{4<p<X}\frac{1}{4p^{22/16}-2p^{11/16}} \\
&\ll \sum_{4<p<X}\frac{1}{p^{22/16}}
\end{aligned}$$

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

$$\exp\left(-\frac{X^{1/4}}{\log X} + O\left(\frac{X^{1/4}}{(\log X)^2}\right) + O(1)\right) \le \prod_{4<p<X}\left[1-\frac{p-1}{2p^2}H(4p-\lfloor 2\sqrt{p}\rfloor^2)\right]$$

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

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

$$\prod_{4<p<X} \left[1 + \frac{1}{2} p^{1/4} \log(p)^2\right] = \exp\left(\frac{1}{4} \sum_{4<p<X} \log(p) + 2 \sum_{4<p<X} \log(\log(p)) - \sum_{4<p<X} \log(2) + \sum_{4<p<X} O\left(\frac{2}{p^{1/4}\log(p)^2}\right)\right).$$

The Prime Number Theorem then implies that

$$\prod_{4<p<X} \left[1 + \frac{1}{2} p^{1/4} (\log p)^2\right] = \exp\left(\frac{1}{4}X + o(X)\right)$$

and

$$\prod_{4<p<X} \left[1 + \frac{1}{2} p^{5/4} (\log p)^2\right] = \exp\left(\frac{5}{4}X + o(X)\right).$$

Putting all of our results together, we find that

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

□

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

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

and

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

Furthermore, $\delta(A(X),B(X),X)$ equals the density of curves $E_{a,b}$ for which there exists a prime $4 < p < X$ such that $E_{a,b}$ 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 with $0 < \epsilon < \frac{8}{5}$, 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 $4 < p < s$ such that $E_{a,b}$ has good reduction at p and p is a champion prime is given by

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

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

$$\left[1 - \prod_{4<p<X}\left[1 - \frac{p-1}{2p^2}H(4p - \lfloor 2\sqrt{p}\rfloor^2)\right]\right] \geq 1 - \exp\Bigg(-\log\log(X) + O\left(\frac{1}{(\log X)^2}\right) + O(1)\Bigg)$$

and that

$$\left[1 - \prod_{4<p<X}\left[1 - \frac{p-1}{2p^2}H(4p - \lfloor 2\sqrt{p}\rfloor^2)\right]\right] \leq 1 - \exp\Bigg(-\frac{X^{1/4}}{\log X} + O\left(\frac{X^{1/4}}{(\log X)^2}\right) + O(1)\Bigg).$$

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

[1] H. Cohen. *A course in computational algebraic number theory.* Graduate texts in mathematics. Springer-Verlag, 1993.

[2] D. 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.