# CHAMPION PRIMES FOR ELLIPTIC CURVES 

Jason Hedetniemi<br>Department of Mathematical Sciences, Clemson University, Clemson, South<br>Carolina 29634, United States of America<br>jhedetn@clemson.edu<br>Kevin James<br>Department of Mathematical Sciences, Clemson University, Clemson, South<br>Carolina 29634, United States of America<br>kevja@clemson.edu<br>Hui Xue<br>Department of Mathematical Sciences, Clemson University, Clemson, South<br>Carolina 29634, United States of America<br>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 $y^{2}=x^{3}+a x+b$ 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

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

or equivalently that

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

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 $\# E_{a, b}\left(\mathbb{F}_{p}\right)=$ $(p+1)+\lfloor 2 \sqrt{p}\rfloor$, then we call $p$ a champion prime for $E_{a, b}$.

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

$$
\left|a_{p}\right|<2 \sqrt{p}
$$

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 $-2 \sqrt{p} \leq a \leq 2 \sqrt{p}$. Then the number of non-isomorphic elliptic curves $E$ over $\mathbb{F}_{p}$ which have $\# E\left(\mathbb{F}_{p}\right)=p+1-a$ is

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

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 $\Omega_{A B}=[-A, A] \times[-B, B]$ 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

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

Similarly, for fixed primes $4<p_{1}<p_{2}<\cdots<p_{k}<X$ we let
$N_{p_{1} p_{2} \cdots p_{k}}(A, B, X)=\#\left\{(a, b) \in \Omega_{A B}: E_{a, b}\right.$ has champion prime $\left.p_{i}, i=1,2, \ldots, k\right\}$.

We define the density of curves in $\Omega_{A B}$ with a champion prime $p, 4<p<X$ to be

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

and if the limit exists, we define

$$
\delta(X):=\lim _{A \rightarrow \infty} \delta(A, A, X)
$$

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 $A(X), B(X) \gg \exp \left(\left(\frac{5}{8}+\epsilon\right) X\right)$ (see Theorem 3) we define

$$
\delta:=\lim _{X \rightarrow \infty} \delta(A(X), B(X), X)
$$

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 $(a, b) \in \Omega_{A B}$ for which there exists a prime $p, 4<p<X$ so that $p$ is a champion prime for $E_{a, b}$ :

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

Proof. Fix a prime $4<p<X$ where $A, B>X$. We first compute the number of integer pairs in $\Omega_{A B}$ 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

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

Thus, by translating this $p \times p$ box within $\Omega_{A B}$, we see that

$$
\begin{equation*}
N_{p}(A, B, X)=\left(\frac{2 A}{p}+O(1)\right)\left(\frac{2 B}{p}+O(1)\right) \frac{p-1}{2} H\left(4 p-\lfloor 2 \sqrt{p}\rfloor^{2}\right) \tag{1}
\end{equation*}
$$

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

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

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

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

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

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

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

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

By inclusion/exclusion

$$
\begin{equation*}
N(A, B, X)=\sum_{k=1}^{\pi(X)-2}(-1)^{k+1} \sum_{\substack{n=p_{1} \cdots p_{k} \\ 4<p_{i}<X}} N_{n}(A, B, X) \tag{2}
\end{equation*}
$$

By the Chinese Remainder Theorem, if $n=p_{1} p_{2} \cdots p_{k}$, then

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

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

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

Note that

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

We next note that

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

and by partial summation,

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

Since

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

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

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

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

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

The Prime Number Theorem then implies that

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

Putting all of our results together, we find that

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

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

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

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, 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

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

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

$$
\delta=\lim _{X \rightarrow \infty} \delta(A(X), B(X), X)=1
$$

Proof. In the proof of Theorem 2 we showed that
$\left[1-\prod_{4<p<X}\left[1-\frac{p-1}{2 p^{2}} H\left(4 p-\lfloor 2 \sqrt{p}\rfloor^{2}\right)\right]\right] \geq 1-\exp \left(-\log \log (X)+O\left(\frac{1}{(\log X)^{2}}\right)+O(1)\right)$
and that

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

Given this, and Corollary 4, we now see that

$$
\delta=\lim _{X \rightarrow \infty} \delta(A(X), B(X), X)=1
$$

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 $4 p-a^{2}$ 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 $\Omega_{A B}$ to be centered at the origin. We could, in fact, center $\Omega_{A B}$ 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.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.

