The absolute discriminant of the endomorphism ring of most reductions of a non-CM elliptic curve is close to maximal

Alina Carmen Cojocaru and Matthew Fitzpatrick

Abstract. Let $E/\mathbb{Q}$ be a non-CM elliptic curve. Assuming GRH, we prove that, for a set of primes $p$ of density 1, the absolute discriminant of the $\mathbb{F}_p$-endomorphism ring of the reduction of $E$ modulo $p$ is close to maximal.

1. Introduction

Let $E/\mathbb{Q}$ be an elliptic curve defined over the field of rational numbers, of conductor $N_E$, and let $p \nmid N_E$ be a prime of good reduction for $E$. We denote by $E_p/\mathbb{F}_p$ the reduction of $E$ modulo $p$ and we recall that it is an elliptic curve defined over the finite field $\mathbb{F}_p$ with $p$ elements, with the property that $|E_p(\mathbb{F}_p)| = p + 1 - a_p$ for some integer $a_p$ satisfying $|a_p| < 2\sqrt{p}$. Consequently, the polynomial $X^2 - a_pX + p$ has two complex conjugate roots, $\pi_p$ and $\overline{\pi}_p$, satisfying $|\pi_p| = \sqrt{p}$. Upon identifying any one of these roots, say $\pi_p$, with the $p$-th power Frobenius endomorphism of $E_p/\mathbb{F}_p$, we obtain the embeddings of imaginary quadratic orders $\mathbb{Z}[\pi_p] \leq \text{End}_{\mathbb{F}_p}(E_p) \leq \mathcal{O}_{\mathbb{Q}(\pi_p)}$ in the field $\mathbb{Q}(\pi_p)$, with $\mathcal{O}_{\mathbb{Q}(\pi_p)}$ denoting the maximal order of $\mathbb{Q}(\pi_p)$. Focusing on the discriminants of these orders, we obtain the relation

$$a_p^2 - 4p = b_p^2 \Delta_p,$$

where $\Delta_p$ denotes the discriminant of $\text{End}_{\mathbb{F}_p}(E_p)$ and $b_p$ denotes the unique positive integer satisfying the $\mathbb{Z}$-module isomorphism $\text{End}_{\mathbb{F}_p}(E_p)/\mathbb{Z}[\pi_p] \simeq \mathbb{Z}/b_p\mathbb{Z}$. If $p \geq 5$ is supersingular, then $\Delta_p \in \{-p, -4p\}$, while if $p$ is ordinary and $\text{End}_{\mathbb{Q}}(E) \not\simeq \mathbb{Z}$, then $\Delta_p$ equals the discriminant of the imaginary quadratic order $\text{End}_{\mathbb{Q}}(E)$.

The goal of this article is to focus on the setting $p$ ordinary and $\text{End}_{\mathbb{Q}}(E) \simeq \mathbb{Z}$ and to investigate the growth of the absolute discriminant $|\Delta_p|$ as a function of $p$, in particular in relation to the upper bound $4p - a_p^2$ arising from (1). In this setting, it was shown in [Sc89] that $|\Delta_p|$ does indeed grow with $p$: there

Key words and phrases: Elliptic curves, endomorphism rings, distribution of primes, sieve methods

2010 Mathematics Subject Classification: 11G05, 11G20, 11N05 (Primary), 11N36, 11N37, 11N57 (Secondary)

A.C.C. was partially supported by a Collaboration Grant for Mathematicians from the Simons Foundation under Award No. 318454.

February 25, 2020.
exists a positive constant $c(E)$ such that, for any prime $p \nmid N_E$,

$$|\Delta_p| \geq c(E) \frac{(\log p)^2}{(\log \log p)^{\frac{1}{4}}}.$$  

Moreover, it was shown in [Sc89] under the assumption of the Generalized Riemann Hypothesis (GRH for short) that there exists a positive constant $c'(E)$ and there exist infinitely many primes $p$ such that

$$|\Delta_p| \leq c'(E)p^{\frac{3}{2}} \log p.$$  

Under similar hypotheses, we will prove that, in fact, the growth of $|\Delta_p|$ is very close to the growth of $4p - a_p^2$ for most primes:

**Theorem 1.** Let $E/\mathbb{Q}$ be an elliptic curve of conductor $N_E$ with $\text{End}_{\mathbb{Q}}(E) \simeq \mathbb{Z}$. Assume that GRH holds for the division fields of $E$. Then, for any function $f : (0, \infty) \to (0, \infty)$ with $\lim_{x \to \infty} f(x) = \infty$,

$$\# \left\{ p \leq x : p \nmid N_E, |\Delta_p| \geq \frac{4p - a_p^2}{f(p)} \right\} \sim \pi(x),$$  

where $\pi(x)$ denotes the number of primes up to $x$.

The growth of $|\Delta_p|$ has also been investigated in other settings, including that of arbitrary elliptic curves over finite fields – see [LuSh07], [Sh10], [Sh15] – and that of finite Drinfeld modules – see [CoPa20].

Regarding Theorem 1, the proximity of $|a_p|$ to $\lfloor 2\sqrt{p} \rfloor$ was studied in several papers by K. James and his co-authors, such as [JaTrTrWeZa16] and [GiJa18] (see also the recent follow-up [DaGaMaPrTB20]). In [JaTrTrWeZa16], it is conjectured that, when $\text{End}_{\mathbb{Q}}(E) \simeq \mathbb{Z}$, the number of primes $p \leq x$ with $|a_p| = \lfloor 2\sqrt{p} \rfloor$, called extremal primes, is asymptotically equal to $C(E) \frac{4}{\log x}$ for some constant $C(E)$; in [GiJa18], it is proved that this conjecture holds on average over two-parameter families of elliptic curves $E/\mathbb{Q}$ (the majority of which have a trivial endomorphism ring $\text{End}_{\mathbb{Q}}(E)$). Thus extremal primes are not expected to contribute to the left hand side of (2).

The proof of Theorem 1 relies on the intimate connection between the integer $b_p$ and the discriminant $\Delta_p$ provided by equation (1), as well as on a characterization criterion of the divisors of $b_p$ through splitting conditions on $p$ in certain subfields of the division fields of $E$. Thanks to these connections, we approach the study of the growth of $|\Delta_p|$ as a potential application of the Chebotarev Density Theorem in an infinite family of number fields. As such, the assumption of GRH facilitates best possible error terms. Even under this assumption, the accumulation of all occurring error terms is overbearing. This we circumvent by resorting to an application of the Square Sieve, which, itself, incorporates another application of the Chebotarev Density Theorem.

**Notation.** In what follows, we use the standard $o$, $O$, $<$, and $\asymp$ notation: given suitably defined real functions $h_1, h_2$, we say that $h_1 = o(h_2)$ if $\lim_{x \to \infty} \frac{h_1(x)}{h_2(x)} = 0$; we say that $h_1 = O(h_2)$ or $h_1 \ll h_2$ if $h_2$ is positive valued and there exists a positive constant $C$ such that $|h_1(x)| \leq Ch_2(x)$ for all $x$ in the domain of $h_1$; we say that $h_1 \asymp h_2$ if $h_1, h_2$ are positive valued and $h_1 \ll h_2 \ll h_1$; we say that $h_1 = O_D(h_2)$ or
2. Proof of the main theorem

Let $E/Q$ be an elliptic curve of conductor $N_E$, with $\text{End}_{\overline{Q}}(E) \simeq \mathbb{Z}$. Let $f : (0, \infty) \rightarrow (0, \infty)$ be a function satisfying $\lim_{x \rightarrow \infty} f(x) = \infty$. Without loss of generality, we may assume that $f(x)$ is increasing, for we may replace $f(x)$ with $\sup\{ f(z) : z \leq x \}$. With notation as in Section 1, we observe that, thanks to (1), in order to prove (2) it is enough to prove
\[
\# \left\{ p \leq x : p \nmid N_E, b_p > \sqrt{f(p)} \right\} = o(\pi(x)).
\]
This we will do by exploring the divisibility properties of $b_p$.

As usual, for a positive integer $n$, we denote by $E[n]$ the group of $\overline{Q}$-rational points of $E$ of order dividing $n$ and by $\mathbb{Q}(E[n])$ the finite, Galois extension of $\mathbb{Q}$ generated by the $x$ and $y$ coordinates of the points of $E[n]$. We view the Galois group $\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ as a subgroup of $\text{GL}_2(\mathbb{Z}/n\mathbb{Z})$ under the residual modulo $n$ Galois representation of $E$. With this notation, the main result of [DuTo02] specialized to elliptic curves over $\mathbb{Q}$ states that, for any prime $p \nmid nN_E$, the reduction modulo $n$ of the integral matrix
\[
\begin{pmatrix}
\frac{a_p+b_p\delta_p}{2} & b_p \\
\frac{b_p(\Delta_p-\delta_p)}{4} & \frac{a_p-b_p\delta_p}{2}
\end{pmatrix},
\]
with $\delta_p := 0, 1$ according to whether $\Delta_p \equiv 0, 1 \pmod{4}$, gives a representative of the conjugacy class defined by the Artin symbol $\left( \frac{\mathbb{Q}(E[n])/\mathbb{Q}}{p} \right)$ in $\text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$. Consequently, upon defining
\[
J_n := \{ z \in \mathbb{Q}(E[n]) : \sigma(z) = z \quad \forall \sigma \in \text{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \text{ a scalar element} \},
\]
we obtain the criterion
\[
(4) \quad n \mid b_p \iff p \text{ splits completely in } J_n/\mathbb{Q}.
\]

For each prime $p$, there are unique positive integers $r_p$ and $m_p$, with $m_p$ squarefree, such that
\[
b_p^2|\Delta_p| = r_p^2m_p.
\]
Observe that we must have $b_p \mid r_p$, which gives $b_p \leq r_p$. Recalling [1], observe that
\[
(5) \quad 4p - a_p^2 = r_p^2m_p,
\]
which gives $r_p < 2\sqrt{p}$ and
\[
(6) \quad m_p = \frac{4p - a_p^2}{r_p^2} \leq \frac{4p}{b_p^2}.
\]
Furthermore, observe that the divisibility $n \mid b_p$ implies that $n \mid r_p$ and, in particular, that $n \leq r_p$. 

Now let us proceed to bounding from above the left hand side of (3). We fix an arbitrary parameter $z = z(x)$ satisfying $0 < z < x$ and define

$$g(z) := \inf \{ f(p) : z < p \leq x \}.$$ 

Note that $f(z) \leq g(z)$. We have the bounds

$$\# \left\{ p \leq x : p \nmid N_E, b_p > \sqrt{f(p)} \right\} \leq \pi(z) + \# \left\{ z < p \leq x : p \nmid N_E, b_p > \sqrt{g(z)} \right\} \leq \pi(z) + \sum_{\sqrt{g(z)} < n \leq 2\sqrt{x}} \# \left\{ p \leq x : p \nmid N_E, b_p = n \right\} \leq \pi(z) + S(\sqrt{g(z)}, 2\sqrt{x}),$$

where, for any $u < v \leq 2\sqrt{x}$,

$$S(u, v) := \sum_{u < n \leq v} \# \left\{ p \leq x : p \nmid N_E, b_p \equiv 0 \pmod{n} \right\}.$$

To estimate $S(\sqrt{g(z)}, 2\sqrt{x})$, it is natural to use criterion [1] and employ an effective version of the Chebotarev Density Theorem as proved in [LaOd77]. However, this strategy leads to limitations on the range of $n$ – indeed, looking at (3) below, we see that an application of the effective version of the Chebotarev Density Theorem to the entire sum $S(\sqrt{g(z)}, 2\sqrt{x})$ gives rise to an error term of $O_E(x \log x)$. As such, we adjust our strategy as follows: we fix an arbitrary parameter $y = y(x)$ with $\sqrt{g(z)} \leq y \leq 2\sqrt{x}$ and analyze each of the sums $S(\sqrt{g(z)}, y)$ and $S(y, 2\sqrt{x})$ separately, using criterion [4] for the first sum and using observation [5] for the second sum.

Specifically, rewriting $S(\sqrt{g(z)}, y)$ via [4] and using the effective Chebotarev Density Theorem, conditional upon GRH, as in [CoDu04, Prop. 4.2, p. 523], we obtain that

$$S(\sqrt{g(z)}, y) = \sum_{\sqrt{g(z)} < n \leq y} \frac{1}{[J_n : \mathbb{Q}]} \pi(x) + O_E \left( \sum_{\sqrt{g(z)} < n \leq y} x^\frac{1}{2} \log(N_E n x) \right) = \sum_{\sqrt{g(z)} < n \leq y} \frac{1}{[J_n : \mathbb{Q}]} \pi(x) + O_E \left( y x^\frac{1}{2} \log(y x) \right) = \sum_{\sqrt{g(z)} < n \leq y} \frac{1}{[J_n : \mathbb{Q}]} \pi(x) + O_E \left( y x^\frac{1}{2} \log x \right),$$

where in the last line we also used that $y < 2\sqrt{x}$.

We estimate the first term on the right hand side of the above equation by using that, thanks to Serre’s Open Image Theorem [Se72], the assumption $\text{End}_E(E) \simeq \mathbb{Z}$ gives

$$n^3 \ll_E [J_n : \mathbb{Q}] \ll n^3.$$
The upper bound is an immediate consequence of the inequality \(|J_n : \mathbb{Q}| \leq |\text{PGL}_2(\mathbb{Z}/n\mathbb{Z})|\), while the lower bound requires a more detailed analysis, which is presented in [CoJo20].

Together with Chebyshev’s Theorem, the lower bound in (9) gives that

\[
S \left( \sqrt{g(z)}, y \right) \ll_E \sum_{\sqrt{g(z)} < n \leq y} \frac{\pi(x)}{n^3} + yx^\frac{1}{2} \log x
\]

\[
\ll_E \pi(x) \int \frac{1}{\sqrt{g(z)}} \frac{dt}{t^3} + yx^\frac{1}{2} \log x
\]

\[
\ll_E \frac{x}{g(z) \log x} + yx^\frac{1}{2} \log x.
\]

To estimate \(S(y, 2\sqrt{x})\), we use (5) - (8) and obtain that

\[
S(y, 2\sqrt{x}) = \sum_{y < n \leq 2\sqrt{x}} \# \{p \leq x : p \nmid N_E, b_p \equiv 0 \pmod{n}\}
\]

\[
\leq \sum_{y < n \leq 2\sqrt{x}} \sum_{n \mid r} \# \{p \leq x : p \nmid N_E, r_p = r\}
\]

\[
\ll \sum_{y < r \leq 2\sqrt{x}} \tau(r) \# \{p \leq x : p \nmid N_E, r_p = r\}
\]

\[
= \sum_{y < r \leq 2\sqrt{x}} \tau(r) \# \{p \leq x : p \nmid N_E, 4p - a_p^2 = r^2m_p\}
\]

\[
\ll \sum_{m \leq 4x} \sum_{y < r \leq 2\sqrt{x}} \tau(r) \# \{p \leq x : p \nmid N_E, 4p - a_p^2 = r^2m\}
\]

where \(\tau(\cdot)\) is the divisor function. Using the standard bound \(\tau(r) \ll \epsilon r^\epsilon\) for any \(\epsilon > 0\) and observing that, for each squarefree \(m\) and each prime \(p\), there is at most one \(y < r \leq 2\sqrt{x}\) such that \(4p - a_p^2 = r^2m\), we deduce that

\[
S(y, 2\sqrt{x}) \ll \epsilon x^\epsilon \sum_{m \leq 4x} S_m(x),
\]

where

\[
S_m(x) := \# \{p \leq x : p \nmid N_E, m(4p - a_p^2) \text{ is a square}\}.
\]

The sum of the counting functions \(S_m(x)\) can be estimated as an indirect application of the conditional effective Chebotarev Density Theorem of [LaOd77] via the Square Sieve of [HB84] (see also the version of this sieve in [CoFoMu05]), by relying once again on GRH and on the assumption \(\text{End}_\mathbb{Q}(E) \simeq \mathbb{Z}\). Such an application was pursued in [CoDu04, CoFoMu05, CoDa08], and [Sh10]. While any of the estimates
proved in these papers suffices to conclude the proof of our theorem, we use the best among all of them, which is the one of [Sh10] Lem. 3.2, p. 260; its proof relies on [CoDa08] Thm. 3, p. 4] and [HB95] Thm. 1, p. 237]. We deduce that

\[ \sum_{\substack{m \leq \frac{x}{3} \\ m \text{ squarefree}}} S_m(x) \ll \varepsilon \frac{x^{\frac{14}{7}+\varepsilon}}{y^{\frac{13}{7}}}. \]

Next, by putting together (7), (10), (11), and (12), we obtain that

\[ \# \left\{ p \leq x : p \mid N_E, b_p > \sqrt{f(p)} \right\} \ll_{E,\varepsilon} \frac{z}{\log z} + \frac{x}{g(z) \log x} + yx^{\frac{14}{7}+\varepsilon} \frac{\log x}{y^{\frac{13}{7}}}. \]

The trivial endomorphism assumption is reflected in each of the second, third and fourth terms on the right hand side of the above estimate, while the GRH assumption is reflected in each of the third and fourth terms.

Finally, we choose \( y \asymp x^{19/40} \) and \( z \asymp x^{1/2} \), we recall that \( f(z) \leq g(z) \), and we use the assumption that \( f \) is increasing. We deduce that

\[ \# \left\{ p \leq x : p \mid N_E, b_p > \sqrt{f(p)} \right\} \ll_{E,\varepsilon} \frac{x^{\frac{14}{7}}}{\log x} + \frac{x}{f\left(\frac{x^{\frac{14}{7}}}{\log x}\right)} + \frac{\log x}{y^{\frac{13}{7}}}. \]

Note that, since \( \lim_{x \to \infty} f(x) = \infty \), the right hand side of the above estimate is \( o(\pi(x)) \). This completes the proof.

Acknowledgments. We thank Nathan Jones for helpful comments on a previous draft of this manuscript. We thank the anonymous referee for suggestions that added to the clarity of the paper.

References

[CoDa08] A.C. Cojocaru and C. David, Frobenius fields for elliptic curves, American Journal of Mathematics 130 (2008), no. 6, pp. 1535–1560.

[CoDu04] A.C. Cojocaru and W. Duke, Reductions of an elliptic curve and their Tate-Shafarevich groups, Mathematische Annalen 329 (2004), no. 3, pp. 513–534.

[CoFoMu05] A.C. Cojocaru, É. Fouvry, and M.R. Murty, The square sieve and the Lang-Trotter conjecture, Canadian Math. Journal 57 (2005), no. 6, pp. 1155–1177.

[CoJo20] A.C. Cojocaru and N. Jones, Degree bounds for projective division fields associated to elliptic modules with a trivial endomorphism ring, preprint 2020; https://arxiv.org/abs/2002.08411

[CoPa20] A.C. Cojocaru and M. Papikian, The growth of the discriminant of the endomorphism ring of the reduction of a rank 2 generic Drinfeld module, preprint 2020; https://arxiv.org/abs/2002.09582

[DaGaMaPrTB20] C. David, A. Gafni, A. Malik, N. Prabhu, and C.L. Turnage-Butterbaugh, Extremal primes for elliptic curves without complex multiplication, Proceedings of the American Mathematical Society 148 (2020), no. 3, pp. 929–943.

[DuTo02] W. Duke and Á. Tóth, The splitting of primes in division fields of elliptic curves, Experimental Mathematics 11 (2002), no. 4, pp. 555–565.

[HB84] D.R. Heath-Brown, The square sieve and consecutive squarefree numbers, Mathematische Annalen 266 (1984), no. 3, pp. 251–259.
[HB95] D.R. Heath-Brown, *A mean value estimate for real character sums*, Acta Arithmetica 72 (1995), no. 3, pp. 235–275.

[GiJa18] L. Giberson and K. James, *An average asymptotic for the number of extremal primes of elliptic curves*, Acta Arithmetica 183 (2018), no. 2, pp. 145–165.

[JaTrTrWeZa16] K. James, B. Tran, M-T. Trinh, P. Werheimer, and D. Zantout, *Extremal primes for elliptic curves*, Journal of Number Theory 164 (2016), pp. 282–298.

[LaOd77] J. Lagarias and A. Odlyzko, *Effective versions of the Chebotarev density theorem*, in: A. Fröhlich (Ed.), *Algebraic Number Fields*, Academic Press, New York, 1977, pp. 409–464.

[LuSh07] F. Luca and I.E. Shparlinski, *Discriminants of complex multiplication fields of elliptic curves over finite fields*, Canadian Math. Bulletin 50 (2007), no. 3, pp. 409–417.

[Sc89] R. Schoof, *The exponents of the groups of points on the reductions of an elliptic curve*, Arithmetic algebraic geometry (Texel, 1989), Progr. Math. Vol. 89, Birkhäuser Boston, Boston, MA, 1991, pp. 325–335.

[Se72] J-P. Serre, *Propriétés galoisiennes des points d’ordre fini des courbes elliptiques*, Inventiones Mathematicae 15 (1972), pp. 259–331.

[Sh10] I.E. Shparlinski, *Tate-Shafarevich groups and Frobenius fields of reductions of elliptic curves*, Quarterly Journal of Mathematics 61 (2010), no. 2, pp. 255–263.

[Sh15] I.E. Shparlinski, *Small discriminants of complex multiplication fields of elliptic curves over finite fields*, Czechoslovak Mathematical Journal 65 (140) (2015), no. 2, pp. 381–388.

(Alina Carmen Cojocaru)

- Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, 851 S Morgan St, 322 SEO, Chicago, 60607, IL, USA;

- Institute of Mathematics “Simion Stoilow” of the Romanian Academy, 21 Calea Grivitei St, Bucharest, 010702, Sector 1, Romania

E-mail address, Alina Carmen Cojocaru: cojocaru@uic.edu

(Matthew Fitzpatrick)

- Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, 851 S Morgan St, 322 SEO, Chicago, 60607, IL, USA;

E-mail address, Matthew Fitzpatrick: mfitzp6@uic.edu