Igor E. Shparlinski

Small discriminants of complex multiplication fields of elliptic curves over finite fields

Czechoslovak Mathematical Journal, Vol. 65 (2015), No. 2, 381–388

Persistent URL: `http://dml.cz/dmlcz/144277`

Czechoslovak Mathematical Journal, 65 (140) (2015), 381–388

SMALL DISCRIMINANTS OF COMPLEX MULTIPLICATION FIELDS OF ELLIPTIC CURVES OVER FINITE FIELDS

Igor E. Shparlinski, Sydney

(Received March 13, 2014)

Abstract. We obtain a conditional, under the Generalized Riemann Hypothesis, lower bound on the number of distinct elliptic curves E over a prime finite field $\mathbb{F}_p$ of p elements, such that the discriminant $D(E)$ of the quadratic number field containing the endomorphism ring of E over $\mathbb{F}_p$ is small. For almost all primes we also obtain a similar unconditional bound. These lower bounds complement an upper bound of F. Luca and I. E. Shparlinski (2007).

Keywords: elliptic curve; complex multiplication field; Frobenius discriminant

MSC 2010: 11G20, 11N32, 11R11

1. Introduction

1.1. Motivation and background. Let $p > 3$ be prime and let E be an elliptic curve over the field $\mathbb{F}_p$ of p elements given by an affine *Weierstrass equation* of the form

$$y^2 = x^3 + ax + b, \tag{1.1}$$

with coefficients $a, b \in \mathbb{F}_p$ such that $4a^3 + 27b^2 \neq 0$. In particular, there are $p^2 + O(p)$ suitable equations of the form (1.1). Furthermore, they generate $2p + O(1)$ distinct (that is, non-isomorphic over $\mathbb{F}_p$) curves, and for most of the curves there are exactly $(p-1)/2$ distinct equations (1.1), see [6] for a discussion of these properties.

We recall that the set $E(\mathbb{F}_p)$ of $\mathbb{F}_p$-rational points on any elliptic curve E forms an Abelian group (with a point at infinity as the identity element) of order which satisfies the *Hasse-Weil* bound

$$|\#E(\mathbb{F}_p) - p - 1| \leqslant 2p^{1/2}.$$

We refer to [10] for these and some other general properties of elliptic curves.

Moreover, we now define the *trace of Frobenius* of E as $t(E) = p + 1 - \#E(\mathbb{F}_p)$. We recall that the polynomial $X^2 - t(E)X + p$ is called the *characteristic polynomial* of E and plays an important role in the description of various properties of E. For example, it is also the characteristic polynomial of the Frobenius automorphism on E; that is, the p-th power automorphism. Furthermore, the quadratic field $\mathbb{K}_E = \mathbb{Q}(\sqrt{t(E)^2 - 4p})$ contains the ring of endomorphisms of E over $\mathbb{F}_p$ which is called the *complex multiplication field of E*.

In fact, writing

$$t(E)^2 - 4p = -d(E)^2 D(E)$$

with some integers $d(E)$ and $D(E)$, where $D(E)$ is square-free, we see that $\mathbb{K}_E = \mathbb{Q}(\sqrt{-D(E)})$ and one of $-D(E)$ or $-4D(E)$ is the discriminant of $\mathbb{K}_E$ (see [10]). Thus both $d(E)$ and $D(E)$ have recently been intensively studied, see [1], [2], [3], [7], [9] and references therein. For example, let $N_p(\Delta)$ be the number of pairs $(a, b) \in \mathbb{F}_p^2$ for which $d(E) \geqslant \Delta$ for the curve E given by (1.1). It has been shown in [7] that for any $\Delta \geqslant (\log p)^2$ we have

$$N_p(\Delta) = O\Big(\frac{p^2(\log p)^2}{\Delta}\Big). \tag{1.2}$$

1.2. Our results. Here we are interested in obtaining a lower bound on $N_p(\Delta)$. In fact, for $\Delta \leqslant p^{1/4}$ our bounds match (1.2) almost precisely. To derive such a lower bound for every prime we need to assume the Generalized Riemann Hypothesis (GRH). However, we obtain a similar unconditional result that holds for almost all primes.

Throughout the paper, the implied constants in the symbols "O", "$\ll$" and "$\gg$" may occasionally depend on the real parameter $\varepsilon > 0$ and are absolute otherwise. We recall that both $A \ll B$ and $B \gg A$ are equivalent to $A = O(B)$.

Theorem 1.1. *Assuming the GRH, for any positive $\Delta \leqslant p^{1/4}$ we have*

$$N_p(\Delta) \gg \frac{p^2}{\Delta \log p \log\log p}.$$

Furthermore, for almost all p we obtain an unconditional version of Theorem 1.1.

Theorem 1.2. *For a sufficiently large real $T \geqslant 2$ and any real Δ with $2 \leqslant \Delta \leqslant T^{1/4}$, for all but $O(T\Delta^{-1}\log\Delta)$ primes $p \leqslant T$ we have*

$$N_p(\Delta) \gg \frac{p^2}{\Delta(\log p)^2}.$$

Clearly Theorem 1.2 is nontrivial only if Δ grows with T and satisfies

$$\frac{\Delta}{\log T \log\log T} \to \infty$$

as $T \to \infty$.

2. Preliminaries

2.1. Bounds of character sums. Let, as usual, $\Lambda(v)$ denote the von Mangoldt function given by

$$\Lambda(v) = \begin{cases} \log l & \text{if } v \text{ is a power of a prime } l, \\ 0 & \text{if } v \text{ is not a prime power.} \end{cases}$$

We start with the following bound of Legendre symbols, which can be found in [8], Chapter 13.

Lemma 2.1. *Assuming the GRH, for any real $L \geqslant 1$ we have*

$$\sum_{v \in [L, 2L]} \Big(1 - \frac{v}{L}\Big) \Lambda(v) \Big(\frac{p}{v}\Big) = O(L^{1/2} \log p).$$

Note that the sum of Lemma 2.1 slightly differs from the traditional sum with the Legendre symbols (v/p). However, it is easy to see that (p/v) is multiplicative character modulo $4p$.

A simple combinatorial argument now implies the following statement:

Corollary 2.2. *Assuming the GRH, there are absolute constants C, $c > 0$ that for $L \geqslant C(\log p)^2$ there are at least $cL/\log L$ primes $l \in [L, 2L]$ with*

$$\Big(\frac{p}{l}\Big) = 1.$$

The following statement is well-known and follows immediately from the Pólya-Vinogradov inequality, see [4], Theorem 12.5. As usual, we use $\pi(x)$ to denote the number of primes $p \leqslant x$.

Lemma 2.3. *Let $T > 2L \geqslant 1$ be sufficiently large real numbers. For all but $O(TL^{-1}\log L + L\log L)$ primes $p \in [T, 2T]$, there are at least $\frac{1}{3}L\log L$ primes $l \in [L, 2L]$ with*

$$\left(\frac{p}{l}\right) = 1.$$

P r o o f. Let $\mathcal{L}$ be the set of primes $l \in [L, 2L]$ and let $\mathcal{P}$ be the set of primes $p \in [T, 2T]$ such that

$$\left(\frac{p}{l}\right) = 1, \quad l \in \mathcal{L}$$

for less than $\frac{1}{3}L\log L$ primes $l \in [L, 2L]$.

Note that the sets $\mathcal{P}$ and $\mathcal{L}$ are disjoint. Hence, by the prime number theorem, for every $p \in \mathcal{P}$,

$$\sum_{l\in\mathcal{L}}\left(\frac{p}{l}\right) \leqslant -\Big(\#\mathcal{L} - \frac{L}{3}\log L\Big) + \frac{L}{3}\log L \leqslant \Big(\frac{1}{3} + O(1)\Big)\#\mathcal{L}$$

as $L \to \infty$. So, for the double sum

$$W \leqslant \sum_{p\in\mathcal{P}}\bigg|\sum_{l\in\mathcal{L}}\left(\frac{p}{l}\right)\bigg|$$

we have

$$W \geqslant \frac{1}{4}\#\mathcal{L}\#\mathcal{P}, \tag{2.1}$$

provided L is large enough.

Using the Cauchy inequality and expanding the summation to all integers $k \in [T, 2T]$ we derive

$$|W|^2 \leqslant \#\mathcal{P}\sum_{p\in\mathcal{P}}\bigg|\sum_{l\in\mathcal{L}}\left(\frac{p}{l}\right)\bigg|^2 \leqslant \#\mathcal{P}\sum_{k\in[T,2T]}\bigg|\sum_{l\in\mathcal{L}}\left(\frac{k}{l}\right)\bigg|^2. \tag{2.2}$$

Now squaring out and changing the order of summations, we obtain

$$W^2 \leqslant \#\mathcal{P}\sum_{l_1,l_2\in\mathcal{L}}\sum_{k\in[T,2T]}\left(\frac{k}{l_1l_2}\right).$$

Finally, estimating the inner sum trivially for $l_1 = l_2$ and using the Pólya-Vinogradov inequality for $l_1 \neq l_2$, see [4], Theorem 12.5, we derive

$$W^2 \ll \#\mathcal{P}(\#\mathcal{L}T + \#\mathcal{L}^2L\log L). \tag{2.3}$$

Comparing (2.1) and (2.3) and using the prime number theorem, we obtain

$$(\#\mathcal{L}\#\mathcal{P})^2 \ll \#\mathcal{P}(\#\mathcal{L}T + \#\mathcal{L}^2L\log L).$$

So the desired result follows. $\square$

Note that using the Burgess bound, see [4], Theorem 12.6, in the proof of Lemma 2.3 one can obtain a series of other estimates. See also the comments in Section 4.

2.2. Hilbert class numbers and the distribution of the number of $\mathbb{F}_q$ rational points on elliptic curves. We recall that two elliptic curves are isogenous over $\mathbb{F}_p$ if they have the same number of $\mathbb{F}_p$-rational points and thus have the same trace of Frobenius.

We need bounds of Lenstra [6] on the number of curves (1.1) in the same isogeny class over $\mathbb{F}_p$, which we formulate in the following form convenient for our applications.

For a set of integers $\mathcal{N}$ we use $M_p(\mathcal{N})$ to denote the number of pairs $(a, b) \in \mathbb{F}_p^2$ such that for the corresponding curve (1.1) we have $\#E(\mathbb{F}_p) \in \mathcal{N}$.

The following two statements are direct combinations of the arguments of Lenstra [6], Sections 1.6 and 1.9.

Lemma 2.4. *Assuming the GRH, for any set of integers $\mathcal{N} \subseteq [p - p^{1/2}, p + p^{1/2}]$ we have*

$$M_p(\mathcal{N}) \gg \frac{\#\mathcal{N} p^{3/2}}{\log\log p}.$$

Lemma 2.5. *For any set of integers $\mathcal{N} \subseteq [p-p^{1/2}, p+p^{1/2}]$ of cardinality $\#\mathcal{N} \geqslant 3$ we have*

$$M_p(\mathcal{N}) \gg \frac{\#\mathcal{N} p^{3/2}}{\log p}.$$

3. Proofs of the main results

Proof of Theorem 1.1. By Corollary 2.2, we can find a set $\mathcal{R}$ of at least $\#\mathcal{R} \gg \Delta/\log\Delta$ primes $l \in [\Delta, 2\Delta]$ for which p is a quadratic residue. Thus the congruence $4p \equiv u^2 \pmod{l}$ has a solution u. Using the Hensel lifting, we can now find a solution s, $0 \leqslant s \leqslant l^2 - 1$, to the congruence $4p \equiv s^2 \pmod{l^2}$. So, provided that $\Delta \leqslant p^{1/4}$, there are

$$\frac{2p^{1/2}}{l^2} + O(1) \gg p^{1/2}\Delta^{-2} \tag{3.1}$$

integers $N \in [p - p^{1/2}, p + p^{1/2}]$ that satisfy the congruences

$$N - p - 1 \equiv s \pmod{l^2}.$$

Clearly the number $N \in [p - p^{1/2}, p + p^{1/2}]$ may come from at most

$$M \ll \frac{\log p}{\log \Delta} \tag{3.2}$$

distinct primes $l \in \mathcal{R}$. Thus, the bounds (3.1) and (3.2) imply that the above construction produces a set $\mathcal{N}$ of integers $N \in [p - p^{1/2}, p + p^{1/2}]$ of cardinality

$$\#\mathcal{N} \gg \#\mathcal{R} M^{-1} p^{1/2} \Delta^{-2} \gg \frac{p^{1/2}}{\Delta \log p}$$

such that for $t = N - p - 1$ we have

$$t^2 - 4p \equiv s^2 - 4p \equiv 0 \pmod{l^2}. \tag{3.3}$$

By Lemma 2.4, this leads to

$$\frac{\#\mathcal{N} p^{3/2}}{\log \log p} \gg \frac{p^2}{\Delta \log p \log \log p}$$

non-isomorphic curves E over $\mathbb{F}_p$ with $p + 1 - t(E) \in \mathcal{N}$ and thus by (3.3) we have $d(E) \geqslant \Delta$. $\square$

P r o o f of Theorem 1.2. We first discard

$$O(T\Delta^{-1} \log \Delta + \Delta \log \Delta) = O(T\Delta^{-1} \log \Delta)$$

(as $\Delta \leqslant T^{1/4}$) primes $p \leqslant T$, described in Lemma 2.3.

After this the proof is identical to that of Theorem 1.1, except that we use the unconditional bound of Lemma 2.5. This leads to

$$\frac{\#\mathcal{N} p^{3/2}}{\log p} \gg \frac{p^2}{\Delta (\log p)^2}$$

non-isomorphic curves E over $\mathbb{F}_p$ with $\#E(\mathbb{F}_p) \in \mathcal{N}$ and thus by (3.3) we have $d(E) \geqslant \Delta$. $\square$

4. Remarks

Note that the bound with $d(E) \geqslant \Delta$ immediately implies the upper bound on $D(E) \ll p/\Delta^2$. Curves with small Frobenius discriminants can be of interest because the degree and the height of the coefficients of the Hilbert class polynomial $H_{D(E)}(Z)$ are smaller than their "generic values". Counting such curves can be of independent interest. Note that one of the approaches is to try to make the value of $|t(E)^2 - 4p|$ small. For this one can take values of t close to $2p^{1/2}$. For instance, if $|2p^{1/2} - t(E)| \leqslant h$ then $D(E) \leqslant |t(E)^2 - 4p| \ll hp^{1/2}$. However, this approach seems to produce fewer curves than that based on Theorems 1.1 and 1.2. This is because there are very few curves in isogeny classes with traces close to $2p^{1/2}$ (or to $-2p^{1/2}$). Actually this is exactly the reason why in Lemmas 2.4 and 2.5 only the middle half of the Hasse-Weil interval $[p - 2p^{1/2}, p + 2p^{1/2}]$ is considered.

Unfortunately, our approach does not work for $\Delta \geqslant p^{1/4}$ and it is certainly interesting to obtain a lower bound on $N_p(\Delta)$ for larger values of Δ, preferably all the way up its natural limit $\Delta \leqslant 2p^{1/2}$.

As we have mentioned, Theorem 1.2 is nontrivial only if Δ is of order at least $\log T \log\log T$. It is quite plausible that using the ideas of Konyagin and Shparlinski [5], one can lower this limit. The idea is, instead of extending the summation to all integers $k \in [T, 2T]$ in (2.2), we extend it only to a sparse set of integers $k \in [T, 2T]$, free of small prime divisors. Then sieving arguments are used to estimate nontrivial character sums along these integers, while the trivial sums are now smaller (as the set of k is now smaller as well).

References

[1] *A. C. Cojocaru*: Questions about the reductions modulo primes of an elliptic curve. Number Theory (H. Kisilevsky et al., eds.). Papers from the 7th Conference of the Canadian Number Theory Association, University of Montreal, Canada, 2002, CRM Proc. Lecture Notes 36, American Mathematical Society, Providence, 2004, pp. 61–79.

[2] *A. C. Cojocaru, W. Duke*: Reductions of an elliptic curve and their Tate-Shafarevich groups. Math. Ann. *329* (2004), 513–534.

[3] *A. C. Cojocaru, E. Fouvry, M. R. Murty*: The square sieve and the Lang-Trotter conjecture. Can. J. Math. *57* (2005), 1155–1177.

[4] *H. Iwaniec, E. Kowalski*: Analytic Number Theory. Amer. Math. Soc. Colloquium Publications 53, American Mathematical Society, Providence, 2004.

[5] *S. V. Konyagin, I. E. Shparlinski*: Quadratic non-residues in short intervals. To appear in Proc. Amer. Math. Soc.

[6] *H. W. Lenstra,* Jr.: Factoring integers with elliptic curves. Ann. Math. (2) *126* (1987), 649–673.

[7] *F. Luca, I. E. Shparlinski*: Discriminants of complex multiplication fields of elliptic curves over finite fields. Can. Math. Bull. *50* (2007), 409–417.

[8] *H. L. Montgomery*: Topics in Multiplicative Number Theory. Lecture Notes in Mathematics 227, Springer, Berlin, 1971.

[9] *I. E. Shparlinski*: Tate-Shafarevich groups and Frobenius fields of reductions of elliptic curves. Q. J. Math. *61* (2010), 255–263.
[10] *J. H. Silverman*: The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics 106, Springer, New York, 2009.

Author's address: Igor E. Shparlinski, Department of Pure Mathematics, School of Mathematics and Statistics, University of New South Wales, Sydney, New South Wales 2052, Australia, e-mail: igor.shparlinski@unsw.edu.au.