Tate-Shafarevich Groups and Frobenius Fields of Reductions of Elliptic Curves

IGOR E. SHPARLINSKI
Dept. of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

February 1, 2008

Abstract

Let $E/\mathbb{Q}$ be a fixed elliptic curve over $\mathbb{Q}$ which does not have complex multiplication. Assuming the Generalized Riemann Hypothesis, A. C. Cojocaru and W. Duke have obtained an asymptotic formula for the number of primes $p \leq x$ such that the reduction of $E$ modulo $p$ has a trivial Tate-Shafarevich group. Recent results of A. C. Cojocaru and C. David lead to a better error term. We introduce a new argument in the scheme of the proof which gives further improvement.

2000 Mathematics Subject Classification: 11G07, 11N35, 11L40, 14H52

1 Introduction

Let $E/\mathbb{Q}$ be a fixed elliptic curve over $\mathbb{Q}$ of conductor $N$, we refer to [7] for the background on elliptic curves. For a prime $p \nmid N$ we denote the reduction of $E$ modulo $p$ as $E_p/\mathbb{F}_p$.

As in [2], we use $\text{III}_p$ to denote the Tate-Shafarevich group of $E_p/\mathbb{F}_p$ which is an analogue of the classical Tate-Shafarevich group (see [7]) defined with
respect to $E_p$ and the function field $\mathbb{K}$ of $E_p$, that is,

$$\Pi_p = \Pi(E_p/K),$$

we refer to [2] for a precise definition.

Let $\pi_{TS}(x)$ be the counting function of primes $p \nmid N$ for which $\Pi_p$ is trivial. More formally,

$$\pi_{TS}(x) = \#\{p \leq x \mid p \nmid N, \ #\Pi_p = 1\}.$$

As usual, we also use $\pi(x)$ to denote the number of primes $p \leq x$.

Cojocaru and Duke [2, Proposition 5.3] have proved that if $E$ does not have complex multiplication then under the Generalized Riemann Hypothesis (GRH) the following asymptotic formula

$$\pi_{TS}(x) = \alpha \pi(x) + R(x)$$

holds for some explicitly defined constant $\alpha$ depending on $E$, where

$$R(x) = O(x^{53/54+o(1)})$$

(hereafter implicit constants in the symbols ‘$O’,$ ‘$\ll$’ and ‘$\gg$’ may depend on $E$). Furthermore, we have $\alpha > 0$ if and only if $E$ has an irrational point of order two.

The proof of (2) is based on the square sieve of Heath-Brown [4] combined with a bound of certain character sums. This character sum has been estimated in a sharper way by Cojocaru and David [1, Theorem 3], who also noticed that using their estimate in the proof of (2) from [2] reduces the error term in (1) to

$$R(x) = O(x^{41/42+o(1)}).$$

Here we introduce some additional element in the approach of [2], which we also combine with the aforementioned stronger bound of character sums of [1, Theorem 3], to obtain a further improvement of (2) and (3). Namely, we obtain an extra saving from taking advantage of averaging over a certain parameter $m$, which appears in the argument of Cojocaru and Duke [2]. To take the most out of this, we apply the bound of double character sums due to Heath-Brown [5]. This yields the following estimate:

**Theorem 1.** Suppose $E$ does not have complex multiplication and also assume that the GRH holds. Then the asymptotic formula (1) holds with

$$R(x) = O(x^{39/40+o(1)}).$$

2
The main goal of \cite{1} is to estimate \( \Pi(I_K, x) \) which is the number of primes \( p \leq x \) with \( p \nmid N \) and such that a root of the Frobenius endomorphism of \( E_p/\mathbb{F}_p \) generates the imaginary quadratic field \( I_K \). The famous Lang-Trotter conjecture, which asserts that if \( E \) does not have complex multiplication then

\[
\Pi(I_K, x) \sim \beta(I_K) \frac{x^{1/2}}{\log x}
\]

with some constant \( \beta > 0 \) depending on \( I_K \) (and on \( E \)), remains open. However, under the GRH, the bound

\[
\Pi(I_K, x) \leq C(I_K) \frac{x^{4/5}}{\log x} \tag{4}
\]

has been given by Cojocaru and David \cite{1, Theorem 2}, where the constant \( C(I_K) \) depends on \( I_K \) (and on \( E \)). Moreover, using the aforementioned new bound of character sums, Cojocaru and David \cite{1, Corollary 4} have given a weaker, but uniform with respect to \( I_K \), bound

\[
\Pi(I_K, x) = O \left( x^{13/14} \log x \right) \tag{5}
\]

For real \( 4x \geq u > v \geq 1 \), we now consider the average value

\[
\sigma(x; u, v) = \sum_{\substack{0 < v \leq m \leq u \\ m \text{ squarefree}}} \Pi(I_K_m, x)
\]

where \( I_K_m = \mathbb{Q}(\sqrt{-m}) \). We also put

\[
\sigma(x; v, v) = \sigma(x; v).
\]

Clearly, the nonuniform bound (4) cannot be used to estimate \( \sigma(x; u, v) \), while (5) immediately implies that uniformly over \( u \),

\[
\sigma(x; u, v) = O \left( v x^{13/14} \log x \right) \tag{6}
\]

Since we trivially have \( \sigma(x; u, v) \leq \pi(x) \), the above bound is nontrivial only for \( v \leq x^{1/14} \). Here we obtain a more accurate bound which remains nontrivial for values of \( v \) up to \( x^{1/13 - \varepsilon} \) for arbitrary \( \varepsilon > 0 \) and sufficiently large \( x \).
Theorem 2. Suppose $E$ does not have complex multiplication and also assume that the GRH holds. Then for $4x \geq u > v \geq 1$ we have

$$\sigma(x; u, v) \leq (vx)^{55/59+o(1)}$$

and

$$\sigma(x; v) \leq v^{13/14}x^{13/14+o(1)}.$$

It is easy to check that the first bound of Theorem 2 is nontrivial and stronger than (6) in the range

$$x^{3/56+\varepsilon} \leq v \leq x^{4/55-\varepsilon}$$

for any fixed $\varepsilon > 0$ and sufficiently large $x$.

Let

$$\mathcal{M}(x) = \{m \in \mathbb{Z} \mid \Pi(\mathbb{K}_m, x) > 0\}$$

(where as before $\mathbb{K}_m = \mathbb{Q}(\sqrt{-m})$). An immediate implication of (5) is the bound

$$\#\mathcal{M}(x) \gg \frac{x^{1/14}}{\log x^2}.$$

see [1, Corollary 4]. We now observe that the first inequality of Theorem 2 implies that for almost all primes $p \leq x$ the corresponding Frobenius field is of discriminant at least $x^{1/13+o(1)}$. In particular, we have

$$\max_{m \in \mathcal{M}(x)} m \geq x^{1/13+o(1)}.$$

2 Character Sums

For $p \nmid N$, we put

$$a_p = p + 1 - \#E_p(\mathbb{F}_p),$$

where $\#E_p(\mathbb{F}_p)$ is the number of $\mathbb{F}_p$-rational points of $E_p$. When $p \mid N$, we simply put $a_p = 1$. We recall that by the Hasse bound, $|a_p| \leq 2p^{1/2}$, see [7].

We recall that the size of $\text{III}_p$ is given by

$$\#\text{III}_p = \begin{cases} s_p^2/4, & \text{if } 4p - a_p^2 \text{ is odd}, \\ s_p^2/4, & \text{if } 4p - a_p^2 \text{ is even}, \end{cases}$$

where the integer $s_p$ is uniquely defined by the relation $4p - a_p^2 = s_p^2r_p$ with a squarefree integer $r_p$ (clearly $4p - a_p^2 \equiv 0, 3 \pmod{4}$). Thus, it is natural
to use the square sieve \cite{4} to study the distribution of \#III_p. This requires nontrivial bounds of sums with the Jacobi symbols with \(4p - a_p^2\) modulo products \(\ell_1\ell_2\) of two distinct primes. Accordingly, for an odd positive integer \(n\) we define

\[
U(x; n) = \sum_{p \leq x} \left( \frac{a_p^2 - 4p}{n} \right),
\]

where, as usual, \((k/n)\) denotes the Jacobi symbol of \(k\) modulo \(n\).

The sum has been estimated by Cojocaru, Fouvry and Murty \cite{3} and then sharpened by Cojocaru and Duke \cite[Proposition 4.3]{2}. Furthermore, when \(n = \ell_1\ell_2\) is a product of two distinct primes, which is the only relevant case for this paper, Cojocaru and David \cite[Theorem 3]{1} give a stronger bound which we present here in the following form:

\textbf{Lemma 3.} Suppose \(E\) does not have complex multiplication and also assume that the GRH holds. Then for any real \(x \geq 1\) and for any distinct primes \(\ell_1, \ell_2 > 3\), we have

\[
U(x; \ell_1\ell_2) = \frac{1}{(\ell_1^2 - 1)(\ell_2^2 - 1)} \pi(x) + O((\ell_1\ell_2)^3 x^{1/2} \log(\ell_1\ell_2x)).
\]

We also need the following special case of the classical Burgess bound, see \cite[Theorems 12.5]{6} taken with \(r = 2\).

\textbf{Lemma 4.} For any real \(u \geq v \geq 1\) and an odd square-free integer \(s\),

\[
\sum_{u-v \leq m \leq u} \left( \frac{m}{s} \right) \ll v^{1/2} s^{3/16 + o(1)}.
\]

As we have mentioned, a part of our improvement of \(\text{(2)}\) and \(\text{(3)}\) comes from bringing into the argument of \(\text{(2)}\) the following result of Heath-Brown \cite{5}.

\textbf{Lemma 5.} For any real positive \(X\) and \(Y\) with \(XY \to \infty\) and complex-valued function \(f(m)\),

\[
\sum_{s \leq Y \text{ odd squarefree}} \left| \sum_{m \leq X \text{ squarefree}} f(m) \left( \frac{m}{s} \right) \right|^2 \leq (XY)^{o(1)} (X + Y) \sum_{1 \leq m \leq X} |f(m)|^2.
\]
3 Square Multiples and Divisors of $4p - a_p^2$

As in [2], we define

$$S_m(x) = \# \{ p \leq x \mid m(4p - a_p^2) \text{ is a square} \}.$$ 

**Lemma 6.** Suppose $E$ does not have complex multiplication and also assume that the GRH holds. Then for any real $4x \geq u \geq v \geq 1$, we have

$$\sum_{u-v \leq m \leq u \atop m \text{ squarefree}} S_m(x) \leq v^{55/59} x^{55/59 + o(1)}.$$ 

**Proof.** Fix some

$$z \geq (\log u)^2$$

and assume that $x$ is sufficiently large. Then by [2] Bound (37) we have

$$S_m(x) \ll \frac{1}{\pi(z)^2} \sum_{n \leq 4x^2} w_m(n) \left( \sum_{z \leq \ell \leq 2z} \left( \frac{n}{\ell} \right) \right)^2,$$  

where the inner sum is taken over all primes $\ell \in [z, 2z]$ and

$$w_m(n) = \# \{ p \leq x \mid m(4p - a_p^2) = n \}.$$ 

We now derive

$$\sum_{u-v \leq m \leq u \atop m \text{ squarefree}} S_m(x) \leq \sum_{u-v \leq m \leq u} S_m(x)$$

$$\leq \frac{1}{\pi(z)^2} \sum_{u-v \leq m \leq u \atop n \leq 4x^2} \sum_{z \leq \ell \leq 2z} \left( \frac{n}{\ell} \right)^2$$

$$= \frac{1}{\pi(z)^2} \sum_{u-v \leq m \leq u} \sum_{z \leq \ell_1, \ell_2 \leq 2z} \sum_{n \leq 4x^2} w_m(n) \left( \frac{n}{\ell_1 \ell_2} \right).$$

Separating $\pi(z)$ diagonal terms with $\ell_1 = \ell_2$, we obtain

$$\sum_{u-v \leq m \leq u} S_m(x) \ll \frac{1}{\pi(z)} \Sigma_1 + \frac{1}{\pi(z)^2} \Sigma_2.$$  

(9)
where
\[ \Sigma_1 = \sum_{u-v \leq m \leq u} \sum_{n \leq 4x^2} w_m(n), \]
\[ \Sigma_2 = \sum_{u-v \leq m \leq u} \sum_{n \leq 4x^2} \sum_{z \leq \ell_1 < \ell_2 \leq 2z} w_m(n) \left( \frac{n}{\ell_1 \ell_2} \right). \]

We estimate the first sums trivially as
\[ \Sigma_1 \leq \sum_{u-v \leq m \leq u} \pi(x) \leq v\pi(x). \] (10)

For the second sum, we note that
\[ \sum_{n \leq 4x^2} w_m(n) \left( \frac{n}{\ell_1 \ell_2} \right) = \sum_{p \leq x} \left( \frac{m(4p - a_p^2)}{\ell_1 \ell_2} \right) \]
\[ = \left( -\frac{m}{\ell_1 \ell_2} \right) \sum_{p \leq x} \left( \frac{a_p^2 - 4p}{\ell_1 \ell_2} \right) = \left( -\frac{m}{\ell_1 \ell_2} \right) U(x; \ell_1 \ell_2). \]

Thus, changing the order of summation, we derive
\[ \Sigma_2 = \sum_{z \leq \ell_1 < \ell_2 \leq 2z} \sum_{u-v \leq m \leq u} \left( -\frac{m}{\ell_1 \ell_2} \right) U(x; \ell_1 \ell_2). \]

By Lemma 3, we have
\[ U(x; \ell_1 \ell_2) \ll x^{1+o(1)}(\ell_1 \ell_2)^{-2} + x^{1/2+o(1)}(\ell_1 \ell_2)^3 = x^{1+o(1)}z^{-4} + x^{1/2+o(1)}z^6, \]
which yields the estimate
\[ \Sigma_2 \leq \left( x^{1+o(1)}z^{-4} + x^{1/2+o(1)}z^6 \right) \sum_{z \leq \ell_1 < \ell_2 \leq 2z} \left| \sum_{u-v \leq m \leq u} \left( \frac{m}{\ell_1 \ell_2} \right) \right|. \] (11)

We now apply Lemma 4 to derive from (11) that
\[ \Sigma_2 \leq x^{o(1)} (xz^{-4} + x^{1/2}z^6) v^{1/2}z^{19/8}. \] (12)

Substitution of (10) and (12) in (9) leads us to the bound:
\[ \sum_{u-v \leq m \leq u} S_m(x) \leq x^{o(1)} \left( xvz^{-1} + v^{1/2}xz^{-29/8} + v^{1/2}x^{1/2}z^{51/8} \right) \]
\[ \leq x^{o(1)} \left( vxz^{-1} + v^{1/2}x^{1/2}z^{51/8} \right). \]
Choosing \( z = (vx)^{4/59} \) (thus (7) holds), we conclude the proof. \( \square \)

For any fixed \( \varepsilon > 0 \), Lemma 6 gives a nontrivial estimate provided that 
\( v \leq x^{4/55-\varepsilon} \) uniformly over \( u \).
In the case of \( u = v \), we now obtain a slightly better bound.

**Lemma 7.** Suppose \( E \) does not have complex multiplication and also assume that the GRH holds. Then for any real \( 4x \geq v \geq 1 \), we have
\[
\sum_{1 \leq m \leq v} S_m(x) \leq v^{13/14}x^{13/14+o(1)}.
\]

**Proof.** We proceed as in the proof of Lemma 6, however, we always preserve the condition that \( m \) is square-free. Then we can estimate \( \Sigma_2 \) by using Lemma 5 instead of Lemma 4.

More precisely, applying the Cauchy inequality and then using Lemma 5 with \( X = v \), \( Y = 4z^2 \) and \( f(m) = 1 \), we obtain
\[
\sum_{z \leq \ell_1 < \ell_2 \leq 2z} \left| \sum_{1 \leq m \leq v \atop m \text{ squarefree}} \left( \frac{m}{\ell_1 \ell_2} \right) \right| \ll \left( \sum_{z \leq \ell_1 < \ell_2 \leq 2z} \sum_{1 \leq m \leq v \atop m \text{ squarefree}} \left( \frac{m}{\ell_1 \ell_2} \right)^2 \right)^{1/2} \leq \left( x^{o(1)}vz^2 (v + z^2) \right)^{1/2} = x^{o(1)} (vz + v^{1/2}z^2).
\]

We now derive from (11) that
\[
\Sigma_2 \leq x^{o(1)} \left( vxz^{-3} + v^{1/2}xz^{-2} + x^{1/2}vz^7 + v^{1/2}x^{1/2}z^8 \right). \tag{13}
\]

Substitution of (10) and (13) in (9) leads us to the bound:
\[
\sum_{1 \leq m \leq v \atop m \text{ squarefree}} S_m(x) \leq x^{o(1)} \left( vxz^{-1} + vxz^{-5} + v^{1/2}xz^{-4} + vx^{1/2}z^5 + v^{1/2}x^{1/2}z^6 \right).
\]

Clearly the second and the third terms are both dominated by the first term. Hence the bound simplifies as
\[
\sum_{1 \leq m \leq v \atop m \text{ squarefree}} S_m(x) \leq x^{o(1)} \left( vxz^{-1} + v^{1/2}x^{1/2}z^5 + v^{1/2}x^{1/2}z^6 \right).
\]
If we choose
\[ z = (vx)^{1/14} \]
(thus (7) holds), to balance the first and the third terms as \((vx)^{13/14}\), which also gives \(v^{19/14}x^{6/7}\) for the second term, we obtain
\[ \sum_{1 \leq m \leq v \atop m \text{ squarefree}} S_m(x) \leq x^{o(1)} \left( (vx)^{13/14} + v^{19/14}x^{6/7} \right). \]

Clearly the bound is nontrivial only if \((vx)^{13/14} \leq x\) or \(v \leq x^{1/13}\) in which case \((vx)^{13/14} > v^{19/14}x^{6/7}\), thus the first term always dominates. \(\square\)

Also as in [2], we define
\[ D(x, y) = \sum_{y \leq n \leq 2x^{1/2}} \pi_n(x), \]
where
\[ \pi_n(x) = \# \{ p \leq x \mid p \nmid N, n^2 \nmid \#\text{III}_p \}. \]

This function is of independent interest. Our next result improves [2, Proposition 5.2].

**Lemma 8.** Suppose \(E\) does not have complex multiplication and also assume that the GRH holds. Then for any real \(1 \leq y \leq 2x^{1/2}\), we have
\[ D(x, y) \leq x^{13/7 + o(1)} y^{-13/7}. \]

**Proof.** It is easy to check that [2, Bound (36)] can in fact be replaced by the following estimate
\[ D(x, y) \leq x^{o(1)} \sum_{m \leq 4x/y^2 \atop m \text{ squarefree}} S_m(x) \]

We note that this bound differs from [2, Bound (36)] only in that we still require \(m\) to be squarefree. This condition is present in all considerations which have lead to [2, Bound (36)], but is not included in that bound. Preserving this condition does not give any advantage for the argument of [2] but is important for us. Using Lemma 6 for \(y < x^{5/12}\) and Lemma 7 otherwise, we obtain the result. \(\square\)
4 Proofs of Theorems 1 and 2

As in the proof of [2, Proposition 5.3] we see that for any $1 \leq y \leq 2^{x^{1/2}}$ we have
\[
\pi_{TS}(x) = \alpha \pi(x) + O \left( D(x, y) + x^{1/2+o(1)} y \right)
\]
where $\alpha$ is as in (1). Using the second bound of Lemma 8 we derive
\[
\pi_{TS}(x) = \alpha \pi(x) + O \left( x^{13/7+o(1)} y^{-13/7} + x^{1/2+o(1)} y \right),
\]
and then selecting $y = x^{19/40}$, we conclude the proof of Theorem 1.

To proof Theorem 2, as in [1], we note that
\[
\sigma(x; u, v) \leq \sum_{m \text{ squarefree}} S_m(x).
\]

Now Lemmas 6 and 7 imply the result.

5 Remarks

Under some additional assumptions, Cojocaru and David [1, Theorem 3] give sharper bounds on the error term in the asymptotic formula of Lemma 3. In turn, this leads to further sharpening the bound of Theorem 1 (under the same additional assumptions).

We also note that, Lemma 8 shows that under the GRH the bound $\#III_p \leq x^{12/13+o(1)}$ holds for all but $o(\pi(x))$ primes $p \leq x$.

It would be very interesting to obtain an unconditional proof of the asymptotic formula (1) with $R(x) = o(\pi(x))$.

In fact, it is possible to obtain an unconditional version of Lemma 8. However, it seems to be too weak to leads to an asymptotic formula for $\pi_{TS}(x)$. Indeed, to use this unconditional version, one needs a nontrivial estimate on $D(x, y)$ for rather small values of $y$. Although the approach of Lemma 8 admits an unconditional version, it seems highly unlikely that without some principally new ideas one can obtain an unconditional asymptotic formula for $\pi_{TS}(x)$. 

10
Acknowledgement

The author is grateful to Alina Cojocaru, Bjorn Poonen and Joseph Silverman for useful comments.

This work was supported in part by ARC grant DP0556431.

References

[1] A. C. Cojocaru and C. David, ‘Frobenius fields for elliptic curves’, *Amer. J. Math.*, (to appear).

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

[3] A. C. Cojocaru, É. Fouvry and M. R. Murty, ‘The square sieve and the Lang–Trotter conjecture’, *Canadian J. Math.*, **57** (2005), 1155–1177.

[4] D. R. Heath-Brown, ‘The square sieve and consecutive squarefree numbers’, *Math. Ann.*, **266** (1984), 251–259.

[5] D. R. Heath-Brown, ‘A mean value estimate for real character sums’, *Acta Arith.*, **72** (1995), 235–275.

[6] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.

[7] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, Berlin, 1995.