Math. Ann. 329, 513–534 (2004) **Mathematische Annalen**

DOI: 10.1007/s00208-004-0517-2

Reductions of an elliptic curve and their Tate-Shafarevich groups

A. C. Cojocaru · W. Duke

Received: 13 November 2002 / Revised version: 19 August 2003 /
Published online: 18 February 2004 –

Abstract. In this paper we study the Tate-Shafarevich groups Ш_p of the reductions modulo primes p of an elliptic curve $E/\mathbb{Q}$ considered as being defined over their function fields. Assuming GRH when E has no CM, we show that Ш_p is trivial for a positive proportion of primes p, provided E has an irrational point of order two.

1. Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$ and of conductor N. For a prime $p \nmid N$, the reduction of E modulo p is an elliptic curve E_p defined over the finite field k with p elements. There is great interest in the behavior of these reductions as p varies. The most basic questions concern the size of $E_p(k)$, the finite abelian group of k rational points of E_p. Define a_p as usual by

$$|E_p(k)| = p + 1 - a_p \tag{1}$$

where, for a set S, we write $|S|$ or $\#S$ for its cardinality. The Riemann hypothesis for E_p, proven by Hasse, states that

$$|a_p| \leq 2\sqrt{p}$$

(see [Si, pp. 131–132] for a proof). Still unproven are the Sato-Tate conjecture [Ta1] in the case of a curve without complex multiplication (CM) counting primes p where $a_p/\sqrt{p}$ lies in a given subinterval of $(-2, 2)$ and the Lang-Trotter conjecture [LTr] counting primes p with a given value of a_p. The most important result known about the latter question is that of Elkies [El] giving infinitely many p with $a_p = 0$ (supersingular E_p).

A. C. Cojocaru*
The Fields Institute for Research in Mathematical Sciences, 222 College Street, Toronto, Ontario M5T 3J1 Canada (e-mail: alina@fields.utoronto.ca)

W. Duke**
Department of Mathematics Box 951555, University of California, Los Angeles, CA 90095-1555, USA (e-mail: duke@math.ucla.edu)

* Research supported in part by an NSERC postdoctoral fellowship.
** Research supported in part by NSF grant DMS-98-01642.

Also of interest is the structure of $E_p(k)$ as an abelian group, in particular its cyclicity. It is easy to see that $E_p(k)$ may be cyclic only if E has an irrational point of order two, that is, a point of order two not in $E(\mathbb{Q})$. Assuming this and the generalized Riemann hypothesis (GRH) for Dedekind zeta functions, Serre [Se2] (see [Mu] for the proof) showed that $E_p(k)$ is cyclic for a positive proportion of primes:

$$\#\{p \leq x : p \nmid N \text{ and } E_p(k) \text{ is cyclic}\} \sim c_E\, \pi(x)$$

as $x \to \infty$, where c_E is a positive constant depending only on E and $\pi(x)$ is the number of primes $\leq x$. His method is analogous to Hooley's [Ho] conditional proof of Artin's primitive root conjecture. Without assuming GRH, R. Murty [Mu] showed this holds for CM elliptic curves. In general, R. Gupta and R. Murty [GM] showed that there are infinitely many, in fact $\gg x/\log^2 x$, such primes. For recent work on this problem see [Co] and [CM].

A new aspect emerges when one considers the reduced curve E_p as being defined over its function field. If $K = K(E_p)$ is the function field of E_p/k, then E_p naturally defines a constant elliptic curve over K.[1] The resulting elliptic curve has a number of nice features. As will be reviewed in §2, the group $E_p(k)$ may be identified with the torsion points $E_p(K)_{\text{tor}}$ of the finitely generated Mordell-Weil group $E_p(K)$ and the k-endomorphisms of E_p may be identified with the Mordell-Weil lattice $E_p(K)/E_p(K)_{\text{tor}}$. In view of these features, one is naturally led to consider the Tate-Shafarevich group of E_p/K.

To define this, let us first recall that a principal homogeneous space over E/F, where for now E is any elliptic curve over an arbitrary field F, is a smooth curve C/F together with a simply transitive algebraic group action of E on C defined over F. The isomorphism classes of principal homogeneous spaces for E/F form an abelian group, the Weil-Châtelet group $WC(E/F)$, whose identity class consists of those homogeneous spaces whose curves have an F-rational point. The group operation comes from a natural identification of $WC(E/F)$ with the cohomology group $H^1(G, E)$, where $G = \mathrm{Gal}(\bar{F}/F)$ with $\bar{F}$ the separable closure of F. For details see [LTa] or [Si], except note that in [Si] F is assumed to be perfect.

Since K is a global field we may define the Tate-Shafarevich group

$$\text{III}_p = \text{III}(E_p/K)$$

to be those elements of $WC(E_p/K)$ which, for all primes v of K, are in the kernel of the canonical map

$$WC(E_p/K) \to WC(E_p/K_v),$$

where K_v is the completion of K at the prime v. We call III_p the Tate-Shafarevich group of E_p and are interested in its behavior as p varies over primes of good reduction for E.

[1] As with k, to ease the notation we will suppress the dependence of K on p.

It is known that $|\text{III}_p|$ is finite, hence a square. In fact, there is an explicit formula for it coming from the Hasse-Weil L-function for E_p/K, since the Birch/Swinnerton-Dyer conjecture is a theorem in this case due to Milne [Mi]. This formula allows us to detect when $|\text{III}_p|$ is divisible by a fixed square. More precisely, there is a Galois extension J_n of $\mathbb{Q}$ so that n^2 divides $|\text{III}_p|$ if and only if p splits in J_n and $p \nmid n$. This field is closely related to the modular curve $X_0(n)$. An application of the Chebotarev theorem (see Proposition 4.2 below) yields the following result which implies, in particular, that $|\text{III}_p|$ may be arbitrarily large.

Theorem 1. *The group* III_p *contains elements of any fixed prime order* ℓ *for a positive proportion of primes* p.

Our principal interest in this paper is to count primes for which III_p is trivial. This happens if and only if for any principal homogeneous space over E_p/K the curve C has a point over K if it does over K_ν for all ν. Our main result shows when this local-global principle holds for many reductions.

Theorem 2. *Suppose that* E *has an irrational point of order two. If* E *does not have CM assume GRH. Then* III_p *is trivial for a positive proportion of primes* p.

Actually, we will give an asymptotic formula in Proposition 5.3 for the number of such primes with a power savings in the remainder term, at least under GRH. Furthermore, since $E_p(k)$ will be seen to be cyclic whenever III_p is trivial, the first assumption of Theorem 2 is necessary and its conclusion may be viewed as a refinement of the existence aspect of Serre's result about cyclicity of $E_p(k)$.

Theorem 2 is proven using a variant of Serre's sieve method. The strong uniformity needed in the non-CM case requires the use of GRH. A serious new difficulty is caused by the fact that the field J_n does not contain the full nth cyclotomic field. Thus the Brun-Titchmarsh theorem, which is used in Serre's argument to estimate the terms with large n, must be replaced. This is possible and essential use is made of the fact that $|\text{III}_p|$ *is a square*. This allows us to employ a second sieving device, a "square sieve", to estimate the remainder term.

2. Hasse-Weil L-functions for reductions

In this section we will give an explicit formula for $|\text{III}_p|$. This follows from the conjecture of Birch and Swinnerton-Dyer for constant elliptic curves over function fields and in particular the analogue of the class number formula given below in (5). Then we give some upper bounds for $|\text{III}_p|$ which follow from this formula.

For now let k be a finite field with $q = p^r$ elements and suppose K is an algebraic function field over k in one variable with genus g and associated curve X. Given a prime ν of K let k_ν be the residue class field, which is a finite extension of k with q_ν elements. The zeta function of K is

$$\zeta_K(s) = \prod_{v} (1 - q_v^{-s})^{-1},$$

where v runs over all the primes of K. After Weil [We], this is known to be a rational function of the form

$$\zeta_K(s) = \frac{\prod_{i=1}^{2g} (1 - \alpha_i q^{-s})}{(1 - q^{-s})(1 - q^{1-s})}, \tag{2}$$

where $\alpha_i \bar{\alpha}_{i+g} = q$, for $i = 1, \dots, g$.

Let A be an elliptic curve defined over K. For a prime v of K of good reduction, the number of points on $A(k_v)$ can be written as

$$|A(k_v)| = q_v + 1 - a_v \quad \text{where} \quad |a_v| \leq 2\sqrt{q_v}.$$

The Hasse-Weil L-function of A/K is

$$L(s, A/K) = \prod_{v \in S} (1 - a_v q_v^{-s})^{-1} \prod_{v \notin S} (1 - a_v q_v^{-s} + q_v^{1-2s})^{-1}, \tag{3}$$

where S consists of the primes v of bad reduction for A and for such v, we have $a_v \in \{0, 1, -1\}$ depending on the type (see [Ta3]). It is known that $L(s, A/K)$ is a polynomial in q^{1-s} with a functional equation relating s to $2 - s$ (see [Ta2, Sh]).

Suppose now that A/K is a constant elliptic curve, so that A is defined over k. Leading up to formula (5) below, we now closely follow the discussion of §3.2 of [Oe], to which we refer for more details. In this case we have the following identity:

$$L(s, A/K) = \prod_{j=1}^{2} \frac{\prod_{i=1}^{2g} (1 - \alpha_i \beta_j q^{-s})}{(1 - \beta_j q^{-s})(1 - \beta_j q^{1-s})}, \tag{4}$$

where α_i are defined in (2) and β_j are defined similarly for A:

$$|A(k)| = q + 1 - (\beta_1 + \beta_2) \quad \text{and} \quad \beta_1 \beta_2 = q.$$

In the constant curve case the Mordell-Weil group $A(K)$ can be identified with the group $\mathrm{Mor}_k(X, A)$ of morphisms from X to A defined over k, the canonical height of a point being identified with the degree of its associated morphism. The torsion subgroup $A(K)_{\mathrm{tor}}$ corresponds to the constants $A(k)$. The Mordell-Weil lattice $A(K)/A(K)_{\mathrm{tor}}$ is canonically isomorphic to the group $\mathrm{Hom}_k(J(X), A)$ of morphisms from the Jacobian $J(X)$ to A defined over k and is an even integral lattice L of rank n with respect to the degree form $\langle u, v \rangle = \deg(u + v) - \deg u - \deg v$, where $u, v \in \mathrm{Hom}_k(J(X), A)$.

The conjecture of Birch and Swinnerton-Dyer is a theorem in this situation (see [Mi]) and states that $L(s, A/K)$ vanishes to order n at $s = 1$ and that

$$\lim_{s \to 1} \frac{L(s, A/K)}{(1 - q^{1-s})^n} = \frac{q^{1-g} |\mathrm{III}(A/K)| \Delta}{|A(k)|^2},$$

where Δ is the discriminant of L and is defined by $\Delta = \det\langle u_i, u_j\rangle$ with $\{u_1, \ldots, u_n\}$ a $\mathbb{Z}$-basis for L. Using (4) we see that n is the number of pairs (i, j) with $\alpha_i = \beta_j$. Milne's formula

$$|\text{Ш}(A/K)|\Delta = q^g \prod_{\alpha_i \neq \beta_j} (1 - \alpha_i/\beta_j) \tag{5}$$

then follows as well.

We are interested in the case $A = E_p$, $|k| = p$ and K the function field of E_p, so E_p is a constant elliptic curve defined over K. In this situation the Mordell-Weil lattice L may be identified with the k-endomorphisms $\text{End}_k(E_p)$. Now $\text{End}_k(E_p)$ is well known to be isomorphic to an order of discriminant Δ_p say, in the imaginary quadratic field $\mathbb{Q}((a_p^2 - 4p)^{1/2})$, where a_p is defined in (1) (see Theorem 4.2 of [Wat]). In this isomorphism the degree form is given by $\langle u, v\rangle = 2\,\text{Re}(u\bar{v})$ and $\Delta = \Delta_p$. This motivates the following definition.

Definition 2.1. *Let b_p be the unique positive integer such that*

$$a_p^2 - 4p = b_p^2 \Delta_p. \tag{6}$$

Now a straightforward calculation of the right hand side of (5) gives the following formula.

Proposition 2.2. *For primes $p \nmid N$ we have that $|\text{Ш}_p| = b_p^2$.*

Upper bounds for $|\text{Ш}_p|$

Proposition 2.2 gives immediately the upper bound

$$|\text{Ш}_p| \leq (4/3)p \tag{7}$$

for all $p \nmid N$. In general this bound is likely sharp. In fact, if E is given by

$$y^2 = x^3 + 1,$$

which has CM by $\mathbb{Q}(\sqrt{-3})$, then for a prime p of the form $p = 3n^2 + 1$ Proposition 2.2 implies that

$$|\text{Ш}_p| = 4n^2 = (4p - 4)/3.$$

There are likely infinitely many such p. In fact, conjecturally the number of such primes $\leq x$ should be asymptotic to $\kappa\sqrt{x}/\log x$ for some positive κ as $x \to \infty$.

On the other hand, for non-CM curves a theorem of Schoof implies that $|\text{Ш}_p|/p = \text{o}(p)$. More precisely, we have the following bound, which is an immediate consequence of Proposition 2.2 and the bound

$$|\Delta_p| \gg (\log p/\log\log p)^2$$

given as Corollary 2.5 in [Sc] under the same conditions.

Proposition 2.3. *Suppose that E does not have CM. Then, for $p \nmid N$,*

$$|\text{III}_p| \ll p\,(\log\log p/\log p)^2$$

where the implied constant depends only on E.

3. Division fields and their subfields

In this section we will develop some properties of the division fields of an elliptic curve and certain of their subfields needed to detect divisibility of $|\text{III}_p|$ by a square. Background for this section on elliptic curves may be found in [Si] and [Ta4] and on cyclotomic fields in [Wa].

As before, let E be an elliptic curve defined over $\mathbb{Q}$ and of conductor N. For a positive integer n let $E[n]$ denote the group of n-division points of E and $L_n := \mathbb{Q}(E[n])$ be the nth division field of E. Then $L_n/\mathbb{Q}$ is a finite Galois extension whose Galois group G_n is a subgroup of $\mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Let us denote[2]

$$\phi_2(n) = \#\,\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) = n^4 \prod_{\substack{\ell|n \\ \ell \text{ prime}}} (1-\ell^{-1})(1-\ell^{-2}). \tag{8}$$

A basic fact is that L_n contains the nth cyclotomic field $\mathbb{Q}(\zeta_n)$, where ζ_n is a primitive nth root of unity, this being a consequence of the non-degeneracy of the Weil pairing. Furthermore, the Galois action of $\sigma \in G_n$ on ζ_n is given by

$$\zeta_n \longmapsto \zeta_n^{\det\sigma}. \tag{9}$$

The following observation is useful for obtaining some needed properties of L_n for square-free n. By a non-trivial subfield of a number field we mean a subfield which is not $\mathbb{Q}$.

Proposition 3.1. *Suppose that n is odd and square-free and that*

$$G_n = \mathrm{Gal}(L_n/\mathbb{Q}) = \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

Then any non-trivial Galois subfield of the division field L_n contains a non-trivial subfield of the cyclotomic field $\mathbb{Q}(\zeta_n)$.

Proof. Since

$$G_n = \prod_{\ell|n} \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}),$$

any proper normal subgroup of G_n has a component H in some $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for $\ell \geq 3$ which is a proper normal subgroup. Thus to prove the Proposition it is enough to show that H fixes a non-trivial subfield of $\mathbb{Q}(\zeta_\ell)$.

[2] In this paper ℓ always denotes a prime and a product over $\ell|n$ is over all prime divisors of n.

Suppose first that $\ell \geq 5$. As is shown in Theorem 9.9 p.78. of [Su], H either contains $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ or is a subgroup of the center Z of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, which consists of the scalars:

$$Z = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : \ a \in (\mathbb{Z}/\ell\mathbb{Z})^* \right\}.$$

In the first case, by (9), the fixed field of H is a non-trivial subfield of $\mathbb{Q}(\zeta_\ell)$, and the result follows. In the second case H is contained in the subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ whose elements have square determinants. Writing

$$m^* = (-1)^{\frac{m-1}{2}} m \qquad (10)$$

for any odd integer m, we see that H fixes the subfield $\mathbb{Q}(\sqrt{\ell^*})$ of $\mathbb{Q}(\zeta_\ell)$.

If $\ell = 3$, the proper normal subgroups of $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ are $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$,

$$\left\{ \pm \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}, \pm \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\},$$

and $\{\pm 1\}$. Thus H fixes $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$ in any case. □

Suppose that m and n are co-prime positive integers. It is easily seen that $L_m L_n = L_{mn}$, where $L_m L_n$ is the compositum of L_m and L_n. As usual, denote by $[L : \mathbb{Q}]$ the degree of the extension $L/\mathbb{Q}$. Since $L_n/\mathbb{Q}$ is Galois we have that $[L_m L_n : \mathbb{Q}] = [L_m : \mathbb{Q}]\,[L_n : \mathbb{Q}]$ if and only if $L_m \cap L_n = \mathbb{Q}$ (see e.g. p.115. of [Ro]). Thus for co-prime m and n

$$[L_{mn} : \mathbb{Q}] = [L_m : \mathbb{Q}]\,[L_n : \mathbb{Q}] \ \text{ if and only if } \ L_m \cap L_n = \mathbb{Q}. \qquad (11)$$

Ramification of primes in L_n is described by the criterion of Néron-Ogg-Shafarevich (see e.g. [Si] VII, §7.1), which states that p is unramified in L_n for all positive integers n not divisible by p if and only if p is a prime of good reduction for E . In particular, L_n is unramified outside of nN.

In case E does not have CM we have the fundamental result due to Serre [Se1] which states that there are at most finitely many primes ℓ so that the Galois group of the full division field L_ℓ is not all of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. We shall denote by A_E the product of these “exceptional” primes ℓ.

Using these results we derive from Proposition 3.1 the following needed properties of L_n.

Proposition 3.2. *Suppose that E does not have CM.*

1. *If n is square-free, odd and prime to A_E, then*

$$\mathrm{Gal}(L_n/\mathbb{Q}) = \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

2. *If n is square-free, odd and prime to NA_E and m is any positive integer prime to n, then*

$$L_n \cap L_m = \mathbb{Q}.$$

Proof. The first statement is proven by induction on the number of primes dividing n. Suppose that for square-free n prime to A_E we have $G_n = \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Let $\ell \nmid 2nA_E$ be another prime. By Serre's theorem we know that $G_\ell = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. We claim that $L_\ell \cap L_n = \mathbb{Q}$. If not, then by Proposition 3.1 we have that $L_\ell \cap L_n$ contains a nontrivial subfield of both $\mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(\zeta_\ell)$. But $\mathbb{Q}(\zeta_\ell) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$. Thus by (11)

$$[L_{\ell n} : \mathbb{Q}] = [L_\ell : \mathbb{Q}][L_n : \mathbb{Q}] = \#\,\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \cdot \#\,\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) = \#\,\mathrm{GL}_2(\mathbb{Z}/\ell n\mathbb{Z}).$$

The first statement follows by induction.

For the second statement, if $L_n \cap L_m$ gives a non-trivial normal subfield of L_n then by Proposition 3.1 some $\ell | n$ must be ramified in $L_n \cap L_m$, hence in L_m. This is impossible since $\ell \nmid mN$ by assumption. □

The modular curve $X_0(n)$

Define J_n to be the subfield of L_n fixed by the scalar elements of G_n. Thus J_n is a Galois extension of $\mathbb{Q}$ which is unramified outside of nN and whose Galois group is a subgroup of $\mathrm{PGL}_2(\mathbb{Z}/n\mathbb{Z})$. The fields J_n are important for us since they allow us to detect the divisibility of $|\mathrm{III}_p|$ by n^2. Before seeing this in Proposition 3.4, we first discuss the relation of J_n to other well known fields and record some needed consequences of Proposition 3.2 for J_n.

Let F_n denote the subfield of the nth cyclotomic field $\mathbb{Q}(\zeta_n)$ fixed by the subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$ consisting of squares. Unless $n = 2$, we clearly have $[F_n : \mathbb{Q}] > 1$. Since the scalars of $G_n = \mathrm{Gal}(L_n/\mathbb{Q})$ acting on $\mathbb{Q}(\zeta_n) \subseteq L_n$ through (9) fix F_n, we have that $F_n \subseteq J_n$. Thus $[J_n : \mathbb{Q}] > 1$ except possibly when $n = 2$, where $J_2 = L_2$. In case n is square-free, it is clear that

$$F_n = \mathbb{Q}(\sqrt{\ell_1^*}, \ldots, \sqrt{\ell_t^*}), \tag{12}$$

where $\ell_1, \ldots, \ell_t$ are the odd prime divisors of n (recall (10)). If n is odd and square-free, then F_n is the genus field of $F = \mathbb{Q}(\sqrt{n^*})$, that is, the maximal abelian extension of $\mathbb{Q}$ containing F which is unramified over F [Ha].

The field J_n is closely related to the modular curve $X_0(n)$ which, roughly speaking, parameterizes the cyclic isogenies of degree n between elliptic curves E and E'. Explicitly, $X_0(n)$ may be defined over $\mathbb{Q}$ by the classical modular polynomial $\Phi_n(X, Y) \in \mathbb{Z}[X, Y]$, which is an irreducible symmetric polynomial of degree

$$\psi(n) = n \prod_{\ell | n} \left(1 + \ell^{-1}\right)$$

which satisfies

$$\Phi_n(j(E), j(E')) = 0$$

exactly when there is a cyclic isogeny of degree n from E to E'. In terms of the modular function $j(z)$ we have explicitly [3]

$$\Phi_n(X, j(z)) = \prod_{i=1}^{\psi(n)} (X - j(\gamma_i z)),$$

where

$$\gamma_i \in \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : \ ad = n, \ (a, d, b) = 1, \ 0 \le b < d \right\}.$$

One can show that J_n is the splitting field of $\Phi_n(X, j(E))$, provided that $\mathrm{Gal}(J_n/\mathbb{Q}) = \mathrm{PGL}_2(\mathbb{Z}/n\mathbb{Z})$ (for a proof see Prop 5.2.3 p.68 of [Ad]).

The following is an immediate consequence of Proposition 3.2 and will be used to show the density of primes in Theorem 2 is positive.

Proposition 3.3. *Suppose that E does not have CM. Let A_E denote the product of the exceptional primes for E.*

1. *If n is square-free, odd and prime to A_E, then* $\mathrm{Gal}(L_n/\mathbb{Q}) = \mathrm{PGL}_2(\mathbb{Z}/n\mathbb{Z})$ *and so*

$$[J_n : \mathbb{Q}] = n^3 \prod_{\ell | n} (1 - \ell^{-2}).$$

2. *If n is square-free, odd and prime to $N A_E$ and m is any positive integer prime to n, then $J_n \cap J_m = \mathbb{Q}$ and so*

$$[J_{nm} : \mathbb{Q}] = [J_n : \mathbb{Q}] \, [J_m : \mathbb{Q}].$$

Divisibility of $|\mathrm{III}_p|$

The field J_n allows us to study divisibility properties of $|\mathrm{III}_p|$ and shows the relation between $|\mathrm{III}_p|$ and the structure of $E_p(k)$.

Proposition 3.4. *Let E be an elliptic curve defined over $\mathbb{Q}$ and of conductor N. Let $p \nmid N$ be a prime and n be a positive integer. Then n^2 divides $|\mathrm{III}_p|$ if and only if $p \nmid n$ and p splits completely in $J_n/\mathbb{Q}$.*

[3] The coefficients of $\Phi_n(X, Y)$ are famously large; already when $n = 2$ we have

$$\Phi_2(X, Y) = X^3 + Y^3 - X^2Y^2 + 1488(X^2Y + XY^2) + 40773375XY - 162000(X^2 + Y^2) + 8748000000(X + Y) - 157464000000000.$$

Proof. Suppose $p \nmid N$. The ring of endomorphisms $\mathrm{End}_k(E_p)$ of E_p over k is an order in $\mathbb{Q}((a_p^2 - 4p)^{\frac{1}{2}})$, of discriminant $\Delta_p < 0$. Recall from Proposition 2.2 that $b_p^2 = |\text{Ш}_p|$ where b_p is given in (6). First observe that we may assume that $p \nmid n$ since this follows from the condition that n^2 divides $|\text{Ш}_p|$ and the upper bound (7).

Consider the matrix

$$\sigma_p = \begin{pmatrix} \frac{a_p + b_p\delta_p}{2} & b_p \\ \frac{b_p(\Delta_p - \delta_p)}{4} & \frac{a_p - b_p\delta_p}{2} \end{pmatrix}, \tag{13}$$

where δ_p is 0 or 1 according to whether $\Delta_p \equiv 0$ or $1 (\mathrm{mod}\, 4)$. Then, as shown in [DT], for an integer n such that $p \nmid n$, the matrix σ_p reduced modulo n represents the class of the Frobenius over p for L_n. The result now follows since it is easy to check that σ_p is congruent to a scalar $\mathrm{mod}\, n$ if and only if $n \mid b_p$. □

For $p \nmid N$, the finite abelian group $E_p(k)$ has the structure

$$E_p(k) \simeq (\mathbb{Z}/d_p\mathbb{Z}) \oplus (\mathbb{Z}/e_p\mathbb{Z})$$

for uniquely determined positive integers d_p, e_p with $d_p | e_p$, the elementary divisors of $E_p(k)$. Here e_p is the exponent of $E_p(k)$. This follows since $E_p(k) \subseteq E_p(\overline{k})[n] \subseteq (\mathbb{Z}/n\mathbb{Z}) \oplus (\mathbb{Z}/n\mathbb{Z})$ for n such that $\#E_p(k)|n$, where $\overline{k}$ denotes an algebraic closure of k.

It is easy to see that a_p does not determine the structure of $E_p(k)$, that is, d_p and e_p are not isogeny invariants. However, these invariants are determined by a_p and b_p as follows. Recall that $\Delta_p = (a_p^2 - 4p)/b_p^2$ and that δ_p is 0 or 1 according to whether $\Delta_p \equiv 0$ or $1 (\mathrm{mod}\, 4)$. The following is an easy consequence of (13) together with the fact that for any $n \in \mathbb{Z}^+$ with $p \nmid n$, we have that $n \mid d_p$ if and only if p splits completely in L_n [Mu]. Note that neither d_p nor b_p can be divisible by p if $p \nmid N$.

Proposition 3.5. *For $p \nmid N$ we have that*

$$d_p = \gcd\left(b_p, \tfrac{1}{2}(a_p + b_p\delta_p - 2)\right) \quad \text{and} \quad e_p = (p + 1 - a_p)/d_p.$$

In particular, if Ш_p *is trivial then* $E_p(k)$ *is cyclic.*

4. Applications of Chebotarev

Given a (finite) Galois extension $L/\mathbb{Q}$ with Galois group G the Chebotarev Theorem says that the Frobenius classes of the unramified primes in $\mathbb{Q}$ are uniformly distributed over G. More precisely, if C is a union of conjugacy classes of G and if $\sigma_p \in G$ is any Frobenius element over an unramified p, let

$$\pi(x, C) = \#\left\{p \le x : \ p \ \text{ is unramified in } L \text{ and } \sigma_p \in C\right\}.$$

Then[4]

$$\pi(x, C) \sim \tfrac{|C|}{|G|}\pi(x) \tag{14}$$

as $x \to \infty$ (see e.g. [LO]).

To obtain a strong uniform remainder estimate we shall to assume the Generalized Riemann Hypothesis (GRH) for the Dedekind zeta function for L. Recall that this is defined for $\mathrm{Re}(s) > 1$ by

$$\zeta(s, L) = \prod_{\mathfrak{p}} (1 - \mathbb{N}(\mathfrak{p})^{-s})^{-1},$$

where $\mathfrak{p}$ runs over the finite primes of L, and has an analytic continuation and functional equation. GRH conjectures that all non-trivial zeros of $\zeta(s, L)$ lie on the line $\mathrm{Re}(s) = \frac{1}{2}$. The following useful conditional version of the Chebotarev Theorem is now well-known.

Proposition 4.1. *Suppose that $\zeta(s, L)$ satisfies GRH. Then*

$$\pi(x, C) - \tfrac{|C|}{|G|}\pi(x) \ll x^{1/2}\,|C|\,\log(x\,|G|\,\delta_L), \tag{15}$$

where δ_L is the product of the ramified primes in L, and the implied constant is absolute.

Proof. We have the conditional Chebotarev Theorem given by Lagarias and Odlyzko [LO], as refined by Serre in Théorème 4 p.133 of [Se3]:

$$\pi(x, C) - \tfrac{|C|}{|G|}\pi(x) \ll x^{1/2}\,|C|\,(|G|^{-1}\log|\,\mathrm{disc}(L/\mathbb{Q})| + \log x).$$

The result then follows from Prop. 6 of [Se3], which implies that

$$|G|^{-1}\log|\,\mathrm{disc}(L/\mathbb{Q})| \le \log(|G|\,\delta_L). \qquad \square$$

We now apply these results to the counting function

$$\pi_n(x) = \#\{p \le x : \ p \nmid N \text{ and } n^2 \text{ divides } |\text{Ш}_p|\} \tag{16}$$

for any $n \in \mathbb{Z}^+$.

Proposition 4.2. *Let E be an elliptic curve defined over $\mathbb{Q}$ and of conductor N. Then, for any $n \in \mathbb{Z}^+$,*

$$\pi_n(x) \sim c_n\,\pi(x)$$

as $x \to \infty$, where $c_n = [J_n : \mathbb{Q}]^{-1}$. Assuming GRH for $\zeta(s, J_n)$ we have, for any $n \in \mathbb{Z}^+$ and any $x \ge 1$, that

$$\pi_n(x) = c_n\,\pi(x) + \mathrm{O}(x^{\frac{1}{2}}\log(xnN)), \tag{17}$$

where the implied constant is absolute.

[4] One may of course replace the term $\pi(x)$ by the logarithmic integral Li(x).

Proof. Consider the Galois extension J_n with C the identity class in $\mathrm{Gal}(J_n/\mathbb{Q})$. The first statement follows from Proposition 3.4 and (14) since

$$\pi_n(x) - \pi(x, C) \ll \log N.$$

The second statement is then a consequence of Proposition 4.1, since clearly we have the bound $[J_n : \mathbb{Q}] \leq n^3$ and the product of the ramified primes is $\leq nN$. □

Theorem 1 follows immediately from the first part of Proposition 4.2.

A character sum

The following result is needed in the proof of Theorem 2 and allows us to take advantage of the fact that $|\text{III}_p|$ is a square. A variant is due to Cojocaru, Fouvry and Murty ([Co, CFM]), who first discovered the relevance of such a result in conjunction with the square sieve.

Proposition 4.3. *Suppose E does not have CM and let $n \in \mathbb{Z}^+$ be square-free, odd and prime to A_E. Assume GRH for $\zeta(s, L_n)$. Then for $x \geq 1$*

$$\sum_{\substack{p \leq x \\ p \nmid N}} \left(\frac{a_p^2 - 4p}{n} \right) = \kappa_n \, \pi(x) + \mathrm{O}(x^{\frac{1}{2}} \, n^4 \, \log(xnN)),$$

with an absolute implied constant. Here $\left(\frac{\cdot}{n}\right)$ denotes the Jacobi symbol and $\kappa_n = \prod_{\ell | n} (1 - \ell^2)^{-1}$.

Proof. By splitting into progressions mod n we have

$$\sum_{\substack{p \leq x \\ p \nmid N}} \left(\frac{a_p^2 - 4p}{n} \right) = \sum_{t \,(\mathrm{mod}\, n)} \sum_{\substack{d \,(\mathrm{mod}\, n) \\ (d,n)=1}} \left(\frac{t^2 - 4d}{n} \right) \pi_E(x; d, t) + \mathrm{O}(\log n), \tag{18}$$

where

$$\pi_E(x; d, t) = \#\{p \leq x : \; p \nmid N, \; a_p \equiv t \,(\mathrm{mod}\, n) \text{ and } p \equiv d \,(\mathrm{mod}\, n)\}.$$

By (1) of Proposition 3.2 we know that

$$\mathrm{Gal}(L_n/\mathbb{Q}) = \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) = \prod_{\ell | n} \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$$

and it is straightforward to check that the number of elements in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ with trace t and determinant d when $(d, n) = 1$ is

$$\alpha_{d,t}(n) = n \prod_{\ell | n} \left(\ell + \left(\tfrac{t^2 - 4d}{\ell} \right) \right) = n \sum_{k | n} \frac{n}{k} \left(\tfrac{t^2 - 4d}{k} \right). \tag{19}$$

Proposition 4.1 applied to this union C of conjugacy classes in $\mathrm{Gal}(L_n/\mathbb{Q})$ then gives

$$\pi_E(x; d, t) = \frac{\alpha_{d,t}(n)}{\phi_2(n)} \pi(x) + \mathrm{O}(x^{\frac{1}{2}} n \log(xnN) \prod_{\ell | n} (\ell + 1)), \tag{20}$$

where $\phi_2(n)$ is defined in (8). Plugging (20) back into (18) we have:

$$\sum_{\substack{p \le x \\ p \nmid N}} \left(\frac{a_p^2 - 4p}{n} \right) = \frac{n^2 \beta(n)}{\phi_2(n)} \pi(x) + \mathrm{O}(x^{\frac{1}{2}} n^2 \log(xnN) \prod_{\ell | n} (\ell^2 - 1)), \tag{21}$$

where the second equation of (19) yields $\beta(n) = \sum_{k|n} S(n, k)$, with

$$S(n, k) = \frac{1}{k} \sum_{t \,(\mathrm{mod}\, n)} \sum_{\substack{d \,(\mathrm{mod}\, n) \\ (d,n)=1}} \left(\tfrac{t^2 - 4d}{nk} \right). \tag{22}$$

In view of (21), in order to finish the proof of Proposition 4.3 it is sufficient to show that $\beta(n) = \kappa_n \phi_2(n)/n^2$. For this it is enough to prove that $\beta(n)$ is multiplicative on odd square-free integers and that $\beta(\ell) = -(\ell - 1)/\ell$ for an odd prime ℓ.

Suppose that n_1, n_2, k_1, k_2 are positive odd square-free integers with $k_1 | n_1$ and $k_2 | n_2$. A standard application of the Chinese remainder theorem and the multiplicative properties of the Jacobi symbol shows that if $(n_1, n_2) = 1$ then

$$S(n_1 n_2, k_1 k_2) = S(n_1, k_1) S(n_2, k_2).$$

Thus from the definition of $\beta(n)$ from above (22) we may write

$$\beta(n) = \sum_{k|n} S(n, k) = \sum_{k|n} S(n/k, 1) S(k, k) \tag{23}$$

as the Dirichlet convolution of two multiplicative functions, namely $S(n, 1)$ and $S(n, n)$, and so $\beta(n)$ is also multiplicative. Now from (22) we obtain

$$S(\ell, 1) = \sum_{t \,(\mathrm{mod}\, \ell)} \left(\sum_{d \,(\mathrm{mod}\, \ell)} \left(\tfrac{t^2 - 4d}{\ell} \right) - \left(\tfrac{t^2}{\ell} \right) \right) = - \sum_{t \,(\mathrm{mod}\, \ell)} \left(\tfrac{t^2}{\ell} \right) = -(\ell - 1),$$

and

$$\ell S(\ell, \ell) = \ell - 1 + \sum_{\substack{t \,(\mathrm{mod}\, \ell) \\ (t,\ell)=1}} \sum_{\substack{d \,(\mathrm{mod}\, \ell) \\ (d,\ell)=1}} \left(\tfrac{t^2 - 4d}{\ell^2} \right) = \ell - 1 + (\ell - 1)(\ell - 2) = (\ell - 1)^2.$$

Hence by (23) we have that $\beta(\ell) = S(\ell, 1) + S(\ell, \ell) = -(\ell - 1)/\ell$, finishing the proof. □

Proof of Theorem 2 in CM case

Theorem 2 in the CM case may be proven using Chebotarev for a fixed finite extension. It is a consequence of the following result.

Proposition 4.4. *Suppose that E has CM by an order of discriminant Δ in $\mathbb{Q}(\sqrt{\Delta})$. Then, as $x \to \infty$,*

$$\#\left\{p \leq x : p \nmid N \text{ and } \text{III}_p \text{ is trivial}\right\} \sim c\,\pi(x),$$

where

$$c = \begin{cases} 1/2, & \text{if } \sqrt{\Delta} \in J_2 \\ (1 - c_2)/2, & \text{otherwise} \end{cases} \tag{24}$$

with $c_2 = [J_2 : \mathbb{Q}]^{-1}$.

Proof. Partition the primes $p \nmid N$ into two classes: ordinary and supersingular. Recall that $|\text{III}_p| = b_p^2$. Suppose first that p is ordinary for E, which means that $a_p \neq 0$ and $\Delta_p = \Delta$. By (6) we have that $b_p = 1$ if and only if $p = (a_p/2)^2 - \Delta/4$. There are few such primes:

$$\#\{p \leq x : \; p \nmid N \text{ is ordinary and } b_p = 1\} \ll \sqrt{x}. \tag{25}$$

In fact, the right hand side can be replaced by $\ll \sqrt{x}/\log x$ (see [HR]).

If p is supersingular for E then we have $a_p = 0$ and from (6) either $b_p = 1$ or $b_p = 2$. By [De] p is supersingular for E if and only if $\left(\frac{\Delta}{p}\right) \neq 1$. Thus by Proposition 3.4, (25) and the Chebotarev Theorem we have that

$$\#\{p \leq x : \; p \nmid N \text{ and } b_p = 1\} \sim c\pi(x)$$

as $x \to \infty$, where

$$\begin{aligned} c &= 1 - [J_2 : \mathbb{Q}]^{-1} - [\mathbb{Q}(\sqrt{\Delta}) : \mathbb{Q}]^{-1} + [J_2(\sqrt{\Delta}) : \mathbb{Q}]^{-1} \\ &= 1/2 - [J_2 : \mathbb{Q}]^{-1} + [J_2(\sqrt{\Delta}) : \mathbb{Q}]^{-1}, \end{aligned}$$

which is easily seen to be given by (24). □

5. Sieving out primes with non-trivial III_p

We now turn to the proof of the main result Theorem 2 in the non-CM case. We shall obtain an asymptotic formula for

$$\pi_{\text{sha}}(x) = \#\left\{p \leq x : p \nmid N \text{ and } \text{III}_p \text{ is trivial}\right\}. \tag{26}$$

Here we must assume GRH for the Dedekind zeta functions of the division fields of E. Based on the strength of Proposition 4.3, we are able to use directly the inclusion-exclusion principle in its most basic form beginning with the expansion of the delta symbol for $m \in \mathbb{Z}^+$:

$$\sum_{n|m} \mu(n) = \delta(m) = \begin{cases} 1, & \text{if } m = 1 \\ 0, & \text{if } m \neq 1, \end{cases}$$

where $\mu(\cdot)$ denotes the Möbius function. Recall that we have written $|\text{III}_p| = b_p^2$. This yields immediately the starting formula

$$\pi_{\text{sha}}(x) = \sum_{\substack{p \le x \\ p \nmid N}} \delta(b_p) = \sum_{\substack{p \le x \\ p \nmid N}} \sum_{n|b_p} \mu(n).$$

We know from (7) that $b_p \le 2\sqrt{p/3}$ and so in this summation $n < 2\sqrt{x}$. After rearrangement, the sum can thus be written

$$\pi_{\text{sha}}(x) = \sum_{n < 2\sqrt{x}} \mu(n) \# \{ p \le x : p \nmid N \text{ and } n | b_p \}.$$

By Proposition 3.4 we have

$$\pi_{\text{sha}}(x) = \sum_{n \le y} \mu(n) \pi_n(x) + \sum_{y < n < 2\sqrt{x}} \mu(n) \pi_n(x),$$

where $\pi_n(x)$ is defined in (16) and $y = y(x)$ is a parameter which shall be chosen later. We now apply the conditional Chebotarev Theorem as given in (17) of Proposition 4.2 to the first term giving

$$\pi_{\text{sha}}(x) = \left(\sum_{n \le y} \mu(n) c_n \right) \pi(x) + \sum_{y < n < 2\sqrt{x}} \mu(n) \pi_n(x) + \mathrm{O}(y x^{\frac{1}{2}} \log xyN), \tag{27}$$

where $c_n = [J_n : \mathbb{Q}]^{-1}$. In this way we are led to seek an asymptotic evaluation in y of

$$C(y) = \sum_{n \le y} \mu(n) c_n \tag{28}$$

and an upper bound in x and y for

$$D(x, y) = \sum_{y < n < 2\sqrt{x}} \pi_n(x). \tag{29}$$

The main term

We shall begin with $C(y)$. Define

$$c = \left(\sum_{n|B} \mu(n) c_n\right) \prod_{\substack{\ell \nmid B \\ \ell \text{ prime}}} \left(1 - \frac{1}{\ell(\ell^2 - 1)}\right), \tag{30}$$

where $c_n = [J_n : \mathbb{Q}]^{-1}$ and $B = 2A_E N$, where again A_E is the product of the exceptional primes for E. Clearly $c \geq 0$.

Proposition 5.1. *Suppose that E does not have CM. Then*

$$C(y) = \sum_{n \leq y} \mu(n) c_n = c + \mathrm{O}(y^{-2} B^2)$$

with an absolute implied constant. Furthermore, $c > 0$ if and only if $c_2 \neq 1$. In fact,

$$c \geq (1 - c_2) \prod_{\substack{\ell \nmid B \\ \ell \text{ prime}}} \left(1 - \frac{1}{\ell(\ell^2 - 1)}\right). \tag{31}$$

Proof. Every square-free positive integer has a unique decomposition as the product of two co-prime square-free factors m and n, where m is a divisor of B and n is prime to B. For such m and n we have by (2) of Proposition 3.3 that

$$c_{mn} = c_m c_n.$$

Thus we may write

$$\begin{aligned} C(y) = \sum_{n \leq y} \mu(n) c_n &= \sum_{m|B} \mu(m) c_m \sum_{\substack{(n,B)=1 \\ nm \leq y}} \mu(n) c_n \\ &= c - \sum_{m|B} \mu(m) c_m \sum_{\substack{(n,B)=1 \\ nm > y}} \mu(n) c_n, \end{aligned} \tag{32}$$

where for the second line we are using (1) of Proposition 3.3 that for a prime $\ell \nmid B$, $c_\ell = (\ell(\ell^2 - 1))^{-1}$. Then, using the obvious bound

$$n^3 c_n = \prod_{\ell | n} (1 - \ell^{-2})^{-1} \leq \prod_{\ell} (1 - \ell^{-2})^{-1} = \frac{\pi^2}{6} \tag{33}$$

for the n with $(n, B) = 1$ in (32), we get

$$C(y) - c \ll \sum_{m|B} \sum_{n > y/m} n^{-3} \ll y^{-2} \sum_{m|B} m^2, \tag{34}$$

the second inequality following by a standard integral comparison. By using the inequality of (33) again we get the we known estimate

$$\sum_{m|B} m^2 = B^2 \prod_{\substack{\ell|B \\ \ell \text{ prime}}} \left(\frac{\ell^2 - \ell^{-2\nu_\ell(B)}}{\ell^2 - 1} \right) \leq B^2 \prod_{\substack{\ell|B \\ \ell \text{ prime}}} (1 - \ell^{-2})^{-1} \leq \frac{\pi^2}{6} B^2, \quad (35)$$

where $\nu_\ell(B)$ is the highest power of ℓ dividing B. Thus from (34) and (35) we have $C(y) - c \ll B^2 y^{-2}$, giving the first part of the proposition.

Now $\sum_{n|B} \mu(n) c_n$ is, by Proposition 4.2, the density of primes not splitting in any J_n for $n|B$. In particular, if $c_2 = 1$ then clearly $c = 0$. In order to finish the proof, it is enough to establish inequality (31). For this observe that

$$c' = 1 - c_2 + \sum_{\substack{n|B \\ n>2}} \mu(n) [F_n : \mathbb{Q}]^{-1},$$

where F_n is the subfield of J_n from above (12), is the density of primes not splitting in any F_n for $n|B$. But

$$\sum_{\substack{n|B \\ n>2}} \mu(n) [F_n : \mathbb{Q}]^{-1} = \sum_{\substack{n|B \\ n>1 \text{ odd}}} \mu(n) [F_n : \mathbb{Q}]^{-1} + \sum_{\substack{n|B \\ n>1 \text{ odd}}} \mu(2n) [F_{2n} : \mathbb{Q}]^{-1} = 0$$

since $F_n = F_{2n}$ for odd $n > 1$ so $1 - c_2 = c'$. Since a prime which does not split in F_n cannot split in J_n we have

$$1 - c_2 = c' \leq \sum_{n|B} \mu(n) c_n,$$

which finishes the proof of (31) in view of the definition of c in (30). □

Secondary sieving

We turn now to the estimation of

$$D(x, y) = \sum_{y<n<2\sqrt{x}} \pi_n(x),$$

where $\pi_n(x) = \#\{p \leq x : \ p \nmid N \text{ and } n^2 \text{ divides } |\text{Ш}_p|\}$.

Proposition 5.2. *Suppose that E does not have CM and let $\varepsilon > 0$ be given. Assume GRH. Then, for $1 \leq y \leq 2\sqrt{x}$ and $x \geq 1$, we have the uniform bound*

$$D(x, y) \ll y^{-2} x^{\frac{35}{18}+\varepsilon},$$

where the implied constant depends only on ε and E.

Proof. By Proposition 2.2 we have

$$\pi_n(x) = \#\left\{p \le x : p \nmid N, b_p \equiv 0 (\operatorname{mod} n)\right\}$$
$$\le \#\left\{p \le x : p \nmid N, 4p - a_p^2 \equiv 0 \left(\operatorname{mod} n^2\right)\right\}.$$

Now this is

$$\le \#\left\{p \le x : p \nmid N, 4p - a_p^2 = n^2k^2m \text{ for some } k \text{ and some square-free } m\right\}.$$

Hence letting $r = nk$ we have that $D(x, y)$ is

$$\le \sum_{y<r\le 2\sqrt{x}} d(r)\#\left\{p \le x : p \nmid N, 4p - a_p^2 = r^2m \text{ for some square-free } m\right\},$$

where $d(r)$ denotes the number of divisors of r. Since $d(r) \ll_\varepsilon r^\varepsilon$ for any $\varepsilon > 0$, and since the decomposition $4p - a_p^2 = r^2m$ above is unique, we obtain that

$$D(x, y) \ll_\varepsilon x^\varepsilon \sum_{m\le 4x/y^2} S_m(x), \tag{36}$$

where

$$S_m(x) = \#\left\{p \le x : p \nmid N,\ m\left(4p - a_p^2\right) \text{ is a square}\right\}.$$

We now obtain a uniform bound for $S_m(x)$ for $1 \le m \le x$. Here we use that if $n \le 4x^2$ is a square, then the sum of Legendre symbols

$$\sum_{z\le\ell\le 2z} \left(\frac{n}{\ell}\right) \gg \pi(z),$$

provided $z \gg \log x$ for a big enough constant, since the number of distinct primes $\ell | n$ is $\ll \log x / \log\log x \ll \pi(z)$. Thus

$$S_m(x) \ll \sum_{n\le 4x^2} w_m(n) \left(\sum_{z\le\ell\le 2z} \left(\frac{n}{\ell}\right)\right)^2 \pi(z)^{-2}, \tag{37}$$

where

$$w_m(n) = \#\left\{p \le x : p \nmid N,\ m\left(4p - a_p^2\right) = n\right\}.$$

Squaring out in (37) we obtain

$$S_m(x) \ll \pi(z)^{-1} \sum_{n\le 4x^2} w_m(n) + \pi(z)^{-2} \left| \sum_{z\le\ell_1\ne\ell_2\le 2z}\ \sum_{n\le 4x^2} w_m(n) \left(\frac{n}{\ell_1\ell_2}\right) \right|$$
$$\ll \frac{\pi(x)}{\pi(z)} + \pi(z)^{-2} \left| \sum_{z\le\ell_1\ne\ell_2\le 2z} \left(\frac{m}{\ell_1\ell_2}\right) \sum_{\substack{p\le x\\ p\nmid N}} \left(\frac{4p - a_p^2}{\ell_1\ell_2}\right) \right|$$

since, for fixed m, the primes $\leq x$ are partitioned by n into distinct sets. Thus

$$S_m(x) \ll \frac{\pi(x)}{\pi(z)} + \pi(z)^{-2} \sum_{z \leq \ell_1 \neq \ell_2 \leq 2z} \left| \sum_{\substack{p \leq x \\ p \nmid N}} \left(\frac{a_p^2 - 4p}{\ell_1 \ell_2} \right) \right| .$$

As long as z is sufficiently large we can apply Proposition 4.3 with $n = \ell_1 \ell_2$ to obtain that

$$\begin{aligned} S_m(x) &\ll \frac{\pi(x)}{\pi(z)} + \frac{\pi(x)}{z^4} + x^{1/2} z^8 \log(xzN) \\ &\ll \frac{x \log z}{z \log x} + x^{1/2} z^8 \log(xzN). \end{aligned}$$

By choosing $z = ax^{1/18}$ for some constant a depending on E, we get the uniform bound for $1 \leq m \leq x$:

$$S_m(x) \ll x^{17/18+\varepsilon}.$$

Plugging this estimate into (36) gives Proposition 5.2. □

The main result

We are now able to prove Theorem 2 in the non-CM case. We have the following more precise result.

Proposition 5.3. *Suppose E does not have CM and assume GRH. Then, for any $\varepsilon > 0$ we have*

$$\# \left\{ p \leq x : p \nmid N \text{ and } Ш_p \text{ is trivial} \right\} = c\,\pi(x) + \mathrm{O}(x^{\frac{53}{54}+\varepsilon}),$$

where the implied constant depends only on ε and E. Here c is positive if and only if E has an irrational point of order two and is given by

$$c = \left(\sum_{n \mid B} \mu(n) c_n \right) \prod_{\ell \nmid B} \left(1 - \frac{1}{\ell(\ell^2 - 1)} \right),$$

where $c_n = [J_n : \mathbb{Q}]^{-1}$ and $B = 2A_E N$, with A_E being the product of the exceptional primes for E.

Proof. As before write $\pi_{\text{sha}}(x) = \# \left\{ p \leq x : p \nmid N \text{ and } Ш_p \text{ is trivial} \right\}$. By (27–29) for $1 \leq y \leq 2\sqrt{x}$ and $x \geq 1$ we have

$$\pi_{\text{sha}}(x) = C(y)\pi(x) + \mathrm{O}(D(x, y) + yx^{\frac{1}{2}} \log(xyN))$$

and so Propositions 5.1 and 5.2 yield

$$\pi_{\mathrm{sha}}(x) - c\,\pi(x) \ll (y^{-2}x^{\frac{35}{18}} + yx^{\frac{1}{2}})(xy)^{\varepsilon}$$

where now the implied constant depends only on ε and E. Choosing

$$y = x^{\frac{13}{27}}$$

gives the remainder estimate. The stated properties of c follow from Proposition 5.1 since the condition that E have an irrational point of order two is equivalent to having $c_2 \neq 1$. This follows since $L_2 = J_2$. □

6. Concluding remarks

For any elliptic curve defined over $\mathbb{Q}$ the proof of Theorem 2 may be modified to show that $|\mathrm{III}_p| = 4$ for a positive proportion of primes p, assuming GRH in the non-CM case. It is also possible to give generalizations of our results for an elliptic curve defined over a number field.

An open problem is to prove unconditionally the existence of infinitely many primes p for which III_p is trivial for any non-CM curve E with an irrational point of order 2. The method used in the cyclicity problem [GM], which relies on sieve arguments for primes in arithmetic progressions, is not directly applicable since the field J_n does not contain the nth cyclotomic field.

It follows from [Mi] that, under the same conditions as in Theorem 2, the Brauer groups of the reductions of $E \times E$ are trivial for a positive proportion of primes. It seems interesting to consider similar questions for the reductions of more general elliptic surfaces.

Acknowledgements. We would like to thank Don Blasius, Ram Murty and Michael Rosen for helpful discussions, and the referee for suggestions leading to improvements in the exposition of the paper.

References

[Ad] Adelmann, C.: The decomposition of primes in torsion point fields. Lecture Notes in Mathematics, 1761, Springer-Verlag, Berlin, 2001

[Co] Cojocaru, A. C.: Cyclicity of elliptic curves modulo p, Ph.D., 2002. Queen's University (Kingston, Canada)

[CFM] Cojocaru, A. C., Fouvry, E., Ram Murty, M.: The square sieve and the Lang-Trotter conjecture. To appear in Canadian J. of Math.

[CM] Cojocaru, A. C., Ram Murty, M.: Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik's problem. Preprint

[De] Deuring, M.: Teilbarkeitseigenschaften der singulären Moduln der elliptischen Funktionen und die Diskriminante der Klassengleichung (German). Comment. Math. Helv. **19**, 74–82 (1946)

[DT] Duke, W., Tóth, Á.: The splitting of primes in division fields of elliptic curves. Experimental Math. **11**, 555–565 (2003)

[El] Elkies, N. D.: The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$. Inventiones Mathematicae **89**, 561–567 (1987)

[GM] Gupta, R., Ram Murty, M.: Cyclicity and generation of points modulo p on elliptic curves. Inventiones Mathematicae **101**, 225–235 (1990)

[HR] Halberstam, H., Richert, H.-E.: Sieve methods, London Mathematical Society Monographs No. 4, Academic Press, London-New York, 1974

[Ha] Hasse, H.: Zur Geschlechtertheorie in quadratischen Zahlkörpern (German). J. Math. Soc. Japan **3**, 45–51 (1951)

[Ho] Hooley, C.: On Artin's conjecture. J. reine angew. Math. **225**, 209–220 (1967)

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

[LTa] Lang, S., Tate, J.: Principal homogeneous spaces over abelian varieties. Am. J. Math. **80**, 659–684 (1958)

[LTr] Lang, S., Trotter, H.: Frobenius distributions in GL_2-extensions. Distribution of Frobenius automorphisms in GL_2-extensions of the rational numbers, Lecture Notes in Mathematics, Vol. **504**, Springer-Verlag, Berlin-New York, 1976, iii+274

[Mi] Milne, J. S.: The Tate-Šafarevič group of a constant abelian variety. Inventiones Mathematicae **6**, 91–105 (1968)

[Mu] Ram Murty, M.: On Artin's conjecture. Journal of Number Theory **16**, 147–168 (1983)

[Oe] Oesterlé, J.: Empilements de sphères (French) [Sphere packings] Séminaire Bourbaki, Vol. 1989/90, Astérisque No. 189-190 (1990), Exp. No. 727, pp. 375–397

[Ro] Roman, S.: Field theory, Graduate Texts in Mathematics 158, Springer-Verlag, New York, 1995

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

[Se1] Serre, J-P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Inventiones Mathematicae 15 (1972), 259–331, also in Collected papers, volume III, Springer-Verlag, 1985

[Se2] Serre, J-P.: Résumé des cours de 1977-1978, Annuaire du Collège de France 1978, 67–70, in Collected papers, volume III, Springer-Verlag, 1985

[Se3] Serre, J-P.: Quelques applications du théorème de densité de Chebotarev. Publ. Math. I. H. E. S., **54** (1981), 123–201, also in Collected papers, volume III, Springer-Verlag, 1985

[Sh] Shioda, T.: Some remarks on elliptic curves over function fields, Journées Arithmétiques 1991 (Geneva), Astérisque No. 209, (1992), 12, 99–114

[Si] Silverman, J.: The arithmetic of elliptic curves, Graduate Texts in Mathematics 106, Springer-Verlag, Berlin-New York, 1986

[Su] Suzuki, M.: Group theory I, Translated from the Japanese by the author, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences] 247, Springer-Verlag, Berlin-New York, 1982

[Ta1] Tate, J.: Algebraic cycles and poles of zeta functions, 1965 Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963), 93–110, Harper and Row, New York

[Ta2] Tate, J.: On the conjectures of Birch and Swinnerton-Dyer and a geometric analog, Séminaire Bourbaki Vol.**9**, Exp. No. 306, 415–440, Soc. Math. France, Paris, 1995

[Ta3] Tate, J.: Algorithm for determining the type of a singular fiber in an elliptic pencil. Modular functions of one variable IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), 33–52, Lecture Notes in Math. Vol. **476**, Springer-Verlag, Berlin, 1975

[Ta4] Tate, J.: The arithmetic of elliptic curves. Inventiones Mathematicae **23**, 179–206 (1974)

[Wa] Washington, L. C.: Introduction to cyclotomic fields, Second edition, Graduate Texts in Mathematics 83, Springer-Verlag, New York, 1997

[Wat] Waterhouse, W.C.: Abelian varieties over finite fields. Ann. Sci. École Norm. Sup. **2**(4), pp. 521–560 (1969)

[We] Weil, A.: Sur les courbes algébriques et les variétés qui s'en déduisent (French), Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg 7 (1945). Hermann et Cie., Paris, 1948. iv+85 pp