THE OPEN BOOK SERIES 1

ANTS X
Proceedings of the Tenth Algorithmic Number Theory Symposium

On the density of abelian surfaces with Tate-Shafarevich group of order five times a square

Stefan Keil and Remke Kloosterman

msp

THE OPEN BOOK SERIES **1** (2013)
Tenth Algorithmic Number Theory Symposium
dx.doi.org/10.2140/obs.2013.1.413

msp

On the density of abelian surfaces with Tate-Shafarevich group of order five times a square

Stefan Keil and Remke Kloosterman

Let $A = E_1 \times E_2$ be the product of two elliptic curves over $\mathbb{Q}$, each having a rational 5-torsion point P_i. Set $B := A/\langle (P_1, P_2) \rangle$. In this paper we give an algorithm to decide whether the order of the Tate-Shafarevich group of the abelian surface B is square or five times a square, under the assumptions that we can find a basis for the Mordell-Weil groups of E_1 and E_2 and that the Tate-Shafarevich groups of E_1 and E_2 are finite.

We considered all pairs (E_1, E_2) with prescribed bounds on the conductor and the coefficients in a minimal Weierstrass equation. In total we considered around 20.0 million abelian surfaces, of which 49.16% have Tate-Shafarevich groups of nonsquare order.

1. Introduction

Let A be an abelian variety over a number field K. The Tate-Shafarevich group $Ш(A/K)$ plays an important role in understanding the arithmetic of A. For example, it contains information on the tightness of the upper bound on the Mordell-Weil rank obtained by m-descent. Moreover, the order of this group, which is conjectured to be finite, plays a role in the Birch and Swinnerton-Dyer conjecture.

The Tate-Shafarevich group comes with a pairing, the *Cassels-Tate pairing*, which depends on the choice of a polarization $\lambda : A \to A^\vee$:

$$\langle \cdot, \cdot \rangle_\lambda : Ш(A/K) \times Ш(A/K) \to \mathbb{Q}/\mathbb{Z}.$$

Let $Ш(A/K)_{\mathrm{nd}}$ denote the Tate-Shafarevich group modulo its maximal divisible subgroup. If λ is an isomorphism, that is, A is principally polarized, then the

MSC2010: primary 11G10; secondary 11G40, 14G10, 14K15.
Keywords: Tate-Shafarevich groups, abelian surface, Cassels-Tate equation.

induced pairing on $Ш(A/K)_{\mathrm{nd}}$ is nondegenerate. If moreover this pairing is alternating, then for all primes p the cardinality of the p-primary part $Ш(A/K)_{\mathrm{nd}}[p^\infty]$ is a perfect square; thus, if $Ш(A/K)$ is finite then it is a perfect square.

Tate [18] showed that if λ is an isomorphism and is induced from a K-rational divisor on A, then the Cassels-Tate pairing is in fact alternating, as for example for elliptic curves. However, if $\dim A > 1$ then A may not admit a principal polarization, and even when A is principally polarized this polarization need not be induced by a K-rational divisor on A. Poonen and Stoll [11] showed that in fact there exist genus-2 curves $C/\mathbb{Q}$ such that $\#Ш(J(C)/\mathbb{Q})$ is twice a square. Moreover, they showed that if one assumes that $Ш(J(C)/\mathbb{Q})$ is finite for all genus-2 curves $C/\mathbb{Q}$, then the density of genus-2 curves whose Jacobians have Tate-Shafarevich groups of nonsquare order exists, and is approximately 13%.

For arbitrary abelian varieties Flach [4] showed that if $\#Ш(A/K) = kn^2$, with k square free, then k divides 2 times the degree of every polarization on A. Hence for principally polarized abelian varieties one has that $\#Ш(A/K)$ is either a square or twice a square, if it is finite, but for general abelian varieties there are more possibilities. Stein [17] constructed, for every prime number $p < 25000$ (excluding $p = 2$ and $p = 37$), an example of a $(p-1)$-dimensional abelian variety $A_p/\mathbb{Q}$ such that $\#Ш(A_p) = pn^2$.

We restrict now to the case of $\dim A = 2$. The constructions of Poonen-Stoll and of Stein yield examples of abelian surfaces such that $\#Ш(A/K)$ is a square, twice a square, or three times a square. One might wonder which further possibilities occur. Recently, the first author [6] showed that there exist abelian surfaces such that the Tate-Shafarevich group has order five times a square and seven times a square.

In this paper we will take a closer look at the construction of abelian surfaces with Tate-Shafarevich group of order five times a square. The examples of [6] are members of a two-dimensional family of abelian surfaces with a polarization of degree 5^2. Moreover, one can show that for a general member of this family, every polarization it possesses has degree a multiple of 5; thus they are not a priori excluded by Flach's theorem and might have a Tate-Shafarevich group of order five times a square.

The construction of this family goes as follows. Let (E, O) be an elliptic curve over $\mathbb{Q}$ with a point P of order 5. Then there exists a $d \in \mathbb{Q}^*$ such that $((E, O), P)$ is isomorphic to $((E_d, O), (0, 0))$, where

$$E_d : \ y + (d+1)xy + dy = x^3 + dx^2.$$

Take two numbers $d_1, d_2 \in \mathbb{Q}^*$ and consider $B_{d_1,d_2} := E_{d_1} \times E_{d_2}/\langle (0,0) \times (0,0) \rangle$. Then $A_{d_1,d_2} := E_{d_1} \times E_{d_2} \to B_{d_1,d_2}$ is an isogeny of degree 5. Moreover, if the two elliptic curves are not isogenous, then all polarizations on B_{d_1,d_2} have degree

divisible by 5. The B_{d_1,d_2}'s are the family we consider. In our case we know that $Ш(A_{d_1,d_2}/\mathbb{Q})$ has square order, if it is finite, since it is isomorphic to the product of the two Tate-Shafarevich groups of E_{d_1} and E_{d_2}.

The behavior of the Tate-Shafarevich group under isogenies is well-known. This behavior is part of Tate's proof of the invariance of the Birch and Swinnerton-Dyer conjecture; for more on this see Section 2. The upshot of this is the following: Let $\varphi : A \to B$ be an isogeny and assume that either $\#Ш(A/K)$ or $\#Ш(B/K)$ is finite (which implies that both are finite). Denote by $\varphi^\vee : B^\vee \to A^\vee$ the dual isogeny. For a field $L \supseteq K$ denote by $\varphi_L : A(L) \to B(L)$ the induced map on L-rational points. Let S be a finite set of places containing the primes where A has bad reduction, the infinite places, and the primes dividing the degree of φ. Then the following holds:

$$\frac{\#Ш(A/K)}{\#Ш(B/K)} = \frac{\#\ker\varphi_K \#\operatorname{coker}\varphi_K^\vee}{\#\ker\varphi_K^\vee \#\operatorname{coker}\varphi_K} \prod_{v\in S} \frac{\#\operatorname{coker}\varphi_{K_v}}{\#\ker\varphi_{K_v}}.$$

In Sections 4 and 5 we show that for our choice of abelian surfaces the above-mentioned cardinalities of kernels and cokernels can be determined, provided one has a basis for the Mordell-Weil group of both E_{d_1} and E_{d_2}. (Actually something weaker is enough; see the end of Section 4.) Hence, given bases for the Mordell-Weil groups of both elliptic curves we can determine whether $\#Ш(B/\mathbb{Q})$, if finite, is a square or a nonsquare.

For all pairs (d_1, d_2) with $d_i = u_i/v_i$ where $\max(|u_i|, |v_i|)$ is bounded by $N = 50{,}000$ and where the conductor of E_{d_i} is bounded by $C = 10^6$, we computed this product of cardinalities of kernels and cokernels. There are 2,445,366 such pairs, and 47.01% of these surfaces have a Tate-Shafarevich group of nonsquare order (assuming that $Ш(E_{d_1}/\mathbb{Q})$ and $Ш(E_{d_2}/\mathbb{Q})$ are finite). We also computed these cardinalities for all pairs (d_1, d_2) such that the absolute value of the numerator and denominator of d_i is bounded by $N = 100$. There are 18,522,741 such pairs, and 49.31% of them have Tate-Shafarevich group of nonsquare order. Based on our computations, we expect that the density of abelian surfaces B_{d_1,d_2} with nonsquare Tate-Shafarevich groups exists and is around 50%. For some heuristics see the end of the final section.

The outline of this paper is as follows. In Section 2 we discuss some preliminaries and in Section 3 we explain in more detail the construction of the family of abelian surfaces we consider. In Section 4 we discuss how we can calculate the global quotient and which conditions on E_{d_1} and E_{d_2} are needed for this. In Section 5 we discuss how we calculate the local quotient, which turns out to be a much simpler computation. In Section 6 we sketch the algorithm used for the computations of the densities, and finally in Section 7 we discuss the results we obtain.

2. Preliminaries

Let K be a number field and let G_K be the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$. For a (finite or infinite) place v of K, denote by K_v the completion of K with respect to v and by G_{K_v} the absolute Galois group of K_v.

Let A/K be an abelian variety. Denote by $A^\vee$ the dual abelian variety. Then the *Tate-Shafarevich group* of A/K is defined as

$$Ш(A/K) := \ker\Big(H^1(G_K, A) \to \prod_v H^1(G_{K_v}, A)\Big),$$

where the product is taken over all finite and infinite places of K. Let $\varphi : A \to B$ be an isogeny of abelian varieties. Then the *φ-Selmer group of A/K* is defined as

$$S^\varphi(A/K) := \ker\Big(H^1(G_K, A[\varphi]) \to \prod_v H^1(G_{K_v}, A)\Big).$$

The Tate-Shafarevich group is a torsion group. It is conjectured to be finite, and the φ-Selmer group is known to be finite. The m-torsion subgroup of the Tate-Shafarevich group fits in an exact sequence

$$0 \to A(K)/mA(K) \to S^{[m]}(A/K) \to Ш(A/K)[m] \to 0.$$

That is, it measures the difference between the m-Selmer group and $A(K)/mA(K)$. In theory the m-Selmer group is computable; hence the Tate-Shafarevich group measures the difference between the upper bound on the Mordell-Weil rank obtained by doing m-descent and the actual Mordell-Weil rank of A.

The Tate-Shafarevich group plays also a role in the Birch and Swinnerton-Dyer conjecture:

Conjecture 2.1 (Birch and Swinnerton-Dyer). *Let A/K be an abelian variety and let $L(A, s)$ be its L-series. Set $r := \mathrm{rk}\, A(K)$. Then $Ш(A/K)$ is finite, $L(A, s)$ has a zero of exact order r at $s = 1$, and*

$$\lim_{s\to 1} \frac{L(A, s)}{(s-1)^r} = \frac{2^r \# Ш(A/K) R_A \prod \int_{A(K_v)} |\omega|_v}{\#A(K)_{\mathrm{tor}} \# A^\vee(K)_{\mathrm{tor}}}. \tag{1}$$

The left hand side of (1) is invariant under isogeny. Cassels [2] (for the case $\dim A = 1$) and Tate [18] (for the general case $\dim A \geq 1$) proved that the right hand side is also invariant under isogeny. That is, if $\varphi : A \to B$ is an isogeny then

$$\frac{\# Ш(A/K)}{\# Ш(B/K)} = \frac{R_B \# A(K)_{\mathrm{tor}} \# A^\vee(K)_{\mathrm{tor}} \prod \int_{B(K_v)} |\omega|_v}{R_A \# B(K)_{\mathrm{tor}} \# B^\vee(K)_{\mathrm{tor}} \prod \int_{A(K_v)} |\omega|_v}.$$

This formula was used by Schaefer and the second author [9] to provide examples of elliptic curves with large Selmer groups, by Matsuno [10] and by the second author [8] to provide examples of elliptic curves with large Tate-Shafarevich groups, and by Flynn and Grattoni [5] to compute several Selmer groups.

However, the right hand side of (1) is not well-suited for calculation. One can rewrite the right hand side as follows: For a field $L \supseteq K$, let φ_L denote the group homomorphism $\varphi_L : A(L) \to B(L)$. Then

$$\frac{\#Ш(A/K)}{\#Ш(B/K)} = \frac{\#\ker\varphi_K \#\operatorname{coker}\varphi_K^\vee}{\#\ker\varphi_K^\vee \#\operatorname{coker}\varphi_K} \prod_v \frac{\#\operatorname{coker}\varphi_{K_v}}{\#\ker\varphi_{K_v}}. \tag{2}$$

We will call the first factor (with the φ_K) the *global factor*, and the second factor (with the φ_{K_v}) the *local factor*. If v is a finite prime of good reduction and v does not divides the degree of the isogeny, then $\#\operatorname{coker}\varphi_{K_v} = \#\ker\varphi_{K_v}$; hence the product on the right hand side is a finite product, where only the bad primes, the infinite primes, and the primes dividing the degree of the isogeny need be taken into account.

It is known that if an elliptic curve has analytic rank at most 1, then its Tate-Shafarevich group is finite and its analytic rank is equal to its Mordell-Weil rank. Throughout this paper we will assume that the same is true even for elliptic curves with larger analytic rank.

3. Constructing a family of abelian surfaces

We will construct a two-dimensional family of abelian surfaces B/K, whose members are quotients of products of two elliptic curves E_1, E_2 by an isogeny of degree 5. Therefore $\#Ш(B/K)\cdot 5^a = \#Ш(E_1 \times E_2)$, for some $a \in \mathbb{Z}$. Since $\#Ш(E_1 \times E_2)$ is a square, it follows that $\#Ш(B/K)$ modulo squares is one of $\{1, 5\}$. Additionally, we have that for a general member of this family every polarization has degree divisible by 5. Thus Flach's theorem does not restrict us further.

Let G/K be a group scheme of prime order ℓ. Let E_1, E_2 be two elliptic curves over K such that G is a subgroup scheme of both E_1 and E_2. Let $A = E_1 \times E_2$ and $B = A/G$, where G is embedded diagonally in A. Then the natural isogeny $\varphi : A \to B$ has degree ℓ. Moreover, one can show that either E_1 and E_2 are isogenous or every polarization on B has degree a multiple of ℓ. Hence for general E_1, E_2 we are in the second case.

Consider the case $G = \mathbb{Z}/\ell\mathbb{Z}$; that is, the case in which G is generated by a K-rational point. Since for $\ell > 4$ the functor $Y_1(\ell)$ is representable, one has a universal family of elliptic curves E with a point P of order ℓ. In the case $\ell = 5$ the universal family is given by

$$E_d : \; y^2 + (d+1)xy + dy = x^3 + dx^2, \quad P = (0, 0),$$

for any $d \in K^*$ with $d^2 + 11d - 1 \neq 0$. The four nontrivial 5-torsion points are $(0,0)$, $(-d, d^2)$, $(-d, 0)$, and $(0, -d)$. If we move $(0, -d)$ to $(0,0)$ and bring the curve into standard form we obtain E_d. If we move $(-d, d^2)$ or $(-d, 0)$ to $(0,0)$ and bring the elliptic curve into standard form we obtain $E_{-1/d}$.

We restrict now to the case where $K = \mathbb{Q}$, $\ell = 5$, and G is generated by a $\mathbb{Q}$-rational point. Fix d_1 and d_2 in $\mathbb{Q}^*$ and set $A := E_{d_1} \times E_{d_2}$. The rational 5-torsion subgroup of A has four diagonally embedded subgroups of order 5. Let $G = \mathbb{Z}/5\mathbb{Z}$ be one of those, so that G is the subscheme of A generated by $(0,0) \times [n](0,0)$ for some $n \in \{1, 2, 3, 4\}$. Let $B := A/G$. Then B is a candidate for an abelian surface such that $Ш(B/\mathbb{Q})$ has order five times a square. To actually check whether $Ш(B/\mathbb{Q})$ has nonsquare order we will now calculate both the local and the global factor.

Note that the 16 surfaces $B/\mathbb{Q}$ one obtains by replacing d_i by $-1/d_i$ and using the four values of n break into two sets of 8 isomorphic surfaces. For fixed d_1, d_2 the surfaces corresponding to $n = 1, 4$ lie in one of these isomorphism classes and those for $n = 2, 3$ in the other one. We will see in the next two sections that for fixed d_1, d_2 the size of $Ш(B/\mathbb{Q})$ is independent of n, and so all 16 surfaces will have Tate-Shafarevich groups of the same cardinality. Therefore, for our computations we will only consider the case $d_1, d_2 > 0$ and $n = 1$.

Let A' be the quotient of $E_{d_1} \times E_{d_2}$ by the group scheme generated by $(0,0) \times O$ and $O \times (0,0)$, let E'_{d_i} be the quotient of E_{d_i} by $\langle (0,0) \rangle$, and let η_i be the natural isogeny from E_{d_i} to E'_{d_i}. The natural isogeny $\rho : A \to A'$ factors as $A \to B \to A'$. Consider now the dual picture

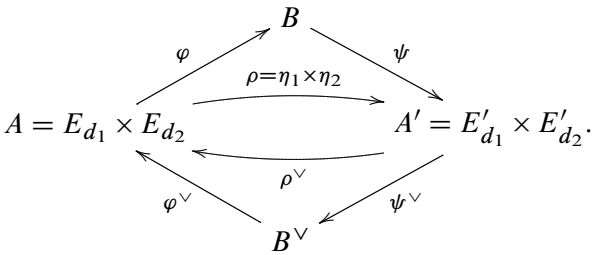
$$(A')^\vee \to B^\vee \to A^\vee.$$

Since A and A' are products of elliptic curves, they are principally polarized. Therefore we have the factorization

$$A' \to B^\vee \to A.$$

The kernel of $A' \to A$ is Cartier dual to the kernel of $A \to A'$, and hence is isomorphic to $(\boldsymbol{\mu}_5)^2$. The kernel of $A' \to B^\vee$ is isomorphic to $\boldsymbol{\mu}_5$ embedded with $(1, -n)$ in $(\boldsymbol{\mu}_5)^2$.

In summary, we have the following diagram:



Lemma 3.1. *Suppose* $L = \mathbb{Q}$. *Then* $\ker \varphi_{\mathbb{Q}} \cong \mathbb{Z}/5\mathbb{Z}$ *and* $\ker \varphi^{\vee}_{\mathbb{Q}} = 0$.

Proof. Since $A[\varphi] = \mathbb{Z}/5\mathbb{Z}$ it follows that $A'[\varphi^{\vee}] = \boldsymbol{\mu}_5$. Taking $\mathbb{Q}$-rational points yields the lemma. □

Lemma 3.2. *Suppose* $L = \mathbb{R}$. *Then* $\ker \varphi_{\mathbb{R}} \cong \mathbb{Z}/5\mathbb{Z}$ *and* $\operatorname{coker} \varphi_{\mathbb{R}} = 0$.

Proof. The first assertion is automatic. The nontrivial element in $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ acts on the fiber of an element of $B(\mathbb{R})$ under $\varphi_{\mathbb{C}}$ either by swapping elements or fixing them. Since the degree of φ is not divisible by 2 at least one element in the fiber is fixed, and hence lies in $A(\mathbb{R})$. □

Let S be the set of primes where A has bad reduction, together with 5. Using the above lemmas it follows that

$$\frac{\#Ш(A/\mathbb{Q})}{\#Ш(B/\mathbb{Q})} = \frac{\#\operatorname{coker} \varphi^{\vee}_{\mathbb{Q}}}{\#\operatorname{coker} \varphi_{\mathbb{Q}}} \prod_{v \in S} \frac{\#\operatorname{coker} \varphi_{\mathbb{Q}_v}}{\#\ker \varphi_{\mathbb{Q}_v}}.$$

In other words, in our situation the global factor from (2) simplifies, and we do not need to consider the local factor at infinity. In the next two sections we will explain how to determine the global and local factors.

4. Determining the global factor

To determine

$$\frac{\#\operatorname{coker} \varphi^{\vee}_{\mathbb{Q}}}{\#\operatorname{coker} \varphi_{\mathbb{Q}}}$$

we assume for the moment that we have a basis for the Mordell-Weil groups $E_{d_1}(\mathbb{Q})$, $E_{d_2}(\mathbb{Q})$, $E'_{d_1}(\mathbb{Q})$, and $E'_{d_2}(\mathbb{Q})$. We will now explain how one can determine $\operatorname{coker} \varphi_{\mathbb{Q}}$ and $\operatorname{coker} \varphi^{\vee}_{\mathbb{Q}}$ from this information.

Using the factorization $\rho^{\vee} = \varphi^{\vee} \circ \psi^{\vee}$ we obtain a surjective homomorphism $\operatorname{coker} \rho^{\vee}_{\mathbb{Q}} \to \operatorname{coker} \varphi^{\vee}_{\mathbb{Q}}$. With Hilbert's Theorem 90 we obtain

$$H^1(G_{\mathbb{Q}}, A'[\rho^{\vee}]) = H^1(G_{\mathbb{Q}}, \boldsymbol{\mu}_5^2) = (\mathbb{Q}^*/\mathbb{Q}^{*5})^2,$$
$$H^1(G_{\mathbb{Q}}, B^{\vee}[\varphi^{\vee}]) = H^1(G_{\mathbb{Q}}, \boldsymbol{\mu}_5) = \mathbb{Q}^*/\mathbb{Q}^{*5}.$$

Under these identifications, the surjection $\operatorname{coker} \rho^{\vee}_{\mathbb{Q}} \to \operatorname{coker} \varphi^{\vee}_{\mathbb{Q}}$ becomes the map $(x, y) \mapsto x^n/y$ from $(\mathbb{Q}^*/\mathbb{Q}^{*5})^2$ to $\mathbb{Q}^*/\mathbb{Q}^{*5}$. One sees immediately that the image of this map is independent of n, so to compute $\operatorname{coker} \varphi^{\vee}_{\mathbb{Q}}$ we may as well set $n = 1$. In order to determine $\operatorname{coker} \varphi^{\vee}_{\mathbb{Q}}$ it suffices to determine a basis in $\mathbb{Q}^*/\mathbb{Q}^{*5}$ for $\operatorname{coker} \eta^{\vee}_{1,\mathbb{Q}}$ and $\operatorname{coker} \eta^{\vee}_{2,\mathbb{Q}}$. By following [15, Exercise 10.1], this can be done quite easily: Suppose that f is a function on E_{d_i} with divisor $5(0,0) - 5O$. Then there exists a unique constant $c \in \mathbb{Q}^*/\mathbb{Q}^{*5}$ such that the map

$$\operatorname{coker} \eta^{\vee}_{i,\mathbb{Q}} \to \mathbb{Q}^*/\mathbb{Q}^{*5}$$

that sends $P \neq (0,0)$, O to $cf(P) \bmod \mathbb{Q}^{*5}$ is a well-defined injective group homomorphism, with image equal to the image of the natural embedding of $\operatorname{coker} \eta_{i,\mathbb{Q}}^{\vee}$ into $H^1(G_{\mathbb{Q}}, E'_{d_i}[\eta_i^{\vee}]) \cong \mathbb{Q}^*/\mathbb{Q}^{*5}$. In our case we can take the function f to be $-x^2 + y + xy$ and the constant c to be 1. The point $(0,0)$ is mapped to d^{-1} and O to 1 by linearity.

An element of $\mathbb{Q}^*/\mathbb{Q}^{*5}$ is determined by its valuations at each prime. Write $d = u/v$ and let S be the set of all primes p dividing five times the minimal discriminant of E_d, that is, $p \mid 5uv(u^2 + 11uv - v^2)$. Define

$$\mathbb{Q}(S,5) := \{x \in \mathbb{Q}^*/\mathbb{Q}^{*5} \mid v_p(x) \equiv 0 \bmod 5 \text{ for all } p \notin S\}.$$

From the same exercise from [15] it follows that $f(\operatorname{coker} \eta_{\mathbb{Q}}^{\vee}) \subset \mathbb{Q}(S,5)$. Hence we can represent an element of $\operatorname{coker} \eta_{\mathbb{Q}}^{\vee}$ by its valuation at each prime number $p \in S$. Once the cokernels of both $\eta_{i,\mathbb{Q}}^{\vee}$ are established, the cokernel of $\varphi_{\mathbb{Q}}^{\vee}$ can be computed easily.

To determine the cokernel of $\varphi_{\mathbb{Q}}$ we use the exact sequence

$$0 \to \ker(\psi_{\mathbb{Q}})/\varphi(\ker \rho_{\mathbb{Q}}) \to \operatorname{coker} \varphi_{\mathbb{Q}} \xrightarrow{\psi} \operatorname{coker} \rho_{\mathbb{Q}} \to \operatorname{coker} \psi_{\mathbb{Q}} \to 0.$$

Note that $\ker(\psi_{\mathbb{Q}}) = \varphi(\ker \rho_{\mathbb{Q}})$. Set $K := \mathbb{Q}(\zeta_5)$, where ζ_5 is a primitive fifth root of unity. Then the restriction map $H^1(G_{\mathbb{Q}}, \mathbb{Z}/5\mathbb{Z}) \to H^1(G_K, \mathbb{Z}/5\mathbb{Z})$ is injective, because its kernel has exponent dividing both $[K : \mathbb{Q}] = 4$ and $\#\mathbb{Z}/5\mathbb{Z}$. Since $A[\varphi]$, $A[\rho]$, and $B[\psi]$ are isomorphic over K to $\boldsymbol{\mu}_5$, $\boldsymbol{\mu}_5 \times \boldsymbol{\mu}_5$, and $\boldsymbol{\mu}_5$ (respectively), we obtain the following commutative diagram, where the vertical maps are embeddings:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \operatorname{coker} \varphi_{\mathbb{Q}} & \xrightarrow{\psi} & \operatorname{coker} \rho_{\mathbb{Q}} & \longrightarrow & \operatorname{coker} \psi_{\mathbb{Q}} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & K^*/K^{*5} & \longrightarrow & (K^*/K^{*5})^2 & \longrightarrow & K^*/K^{*5} & \longrightarrow & 0. \end{array} \tag{3}$$

As above, the third of the lower horizontal maps is just $(x,y) \mapsto x^n/y$. Hence, to determine the cokernel of $\varphi_{\mathbb{Q}}$ it suffices to determine the kernel of x^n/y on $\operatorname{coker} \eta_{1,\mathbb{Q}} \times \operatorname{coker} \eta_{2,\mathbb{Q}} \to \operatorname{coker} \psi_{\mathbb{Q}}$. Again this is independent of n, so we may take $n = 1$. We compute the kernel as follows:

(1) For some $\tilde{d} \in K$ there is a K-isomorphism $\tau : E'_d \to E_{\tilde{d}}$ that sends a generator of $\ker \eta^{\vee}$ to $(0,0)$. The map $f : E'_d \to K^*/K^{*5}$ is then

$$P \mapsto -x(\tau(P))^2 + y(\tau(P)) + x(\tau(P))y(\tau(P)).$$

Hence we have to determine τ. This can be done easily for each individual curve E'_d.

(2) To represent elements in $\operatorname{coker}\eta_{\mathbb{Q}} \subset K^*/K^{*5}$, note that the class number of K^* equals 1. Set

$$K(S,5) := \{x \in K^*/K^{*5} \mid v_{\mathfrak{p}}(x) \equiv 0 \bmod 5 \text{ for all } \mathfrak{p} \notin S\},$$

where S contains all primes $\mathfrak{p}$ of K that are bad primes for E_d or that divide 5; that is, all primes $\mathfrak{p}$ of K lying over a prime p of $\mathbb{Q}$ such that

$$p \mid 5uv(u^2 + 11uv - v^2).$$

From [15, Exercise 10.9] it follows that $f(\operatorname{coker}\eta_{\mathbb{Q}}) \subset K(S,5)$. Hence to represent elements in $\operatorname{coker}\eta_{\mathbb{Q}}$ we have to fix a generator $t_{\mathfrak{p}}$ for each prime $\mathfrak{p} \in S$, and we have to fix generators for the unit group of K modulo fifth powers. The field K is well-understood, and it is easy to see that its unit group is generated by $-\zeta_5$ and $(1+\zeta_5)$. Hence we can write

$$f(P) \equiv \zeta_5^{a_0}(1+\zeta_5)^{a_1} \prod_{\mathfrak{p}\in S} t_{\mathfrak{p}}^{v_{\mathfrak{p}}(f(P))}$$

modulo fifth powers.

Remark. We can weaken the assumption of having a basis for the Mordell-Weil groups $E_{d_1}(\mathbb{Q})$, $E_{d_2}(\mathbb{Q})$, $E'_{d_1}(\mathbb{Q})$, and $E'_{d_2}(\mathbb{Q})$. It is actually sufficient to just have generators of finite-index sublattices of these four groups, such that the indices are not divisible by 5; that is, the generators of infinite order are not divisible by 5 modulo torsion. Such sublattices suffice because their images in the cokernels of $\eta_i^\vee$, respectively η_i, are the entire cokernels. Also, it is sufficient to just know such sublattices for $E_{d_1}(\mathbb{Q})$ and $E_{d_2}(\mathbb{Q})$, because suitable dual sublattices can be easily computed using the isogenies η_i. One only has to calculate the images of the generators under η_i and then check whether their span contains points divisible by 5 modulo torsion.

5. Determining the local factor

We want to calculate

$$\frac{\#\operatorname{coker}\varphi_{\mathbb{Q}_p}}{\#\ker\varphi_{\mathbb{Q}_p}}$$

for all bad primes p and for $p = \deg\varphi = 5$. Since the kernel of $\varphi_{\mathbb{Q}_p}$ is generated by a $\mathbb{Q}$-rational point it follows that $\#\ker\varphi_{\mathbb{Q}_p} = 5$. The size of the cokernel of $\varphi_{\mathbb{Q}_p}$ depends on the reduction of E_{d_1} and E_{d_2}, but turns out to be independent of n.

For $\eta := \eta_i$, we first describe how $\operatorname{coker}\eta_{\mathbb{Q}_p}$ depends on the reduction type of $E := E_{d_i}$. Write $d_i =: u/v$ with $u, v \in \mathbb{Z}$ and $\gcd(u,v) = 1$. Then E has global minimal equation

$$E : y^2 + (u+v)xy + uvy = x^3 + uv^2x^2$$

and discriminant $-(uv)^5(u^2+11uv-v^2)$.

Lemma 5.1. *The elliptic curve E has the following reduction type at a prime p.*

(1) *If $p \mid uv$ then the reduction is split multiplicative and the point $(0,0)$ does not lie on the identity component of the Néron model of E.*

(2) *If $p \mid u^2+11uv-v^2$ then $(0,0)$ lies on the identity component of the Néron model of E and either $p=5$, or $p \equiv \pm 1 \bmod 5$ holds. If $p=5$ the reduction is additive, if $p \equiv 1 \bmod 5$ then the reduction is split multiplicative, and if $p \equiv 4 \bmod 5$ then the reduction type is nonsplit multiplicative.*

Proof. Let $\overline{E}$ be $E \bmod p$ and let $\overline{E}_{\mathrm{ns}}$ be the smooth locus of $\overline{E}$. If $p \mid uv$ then $\overline{E}$ has equation $y^2+\alpha xy = x^3$ for some nonzero $\alpha \in \mathbb{Z}/p\mathbb{Z}$. In particular, $(0,0) \bmod p$ is a node of $\overline{E}$ and the tangent cone is generated by $x=-\alpha y$ and $y=0$, hence the reduction is split multiplicative. Since $(0,0)$ reduces to the singular point of $\overline{E}$ this point does not lie on the identity component of the Néron model of E.

If $p \mid u^2+11uv-v^2$ then the reduction of $(0,0)$ is both on $\overline{E}_{\mathrm{ns}}$ and is nontrivial. In particular the order of the reduction of $(0,0)$, which is 5, divides $\#\overline{E}_{\mathrm{ns}}(\mathbb{F}_p)$. If the reduction is split multiplicative this group has order $p-1$, if the reduction is nonsplit this group has order $p+1$, and if the reduction is additive this group has order p; that is, $p \equiv 1 \bmod 5$, $p \equiv -1 \bmod 5$, and $p=5$ respectively. □

Let $E' := E'_{d_i}$ be the isogenous elliptic curve. Denote by $c_{E,p}$ and $c_{E',p}$ the local Tamagawa numbers, that is, the number of components of the Néron model. We refer to the ratio of $c_{E',p}$ to $c_{E,p}$ as the *Tamagawa quotient*.

Lemma 5.2. *For the Tamagawa quotient we have*

$$\frac{c_{E',p}}{c_{E,p}} = \begin{cases} 1/5 & \text{if } p \mid uv, \\ 5 & \text{if } p \mid u^2+11uv-v^2 \text{ and } p \equiv 1 \bmod 5, \\ 1 & \text{otherwise.} \end{cases}$$

Proof. Since η has degree 5 it follows that $c_{E',p}/c_{E,p} = 5^a$ for some $a \in \mathbb{Z}$. If the reduction is different from split multiplicative then $c_{E,p}$ and $c_{E',p}$ are at most 4, hence $a=0$ and $c_{E,p} = c_{E',p}$.

In [6, Proposition 2.16] it is shown by using Tate curves that if the reduction is split multiplicative then $a \in \{-1,1\}$, depending on whether or not the kernel is on the identity component of the Néron model. □

If $p \nmid \deg \eta = 5$ then from [12, Lemma 3.8] it follows that

$$\frac{\#\operatorname{coker} \eta_{\mathbb{Q}_p}}{\#\ker \eta_{\mathbb{Q}_p}} = \frac{c_{E',p}}{c_{E,p}}.$$

Using this, we easily obtain the following lemma:

Lemma 5.3. *Suppose p is a prime different from 5. We have*

$$\operatorname{coker}\eta_{\mathbb{Q}_p} \cong \begin{cases} \mathbb{Z}/5\mathbb{Z} & \text{if } p \text{ is good for } E, \\ 0 & \text{if } p \mid uv, \\ (\mathbb{Z}/5\mathbb{Z})^2 & \text{if } p \mid u^2 + 11uv - v^2 \text{ and } p \equiv 1 \bmod 5, \\ \mathbb{Z}/5\mathbb{Z} & \text{if } p \mid u^2 + 11uv - v^2 \text{ and } p \equiv 4 \bmod 5. \end{cases}$$

Now $\operatorname{coker}\eta_{\mathbb{Q}_p} \subset H^1(G_{\mathbb{Q}_p}, \mathbb{Z}/5\mathbb{Z})$. From Theorem 2 and Proposition 17 of [14, §II.5] it follows that for $p \nmid \deg\eta = 5$ we have

$$\#H^1(G_{\mathbb{Q}_p}, \mathbb{Z}/5\mathbb{Z}) = \#H^0(G_{\mathbb{Q}_p}, \mathbb{Z}/5\mathbb{Z})\,\#H^0(G_{\mathbb{Q}_p}, \boldsymbol{\mu}_5) = 5^a,$$

where $a = 1$ if $p \equiv 4 \bmod 5$ and $a = 2$ if $p \equiv 1 \bmod 5$. From this we deduce the following:

Proposition 5.4. *Suppose that $p \neq 5$ is a prime dividing $u^2 + 11uv - v^2$ (so that E has bad reduction at p). Then* $\operatorname{coker}\eta_{\mathbb{Q}_p} = H^1(G_{\mathbb{Q}_p}, \mathbb{Z}/5\mathbb{Z})$.

We now return to our abelian surface A. The above proposition enables us to determine $\operatorname{coker}\varphi_{\mathbb{Q}_p}$ for bad primes different from 5.

Proposition 5.5. *Suppose p is a prime of bad reduction for A and $p \neq 5$. Then*

$$\operatorname{coker}\varphi_{\mathbb{Q}_p} \cong \begin{cases} 0 & \text{if } p \mid u_1v_1u_2v_2, \\ (\mathbb{Z}/5\mathbb{Z})^2 & \text{if } p \mid \gcd(u_1^2 + 11u_1v_1 - v_1^2, u_2^2 + 11u_2v_2 - v_2^2) \\ & \quad \text{and } p \equiv 1 \bmod 5, \\ \mathbb{Z}/5\mathbb{Z} & \text{otherwise}. \end{cases}$$

Proof. Recall that

$$\operatorname{coker}\varphi_{\mathbb{Q}_p} = \ker(\operatorname{coker}\eta_{1,\mathbb{Q}_p} \times \operatorname{coker}\eta_{2,\mathbb{Q}_p} \to \operatorname{coker}\psi_{\mathbb{Q}_p}),$$

which equals

$$(\operatorname{coker}\eta_{1,\mathbb{Q}_p} \times \operatorname{coker}\eta_{2,\mathbb{Q}_p}) \cap \ker\big(H^1(G_{\mathbb{Q}_p}, \mathbb{Z}/5\mathbb{Z})^2 \to H^1(G_{\mathbb{Q}_p}, \mathbb{Z}/5\mathbb{Z})\big).$$

The surjective map $H^1(G_{\mathbb{Q}_p}, \mathbb{Z}/5\mathbb{Z})^2 \to H^1(G_{\mathbb{Q}_p}, \mathbb{Z}/5\mathbb{Z})$ is given by $(x, y) \mapsto nx - y$. Suppose that $p \mid u_1v_1u_2v_2$. Then by Lemma 5.3 we have $\operatorname{coker}\eta_{i,\mathbb{Q}_p} = 0$ for at least one i, and therefore $\operatorname{coker}\varphi_{\mathbb{Q}_p} = 0$.

Suppose now $p \nmid u_1v_1u_2v_2$. By assumption one of the E_{d_i}, say E_{d_1}, has bad reduction at p. Since $p \nmid 5u_1v_1$ it follows from the above proposition that $\operatorname{coker}\eta_{1,\mathbb{Q}_p} = H^1(G_{\mathbb{Q}_p}, \mathbb{Z}/5\mathbb{Z})$ and hence $\operatorname{coker}\varphi_{\mathbb{Q}_p} \cong \operatorname{coker}\eta_{2,\mathbb{Q}_p}$. Now E_{d_2} has either additive or good reduction. The reduction of E_{d_2} is additive if and only if $p \mid \gcd(u_1^2 + 11u_1v_1 - v_1^2, u_2^2 + 11u_2v_2 - v_2^2)$. Now apply Lemma 5.3 to deduce the structure of $\operatorname{coker}\eta_{2,\mathbb{Q}_p}$, hence the structure of $\operatorname{coker}\varphi_{\mathbb{Q}_p}$. □

It remains to check the case $p = 5$. As before, we first have a look at the elliptic curve E. If $5 \mid uv$ then as above the reduction is split multiplicative and $c_{E',p}/c_{E,p} = 1/5$. Using Tate curves one easily shows that $\operatorname{coker} \eta_{\mathbb{Q}_p} = 0$.

If $5 \mid u^2 + 11uv - v^2$ then the reduction is additive. In particular, the component groups of E and E' have the same order, which is also the case if the reduction is good. Therefore $c_{E',p}/c_{E,p} = 1$. The isogeny $\eta : E \to E'$ can be written as a power series in one variable in a neighborhood of the point O. Again from [12, Lemma 3.8] it follows that

$$\frac{\#\operatorname{coker} \eta_{\mathbb{Q}_5}}{\#\ker \eta_{\mathbb{Q}_5}} = |\eta'(0)|_5^{-1},$$

where $|\eta'(0)|_5$ is the normalized 5-adic absolute value of the leading coefficient of the power series representation of η evaluated at 0. This can be easily computed using Vélu's algorithm [19]. In Lemma 4.1 and Proposition 4.2 of [6] it is shown that in the additive case we have $v_5(u^2 + 11uv - v^2) \in \{2, 3\}$; furthermore, if $v_5(u^2 + 11uv - v^2) = 2$ then $|\eta'(0)|_5 = 1$, while if $v_5(u^2 + 11uv - v^2) = 3$ then $|\eta'(0)|_5 = 1/5$. If E has good reduction at $p = 5$ then it follows that $\#\operatorname{coker} \eta_{\mathbb{Q}_p} = \#\ker \eta_{\mathbb{Q}_p}$, because in this case we also have $|\eta'(0)|_5 = 1$. We summarize as follows.

Lemma 5.6. *We have*

$$\operatorname{coker} \eta_{\mathbb{Q}_p} \cong \begin{cases} \mathbb{Z}/5\mathbb{Z} & \text{if } 5 \text{ is good for } E, \\ 0 & \text{if } 5 \mid uv, \\ (\mathbb{Z}/5\mathbb{Z})^2 & \text{if } 5^3 \mid u^2 + 11uv - v^2, \\ \mathbb{Z}/5\mathbb{Z} & \text{if } 5 \mid u^2 + 11uv - v^2 \text{ and } 5^3 \nmid u^2 + 11uv - v^2. \end{cases}$$

Now we can calculate $\operatorname{coker} \varphi_{\mathbb{Q}_p}$ in the remaining case $p = 5$.

Lemma 5.7. *We have*

$$\#\operatorname{coker} \varphi_{\mathbb{Q}_5} = \begin{cases} 1 & \text{if } 5 \mid u_1 v_1 u_2 v_2, \\ 5^2 & \text{if } 5^3 \mid \gcd(u_1^2 + 11u_1v_1 - v_1^2, u_2^2 + 11u_2v_2 - v_2^2), \\ 5 & \text{otherwise.} \end{cases}$$

Proof. If $\operatorname{coker} \eta_{i,\mathbb{Q}_5} = 0$ for one i, then $\operatorname{coker} \varphi_{\mathbb{Q}_5} = 0$. The first condition is equivalent to $5 \mid u_1 v_1 u_2 v_2$.

Suppose now that $\operatorname{coker} \eta_{i,\mathbb{Q}_5} \neq 0$ for both i, which implies that $p = 5$ is additive or good for E_{d_i}. From Proposition 18 and Theorem 5 of [14, §II.5], we find that $H^1(G_{\mathbb{Q}_5}, \mathbb{Z}/5\mathbb{Z}) = (\mathbb{Z}/5\mathbb{Z})^2$ and $H^1_{\mathrm{nr}}(G_{\mathbb{Q}_5}, \mathbb{Z}/5\mathbb{Z}) = \mathbb{Z}/5\mathbb{Z}$. As in the proof of Proposition 5.5, we have that if $\operatorname{coker} \eta_{1,\mathbb{Q}_5} = H^1(G_{\mathbb{Q}_5}, \mathbb{Z}/5\mathbb{Z})$, then $\operatorname{coker} \varphi_{\mathbb{Q}_5} \cong \operatorname{coker} \eta_{2,\mathbb{Q}_5}$ and vice versa. This gives the second case of the lemma, since $\operatorname{coker} \eta_{i,\mathbb{Q}_5} = (\mathbb{Z}/5\mathbb{Z})^2$ if and only if $5^3 \mid u_i^2 + 11u_i v_i - v_i^2$, and $\operatorname{coker} \eta_{i,\mathbb{Q}_5} = \mathbb{Z}/5\mathbb{Z}$ otherwise.

It remains to consider $\operatorname{coker}\eta_{1,\mathbb{Q}_5} = \operatorname{coker}\eta_{2,\mathbb{Q}_5} = (\mathbb{Z}/5\mathbb{Z})$. In this case one can show that $\operatorname{coker}\eta_{i,\mathbb{Q}_5} = H^1_{\mathrm{nr}}(G_{\mathbb{Q}_5}, \mathbb{Z}/5\mathbb{Z})$, for both i; see [6, Propositions 2.10 and 3.5; 13, §3]. Thus the kernel of $\operatorname{coker}\eta_{1,\mathbb{Q}_5} \times \operatorname{coker}\eta_{2,\mathbb{Q}_5} \to \operatorname{coker}\psi_{\mathbb{Q}_5}$, which equals $\operatorname{coker}\varphi_{\mathbb{Q}_5}$, has five elements. This finishes the proof. □

Putting everything together yields the following proposition:

Proposition 5.8. *Let p be a prime. Then*

$$\frac{\#\operatorname{coker}\varphi_{\mathbb{Q}_p}}{\#\ker\varphi_{\mathbb{Q}_p}}$$

is a nonsquare if and only if one of the following occurs:

(1) $p \mid u_1 v_1 u_2 v_2$,

(2) $p \mid \gcd(u_1^2 + 11u_1v_1 - v_1^2, u_2^2 + 11u_2v_2 - v_2^2)$ *and* $p \equiv 1 \bmod 5$, *or*

(3) $p^3 \mid \gcd(u_1^2 + 11u_1v_1 - v_1^2, u_2^2 + 11u_2v_2 - v_2^2)$ *and* $p = 5$.

6. Algorithm

In this section we present the algorithm that we used to produce the databases of abelian surfaces that we studied. Our code was implemented in Sage [16] and is available at [7]. The algorithm consists of two main steps and an initialization step, which we call step 0. In step 1 one creates a database of elliptic curves having a point P of order 5, which are parametrized by two coprime positive integers (u, v). One has to specify which pairs (u, v) one wants to consider. In step 2 one takes such a database of elliptic curves E_d, for $d = u/v$, goes over all pairs of these curves and determines whether the order of the Tate-Shafarevich group of the abelian surfaces $B_{d_1,d_2} = E_{d_1} \times E_{d_2}/\langle(P_1, P_2)\rangle$ is a square. For trivial reasons, pairs of the same elliptic curve are omitted and pairs are considered to be without order.

Algorithm 6.1.

Input: A height bound N and, optionally, a conductor bound C.

Output: The list of all unordered pairs $\{d_1, d_2\}$, where d_1 and d_2 are distinct positive rationals of height at most N such that the elliptic curves E_{d_1} and E_{d_2} have conductor at most C, together with an indication of whether $Ш(B_{d_1,d_2}/\mathbb{Q})$ has square order.

0. *Initialization.* Fix a (large) integer M. For each prime number $p \le M$ determine the prime ideals $\mathfrak{p}$ of $K = \mathbb{Q}(\zeta_5)$ above p and fix an ordering of them. Then fix for each prime ideal $\mathfrak{p}$ a generator $t_{\mathfrak{p}}$.

1. *Creation of a database $\mathcal{D}$ of elliptic curves.* For each pair of coprime positive integers (u, v) such that $\max(u, v) \leq N$, set $E := E_d$, where $d = u/v$. If no conductor bound is given or the conductor of E is at most C, do the following:
   (a) Collect all the primes dividing $5uv(u^2 + 11uv - v^2)$ in a set S.
   (b) Collect all the primes dividing uv in a set T.
   (c) Collect all the primes $p \equiv 1 \bmod 5$ dividing $u^2 + 11uv - v^2$ in a set U.
   (d) If $v_5(u^2 + 11uv - v^2) = 3$, add $p = 5$ to the set U.
   (e) Determine the analytic rank r of E.
   (f) Determine a system of r generators of a sublattice Λ of $E(\mathbb{Q})$, such that the points of infinite order modulo torsion are not divisible by 5. Take the image of Λ in $\mathbb{Q}(S, 5)$ to determine a basis P of $\operatorname{coker} \eta_{\mathbb{Q}}^{\vee} \subset \mathbb{Q}(S, 5)$. The data for each basis element consists of a pair for each prime in S, where the first entry is the corresponding element in S and the second entry is the exponent as an element in $\mathbb{Z}/5\mathbb{Z}$.
   (g) Calculate the image of Λ under η in $E'(\mathbb{Q})$ and determine which image points are divisible by 5 modulo torsion. Divide if possible and determine the nontrivial 5-torsion points of $E'(\mathbb{Q})$ to get a sublattice Λ' of $E'(\mathbb{Q})$, such that the points of infinite order modulo torsion are not divisible by 5. Use this information to compute $\dim \operatorname{coker} \eta_{\mathbb{Q}}$.
   (h) Take the image of Λ' in $K(S, 5)$ to determine a basis Q for $\operatorname{coker} \eta_{\mathbb{Q}} \subset K(S, 5)$. The data for each basis element consists of a pair for each prime in S and a pair for the units. For the primes p in S, the first entry is p and the second entry is a list of elements in $\mathbb{Z}/5\mathbb{Z}$, containing as many entries as there are prime ideals $\mathfrak{p}$ in K over p; for the units, the first element is 1 and the second is the list of exponents of the units.
   (i) Append $((u, v), S, T, U, P, Q)$ to the database $\mathcal{D}$.
2. *Determination of surfaces with* Ш *of nonsquare order.* For each pair

$$((u_1, v_1), S_1, T_1, U_1, P_1, Q_1) \quad \text{and} \quad ((u_2, v_2), S_2, T_2, U_2, P_2, Q_2)$$

   of distinct elements $\mathcal{D}$ (modulo ordering), do the following:
   (a) Set $L := \#(U_1 \cap U_2) - \#(T_1 \cup T_2)$.
   (b) Fix an ordering for $\mathcal{S} := S_1 \cup S_2$.
   (c) Write out the elements from $P_1 \cup P_2$ into a matrix with respect to $\mathcal{S}$. This gives a matrix with entries in $\mathbb{Z}/5\mathbb{Z}$. Calculate the rank of this matrix, which equals the dimension of $\operatorname{coker} \varphi_{\mathbb{Q}}^{\vee}$.
   (d) Write out the elements from $Q_1 \cup Q_2$ into a matrix with respect to the prime ideals $(t_{\mathfrak{p}})$ lying over the primes of $\mathcal{S}$ (and with respect to the units).

This gives a matrix with entries in $\mathbb{Z}/5\mathbb{Z}$. Calculate the rank of this matrix, which equals the dimension of coker $\psi_{\mathbb{Q}}$.

(e) Set $G := \dim \operatorname{coker} \varphi_{\mathbb{Q}}^{\vee} - \dim \operatorname{coker} \eta_{1,\mathbb{Q}} - \dim \operatorname{coker} \eta_{2,\mathbb{Q}} + \dim \operatorname{coker} \psi_{\mathbb{Q}}$. (We have $\dim \operatorname{coker} \varphi_{\mathbb{Q}} = \dim \operatorname{coker} \eta_{1,\mathbb{Q}} + \dim \operatorname{coker} \eta_{2,\mathbb{Q}} - \dim \operatorname{coker} \psi_{\mathbb{Q}}$ from the sequence (3), so $G = \dim \operatorname{coker} \varphi_{\mathbb{Q}}^{\vee} - \dim \operatorname{coker} \varphi_{\mathbb{Q}}$.)

(f) Output $(d_1, d_2, L+G \bmod 2)$, where $d_i = u_i/v_i$.

Remark. The final step is justified as follows: The local factor (without the infinite prime) is a nonsquare if and only if L is odd, and the global factor (without the kernels) is a nonsquare if and only if G is odd. Since the contribution of the infinite prime and the kernels cancel, we have that $Ш(B_{d_1,d_2}/\mathbb{Q})$ has nonsquare order if and only if $L + G$ is odd.

The databases we constructed and the results we obtained are summarized in the following section. To conclude this section, we make some comments on our implementation.

In the cases we considered, Step 0 is not computationally demanding. For example, on a desktop computer it may take some seconds up to a few minutes to compute all generators for all prime ideals of K lying over all primes up to 500,000. Step 2 is also no problem. It consists only of simple set operations and the calculation of the ranks of small matrices with coefficients in $\mathbb{Z}/5\mathbb{Z}$. A few million pairs of elliptic curves can be considered in under an hour.

The computationally demanding part is step 1. There are two main issues. The most problematic calculation is the determination of r generators of a finite index subgroup of the Mordell-Weil group, where r is the analytic rank. We used the standard Sage method `E.point_search(height_limit=18,rank_bound=r)`, and in case this did not come up with enough points we tried some of the remaining curves with `E.gens()`. In several cases these methods did not provide an answer within 48 hours on a single CPU. For these curves we used the method `MordellWeilShaInformation()` in Magma [1], which could handle all our problematic curves in a few seconds each.

The second problematic calculation in the actual code is the computation of the image of coker $\eta_{\mathbb{Q}}$ in $K(S, 5)$. The computation involves factoring ideals of K that are generated by elements of possibly very big norm. For example, the curve E_d, for $d = 1/94$, has analytic rank 1; the numerator and denominator of the image of the point of infinite order in $K(S, 5)$ each have about 600 digits, and Sage was not able to factor the corresponding ideal. As we already knew that the image was trivial, since the dimension of coker $\eta_{\mathbb{Q}}$ was zero, we could skip this calculation. Considering this additional information in the algorithm allowed us to deal with all of the curves we tried. This problem might be avoidable by trying another strategy working modulo primes. The rest of step 1 is not a problem for moderately

chosen $d = u/v$, because it consists mainly of finding the prime factorizations of integers and of rational polynomials of degree 25 (to divide points by 5), as well as calculating isogenies and analytic ranks. In a few hours on a desktop computer, one could produce a database of a few thousand curves.

Remark. At various places in the algorithm we need to assume the Birch and Swinnerton-Dyer conjecture. In step 1(e) we compute the analytic rank of an elliptic curve. To actually compute the analytic rank of a curve E of analytic rank r, we need to assume that the Birch and Swinnerton-Dyer conjecture holds for all elliptic curves with analytic rank at most $r-2$ and that the Mordell-Weil rank of E is at least the analytic rank minus 1. Step 1(f) terminates if and only if the analytic rank of E is at least the Mordell-Weil rank of E.

A second place where we use the Birch and Swinnerton-Dyer conjecture is in the computation of the quantity G in step 2(e). For this we have to assume that for both curves under consideration the analytic rank is precisely the Mordell-Weil rank. However, if we have come this far in the algorithm then we know already that the Mordell-Weil rank is at least the analytic rank.

One may replace steps 1(e) and 1(f) by an algorithm that actually computes a basis for the Mordell-Weil group. This would make the output of the algorithm unconditional. However, in the sample we take below, all elliptic curves have analytic rank at most 3, and for each of them step 1(f) terminated. Hence, to speed up our computations we preferred to determine analytic ranks rather than do full descents.

For the elliptic curves of analytic rank at least 2 we have also to assume that the Tate-Shafarevich group is finite. If this group were infinite then our algorithm would detect whether $\#\ker\varphi^*/\#\operatorname{coker}\varphi^*$ is a square. Here φ^* is the induced morphism on the Tate-Shafarevich groups.

7. Results

Using Algorithm 6.1, in a short time one can produce millions of examples of abelian surfaces over $\mathbb{Q}$ such that the order of the Tate-Shafarevich group is either a square or five times a square. In the cases arising from two elliptic curves each of analytic rank at most 1, the examples are completely unconditional. We constructed two databases of elliptic curves using step 1 of the algorithm. The first database consists of all elliptic curves E_d, where $d = u/v$ for positive integers u and v with $\max(u, v) \leq 50{,}000$, and where the conductor of E_d is bounded by $C = 10^6$. The second database consists of all elliptic curves E_d, where $d = u/v$ for positive integers u and v such that $\max(u, v) \leq 100$.

Database 1 contains 2212 elliptic curves, all of them having analytic rank $r \leq 2$. It is likely that there are no further elliptic curves of conductor at most 10^6 that

		Number of E_d of rank r					Number of E_d of rank r		
N	$\#E_d$	$r=0$	$r=1$	$r=2$	N	$\#E_d$	$r=0$	$r=1$	$r=2$
50,000	2,212	987	1,109	116	800	2,159	956	1,088	115
4,617	2,212	987	1,109	116	700	2,145	951	1,079	115
3,375	2,211	986	1,109	116	600	2,119	941	1,063	115
3,072	2,210	986	1,108	116	500	2,088	921	1,052	115
2,695	2,209	986	1,107	116	400	2,066	912	1,039	115
2,000	2,200	982	1,102	116	300	1,993	872	1,009	112
1,000	2,174	963	1,095	116	200	1,818	786	929	103
900	2,170	961	1,093	116	100	1,391	616	697	78
					50	845	394	405	46

Table 1. Summary of database 1. For each N, we give the number of curves E_d of conductor at most 10^6, where $d>0$ has height at most N. The final three columns give the number of such curves of analytic rank 0, 1, and 2.

have a rational torsion point of order 5, since there is no such curve with $4617 < \max(u, v) \leq 50{,}000$. The database is described in more detail in Table 1, where we state for each analytic rank the number of elliptic curves with conductor at most 10^6 and with $\max(u, v) \leq N$. Database 2 contains 6,087 elliptic curves. All of them have analytic rank $r \leq 3$. See Table 2 for more details. In the following we will present the results of step 2 of the algorithm applied to the two databases described above.

Database 1 yields 2,445,366 abelian surfaces B_{d_1,d_2}. It turns out that 47.01% of these surfaces have Tate-Shafarevich groups of nonsquare order. Database 2 leads to 18,522,741 abelian surfaces. The percentage of the nonsquare case is 49.31. The intersection of the two databases consists of 1,391 curves, hence we considered 966,745 surfaces twice. In total this gives 20,001,362 surfaces, of which 49.16% have a Tate-Shafarevich group of nonsquare order.

		Number of E_d of rank r					Number of E_d of rank r			
N	$\#E_d$	$r=0$	$r=1$	$r=2$	$r=3$	N	$\#E_d$	$r=0$	$r=1$	$r=2$	$r=3$
100	6,087	2,390	3,038	633	26	50	1,547	660	760	123	4
90	4,959	1,987	2,463	490	19	40	979	412	494	70	3
80	3,931	1,597	1,940	380	14	30	555	245	277	33	0
70	2,987	1,235	1,455	287	10	20	255	130	115	10	0
60	2,203	925	1,074	198	6	10	63	40	22	1	0

Table 2. Summary of database 2. For each N, we give the number of curves E_d, where $d>0$ has height at most N. The final four columns give the number of such curves of analytic rank 0, 1, 2, and 3.

rk E_1	rk E_2	$\#B$	$\%(Ш = \square)$	$\%(\mathrm{RE} \equiv \mathrm{rk}\ B)$
0	0	486,591	54.041	100.00
1	1	614,386	58.614	63.51
2	2	6,670	92.039	55.53
0	1	1,094,583	46.634	83.44
0	2	114,492	52.867	47.96
1	2	128,644	74.314	42.48
≤ 1	≤ 1	2,195,560	51.628	81.53

Table 3. Results of experiment 1 for database 1, the curves E_d of conductor at most 10^6 and with $d > 0$ of height at most 50,000. For each pair of ranks, we list the number of surfaces B obtained from elliptic curves in database 1 with those ranks. The fourth column gives the percentage of these surfaces for which Ш has square order, and the fifth column gives the percentage for which the exponent of the regulator quotient is congruent modulo 2 to the rank of the surface.

We did two different experiments with the two databases. In experiment 1 we investigated how the rank influences the squareness of the Tate-Shafarevich group. We list the result in Table 3 for database 1 and in Table 4 for database 2. The first three, respectively four, entries correspond to pairs (E_1, E_2) with the same analytic rank. The following three, respectively six, lines correspond to pairs with different

rk E_1	rk E_2	$\#B$	$\%(Ш = \square)$	$\%(\mathrm{RE} \equiv \mathrm{rk}\ B)$
0	0	2,854,855	48.598	100.00
1	1	4,613,203	48.882	80.91
2	2	200,028	73.031	44.03
3	3	325	98.154	51.08
0	1	7,260,820	51.366	91.02
0	2	1,512,870	50.567	71.36
0	3	62,140	49.891	52.73
1	2	1,923,054	52.717	59.50
1	3	78,988	60.632	46.23
2	3	16,458	84.470	48.23
≤ 1	≤ 1	14,728,878	50.051	89.59

Table 4. Results of experiment 1 for database 2, the curves E_d with $d > 0$ of height at most 100. For each pair of ranks, we list the number of surfaces B obtained from elliptic curves in database 2 with those ranks. The fourth column gives the percentage of these surfaces for which Ш has square order, and the fifth column gives the percentage for which the exponent of the regulator quotient is congruent modulo 2 to the rank of the surface.

C	$\#E$	$\#B$	$\%(Ш = \square)$	$\%(\mathrm{RE} \equiv \mathrm{rk}\, B)$
1,000,000	2,212	2,445,366	52.990	77.84
800,000	1,966	1,931,595	53.232	77.16
600,000	1,683	1,415,403	53.758	76.06
400,000	1,351	911,925	54.215	75.24
200,000	924	426,426	55.001	73.91
100,000	623	193,753	57.074	74.29
80,000	547	149,331	57.776	74.03
60,000	470	110,215	57.990	72.75
40,000	376	70,500	59.306	73.34
20,000	245	29,890	61.288	71.72
10,000	152	11,476	62.182	72.59
5,000	110	5,995	59.783	71.79
1,000	45	990	65.556	76.77

Table 5. Results of experiment 2 for database 1. For each value of C, we list the number of elliptic curves E_d having conductor at most C and with $d > 0$ of height at most 50,000. In the third column we list the number of abelian surfaces B obtained from pairs of such curves. The fourth column gives the percentage of these surfaces for which Ш has square order, and the fifth column gives the percentage for which the exponent of the regulator quotient is congruent modulo 2 to the rank of the surface.

analytic ranks, and the final line corresponds to pairs with analytic rank $r \leq 1$. If we consider abelian surfaces of fixed analytic rank of at least 4 then the density of the surfaces with square Tate-Shafarevich group seems to be significant larger than 0.5. However the surfaces with rank larger than 2 inside our family are conjectured to have density zero and our database contains very few such cases. The calculations with curves of rank $r \leq 1$ all show that the nonsquare case happens in about 50% of all cases. For both experiments we list how many abelian surfaces B_{d_1,d_2} occur in each of the cases, we state the percentage of the surfaces with square Tate-Shafarevich group, and we give the percentage of in how many cases the parity of the rank of the abelian surface agrees with the parity of the exponent of the regulator quotient (RE). Note that the results are unconditional in case $\mathrm{rk}(E_i) \leq 1$, for both E_i. If one of the analytic ranks is at least 2 then we need to make some assumptions; see the remark at the send of Section 6.

In experiment 2 we looked for the behavior of the distribution of square and nonsquare Tate-Shafarevich group orders for increasing conductor (for database 1) and height (for database 2) of the elliptic curves. For low bounds on the conductor and height, the nonsquare case was less likely. When we increase these bounds the frequency of nonsquares tends to approximately 50%. The results of experiment 2 is given in Table 5 for database 1 and Table 6 for database 2. Note that for

N	$\#E$	$\#B$	$\%(Ш = \square)$	$\%(\mathrm{RE} \equiv \mathrm{rk}\, B)$
100	6,087	18,522,741	50.694	84.14
90	4,959	12,293,361	50.821	83.66
80	3,931	7,724,415	50.941	83.32
70	2,987	4,459,591	51.235	82.51
60	2,203	2,425,503	51.461	82.00
50	1,547	1,195,831	52.211	80.85
40	979	478,731	52.764	79.92
30	555	153,735	54.157	77.12
20	255	32,385	56.384	77.11
10	63	1,953	67.179	74.04

Table 6. Results of experiment 2 for database 2. For each value of N, we list the number of curves E_d with $d > 0$ of height at most N, as well as the number of abelian surfaces B obtained from pairs of such curves. The fourth column gives the percentage of these surfaces for which Ш has square order, and the fifth column gives the percentage for which the exponent of the regulator quotient is congruent modulo 2 to the rank of the surface.

some of the surfaces we assume the weak form of the Birch and Swinnerton-Dyer conjecture mentioned above.

The two ways we ordered the elliptic curves, via conductor and via height, are natural orderings. It is conjectured that the densities obtained with respect to these orderings agree. In both cases the densities seem to exist and are around 0.5. This is in contrast to the results of Poonen and Stoll [11], who showed that the density of nonsquare #Ш for Jacobians of genus-2 curves is about 0.13, while for higher-genus curves the density tends to zero as the genus increases.

We end by giving some heuristics why we expect the density to be 50%. We expect that for a random pair $(d_1 = u_1/v_1, d_2 = u_2/v_2)$ in $\mathbb{Q}^* \times \mathbb{Q}^*$ the global factor is a square for 50% of the abelian surfaces and that the local factor is a square for 50% of them, too. We also expect these distributions to be independent. Using the 18,522,741 pairs obtained from the second database, we get numerical evidence for the independence, as illustrated in Table 7.

Global quotient	Local quotient	Percentage
square	square	26.08
square	nonsquare	24.04
nonsquare	square	25.26
nonsquare	nonsquare	24.61

Table 7. Fraction of surfaces coming from database 2 with square and nonsquare local and global quotients.

$\#(U_1 \cap U_2)$	$\#(T_1 \cup T_2)$	Percentage
even	even	46.71
even	odd	49.55
odd	even	1.80
odd	odd	1.95

Table 8. Fraction of surfaces coming from database 2 with even and odd values of $\#(U_1 \cap U_2)$ and $\#(T_1 \cup T_2)$.

Recall that the exponent of the local quotient equals $\#(U_1 \cap U_2) - \#(T_1 \cup T_2)$, hence one could prove the expected densities for the local quotient by showing that the probability that the set $(T_1 \cup T_2)$ has an even number of elements is independent of the probability that the set $(U_1 \cap U_2)$ has an even number of elements. The corresponding numerical result for database 2 is gathered in Table 8.

The global quotient is harder to control. The exponent of the torsion quotient equals 3 on a density-1 subset of the pairs (d_1, d_2); see [6, Proposition 4.6]. The results of Tables 3–6 suggest that the squareness of the regular quotient, and hence the squareness of the global quotient, is not independent of the parity of the rank. If the ranks of both of the elliptic curves E_1 and E_2 are equal to 0, hence are even, the regulator quotient equals 1, hence is a square. If one elliptic curve is of rank 0 and the other is of rank 1, then the regulator quotient is a nonsquare if and only if $\operatorname{coker} \eta_{\mathbb{Q}}$ can be generated by torsion points, where η is the usual isogeny belonging to the elliptic curve of rank 1. In database 2 we have the following situation. For the rank-1 curves it happens in about 91.2% of the cases that $\eta_{\mathbb{Q}}$ is surjective on the free part. In case both ranks are equal to 1, the regulator quotient is a square in about 80.9% of the cases. For the complete second database we get that the parity of the exponent of the regulator quotient agrees with the parity of the rank in 84.14% of the cases. If we consider only all the elliptic curves of rank ≤ 1, then we have that for abelian surfaces B_{d_1,d_2} of even rank the regulator quotient is a square in about 88.2% of the cases, and for abelian surfaces B_{d_1,d_2} of odd rank the regulator quotient is a nonsquare in about 91.0% of the cases; together, this means there is agreement 89.6% of the time. Table 9 gives the situation for the complete database 2.

Regulator quotient	$\operatorname{rk}(B_{d_1,d_2})$	Percentage
square	even	42.067
square	odd	7.931
nonsquare	even	7.927
nonsquare	odd	42.075

Table 9. Fraction of surfaces B_{d_1,d_2} coming from database 2 with square and nonsquare regulator quotient and even and odd rank.

Local quotient	$\mathrm{rk}(B_{d_1,d_2})$	Percentage
square	even	25.670
square	odd	25.675
nonsquare	even	24.324
nonsquare	odd	24.331

Table 10. Fraction of surfaces B_{d_1,d_2} coming from database 2 with square and nonsquare local quotient and even and odd rank.

In contrast to the global quotient, the squareness of the local quotient seems to be independent of the parity of the rank of the abelian surfaces. Table 10 gives the numerical results for database 2.

Acknowledgments

Keil is supported by a scholarship from the Berlin Mathematical School (BMS). Both authors thank Tom Fisher for pointing out the method `MordellWeilSha-Information` in Magma, and the referees for their comments and suggestions.

References

[1] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. MR 1484478

[2] J. W. S. Cassels, *Arithmetic on curves of genus* 1. *VIII. On conjectures of Birch and Swinnerton-Dyer*, J. Reine Angew. Math. **217** (1965), 180–199. MR 31 #3420

[3] John Cremona, Joan-Carles Lario, Jordi Quer, and Kenneth Ribet (eds.), *Modular curves and abelian varieties*: *Papers from the conference held in Bellaterra*, *July* 15–18, 2002, Progress in Mathematics, no. 224, Birkhäuser, Basel, 2004. MR 2004k:11004

[4] Matthias Flach, *A generalisation of the Cassels-Tate pairing*, J. Reine Angew. Math. **412** (1990), 113–127. MR 92b:11037

[5] E. V. Flynn and C. Grattoni, *Descent via isogeny on elliptic curves with large rational torsion subgroups*, J. Symbolic Comput. **43** (2008), no. 4, 293–303. MR 2009c:11080

[6] Stefan Keil, *Examples of abelian varieties with non-square Tate-Shafarevich group*, 2012. arXiv 1206.1822v1 [math.NT]

[7] ———, *Sage worksheet*: *On the density of abelian surfaces with Tate-Shafarevich group of order five times a square*, 2012. http://www.sagenb.org/home/pub/4330/

[8] Remke Kloosterman, *The p-part of the Tate-Shafarevich groups of elliptic curves can be arbitrarily large*, J. Théor. Nombres Bordeaux **17** (2005), no. 3, 787–800. MR 2006k:11102

[9] Remke Kloosterman and Edward F. Schaefer, *Selmer groups of elliptic curves that can be arbitrarily large*, J. Number Theory **99** (2003), no. 1, 148–163. MR 2003m:11081

[10] Kazuo Matsuno, *Construction of elliptic curves with large Iwasawa λ-invariants and large Tate-Shafarevich groups*, Manuscripta Math. **122** (2007), no. 3, 289–304. MR 2008h:11106

[11] Bjorn Poonen and Michael Stoll, *The Cassels-Tate pairing on polarized abelian varieties*, Ann. of Math. (2) **150** (1999), no. 3, 1109–1149. MR 2000m:11048

[12] Edward F. Schaefer, *Class groups and Selmer groups*, J. Number Theory **56** (1996), no. 1, 79–114. MR 97e:11068

[13] Edward F. Schaefer and Michael Stoll, *How to do a p-descent on an elliptic curve*, Trans. Amer. Math. Soc. **356** (2004), no. 3, 1209–1231. MR 2004g:11045

[14] Jean-Pierre Serre, *Galois cohomology*, Springer, Berlin, 2002. MR 2002i:12004

[15] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, no. 106, Springer, New York, 1986. MR 87g:11070

[16] W. A. Stein et al., *Sage Mathematics Software* (*version* 4.6.2), The Sage Development Team, 2011. http://www.sagemath.org

[17] William A. Stein, *Shafarevich-Tate groups of nonsquare order*, in Cremona et al. [3], 2004, pp. 277–289. MR 2005c:11072

[18] John Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki (reprint), vol. 9, Soc. Math. France, Paris, 1995, pp. 415–440, Exp. No. 306. MR 1610977

[19] Jacques Vélu, *Isogénies entre courbes elliptiques*, C. R. Acad. Sci. Paris Sér. A-B **273** (1971), A238–A241. http://gallica.bnf.fr/ark:/12148/bpt6k56191248/f52.image MR 45 #3414

STEFAN KEIL: keil@math.hu-berlin.de
Institut für Mathematik, Humboldt-Universität zu Berlin, Unter den Linden 6, D-10099 Berlin, Germany

REMKE KLOOSTERMAN: klooster@math.hu-berlin.de
Institut für Mathematik, Humboldt-Universität zu Berlin, Unter den Linden 6, D-10099 Berlin, Germany

VOLUME EDITORS

Everett W. Howe
Center for Communications Research
4320 Westerra Court
San Diego, CA 92121-1969
United States

Kiran S. Kedlaya
Department of Mathematics
University of California, San Diego
9500 Gilman Drive #0112
La Jolla, CA 92093-0112

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-00-2 (print), 978-1-935107-01-9 (electronic)

First published 2013.

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org **http://msp.org**

THE OPEN BOOK SERIES 1

Tenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the tenth ANTS meeting, held July 9–13, 2012, at the University of California, San Diego. It includes revised and edited versions of the 25 refereed papers presented at the conference, together with extended abstracts of two of the five invited talks.

TABLE OF CONTENTS