ON THE DENSITY OF ABELIAN SURFACES WITH TATE-SHAFAREVICH GROUP OF ORDER FIVE TIMES A SQUARE

STEFAN KEIL AND REMKE KLOOSTERMAN

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

We considered all pairs (E_1, E_2), such that the E_i have conductor or coefficients smaller than some given bounds. This gives 20.0 million of pairs and we could apply the algorithm to 18.6 million of them. It turns out that about 49% of these pairs have a Tate-Shafarevich group of non-square order.

1. Introduction

Let A be an abelian variety over a number field K. Then 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 so-called Cassels-Tate pairing, which depends on the choice of a polarization $\lambda : A \to A^\vee$:

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

Let $Ш(A/K)_{\mathrm{nd}}$ denote the Tate-Shafarevich group modulo its maximal divisible subgroup. If λ is an isomorphism, i.e., A is principally polarized, then the induced pairing on $Ш(A/K)_{\mathrm{nd}}$ is non-degenerate. If moreover this pairing is alternating, then for all primes p the cardinality of the p-divisible part $Ш(A/K)_{\mathrm{nd}}[p^\infty]$ is a perfect square, thus if $Ш(A/K)$ is finite, its order is a perfect square.

Tate [16] showed that if λ is an isomorphism and is also induced from a K-rational divisor on A then the Cassels-Tate pairing is actually 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 then this polarization need not to be induced by a K-rational divisor on A. Poonen and Stoll [9] in fact showed that there exist genus 2 curves C such that $\#Ш(J(C))$ is twice a square. Moreover, they showed that if one assumes that $Ш(J(C))$ is finite for all genus 2 curves $C/\mathbf{Q}$ then the density of the Jacobians of genus 2 curves that have non-square order Tate-Shafarevich groups exists, and they showed numerically that it is about 0.13.

Date: May 16, 2012.

The first author is supported by a scholarship from the Berlin Mathematical School (BMS). Both authors thank the referees for their comments and suggestions.

For arbitrary abelian varieties Flach [2] showed that if $\#Ш(A/K) = kn^2$, with k square free, then k divides two times the degree of any 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 [14] constructed for every prime number $p < 25,000$ an example of a $p-1$-dimensional abelian variety $A_p/\mathbf{Q}$ 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 [4] 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 have a closer look on the construction of abelian surfaces with Tate-Shafarevich group of order five times a square. The examples of [4] 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 $\mathbf{Q}$ with a point P of order 5, then there exists a $d \in \mathbf{Q}^*$ such that $((E, O), P)$ is isomorphic to $((E_d, O), (0, 0))$ with

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

Take now two numbers $d_1, d_2 \in \mathbf{Q}^*$ 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 polarization 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 $Ш(A_{d_1,d_2}/\mathbf{Q})$ 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 $L \supset K$ 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 co-kernels 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 end of Section 4.) Hence, given a basis for the Mordell-Weil groups of both elliptic curves we can determine whether $\#Ш(B/\mathbf{Q})$ is a square or a non-square.

For almost all pairs (d_1, d_2), such that $\max(|u_i|, |v_i|)$, for $d_i = u_i/v_i$, is bounded by $N = 50,000$ and 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 we computed $2,418,900$ of them. 47.00% of these surfaces have a Tate-Shafarevich group of non-square order. Also we computed these cardinalities for a lot of 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 $18,522,741$ of such pairs and we could compute this product for $17,155,153$ of them. We obtain that for 49.22% of the abelian surfaces for which we could determine this product, it turned out not to be a square. We expect that a density exists and that it is around 0.5. For some heuristics see the end of the last 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 considered familiy of abelian surfaces. 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 much easier computationally. In Section 6 we sketch the algorithm used for the computations of the densities and finally in Section 7 we discuss the obtained results.

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 its completion with respect to v and G_{K_v} its absolute Galois group.

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

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

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

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

Here $[\cdot]$ means "kernel of".

The Tate-Shafarevich group is torsion. 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

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

I.e., 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 Swinnteron-Dyer). *Let A/K be an abelian variety and $L(A, s)$ 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*

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

The left hand side of this conjecture is invariant under isogeny. Cassels [1] ($\dim A=1$) and Tate [16] ($\dim A\geq 1$) proved that the right hand side is also invariant under isogeny. I.e., if $\varphi:A\to B$ is an isogeny then

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

This formula was used by Schaefer and the second author [7] to provide examples of elliptic curves with large Selmer groups, by Matsuno [8] and by the second author [6] to provide examples of elliptic curves with large Tate-Shafarevich groups and by Flynn and Grattoni [3] to compute several Selmer groups.

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

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

We will call the first factor with the φ_K the *global factor*, 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 are taken into account.

It is known that if the analytic rank of an elliptic curve is at most 1, then its Tate-Shafarevich group is finite and the analytic rank equals the Mordell-Weil rank; otherwise we will assume these two conjectures.

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 $\#\text{Ш}(B/K)\cdot 5^a=\#\text{Ш}(E_1\times E_2)$, for an $a\in\mathbf{Z}$. Since $\#\text{Ш}(E_1\times E_2)$ is a square it follows that $\#\text{Ш}(B/K)$ 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 $E_1,E_2/K$ be two elliptic curves such that G is a subgroup scheme of both E_1 and E_2. Let $A=E_1\times E_2$ and $B=A/G$. Then $\varphi:A\to B$ 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 $G=\mathbf{Z}/\ell\mathbf{Z}$, i.e., 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

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

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

We restrict now to the case $K = \mathbf{Q}$, $\ell = 5$, and G is generated by a $\mathbf{Q}$-rational point. Fix d_1 and d_2 in $\mathbf{Q}^*$, 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 $G = \mathbf{Z}/5\mathbf{Z}$ be one of those, i.e., it is the subscheme of A generated by $(0, 0) \times [n](0, 0)$, with $n \in \{1, 2, 3, 4\}$. Let $B := A/G$. Then B is a candidate for an abelian surface such that $\text{Ш}(B/\mathbf{Q})$ has order five times a square. To actually check whether $\text{Ш}(B/\mathbf{Q})$ has non-square order we will now calculate both the local and the global factor.

Note, that the 16 surfaces $B/\mathbf{Q}$ one obtains by replacing d_i by $-1/d_i$ and using the four values of n break into two pairs 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 $\text{Ш}(B/\mathbf{Q})$ is independent of n, thus all 16 surfaces will have Tate-Shafarevich groups of same cardinality. Therefore, for the 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 $\langle (0, 0) \times O, O \times (0, 0) \rangle$ and E'_{d_i} be the quotient of E_{d_i} by $\langle (0, 0) \rangle$. The isogeny $A \to A'$ 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 following 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 $(\boldsymbol{\mu}_5)^2$.

Summarizing we have the following diagram:

$$\begin{tikzcd}
 & B \arrow[dr, "\psi"] & \\
A = E_{d_1} \times E_{d_2} \arrow[ur, "\varphi"] \arrow[rr, bend left, "\rho=\eta_1\times\eta_2"] & & A' = E'_{d_1} \times E'_{d_2} \arrow[ll, bend left, "\rho^\vee"] \arrow[dl, "\psi^\vee"] \\
 & B^\vee \arrow[ul, "\varphi^\vee"] &
\end{tikzcd}$$

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

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

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

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

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

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

In the next two sections we will first explain how to determine the first factor, the *global factor*, then how to determine the second factor, the *local factor*.

4. Determining the global factor

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

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

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

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

The surjection $\operatorname{coker}\rho^\vee_{\mathbf{Q}} \to \operatorname{coker}\varphi^\vee_{\mathbf{Q}}$ becomes $(x,y) \mapsto x^n/y$ as the map from $(\mathbf{Q}^*/\mathbf{Q}^{*5})^2$ to $\mathbf{Q}^*/\mathbf{Q}^{*5}$. One sees immediately that the image of this map is independent of n, hence to compute $\operatorname{coker}\varphi^\vee_{\mathbf{Q}}$ we may set $n=1$. In order to determine $\operatorname{coker}\varphi^\vee_{\mathbf{Q}}$ it suffices to determine a basis for both $\operatorname{coker}\eta^\vee_{i,\mathbf{Q}}$ in $\mathbf{Q}^*/\mathbf{Q}^{*5}$. This can be done quite easily following [13, Exercise 10.1]: Suppose that f is a function on E_{d_i} with divisor $5(0,0) - 5O$. Then there exists a unique constant $c \in \mathbf{Q}^*/\mathbf{Q}^{*5}$ such that the map

$$\operatorname{coker}\eta^\vee_{i,\mathbf{Q}} \to \mathbf{Q}^*/\mathbf{Q}^{*5},$$

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

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

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

From the same exercise from [13] it follows that $f(\operatorname{coker}\eta^\vee_{\mathbf{Q}}) \subset \mathbf{Q}(S,5)$. Hence we can represent an element of $\operatorname{coker}\eta^\vee_{\mathbf{Q}}$ by its valuation at each prime number $p \in S$. Once the cokernels of both $\eta^\vee_{i,\mathbf{Q}}$ are established, the cokernel of $\varphi^\vee_{\mathbf{Q}}$ can be computed easily.

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

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

Note that $\ker(\psi_{\mathbf{Q}}) = \varphi(\ker\rho_{\mathbf{Q}})$. Set $K := \mathbf{Q}(\zeta_5)$, where ζ_5 is a primitive fifth root of unity. Then the restriction map $H^1(G_{\mathbf{Q}}, \mathbf{Z}/5\mathbf{Z}) \to H^1(G_K, \mathbf{Z}/5\mathbf{Z})$ is injective since the kernel of this map has exponent dividing both $[K:\mathbf{Q}] = 4$ and $\#\mathbf{Z}/5\mathbf{Z}$.

Since $A[\varphi], A[\rho]$ and $B[\psi]$ are isomorphic to $\boldsymbol{\mu}_5$, $\boldsymbol{\mu}_5 \times \boldsymbol{\mu}_5$ and $\boldsymbol{\mu}_5$ over K we obtain the following commutative diagram with embeddings as vertical maps.

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{coker} \varphi_{\mathbf{Q}} \arrow[r, "\psi"] \arrow[d] & \operatorname{coker} \rho_{\mathbf{Q}} \arrow[r] \arrow[d] & \operatorname{coker} \psi_{\mathbf{Q}} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & K^*/K^{*5} \arrow[r] & (K^*/K^{*5})^2 \arrow[r] & K^*/K^{*5} \arrow[r] & 0
\end{tikzcd}$$

As above the lower second horizontal map is just $(x, y) \mapsto x^n/y$. Hence to determine $\operatorname{coker} \varphi_{\mathbf{Q}}$ it suffices to determine the kernel of x^n/y on $\operatorname{coker} \eta_{1,\mathbf{Q}} \times \operatorname{coker} \eta_{2,\mathbf{Q}} \to \operatorname{coker} \psi_{\mathbf{Q}}$. Again this is independent of n. We do this as follows:

(1) For some $\tilde{d} \in K$ there is a K-isomorphism $\tau : E'_d \to E_{\tilde{d}}$, sending 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 $\operatorname{coker} \eta_{\mathbf{Q}} \subset K^*/K^{*5}$ note that the class number of K^* equals 1. Set

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

where S contains all primes $\mathfrak{p}$ of K being a bad prime of E_d or dividing 5, i.e., all primes $\mathfrak{p}$ of K lying over a primes p, such that $p \mid 5uv(u^2+11uv-v^2)$. From [13, Exercise 10.9] it follows that $f(\operatorname{coker} \eta_{\mathbf{Q}}) \subset K(S, 5)$. Hence to represent elements in $\operatorname{coker} \eta_{\mathbf{Q}}$ 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-known and it is easy to see that the 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 4.1. We can weaken the assumption of having a basis for the Mordell-Weil groups $E_{d_1}(\mathbf{Q}), E_{d_2}(\mathbf{Q}), E'_{d_1}(\mathbf{Q})$ and $E'_{d_2}(\mathbf{Q})$. It is actually sufficient to just have generators of a finite index sublattice of these four groups, such that the index is not divisible by 5, i.e., the generators of infinite order are not divisible by 5 modulo torsion. This is the case, since the images of such sublattices in the co-kernels of $\eta_i^\vee$, respectively η_i, are the complete co-kernels. Also it is sufficient to just know such sublattices of $E_{d_1}(\mathbf{Q})$ and $E_{d_2}(\mathbf{Q})$, since 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 if their span contains points divisible by 5 modulo torsion.

5. Determining the local factor

We want to calculate $\frac{\# \operatorname{coker} \varphi_{\mathbf{Q}_p}}{\# \ker \varphi_{\mathbf{Q}_p}}$ for all bad primes p and for $p = \deg \varphi = 5$. Since the kernel of $\varphi_{\mathbf{Q}_p}$ is generated by a $\mathbf{Q}$-rational point it follows that $\# \ker \varphi_{\mathbf{Q}_p} = 5$. The size of the co-kernel of $\varphi_{\mathbf{Q}_p}$ 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 $\operatorname{coker} \eta_{\mathbf{Q}_p}$ depends on the reduction type of $E := E_{d_i}$. Write $d_i =: u/v$ with $u, v \in \mathbf{Z}$ and $\gcd(u,v) = 1$. Then E has the following 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. *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 non-split multiplicative.*

Proof. Let $\overline{E}$ be $E \bmod p$ and $\overline{E}_{\text{ns}}$ be the smooth locus of $\overline{E}$. If $p \mid uv$ then $\overline{E}$ has equation $y^2 + \alpha xy = x^3$, for some non-zero $\alpha \in \mathbf{Z}/p\mathbf{Z}$. 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 $\overline{E}_{\text{ns}}$ and is non-trivial. In particular the order of the reduction of $(0,0)$, which is 5, divides $\#\overline{E}_{\text{ns}}(\mathbf{F}_p)$. If the reduction is split multiplicative then this group has order $p-1$, if the reduction is non-split then this group has order $p+1$, and if the reduction is additive then this group has order p, i.e., $p \equiv 1 \bmod 5$, $p \equiv -1 \bmod 5$, 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, i.e., the number of components of the Néron model.

Lemma 5.2. *For the Tamagawa quotient we have*

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

Proof. Since η has degree 5 it follows that that $\frac{c_{E',p}}{c_{E,p}} = 5^a$ for some $a \in \mathbf{Z}$. 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 [4, Proposition 2.25] it is shown by using Tate curves that if the reduction is split multiplicative then $a \in \{-1, 1\}$, depending on whether the kernel is on the identity component of the Néron model or not. □

If $p \nmid \deg \eta = 5$ then from [10, Lemma 3.8] it follows that $\frac{\# \operatorname{coker} \eta_{\mathbf{Q}_p}}{\# \ker \eta_{\mathbf{Q}_p}} = \frac{c_{E',p}}{c_{E,p}}$. Using this it follows easily that

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

(1) *If $p \mid u^2 + 11uv - v^2$ and $p \equiv 4 \bmod 5$, then $\operatorname{coker} \eta_{\mathbf{Q}_p} = \mathbf{Z}/5\mathbf{Z}$.*
(2) *If $p \mid u^2 + 11uv - v^2$ and $p \equiv 1 \bmod 5$, then $\operatorname{coker} \eta_{\mathbf{Q}_p} = (\mathbf{Z}/5\mathbf{Z})^2$.*
(3) *If $p \mid uv$, then $\operatorname{coker} \eta_{\mathbf{Q}_p} = 0$.*
(4) *If p is good for E, then $\operatorname{coker} \eta_{\mathbf{Q}_p} = \mathbf{Z}/5\mathbf{Z}$.*

Now $\operatorname{coker} \eta_{\mathbf{Q}_p} \subset H^1(G_{\mathbf{Q}_p}, \mathbf{Z}/5\mathbf{Z})$. From [12, Section II.5 Theorem 2, Proposition 17] it follows that for $p \nmid \deg \eta = 5$

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

with $a = 1$, if $p \equiv 4 \bmod 5$, and $a = 2$, if $p \equiv 1 \bmod 5$. From this it follows that

Proposition 5.4. *Suppose p is a prime of bad reduction for E and $p \neq 5$ with $p \mid u^2 + 11uv - v^2$. Then* $\operatorname{coker} \eta_{\mathbf{Q}_p} = H^1(G_{\mathbf{Q}_p}, \mathbf{Z}/5\mathbf{Z})$.

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

Proposition 5.5. *Suppose p is a prime of bad reduction for A, $p \neq 5$. Then* $\operatorname{coker} \varphi_{\mathbf{Q}_p}$ *is isomorphic as an abelian group to*

$$\begin{cases} 0, & \text{if } p \mid u_1 v_1 u_2 v_2, \\ (\mathbf{Z}/5\mathbf{Z})^2, & \text{if } p \mid \gcd(u_1^2 + 11u_1v_1 - v_1^2, u_2^2 + 11u_2v_2 - v_2^2),\ p \equiv 1 \bmod 5, \\ \mathbf{Z}/5\mathbf{Z}, & \text{otherwise.} \end{cases}$$

Proof. Recall that $\operatorname{coker} \varphi_{\mathbf{Q}_p} = \ker\left(\operatorname{coker} \eta_{1,\mathbf{Q}_p} \times \operatorname{coker} \eta_{2,\mathbf{Q}_p} \to \operatorname{coker} \psi_{\mathbf{Q}_p}\right)$, which equals

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

The surjective map $H^1(G_{\mathbf{Q}_p}, \mathbf{Z}/5\mathbf{Z})^2 \to H^1(G_{\mathbf{Q}_p}, \mathbf{Z}/5\mathbf{Z})$ is given by $(x, y) \mapsto nx - y$. Suppose that $p \mid u_1 v_1 u_2 v_2$, then by Lemma 5.3 we have that $\operatorname{coker} \eta_{i,\mathbf{Q}_p} = 0$, for at least one i, and therefore $\operatorname{coker} \varphi_{\mathbf{Q}_p} = 0$.

Suppose now $p \nmid u_1 v_1 u_2 v_2$. By assumption one of the E_{d_i} has bad reduction at p, let's say E_{d_1}. Since $p \nmid 5u_1v_1$ it follows from the above proposition that $\operatorname{coker} \eta_{1,\mathbf{Q}_p} = H^1(G_{\mathbf{Q}_p}, \mathbf{Z}/5\mathbf{Z})$ and hence $\operatorname{coker} \varphi_{\mathbf{Q}_p} \cong \operatorname{coker} \eta_{2,\mathbf{Q}_p}$. 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 $\operatorname{coker} \eta_{2,\mathbf{Q}_p}$, hence the structure of $\operatorname{coker} \varphi_{\mathbf{Q}_p}$. □

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 $\frac{c_{E',p}}{c_{E,p}} = \frac{1}{5}$. Using Tate curves one easily shows that $\operatorname{coker} \eta_{\mathbf{Q}_p} = 0$.

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 $\frac{c_{E',p}}{c_{E,p}} = 1$. The isogeny $\eta : E \to E'$ can be written as a power series in one variable in a neighbourhood of the point O. Again from [10, Lemma 3.8] it follows that

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

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 [17]. In [4, Proposition 2.9] it is shown that in the additive case $v_5(u^2 + 11uv - v^2) \in \{2, 3\}$ and that if $v_5(u^2 + 11uv - v^2) = 2$ then $|\eta'(0)|_5 = 1$, and 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 $\# \operatorname{coker} \eta_{\mathbf{Q}_p} = \# \ker \eta_{\mathbf{Q}_p}$, because in this case we also have $|\eta'(0)|_5 = 1$. We summarize as follows.

Lemma 5.6. *Suppose $p = 5$.*

(1) *If $p \mid uv$, then* $\operatorname{coker} \eta_{\mathbf{Q}_p} = 0$.
(2) *If p is good for E, then* $\operatorname{coker} \eta_{\mathbf{Q}_p} = \mathbf{Z}/5\mathbf{Z}$.
(3) *If $p \mid u^2 + 11uv - v^2$, then* $\operatorname{coker} \eta_{\mathbf{Q}_p} = \begin{cases} (\mathbf{Z}/5\mathbf{Z})^2, & 5^3 \mid u^2 + 11uv - v^2, \\ \mathbf{Z}/5\mathbf{Z}, & \text{otherwise.} \end{cases}$

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

Lemma 5.7. *The cardinality of* $\operatorname{coker} \varphi_{\mathbf{Q}_5}$ *equals the cardinality of* $\ker \varphi_{\mathbf{Q}_5}$*, unless*

(1) $5 \mid u_1 v_1 u_2 v_2$*. In this case* $\# \operatorname{coker} \varphi_{\mathbf{Q}_5} = 0$.
(2) $5^3 \mid \gcd(u_1^2 + 11u_1v_1 - v_1^2, u_2^2 + 11u_2v_2 - v_2^2)$*. In this case* $\# \operatorname{coker} \varphi_{\mathbf{Q}_5} = 5^2$.

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

Suppose now that $\operatorname{coker} \eta_{i,\mathbf{Q}_5} \neq 0$ for both i, which implies that $p = 5$ is additive or good for E_{d_i}. We need two facts from [12, Section II.5 Proposition 18, Theorem 5], namely $H^1(G_{\mathbf{Q}_5}, \mathbf{Z}/5\mathbf{Z}) = (\mathbf{Z}/5\mathbf{Z})^2$ and $H^1_{nr}(G_{\mathbf{Q}_5}, \mathbf{Z}/5\mathbf{Z}) = \mathbf{Z}/5\mathbf{Z}$. As in the previous proposition we have that if $\operatorname{coker} \eta_{1,\mathbf{Q}_5} = H^1(G_{\mathbf{Q}_5}, \mathbf{Z}/5\mathbf{Z})$, then $\operatorname{coker} \varphi_{\mathbf{Q}_5} \cong \operatorname{coker} \eta_{2,\mathbf{Q}_5}$ and vice versa. This gives the second case of the lemma, since $\operatorname{coker} \eta_{i,\mathbf{Q}_5} = (\mathbf{Z}/5\mathbf{Z})^2$ if and only if $5^3 \mid u_i^2 + 11u_iv_i - v_i^2$, and $\operatorname{coker} \eta_{i,\mathbf{Q}_5} = \mathbf{Z}/5\mathbf{Z}$ otherwise.

It remains to consider $\operatorname{coker} \eta_{1,\mathbf{Q}_5} = \operatorname{coker} \eta_{2,\mathbf{Q}_5} = (\mathbf{Z}/5\mathbf{Z})$. In this case one can show that $\operatorname{coker} \eta_{i,\mathbf{Q}_5} = H^1_{nr}(G_{\mathbf{Q}_5}, \mathbf{Z}/5\mathbf{Z})$, for both i; see [4, Proposition 3.5] and [11, Section 3]. Thus the kernel of $\operatorname{coker} \eta_{1,\mathbf{Q}_5} \times \operatorname{coker} \eta_{2,\mathbf{Q}_5} \to \operatorname{coker} \psi_{\mathbf{Q}_5}$, which equals $\operatorname{coker} \varphi_{\mathbf{Q}_5}$, has five elements. This finishes the proof. □

Putting everything together yields

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

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

is a non-square 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* $p \equiv 1 \bmod 5$,
(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

The code was implemented in Sage [15] and is available at [5]. 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 $d = u/v$, and goes over all pairs of these curves and determines whether the order of the Tate-Shafarevich group of the abelian surfaces $B = E_{d_1} \times E_{d_2} / \langle (P_1, P_2) \rangle$ is a square. For trivial reasons, pairs of the same elliptic curve are omitted and pairs are considered to be without order.

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

Step 1: Fix a positive integer N. For each pair of coprime positive integers (u, v), such that $\max(u, v) \leq N$, we collect the following data associated to $E := E_d$, for $d = u/v$. (Optional: Filter the pairs (u, v) by other limitations, e.g., considering only those for which the corresponding elliptic curves have conductor $\leq C$.)

- Collect all the primes dividing $5uv(u^2 + 11uv - v^2)$ in a set S.
- Collect all the primes dividing uv in a set T.
- Collect all the primes $p \equiv 1 \bmod 5$ dividing $u^2 + 11uv - v^2$ in a set U.
- If $v_5(u^2 + 11uv - v^2) = 3$, put also $p = 5$ into the set U.
- Determine the analytic rank r of E.
- Determine a system of r generators of a sublattice Λ of $E(\mathbf{Q})$, such that the points of infinite order modulo torsion are not divisible by 5. Take the image of Λ in $\mathbf{Q}(S, 5)$ to determine a basis P of $\operatorname{coker} \eta_{\mathbf{Q}}^{\vee} \subset \mathbf{Q}(S, 5)$. 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 $\mathbf{Z}/5\mathbf{Z}$.
- Calculate the image of Λ under η in $E'(\mathbf{Q})$ and determine which image points are divisible by 5 modulo torsion. Divide if possible and determine the non-trivial 5-torsion points of $E'(\mathbf{Q})$ to get a sublattice Λ' of $E'(\mathbf{Q})$, such that the points of infinite order modulo torsion are not divisible by 5. Use this information to get $\dim \operatorname{coker} \eta_{\mathbf{Q}}$.
- Take the image of Λ' in $K(S, 5)$ to determine a basis Q for $\operatorname{coker} \eta_{\mathbf{Q}} \subset K(S, 5)$. The data for each basis element consists of a pair for each prime in S and a pair for the units, where the first entry is the corresponding element in S, respectively 1, and the second entry is a list of elements in $\mathbf{Z}/5\mathbf{Z}$, which contains as many entries as there are prime ideals $\mathfrak{p}$ in K over p, respectively two entries, and these entries are the exponents corresponding to the prime ideals $(t_{\mathfrak{p}})$ with the chosen order, respectively the exponents of the units.

Step 2: To determine whether the order of $\text{Ш}(B_{d_1,d_2}/\mathbf{Q})$ is a square, for each pair of pairs $(u_1, v_1), (u_2, v_2)$ from the first step (modulo ordering and equality), do the following:

- Set $L := -\#(T_1 \cup T_2) + \#(U_1 \cap U_2)$.
- Fix an ordering for $\mathcal{S} := S_1 \cup S_2$.
- 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 $\mathbf{Z}/5\mathbf{Z}$. Calculate the rank of this matrix, which equals the dimension of $\operatorname{coker} \varphi_{\mathbf{Q}}^{\vee}$.
- 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 $\mathbf{Z}/5\mathbf{Z}$. Calculate the rank of this matrix, which equals the dimension of $\operatorname{coker} \psi_{\mathbf{Q}}$.
- Set $G := \dim \operatorname{coker} \varphi_{\mathbf{Q}}^{\vee} - \dim \operatorname{coker} \eta_{1,\mathbf{Q}} - \dim \operatorname{coker} \eta_{2,\mathbf{Q}} + \dim \operatorname{coker} \psi_{\mathbf{Q}}$. (Recall that $\dim \operatorname{coker} \varphi_{\mathbf{Q}} = \dim \operatorname{coker} \eta_{1,\mathbf{Q}} + \dim \operatorname{coker} \eta_{2,\mathbf{Q}} - \operatorname{coker} \psi_{\mathbf{Q}}$.)

Then the local factor (without the infinite prime) is a non-square if and only if L is odd, and the global factor (without the kernels) is a non-square if and only if G is odd. Since the contribution of the infinite prime and the kernels cancel, we have that $\text{Ш}(B_{d_1,d_2}/\mathbf{Q})$ has non-square order if and only if $L + G$ is odd.

The constructed databases and obtained results are given in the next section. To conclude this section, we make some comments on the implementation. Step 0 in the cases considered is not computational 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 lying over all primes up to $500,000$. Step 2 is also no problem. It consists only of simple set operations and calculating ranks of small matrices with coefficients in $\mathbf{Z}/5\mathbf{Z}$. Even a few million of pairs of elliptic curves can be considered in under an hour.

The computational demanding part is step 1. There are two main issues. The most problematic calculation is determining r generators of a sublattice 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 fact we tried all remaining curves with conductor $\leq 10^6$, but for 12 curves this did not terminate after 48 hours for each single curve on an individual CPU. The second problematic calculation in the actual code is computing the image of $\operatorname{coker}\eta_{\mathbf{Q}}$ in $K(S,5)$. We try to factor ideals of K, which are generated by elements of possibly very big norm. For example, the curve E_d, for $d = 1/94$, has analytic rank 1 and the numerator and denominator of the image of the point of infinite order in $K(S,5)$ have about 600 digits and Sage was not able to factor the corresponding ideal. As we already knew that the image is trivial, since the dimension of $\operatorname{coker}\eta_{\mathbf{Q}}$ was zero, we could skip this calculation. Considering this information in the algorithm all curves we tried worked fine. This problem might be avoidable by trying another strategy working modulo primes. The rest of step 1 is no problem for moderately chosen $d = u/v$, since it is mainly prime factorization of integers and of rational polynomials of degree 25 (to divide points by 5), as well as calculating isogenies and analytic ranks. On a desktop computer one could produce in a few hours a database of a few thousand curves, if one skips those which resist to divulge their data after some seconds.

Remark 6.1. Step 0 and 2 do not use any assumptions, but for step 1 we assume the Birch and Swinnerton-Syer conjecture in case the elliptic curve is of analytic rank $r \geq 2$, to conclude that the calculated sublattices Λ and Λ' are of finite index and that the Tate-Shafarevich groups are finite. Thus, only in case that both elliptic curves E_{d_i} have analytic rank $r \leq 1$ the result of the algorithm about $\#Ш(B_{d_1,d_2})$ modulo squares is completely unconditional.

7. Results

Given the above described algorithm, one can produce in short time millions of examples of both kinds of abelian surfaces over $\mathbf{Q}$, such that either the order of the Tate-Shafarevich group is a square or five times a square, respectively. In case the two elliptic curves were both of analytic rank $r \leq 1$ these examples are completely unconditional. We constructed two databases of elliptic curves using step 1 of the algorithm. The first database consists of elliptic curves E_d, $d = u/v$, with $\max(u, v) \leq 50,000$, such that the conductor of E_d is bounded by $C = 10^6$. The second database consists of elliptic curves, such that $\max(u, v) \leq 100$.

Database 1 consists of 2212 elliptic curves, all of them having analytic rank $r \leq 2$. It is most likely that these curves are a complete list of all (isomorphism classes of) elliptic curves of conductor $\leq 10^6$ having a rational torsion point of order 5, since for all such curves we have $u \leq 2,197$ and $v \leq 4,617$ and we checked up to $N = 50,000$. For 12 of these curves, all having analytic rank $r = 1$, step 1 of the algorithm did not succeed. The database is described in more detail in Table 1. We state for each analytic rank the number of elliptic curves with conductor $\leq 10^6$, with $\max(u, v) \leq N$, as well as the number of those curves for which step 1 was not successful.

Database 2 consists of $6,087$ elliptic curves. All of them have analytic rank $r \leq 3$. See Table 2 for more details. Again the number of curves for which step 1 did not succeed is given in brackets.

In the following we will present the results of step 2 of the algorithm applied to the two databases described above. As there are elliptic curves with incomplete data, we omit them. Thus some percentage of the abelian surfaces cannot be considered. We will state this amount in the tables. The given percentage of surfaces with square order Tate-Shafarevich group refers to those abelian surfaces which could be calculated.

N	$\#\{E_d, C = 10^6\}$		$\#\{r = 0\}$		$\#\{r = 1\}$		$\#\{r = 2\}$	
50,000	2,212	(12)	987	-	1,109	(12)	116	-
4,617	2,212	(12)	987	-	1,109	(12)	116	-
3,375	2,211	(12)	986	-	1,109	(12)	116	-
3,072	2,210	(12)	986	-	1,108	(12)	116	-
2,695	2,209	(11)	986	-	1,107	(11)	116	-
2,000	2,200	(10)	982	-	1,102	(10)	116	-
1,000	2,174	(9)	963	-	1,095	(9)	116	-
900	2,170	(9)	961	-	1,093	(9)	116	-
800	2,159	(8)	956	-	1,088	(8)	115	-
700	2,145	(5)	951	-	1,079	(5)	115	-
600	2,119	(2)	941	-	1,063	(2)	115	-
500	2,088	-	921	-	1,052	-	115	-
400	2,066	-	912	-	1,039	-	115	-
300	1,993	-	872	-	1,009	-	112	-
200	1,818	-	786	-	929	-	103	-
100	1,391	-	616	-	697	-	78	-
50	845	-	394	-	405	-	46	-

Table 1. Database 1: Number of elliptic curves E_d with conductor $\leq 10^6$ and $\max(u, v) \leq N$. In brackets is given the number of those curves, for which step 1 of the algorithm failed so far.

Database 1 yields $2,445,366$ abelian surfaces B. Of them we could decide in $2,418,900$ cases, i.e., in 98.92%, whether the order of $Ш(B)$ is a non-square. It turns out that 47.00% of these surfaces have a Tate-Shafarevich group of non-square order. Database 2 leads to $18,522,741$ abelian surfaces. We computed $17,155,153$ of them, which is 92.62%. The percentage of the non-square case of the computable ones is 49.22. The intersection of the two databases consists of $1,391$ curves, hence we considered $966,745$ of the computable surfaces twice. In total this gives $18,607,308$ computed surfaces, of which 49.07% have a Tate-Shafarevich group of non-square order.

N	$\#\{E_d\}$		$\#\{r=0\}$		$\#\{r=1\}$		$\#\{r=2\}$		$\#\{r=3\}$	
100	6,087	(229)	2,390	-	3,038	(223)	633	(6)	26	-
90	4,959	(141)	1,987	-	2,463	(140)	490	(1)	19	-
80	3,931	(57)	1,597	-	1,940	(57)	380	-	14	-
70	2,987	(7)	1,235	-	1,455	(7)	287	-	10	-
60	2,203	(2)	925	-	1,074	(2)	198	-	6	-
50	1,547	-	660	-	760	-	123	-	4	-
40	979	-	412	-	494	-	70	-	3	-
30	555	-	245	-	277	-	33	-	-	-
20	255	-	130	-	115	-	10	-	-	-
10	63	-	40	-	22	-	1	-	-	-

Table 2. Database 2: Number of elliptic curves E_d, such that $\max(u, v) \leq N$. In brackets is given the number of those curves, for which step 1 of the algorithm failed so far.

We did two different experiments with the two databases. The results of experiment 1 is given in Table 3 for both databases, the results of experiment 2 is given in Table 4 for database 1 and Table 5 for database 2.

In experiment 1 we investigated how the rank influences the squareness of the Tate-Shafarevich group. For this we filtered the full databases in three different ways: For curves of the same rank; for curves of two different ranks and considered only pairs of different rank; for all curves of 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 that 0.5. But the surfaces with rank larger than 2 inside our family are conjectured to have density zero, since one expects the elliptic curves with analytic rank $r \leq 1$ to have density 1 among all curves. The calculations with curves of rank $r \leq 1$ all show that the non-square case happens about in 50% of all cases.

	$C = 10^6,\ N = 50,000$		$N = 100$	
	$\%\text{Ш} = \square$	% unknown	$\%\text{Ш} = \square$	% unknown
$r = 0$	54.041	-	48.598	-
$r = 1$	58.657	2.153	48.893	14.144
$r = 2$	92.039	-	73.068	1.888
$r = 3$			98.154	-
$r = 0, r = 1$	46.645	1.082	51.391	7.340
$r = 0, r = 2$	52.867	-	50.567	0.948
$r = 0, r = 3$			49.891	-
$r = 1, r = 2$	74.361	1.082	53.196	8.219
$r = 1, r = 3$			61.279	7.340
$r = 2, r = 3$			84.425	0.948
$r \leq 1$	51.630	1.142	50.071	8.049

Table 3. Results of experiment 1 for both databases.

In experiment 2 we looked for the behaviour of the distribution of square and non-square order Tate-Shafarevich groups for increasing conductor, respectively height, of the elliptic curves. Hence we filtered database 1 for different values of conductor bounds C and database 2 for different values of height bounds N. For low bounds, the non-square case was less likely. When we increase these bounds this frequency tends to approximately 50%.

The two ways we ordered the elliptic curves, via conductor or via height, are natural ways of ordering elliptic curves. It is conjectured that densities obtained concerning 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, who showed that for genus 2 curves the density of the non-square Jacobians is about 0.13 and this density tends to zero, as the genus goes to infinity.

C	$\#\ E_d$		$\%Ш = \square$	% unknown
1,000,000	2,212	(12)	52.996	1.082
800,000	1,966	(9)	53.224	0.914
600,000	1,683	(6)	53.760	0.712
400,000	1,351	(3)	54.222	0.444
200,000	924	(1)	55.015	0.216
100,000	623	-	57.074	-
80,000	547	-	57.776	-
60,000	470	-	57.990	-
40,000	376	-	59.306	-
20,000	245	-	61.288	-
10,000	152	-	62.182	-
5,000	110	-	59.783	-
1,000	45	-	65.556	-

Table 4. Results of experiment 2 for Database 1.

N	$\#\ E_d$		$\%Ш = \square$	% unknown
100	6,087	(229)	50.780	7.383
90	4,959	(141)	50.890	5.606
80	3,931	(57)	50.982	2.879
70	2,987	(7)	51.247	0.468
60	2,203	(2)	51.466	0.182
50	1,547	-	52.211	-
40	979	-	52.764	-
30	555	-	54.157	-
20	255	-	56.384	-
10	63	-	67.179	-

Table 5. Results of experiment 2 for Database 2.

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 $\mathbf{Q}^* \times \mathbf{Q}^*$ 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 $17,155,153$ pairs obtained from the second database, we get numerical evidence for the independence, as illustrated in the following table.

	global quotient $= \square$	global quotient $\neq \square$
local quotient $= \square$	26.1%	25.3%
local quotient $\neq \square$	23.9%	24.7%

Recall that the exponent of the local quotient equals $-\#(T_1 \cup T_2) + \#(U_1 \cap U_2)$, hence one could prove the expected densities for the local quotient by showing that the set $T_1 \cup T_2$ has an even number of elements for 50% of the pairs (d_1, d_2), and that the set $(U_1 \cap U_2)$ is empty for a density 1 subset of pairs (d_1, d_2). Considering all pairs obtained from the second database the sets $T_1 \cup T_2$ have an even number of elements for about 48% of the pairs, and the sets $(U_1 \cap U_2)$ are empty in more than 96% of all pairs.

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 [4]. The exponent of the regulator quotient seems to be strongly influenced by the parity of the rank of the abelian surface. We now assume that the elliptic curves with rank 0, or with rank 1, have both density 0.5. If both ranks 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 non-square if and only if $\operatorname{coker} \eta_{\mathbf{Q}}$ is trivial modulo torsion, where η is the usual isogeny belonging to the elliptic curve of rank 1. For the rank 1 curves in the two databases it happens in about 90% of the cases that $\eta_{\mathbf{Q}}$ is surjective on the free part. In case both ranks are equal to 1, the regulator quotient is a square in about 80% of the cases. If we consider only the elliptic curves of rank ≤ 1 of the second database, then we have that for abelian surfaces of even rank the regulator quotient is a square in about 88% of the cases, and for abelian surfaces of odd rank the regulator quotient is a non-square in about 91% of the cases.

References

[1] J. W. S. Cassels. Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer. *J. Reine Angew. Math.*, 217:180–199, 1965.

[2] Matthias Flach. A generalisation of the Cassels-Tate pairing. *J. Reine Angew. Math.*, 412:113–127, 1990.

[3] E. V. Flynn and C. Grattoni. Descent via isogeny on elliptic curves with large rational torsion subgroups. *J. Symbolic Comput.*, 43(4):293–303, 2008.

[4] Stefan Keil. Examples of abelian varieties with non-square Tate-Shafarevich group. Preprint, 2012.

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

[6] Remke Kloosterman. The p-part of the Tate-Shafarevich groups of elliptic curves can be arbitrarily large. *J. Théor. Nombres Bordeaux*, 17(3):787–800, 2005.

[7] Remke Kloosterman and Edward F. Schaefer. Selmer groups of elliptic curves that can be arbitrarily large. *J. Number Theory*, 99(1):148–163, 2003.

[8] Kazuo Matsuno. Construction of elliptic curves with large Iwasawa λ-invariants and large Tate-Shafarevich groups. *Manuscripta Math.*, 122(3):289–304, 2007.

[9] Bjorn Poonen and Michael Stoll. The Cassels-Tate pairing on polarized abelian varieties. *Ann. of Math. (2)*, 150(3):1109–1149, 1999.

[10] Edward F. Schaefer. Class groups and Selmer groups. *J. Number Theory*, 56(1):79–114, 1996.

[11] Edward F. Schaefer and Michael Stoll. How to do a p-descent on an elliptic curve. *Trans. Amer. Math. Soc.*, 356(3):1209–1231 (electronic), 2004.

[12] Jean-Pierre Serre. *Galois cohomology.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, English edition, 2002.

[13] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1986.

[14] William A. Stein. Shafarevich-Tate groups of nonsquare order. In *Modular curves and abelian varieties*, volume 224 of *Progr. Math.*, pages 277–289. Birkhäuser, Basel, 2004.

[15] William A. Stein et al. Sage, open-source mathematics software system licensed under the GPL. http://www.sagemath.org/.

[16] John Tate. On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. In *Séminaire Bourbaki, Vol. 9*, pages 415–440. Soc. Math. France, Paris, 1995.

[17] Jacques Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A-B*, 273:A238–A241, 1971.

Institut für Mathematik, Humboldt-Universität zu Berlin, Unter den Linden 6, D-10099 Berlin, Germany

E-mail address: keil@math.hu-berlin.de

Institut für Mathematik, Humboldt-Universität zu Berlin, Unter den Linden 6, D-10099 Berlin, Germany

E-mail address: klooster@math.hu-berlin.de