Acta Math. Univ. Comenianae
Vol. LXXII, 1(2003), pp. 73–80

ON TATE-SHAFAREVICH GROUPS OF $y^2 = x(x^2 - k^2)$

F. LEMMERMEYER and R. MOLLIN

1. Introduction

In [**10**] Wada and Tairo computed the rank of the elliptic curves $E_k : y^2 = x(x^2 - k^2)$ connected with the problem of congruent numbers. For some values of k, they only found lower and upper bounds without being able to conclude that their lower bounds were correct. Later, Wada [**11**] and Nemenzo [**7**] showed that the lower bound is indeed correct for two of the curves left undecided by [**10**]. In this article, we investigate families of elliptic curves that cover some of the remaining cases.

In [**6**] and [**1**], families of elliptic curves were constructed whose Tate-Shafarevich groups have arbitrarily high 2-rank; the proof used (rather elementary) arithmetic of quadratic number fields. In this paper, we get such a family using only the arithmetic of rational integers.

Consider the elliptic curves $E_k : y^2 = x(x^2 - k^2)$ for integers $k \geq 1$. Elliptic curves with a rational point T of order 2 such as our curves E_k come attached with a 2-isogeny $\phi : E_k \longrightarrow \widehat{E}_k$ (depending on the choice of T if E has three rational points of order 2). For $T = (0, 0)$ we find the isogenous curve $\widehat{E}_k : y^2 = x(x^2 + 4k^2)$ if k is odd and $\widehat{E}_k : y^2 = x(x^2 + k^2/4)$ if k is even. The dual isogeny $\widehat{E}_k \longrightarrow E_k$ will be denoted by ψ. If k is fixed, we will suppress this index and write E and $\widehat{E}$ for E_k and $\widehat{E}_k$.

We are interested in rational points on the elliptic curves E_k; it is an elementary observation that these rational points come from nontrivial rational points on one of the torsors

$$\mathcal{T}^{(\psi)}(b_1): \quad N^2 = b_1 M^4 + b_2 e^4, \quad b_1 b_2 = -k^2 \quad \text{and}$$
$$\mathcal{T}^{(\phi)}(b_1): \quad N^2 = b_1 M^4 + b_2 e^4, \quad b_1 b_2 = \begin{cases} 4k^2 & \text{if } k \text{ is odd,} \\ k^2/4 & \text{if } k \text{ is even.} \end{cases}$$

Here nontrivial means different from $(N, M, e) = (0, 0, 0)$, and whenever we talk about rational points on torsors from now on we shall always mean nontrivial

Received February 5, 2003.
2000 *Mathematics Subject Classification.* Primary Primary: 11G04; Secondary Secondary: 11D09.
Key words and phrases. Elliptic Curve, Congruent Number, Rational Point, Torsor, Mordell-Weil Rank, Selmer group.

points. We also may (and do) assume moreover that its coordinates are integral and primitive, that is, $(M, e) = 1$.

There are only finitely many such torsors because the integers b_1, b_2 divide $4k^2$. Moreover, we can give these sets of torsors a group structure by setting e.g. $\mathcal{T}^{(\phi)}(b)\mathcal{T}^{(\phi)}(c) = \mathcal{T}^{(\phi)}(d)$, where d is the squarefree kernel of bc. Another way to define the same group structure (and this is the definition that will be used below) is to associate the coset $b\mathbb{Q}^{\times 2} \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ to $\mathcal{T}(b)$ and then work in the group $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$.

Determining whether these torsors contain a (nontrivial) rational point is difficult; on the other hand, checking whether they have a nontrivial rational point over all completions $\mathbb{Q}_v$ of $\mathbb{Q}$ is easy, and so we define the Selmer group $S^{(\psi)}(\widehat{E}/\mathbb{Q})$ as the subgroup of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ consisting of classes $b_1\mathbb{Q}^{\times 2}$ such that $\mathcal{T}^{(\psi)}(b_1)$ has a rational point in every completion $\mathbb{Q}_v$ of $\mathbb{Q}$; the subgroup of $S^{(\psi)}(\widehat{E}/\mathbb{Q})$ such that the torsors $\mathcal{T}^{(\psi)}(b_1)$ corresponding to $b_1\mathbb{Q}^{\times 2}$ have a rational point will be denoted by $W(\widehat{E}/\mathbb{Q})$. The proof that these sets actually are groups is an elementary consequence of the group structure of the set of rational points on elliptic curves. Similarly we define $S^{(\phi)}(E/\mathbb{Q})$ and $W(E/\mathbb{Q})$. Finally, the Tate-Shafarevich groups measure the difference between Selmer groups and the groups of torsors with $\mathbb{Q}$-rational points; they are defined via the exact sequences

$$0 \longrightarrow W(E/\mathbb{Q}) \longrightarrow S^{(\phi)}(E/\mathbb{Q}) \longrightarrow Ш(E/\mathbb{Q})[\phi] \longrightarrow 0,$$

$$0 \longrightarrow W(\widehat{E}/\mathbb{Q}) \longrightarrow S^{(\psi)}(\widehat{E}/\mathbb{Q}) \longrightarrow Ш(\widehat{E}/\mathbb{Q})[\psi] \longrightarrow 0.$$

Thus the Selmer groups consist of nonzero rational numbers modulo squares and keep track of the torsors that have solutions in every completion, the elements of the subgroups $W(E/\mathbb{Q})$ correspond to torsors with a rational point, and the Tate-Shafarevich groups, their factor group, measures how far these two groups are apart. In particular, a torsor $\mathcal{T}^{(\phi)}(b)$ gives rise to a nontrivial element $[b\mathbb{Q}^{\times 2}]$ (of order 2) in the Tate-Shafarevich group $Ш(E/\mathbb{Q})[\phi]$ if it has rational points everywhere locally but does not have a global rational point (in $\mathbb{Q}$).

Finding out which of our torsors have rational points is important in view of Tate's formula

$$2^{2+\text{rank } E} = \#W(E/\mathbb{Q}) \cdot \#W(\widehat{E}/\mathbb{Q}) \tag{1}$$

for rank E, the Mordell-Weil rank of the elliptic curve E. The fact that $\#W(E/\mathbb{Q}) \mid \#S^{(\phi)}(E/\mathbb{Q})$ shows that the calculation of Selmer groups gives an upper bound for the Mordell-Weil rank.

Note that the formula gives non-negative values for rank E because $W(\widehat{E}/\mathbb{Q})$ has a subgroup of order 4; in fact,

the torsor	has the rational point $(N, M, e) =$
$\mathcal{T}^{(\psi)}(+1) : N^2 = M^4 - k^2e^4$	$(1, 1, 0)$
$\mathcal{T}^{(\psi)}(-1) : N^2 = -M^4 + k^2e^4$	$(k, 0, 1)$
$\mathcal{T}^{(\psi)}(+k) : N^2 = kM^4 - ke^4$	$(0, 1, 1)$
$\mathcal{T}^{(\psi)}(-k) : N^2 = -kM^4 + ke^4$	$(0, 1, 1)$

This shows that $\langle -1 \cdot \mathbb{Q}^{\times 2}, k \cdot \mathbb{Q}^{\times 2}\rangle$ is a subgroup of $W(\widehat{E}/\mathbb{Q})$ of order 4; we will abbreviate this subgroup below by $\langle -1, k\rangle$.

2. Computing the Selmer Groups

For computing the Selmer groups we collect a number of lemmas. The first one is the simplest version of Hensel's Lemma one can imagine:

Lemma 1 (Hensel's Lemma)**.** *Let p be a prime. An element $a \in \mathbb{Z} \setminus p\mathbb{Z}$ has a square root in $\mathbb{Z}_p$ if and only if $(a/p) = 1$ for p odd or $a \equiv 1 \bmod 8$ for $p = 2$.*

We also need a special case of a well known result due to F.K. Schmidt ([**9**, Chap. X, Prop. 4.9]):

Lemma 2. *For nonzero integers $b_1, b_2 \in \mathbb{Z}$, the torsor $N^2 = b_1M^4 + b_2e^4$ has nontrivial solutions in $\mathbb{Z}_p$ for all primes $p \nmid 2b_1b_2\infty$.*

Now we want to compute the Selmer groups $S^{(\phi)}(E_k/\mathbb{Q})$ and $S^{(\psi)}(\widehat{E}_k/\mathbb{Q})$ in some cases when k is the product of odd primes. First we give criteria that allow to decide whether a torsor $\mathcal{T}(b_1)$ is an element in the Selmer group (that is, has local solutions everywhere), and then we use these criteria to determine the cardinality of the Selmer groups.

Lemma 3. *Let $k = p_1 \cdots p_t$ be a product of distinct odd primes p_i and write $k = b_1c_1$ for some squarefree $b_1 > 0$. Then $b_1\mathbb{Q}^{\times 2} \in S^{(\psi)}(\widehat{E}/\mathbb{Q})$ if and only if the following conditions are satisfied:*

i) $(c_1/p) = 1$ *or* $(-c_1/p) = 1$ *for all primes* $p \mid b_1$*;*

ii) $(b_1/p) = 1$ *or* $(-b_1/p) = 1$ *for all primes* $p \mid c_1$*;*

iii) $b_1 \equiv \pm 1 \bmod 8$ *or* $c_1 \equiv \pm 1 \bmod 8$*.*

Proof. We first check that these conditions are necessary. To this end, consider the torsor $\mathcal{T}^{(\psi)}(b_1) : N^2 = b_1M^4 + b_2e^4$ with $b_1 > 0$ squarefree and $b_1b_2 = -k^2$; we assume that $\mathcal{T}^{(\psi)}(b_1)$ has a nontrivial solution with $N, M, e \in \mathbb{Z}_p$ and $(M, e) = 1$. Since $b_1 \mid k^2$ and b_1 is squarefree, we can write $k = b_1c_1$ for some integer c_1. This gives $N^2 = b_1M^4 - b_1c_1^2e^4$. Since b_1 is squarefree, we have $N = b_1n$ and $b_1n^2 = M^4 - c_1^2e^4 = (M^2 + c_1e^2)(M^2 - c_1e^2)$.

Now there are three cases to consider:

1. $p \mid b_1$; then p is odd and $p \mid e$ if and only if $p \mid M$, contradicting $(M, e) = 1$. Thus $p \nmid Me$, hence $-c_1 \equiv (M/e)^2 \bmod p$ or $c_1 \equiv (M/e)^2 \bmod p$, and this implies $(-c_1/p) = 1$ or $(c_1/p) = 1$, i.e. i).
2. $p \mid c_1$; if $p \nmid n$, then $b_1n^2 \equiv M^4 \bmod p$ implies $(b_1/p) = 1$; if $p \mid n$, on the other hand, we get $n = pr$, $M = pm$, $c_1 = pc_2$ and so $-b_1r^2 \equiv c_2^2e^4 \bmod p$, hence $(-b_1/p) = 1$, i.e. ii).
3. $p = 2$; if M is even, then e and c_1 are odd, and $b_1n^2 \equiv -c_1^2e^4 \equiv -1 \bmod 8$ shows that $b_1 \equiv -1 \bmod 8$. If e is even, then M is odd, and $b_1n^2 \equiv M^4 \bmod 8$ shows $b_1 \equiv 1 \bmod 8$. Finally, if M and e are odd, then $b_1n^2 \equiv 1 - c_1^2 \equiv 0 \bmod 8$; but then $4 \mid n$, hence $c_1^2 \equiv 1 \bmod 16$ and hence $c_1 \equiv \pm 1 \bmod 8$, and we have proved iii).

This proves necessity. Now assume that the conditions i) – iii) are satisfied; we have to show that the torsor then has rational points in every completion of $\mathbb{Q}$. By Lemma 2, the torsor $\mathcal{T}^{(\psi)}(b_1)$ has a nontrivial solution in $\mathbb{Q}_p$ for every prime $p \nmid 2k$. The finitely many other primes will now be treated with Hensel's Lemma.

Again there are three cases:

1. $p \mid b_1$: by assumption, one of $\pm c_1$ is a square modulo p, hence $\sqrt{\pm c_1} \in \mathbb{Z}_p$ for some choice of sign, and $n = 0$, $M = \sqrt{\pm c_1}$ and $e = 1$ provide us with a $\mathbb{Z}_p$-rational point on the torsor $b_1n^2 = M^4 - c_1^2e^4$.
2. $p \mid c_1$: if $(b_1/p) = 1$ then $M = 1$, $e = 0$ and $n = 1/\sqrt{b_1}$ solve $b_1n^2 = M^4 - c_1^2e^4$. If $(-b_1/p) = 1$, then $n = c_1/\sqrt{b_1}$, $M = 1$ and $e = 0$ do the job.
3. $p = 2$: If $b_1 \equiv -1 \bmod 8$, then $\sqrt{-b_1} \in \mathbb{Z}_2$, and $n = c_1/\sqrt{-b_1}$, $M = 0$ and $e = 1$ solve the torsor in question. If $b_1 \equiv 1 \bmod 8$, then $n = 1/\sqrt{b_1}$, $M = 1$ and $e = 0$ do it. The cases $c_1 \equiv \pm 1 \bmod 8$ are taken care of similarly.

This proves our claims. $\square$

The next lemma addresses torsors $\mathcal{T}^{(\phi)}(b) \in S^{(\phi)}$ for odd values of $b \mid 2k$:

Lemma 4. *Let $k = p_1 \cdots p_t$ be a product of distinct odd primes p_i and write $k = b_1c_1$ for some squarefree b_1. Then $b_1\mathbb{Q}^{\times 2} \in S^{(\phi)}(E/\mathbb{Q})$ if and only if $b_1 > 0$ and the following conditions are satisfied:*

i) $(b_1/p) = +1$ *for all* $p \mid c_1$;
ii) $(c_1/p) = +1$ *for all* $p \mid b_1$;
iii) $p \equiv 1 \bmod 4$ *for all* $p \mid b_1$.

Proof. Consider $\mathcal{T}^{(\phi)}(b_1) : N^2 = b_1M^4 + b_2e^4$ with b_1 squarefree and $b_1b_2 = 4k^2$; if $\mathcal{T}^{(\phi)}(b_1)$ is solvable in $\mathbb{R}$, then we must have $b_1 > 0$. As above, we assume that $\mathcal{T}^{(\phi)}(b_1)$ has a nontrivial solution with $N, M, e \in \mathbb{Z}_p$ and $(M, e) = 1$.

Using $k = b_1c_1$, we find $N = b_1n$ and $b_1n^2 = M^4 + 4c_1^2e^4$. Let $p \mid b_1$; then $p \nmid M$ and $-1 \equiv (2c_1e^2/M^2)^2 \bmod p$, hence $p \equiv 1 \bmod 4$. For primes $p \mid c_1$, we get $(b_1/p) = +1$.

Now for the converse. If $p \mid b_1$, let $i \in \mathbb{Z}_p$ denote a square root of -1, which exists by iii). Then $e = 1$, $n = 0$ and $M = (1 + i)\sqrt{c_1} \in \mathbb{Z}_p$ give us the desired $\mathbb{Z}_p$-rational point.

If $p \mid c_1$, we can take $e = 0$, $M =$ and $n = 1/\sqrt{b_1}$. Finally, consider $p = 2$. If $b_1 \equiv 5 \bmod 8$, then $M = e = 1$ and $n = \sqrt{(1 + 4c_1^2)/b_1}$ do it, if $b_1 \equiv 1 \bmod 8$, we can take $e = 0$, $M = 1$ and $n = 1/\sqrt{b_1}$. $\square$

Finally, we have to describe torsors $\mathcal{T}^{(\phi)}(b) \in S^{(\phi)}$ for even values of $b \mid 2k$:

Lemma 5. *Let $k = p_1 \cdots p_t$ be a product of distinct odd primes p_i and write $k = b_1c_1$ for some squarefree $b_1 > 0$. Then $2b_1\mathbb{Q}^{\times 2} \in S^{(\phi)}(E/\mathbb{Q})$ if and only if the following conditions are satisfied:*

i) $(2b_1/p) = +1$ *for all* $p \mid c_1$;
ii) $(2c_1/p) = +1$ *for all* $p \mid b_1$;
iii) $p \equiv 1 \bmod 4$ *for all* $p \mid b_1$.

Proof. The proof is analogous to that of Lemma 4, so we'll skip some details. As above, solvability in $\mathbb{Z}_p$ implies $2b_1n^2 = M^4 + c_1^2e^4$. If $p \mid b_1$, then -1 is a square modulo p, and iii) follows. Moreover, the congruence $M^4 \equiv -c_1^2e^4 \bmod p$ shows that $(c_1/p) = (-1/p)_4$, and since $(-1/p)_4 = (2/p)$ for primes $p \equiv 1 \bmod 4$, we have ii). Finally, $p \mid c_1$ implies $2b_1n^2 \equiv M^4 \bmod p$, hence i).

Showing that these conditions imply solvability over every completion is just as straight forward. □

These lemmas allow us to compute the Selmer groups attached to ϕ and ψ in many cases.

Proposition 6. *Consider the elliptic curve $E = E_k$ with $k = qp_1 \cdots p_{2t}$, where $p_1 \equiv \ldots \equiv p_{2t} \equiv 5 \bmod 8$ and $q \equiv 3 \bmod 8$ are primes such that $(p_i/p_j) = (p_i/q) = = +1$ for all $i \neq j$. Then*

$$\begin{aligned} S^{(\psi)}(\widehat{E}/\mathbb{Q}) &= \langle -1, q, p_i : 1 \le i \le 2t \rangle \\ S^{(\phi)}(E/\mathbb{Q}) &= \langle p_i : 1 \le i \le 2t \rangle \end{aligned}$$

Proof. There are two things to do: for showing that, say, $\langle p_1, \ldots, p_{2t} \rangle \subseteq \subseteq S^{(\phi)}(E/\mathbb{Q})$ it is sufficient to show that these generators p_i satisfy the conditions in Lemma 4; for showing that $S^{(\phi)}(E/\mathbb{Q})$ is not larger we have to show that none of the squarefree divisors $b_1 \mid k$ that are not in $\langle p_i : 1 \le i \le 2t \rangle$ satisfy these conditions.

Let us start with $S^{(\psi)}(\widehat{E}/\mathbb{Q})$ and write $k = b_1c_1$; then all positive prime divisors of b_1 and c_1 are among $\{q, p_1, \ldots, p_{2t}\}$, hence conditions i) and ii) of Lemma 3 are clearly satisfied. As for iii), we simply observe that $b_1c_1 = k \equiv 3 \bmod 8$, hence either $b_1 \equiv 7 \bmod 8$ or $c_1 \equiv 7 \bmod 8$, and we find that iii) is satisfied as well. This shows that $\langle q, p_1, \ldots, p_{2t} \rangle \subseteq S^{(\psi)}(\widehat{E}/\mathbb{Q})$; but since $-1 \in W(\widehat{E}/\mathbb{Q})$, we conclude that $\langle -1, q, p_1, \ldots, p_{2t} \rangle \subseteq S^{(\psi)}(\widehat{E}/\mathbb{Q})$ as claimed.

Now consider $S^{(\phi)}(E/\mathbb{Q})$: each $\mathcal{T}^{(\phi)}(p_i)$ is clearly solvable since the conditions of Lemma 4 are satisfied. Next, no negative $b_1 \mid b$ leads to solvable torsors; finally consider the even torsors $\mathcal{T}^{(\phi)}(2b_1)$ with $b_1 \mid b$ odd: condition ii) shows that b is a product of p_i, condition iii) then implies $b_1 = 1$ since $1 = (c_1/p_i)$ and $(2/p_i) = -1$ for all $1 \le i \le 2t$. But then i) says that $(2/p_i) = 1$ for all p_i ($b_1 = 1$ implies $c_1 = k$) which is a contradiction. □

Since we know that $W(\widehat{E}/\mathbb{Q}) \supseteq \langle -1, k \rangle$, Proposition 6 and Tate's formula (1) tell us that E and $\widehat{E}$ have rank at most $4t$. We will improve this bound by constructing nontrivial elements in the Tate-Shafarevich groups of $\widehat{E}$ in the next section.

3. Computing nontrivial elements in Ш$(E/\mathbb{Q})$

The following result shows that $W(\widehat{E}_k/\mathbb{Q})$ is as small as possible for quite a large class of integers k:

Theorem 7. *Assume that k is a product of primes of the form $\pm 3 \bmod 8$, and that these primes are quadratic residues of each other (in particular, at most one of these primes is $\equiv 3 \bmod 8$). Then $W(\widehat{E}/\mathbb{Q}) = \langle -1, k\rangle$.*

Proof. Since $\mathcal{T}^{(\psi)}(-1) : N^2 = -M^4 + k^2e^4$ has the rational point $(N, M, e) = (k, 0, 1)$ and since $W(\widehat{E}/\mathbb{Q})$ is a group, it is sufficient to consider torsors $\mathcal{T}^{(\psi)}(b_1)$ with $b_1 > 0$. Writing $k = cd$, we have $\mathcal{T}^{(\psi)}(c) : N^2 = cM^4 - cd^2e^4$, and putting $N = cn_0$ gives

$$cn_0^2 \;=\; M^4 - d^2e^4.$$

Now put $d_1 = \gcd(M, d)$ and write $M = d_1m$, $d = d_1d_2$, and $n_0 = d_1n$. Then we find

$$\mathcal{T}^{(\psi)}(c) : cn^2 = d_1^2m^4 - d_2^2e^4 \;=\; (d_1m^2 - d_2e^2)(d_1m^2 + d_2e^2).$$

Now consider the following cases:

A) $2 \nmid m$ and $2 \mid e$. Then $\gcd(d_1m^2 - d_2e^2, d_1m^2 + d_2e^2) = 1$, hence $d_1m^2 - d_2e^2 = c_1n_1^2$ and $d_1m^2 + d_2e^2 = c_2n_2^2$ with $c_1c_2 = c$ and $n_1n_2 = n$. Adding both equations gives $2d_1m^2 = c_1n_1^2 + c_2n_2^2$. Reducing modulo any prime $r \mid c_1$ gives $1 = (2d_1c_2/r) = (2/r)$ which is a contradiction unless $c_1 = 1$ (the case $c_1 = -1$ being clearly impossible). The same argument implies $c_2 = 1$, hence rational solvability in case A) implies $c = 1$.

B) $2 \nmid me$. Here $\gcd(d_1m^2 - d_2e^2, d_1m^2 + d_2e^2) = 2$, hence $d_1m^2 - d_2e^2 = 2c_1n_1^2$ and $d_1m^2 + d_2e^2 = 2c_2n_2^2$ with $c_1c_2 = c$ and $n_1n_2 = 4n$. Reducing the second equation modulo some prime $r \mid d_1$ gives $1 = (2c_2d_2/r) = (2/r) = -1$, hence a contradiction unless $d_1 = 1$. Reduction modulo some prime $r \mid d_2$ gives a contradiction unless $d_2 = 1$. Thus solvability in case 1B) implies $c = k$.

C) $2 \mid m$ and $2 \nmid e$. Here we find $c = k$ exactly as above.

Thus if $\mathcal{T}^{(\psi)}(c) \in W(\widehat{E}/\mathbb{Q})$ for $c \mid k$, then $c = 1$ or $c = k$; but these torsors do have rational points, and we conclude that $W(\widehat{E}/\mathbb{Q}) = \langle -1, k\rangle$. □

Corollary 8. *If k is as in Proposition 6, then $Ш(\widehat{E}/\mathbb{Q})[\psi] \simeq (\mathbb{Z}/2\mathbb{Z})^{2t}$, and in particular we have* rank E = rank $\widehat{E} \le 2t$.

Proof. Since $S^{(\psi)}(\widehat{E}/\mathbb{Q})$ has rank $2t + 2$ by Proposition 6, Theorem 7 and the definition of $Ш(\widehat{E}/\mathbb{Q})[\psi]$ gives $Ш(\widehat{E}/\mathbb{Q}) \simeq S^{(\psi)}(\widehat{E}/\mathbb{Q})/W(\widehat{E}/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^{2t}$. □

Corollary 9. *Let $k = pqr$, where $p \equiv q \equiv 5 \bmod 8$ and $r \equiv 3 \bmod 4$ are primes such that $(p/q) = (p/r) = (q/r) = +1$. Then* rank $E_k \le 2$.

Proof. Put $t = 1$ in Corollary 8. □

In particular, this applies to the following curves taken from [**7**]:

k	factorization
2379	$3 \cdot 13 \cdot 61$
6355	$5 \cdot 31 \cdot 41$
8555	$5 \cdot 29 \cdot 59$
9595	$5 \cdot 19 \cdot 101$

Our methods can also be used to prove

Proposition 10. *Let $k = p_1 \cdots p_m$ be a product of primes $p_i \equiv 5 \bmod 8$ such that $(p_i/p_j) = +1$ whenever $i \neq j$. Then $\#\text{Ш}(\widehat{E}/\mathbb{Q}) \geq 2^{m-1}$ if m is odd and $\#\text{Ш}(\widehat{E}/\mathbb{Q}) \geq 2^{m-2}$ if m is even.*

This is the corrected version of a corollary of the results of Aoki [**2**].

4. What Next?

Showing that the curves in [**7**] whose rank was conjectured to be 2 actually equals 2 can be done with Cremona's software [**3**]; it is similarly straight forward to come up with a lot of results like those in Section 3 above. What is needed, however, is a general result embracing these special cases; since the conditions that guarantee nontrivial elements in $\text{Ш}(\widehat{E}/\mathbb{Q})[\psi]$ can be formulated using the splitting of primes in the genus field of $\mathbb{Q}(i, \sqrt{2}, \sqrt{k}\,)$, one might start looking for some kind of governing field (see Cohn & Lagarias) predicting nontrivial elements in $\text{Ш}(\widehat{E}/\mathbb{Q})[\psi]$ or, more generally, in $\text{Ш}(\widehat{E}/\mathbb{Q})[2]$.

It is also possible that the methods described here allow us to prove that the set of integers k for which the Mordell-Weil rank of $E_k : y^2 = x(x^2 - k^2)$ is 0 has density 1; without a better framework for proving the existence of nontrivial elements in $\text{Ш}[2]$ such an investigation is, however, too technical to be practical.

Acknowledgements: The work on this article was begun while the first author was visiting the University of Calgary in 1998; he would like to thank the University and the second author for their hospitality. The second author's research is supported by NSERC Canada grant # A8484. Also, the authors would like to thank Hideo Wada for his valuable comments on the manuscript.

References

1. Atake D., *On Elliptic Curves with Large Tate-Shafarevich Groups*, Journal of Number Theory **87** (2001), 282–300

2. Aoki N., *On the 2-Selmer groups of elliptic curves arising from the congruent number problem*, Comment. Math. Univ. St. Paul. **48** (1999), 77–101

3. Cremona J., `http://www.maths.nottingham.ac.uk/personal/jec/ftp/progs/`

4. Cohn H.and Lagarias J., *On the existence of fields governing the 2-invariants of the class-group of $Q(\sqrt{dp}\,)$ as p varies*, Math. Comp. **41** (1983), 711–730

5. Lagrange J., *Nombres congruents et courbes elliptiques*, Sémin. Delange-Pisot-Poitou 1974/75, Fasc. 1, Exposé 16, 17 p. (1975)

6. Lemmermeyer F., *On Tate-Shafarevich groups of some elliptic curves*, Algebraic number theory and Diophantine analysis, Graz 1998, de Gruyter 2000, 277–291

7. Nemenzo F. R., *On the rank of the elliptic curve $y^2 = x^3 - 2379^2 x$*, Proc. Japan Acad. **72** (1996), 206–207

8. Serf P., *Congruent numbers and elliptic curves*, Proc. Colloq. Debrecen/Hung. 1989, 227–238 (1991)

9. Silverman J., *The arithmetic of Elliptic Curves*, Springer Verlag 1986

10. Wada H. and Tairo M., *Computations of the rank of elliptic curve* $y^2 = x^3 - n^2x$, Proc. Japan Acad. **70** (1994), 154–157

11. Wada H., *On the rank of the elliptic curve* $y^2 = x^3 - 1513^2x$, Proc. Japan Acad. **72** (1996), 34–35

F. Lemmermeyer, CSU San Marcos, Dept. Mathematics, 333 S Twin Oaks Valley Rd, San Marcos, CA 92096-0001, USA, *e-mail*: `franzl@csusm.edu`,
`http://www.rzuser.uni-heidelberg.de/~hb3/`

R. Mollin, Mathematics Department, Univ. of Calgary, Calgary, Alberta T2N 1N4, Canada, *e-mail*: `ramollin@math.ucalgary.ca`,
`http://www.math.ucalgary.ca/~ramollin/`