FAMILIES OF NON-CONGRUENT NUMBERS

FRANZ LEMMERMEYER

Abstract. In this article we study the Tate-Shafarevich groups corresponding to 2-isogenies of the curve $E_k : y^2 = x(x^2 - k^2)$ and construct infinitely many examples where these groups have odd 2-rank. Our main result is that among the curves $E_k$, where $k = pl \equiv 1 \mod 8$ for primes $p$ and $l$, the curves with rank 0 have density $\geq \frac{1}{2}$.

1. Introduction

The elliptic curves $E_k : y^2 = x(x^2 - k^2)$ with $k \in \mathbb{Z}$ have been studied extensively, mainly because of the connection with the ancient problem of congruent numbers (see Guy [10] or Koblitz [14]). Many authors constructed families of non-congruent numbers by minimizing the Selmer groups attached to 2-isogenies of $E_k$ (see Feng [7, 8], Iskra [12], T. Ono [28], Serf [33], to name but the most recent contributors; actually results of this type go back to Genocchi [9] in the last century). Sharper results were obtained notably by J. Lagrange [16, 17] (see also Wada [36] and Nemenzo [25]), who found better bounds on the rank of $E_k$ by taking the 2-part of the Tate-Shafarevich groups into account. In this article, we will refine the criteria obtained by Lagrange and show that curves $E_k$, where $k = pl$ for primes $p \equiv l \equiv 1 \mod 8$, very rarely have Tate-Shafarevich groups with trivial 2-part.

Notation. We recall the relevant notation from [18] (the standard reference for notions not explained here is Silverman [34]): elliptic curves $E$ with a rational point $T$ of order 2 as our curves $E_k$ come attached with a 2-isogeny $\phi : E \to \hat{E}$ (depending on the choice of $T$ if $E$ has three rational points of order 2). For $T = (0,0)$ we find the isogenous curve

$$\hat{E}_k : y^2 = \begin{cases} x(x^2 + 4k^2) & \text{if } k \text{ is odd,} \\ x(x^2 + k^2/4) & \text{if } k \text{ is even.} \end{cases}$$

(the distinction is made in order to minimize the coefficients of the curve; we could just as well work with only $y^2 = x(x^2 + 4k^2)$ as both models are isomorphic). The dual isogeny $\hat{E}_k \to E_k$ will be denoted by $\psi$. If $k$ is fixed, we will suppress this index and write $E$ and $\hat{E}$ for $E_k$ and $\hat{E}_k$.

Consider the torsors

$$\mathcal{T}(\psi)(b_1) : N^2 = b_1M^4 + b_2e^4, \quad b_1b_2 = -k^2$$

and

$$\mathcal{T}(\phi)(b_1) : N^2 = b_1M^4 + b_2e^4, \quad b_1b_2 = \begin{cases} 4k^2 & \text{if } k \text{ is odd,} \\ k^2/4 & \text{if } k \text{ is even.} \end{cases}$$

The main part of this article was written in 1999 while the author was at the MPI Bonn; he would like to thank everyone there for the hospitality and the stimulating environment, and the DFG for financial support during that time.
The Selmer group $S^{(\psi)}(\hat{E}/\mathbb{Q})$ is defined as the subgroup of $\mathbb{Q}^x/\mathbb{Q}^{x2}$ consisting of classes $b_1\mathbb{Q}^{x2}$ such that $T^{(\psi)}(b_1)$ has a nontrivial $(\neq (0,0,0))$ rational point in every completion $\mathbb{Q}_v$ of $\mathbb{Q}$; the subgroup of $S^{(\psi)}(\hat{E}/\mathbb{Q})$ such that the torsors $T^{(\psi)}(b_1)$ corresponding to $b_1\mathbb{Q}^{x2}$ have a rational point will be denoted by $W(\hat{E}/\mathbb{Q})$ (from now on, rational point will stand for non-trivial rational point; we may and do assume moreover that its coordinates are integral and primitive, that is, $(M,e) = 1$). Similarly we define $S^{(\phi)}(E/\mathbb{Q})$ and $W(E/\mathbb{Q})$. Finally, the Tate-Shafarevich groups are defined via the exact sequences

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

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

There exist various methods for constructing elements of order 2 in Tate-Shafarevich groups: one can perform a second 2-descent (cf. Birch and Swinnerton-Dyer [2], Razar [29], Lagrange [16, 17], Wada [36] and Nemenzo [24]), employ the Cassels pairing (see e.g. Aoki [1], Bölling [3], Cassels [4], and McGuinness [23]), Dyer [2], Razar [29], Lagrange [16, 17], Wada [36] and Nemenzo [24]), employ the Farevich groups: one can perform a second 2-descent (cf. Birch and Swinnerton-Dyer [2], Razar [29], Lagrange [16, 17], Wada [36] and Nemenzo [24]), employ the Cassels pairing (see e.g. Aoki [1], Bölling [3], Cassels [4], and McGuinness [23]), Dyer [2], Razar [29], Lagrange [16, 17], Wada [36] and Nemenzo [24]), employ the Cassels pairing (see e.g. Aoki [1], Bölling [3], Cassels [4], and McGuinness [23]).

Our main results are the solvability criteria in Table 3 below; this will imply the lower bounds for density of rank-0 curves among the $E_{pt}$.

## 2. Preliminaries

In the calculations below we will have use quite a number of elementary results on quadratic reciprocity and genus theory. The following subsections recall what we will need.

### 2.1. Some reciprocity laws

In the following, $p$ and $l$ will denote primes $\equiv 1$ mod 8, and $\pi$ and $\lambda$ will denote primary primes in $\mathbb{Z}[i]$ with norms $p$ and $l$, respectively. A prime $\pi$ of norm $p \equiv 1$ mod 8 is called primary if $\pi$ is congruent to a square modulo 4. For $\pi \in \mathbb{Z}[i]$, $\Pi \in \mathbb{Z}[\sqrt{2}]$ and $\Pi^* \in \mathbb{Z}[\sqrt{-2}]$ we can always choose associates satisfying $\pi \equiv 1 \bmod 2 + 2i$, $\Pi \equiv 1 \bmod 2\sqrt{2}$ and $\Pi^* \equiv 1 \bmod 2\sqrt{-2}$, and these elements are primary.

We will need a few elementary results on quadratic residue symbols; as in [18], we let $(p/l)_4$ denote the biquadratic residue symbol for primes $l \equiv 1$ mod 8 such that $(p/l) = 1$, and we let $[\cdot/\cdot]$ denote the quadratic residue symbol in $\mathbb{Z}[i]$. We also note that, for primes $l = \lambda \overline{\lambda} \equiv 1$ mod 8, the relation $(1 + i)^4 = -4$ implies that $[1 + i/\lambda] = (-4/l)_8$ (this is the rational octic residue symbol). Moreover, $[\pi/\lambda] = (p/l)_4(l/p)_4$ for primes $p = \pi \overline{\pi}$ and $l = \lambda \overline{\lambda}$ such that $(p/l) = 1$ by Burde’s rational reciprocity law. Finally, it is easy to check that $(\varepsilon_2/p) = [1 + i/\pi] = (-4/l)_8$, where $\varepsilon_2 = 1 + \sqrt{2}$ (see [19]).

Now recall that primes $p \equiv 1$ mod 8 are norms from $\mathbb{Z}[\zeta_8]$, say $p = N\alpha$ for some $\alpha \equiv 1$ mod $(2 + 2\zeta)$, and in fact there exist primary elements $\pi \in \mathbb{Z}[i]$, $\Pi \in \mathbb{Z}[\sqrt{2}]$ and $\Pi^* \in \mathbb{Z}[\sqrt{-2}]$ with norm $p$. For primes $l \equiv 1$ mod 8, we define $\lambda$, $\Lambda$ and $\Lambda^*$ similarly. Unless explicitly stated otherwise, this notation is valid for the rest of this article.
The following result shows that solvability criteria involving the quadratic symbol $[(\Pi^*/\Lambda^*)]$ can be reduced to criteria involving only $[\Pi/\Lambda]$ and rational quartic residue symbols:

**Proposition 1.** Let $p \equiv l \equiv 1 \mod 8$ be primes such that $(p/l) = +1$. Then

$$
\frac{[\Pi]}{[\Lambda]} \cdot \frac{[\Pi^*/\Lambda^*]}{[\Lambda^*/\Pi^*]} = \left[ \frac{\pi}{\lambda} \right] = \left( \frac{p}{l} \right)_4 \left( \frac{l}{p} \right)_4,
$$

where the first three symbols $[\cdot/\cdot]$ denote the quadratic residue symbol in $\mathbb{Z}[^{\sqrt{2}}]$, $\mathbb{Z}[\sqrt{-2}]$, and $\mathbb{Z}[i]$, respectively.

**Proof.** We know that there exists an element $\alpha \in \mathbb{Z}[\zeta_8]$ such that $\Pi^* = \alpha_1 \alpha_3$ (here $\alpha_j = \sigma_j(\alpha)$, where $\sigma_j$ is the automorphism that sends $\zeta_8$ to $\zeta_8^j$; in particular $\alpha_1 = (\alpha)$, $\pi = \alpha_1 \alpha_5$ and $\Pi = \alpha_1 \alpha_7$ (observe that such norms are necessarily totally positive). Defining $\beta$ accordingly we have $[\Pi/\Lambda] = (\alpha_1 \alpha_7/\beta)$, where $\left( \cdot/\cdot \right)$ is the quadratic residue symbol in $\mathbb{Z}[\zeta_8]$. Similarly, we have $[\Pi^*/\Lambda^*] = (\alpha_1 \alpha_3/\beta)$, hence $[\Pi/\Lambda][\Pi^*/\Lambda^*] = (\alpha_3 \alpha_7/\beta)$. But this last symbol equals $[\pi/\lambda]$, and since $(p/l) = +1$ this coincides with $[\pi/\lambda]$. This proves our claim by Burde’s reciprocity law. \hfill $\Box$

We also note that $[\Lambda/\Pi] = [\Pi/\Lambda]$ and $[\Lambda^*/\Pi^*] = [\Pi^*/\Lambda^*]$ by the quadratic reciprocity laws in $\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[\sqrt{-2}]$, respectively. Finally, if $K/k$ is an extension of number fields, if $[\cdot/\cdot]$ and $\left( \cdot/\cdot \right)$ denote the quadratic residue symbols in $K$ and $k$, respectively, and if $a$ is an ideal in $O_k$ with odd norm, then $[\alpha/a] = (N\zeta/K\alpha/a)$ right from the definition of residue symbols. Similarly, for ideals $A$ in $O_K$ with relative norm $\mathfrak{a}$ and elements $\alpha \in K$ coprime to $\mathfrak{a}$, we have $[\alpha/\mathfrak{A}] = (\alpha/\mathfrak{a})$. For more on rational reciprocity laws, see [13] Chap. 5.

### 2.2. The class groups of $\mathbb{Q}(\sqrt{\pm 2l})$

Let us begin by reviewing the basic results of Scholz as pertaining to the special case $k = \mathbb{Q}(\sqrt{2l})$, where $l \equiv 1 \mod 4$ is prime. Let $\varepsilon$, $h$, and $h^+$ denote the fundamental unit, the class number and the class number in the strict sense of $k$. Moreover, define $(l/2)_4 = (-1/l)_8$ for primes $l \equiv 1 \mod 8$ and $(4/l)_8 = (2/l)_4(4/l)_4$. The following proposition is the special case $p = 2$ of a more general result due to Scholz [11].

**Proposition 2.** With the notation as above, there are the following cases:

- $(2/l) = -1$: then $N\varepsilon = -1$ and $h \equiv h^+ \equiv 2 \mod 4$;
- $(2/l) = +1$:
  - (1) if $(2/l)_4 = -(l/2)_4$, then $N\varepsilon = +1$, $h \equiv 2 \mod 4$, and $h^+ \equiv 4 \mod 8$.
  - (2) if $(2/l)_4 = (l/2)_4 = -1$, then $N\varepsilon = -1$ and $h \equiv h^+ \equiv 4 \mod 8$;
  - (3) if $(2/l)_4 = (l/2)_4 = +1$, then $4 \mid h$ and $8 \mid h^+$.

Note that e.g. by the class number formula for strictly ambiguous ideals $C_{am} = 2^{t-1}/(E_F/N_E_K)$ in quadratic extensions $K/F$ with $t$ ramified primes and unit groups $E_F$ and $E_K$, the prime ideal 2 above 2 in $\mathbb{Q}(\sqrt{2})$ is principal in the usual sense if and only if $N\varepsilon = -1$ for the fundamental unit $\varepsilon$ of $\mathbb{Q}(\sqrt{2})$.

Let $\mathfrak{a} \sim [2]$ be short for “the ideal $\mathfrak{a}$ is equivalent in the strict sense to the square of some ideal”, and define $\mathfrak{a} \sim [4]$ similarly.

If $d = d_1d_2$ is a product of two prime discriminants, then classical genus theory tells us that, for some ideal $\mathfrak{a}$ with norm $a$ (the existence of $\mathfrak{a}$ implies $(d/a) = +1$), we have $\mathfrak{a} \sim [2]$ if and only if $(d_1/a) = (d_2/a) = +1$. 

FAMILIES OF NON-CONGRUENT NUMBERS 3

3

3
Lemma 3. Let \( p \equiv t \equiv 1 \mod 8 \) be primes such that \( (p/l) = +1 \), and let \( p \) denote the prime ideal above \( p \) in \( k = \mathbb{Q}(\sqrt{2l}) \). Then \( p \sim [4] \iff [\Lambda/\Pi] = 1 \).

Proof. If \( 4 \mid h^+ \), then the corresponding quartic cyclic unramified extension \( K/k \) is given by \( K = k(\sqrt{\Lambda}) \). A prime ideal \( p \) of degree 1 will split completely in \( K/k \) if and only if its ideal class is a fourth power in \( \text{Cl}^+(k) \); on the other hand, Kummer theory shows that it splits if and only if \( \Lambda \) is a quadratic residue modulo any prime ideal above \( p \) in \( \mathbb{Q}(\sqrt{2l}) \), that is, if and only if \( [\Lambda/\Pi] = 1 \).

Lemma 4. Let \( k = \mathbb{Q}(\sqrt{2l}) \) and assume that \( (-4/l)_8 = -1 \). Then the prime ideal \( 2 \) above \( 2 \) in \( \mathcal{O}_k \) is principal in the strict sense if and only if \( (2/l)_4 = -1 \).

Proof. First observe that our assumption implies by Proposition 2 that the fundamental unit of \( k \) has positive norm, that \( 2 \) is principal in the wide sense, and that \( h^+ \equiv 4 \mod 8 \).

Assume that \( 2 \) is principal in the strict sense. Then \( X^2 - 2ly^2 = +2 \) is solvable, hence so is \( 2x^2 - ly^2 = 1 \) (we have put \( X = 2x \)). Now clearly \( 2 \nmid x \), hence \( x^2 \equiv 1 \mod 8 \) and \( 2x^2 \equiv 2 \mod 16 \); on the other hand, \( (2/y) = +1 \), hence \( y^2 \equiv 1 \mod 16 \). Together this implies that \( l \equiv 1 \mod 16 \), that is, \( (-1/l)_8 = +1 \). Since \( (-4/l)_8 = -1 \) by assumption, this is equivalent to \( (2/l)_4 = -1 \).

Now assume that \( 2 \) is not principal in the strict sense. Then \( X^2 - 2ly^2 = -2 \), and with \( X = 2x \) we get \( 2x^2 - ly^2 = -1 \). Now \( (2/l)_4 = (x/l) = (l/x') \), where \( x = 2x' \) with \( x' \) odd, and \((l/x') = +1\) by reducing our equation modulo \( x' \). Thus \( (2/l)_4 = +1 \).

\[ \square \]

3. The case \( k = 2p \)

We will now investigate which torsors of \( E_{2p} \) do not have rational points although they are everywhere locally solvable. These curves were already studied by Lagrange [17] using second 2-descents and by Kings [13] using the Cassels pairing on \( \text{III}(E/\mathbb{Q}) \). The curves \( E_{2p} \) are the simplest examples where \( \text{III}(E/\mathbb{Q})[\phi] \) and \( \text{III}(E/\mathbb{Q})[\psi] \) may have odd dimension:

Theorem 5. Let \( p \equiv 1 \mod 8 \) be a prime and consider the elliptic curve \( E : y^2 = x(x^2 - 4p^2) \). Then the Selmer groups are given by

\[ S^{(\psi)}(E/\mathbb{Q}) = (-1, 2, \psi), \quad S^{(\phi)}(E/\mathbb{Q}) = (p), \]

and if \( p \equiv 9 \mod 16 \), then we have \( \text{III}(E/\mathbb{Q})[\psi] = (p) \) and \( \text{III}(E/\mathbb{Q})[\phi] = (p) \). Here \( (x, \ldots, z) \) denotes the subgroup of \( \mathbb{Q}^x/\mathbb{Q}^{x^2} \) generated by \( x, \ldots, z \). Moreover, \( \text{III}(E/\mathbb{Q})[2] \simeq \text{III}(E/\mathbb{Q})[2] \simeq (\mathbb{Z}/2\mathbb{Z})^2 \).

Proof. We leave the proofs that \( \text{III}(E/\mathbb{Q})[\psi] \) and \( \text{III}(E/\mathbb{Q})[\phi] \) both have order 2 as an exercise to the reader (they are much simpler than the proofs in the sections below). The claims \( \text{III}(E/\mathbb{Q})[2] \simeq \text{III}(E/\mathbb{Q})[2] \simeq (\mathbb{Z}/2\mathbb{Z})^2 \) follow from the exact sequences (see diagram (3.9) in Razar [27], p. 139); Feng [7, 8] erroneously claims that \( C = \tilde{C} = 0 \)

\[ \begin{array}{cccccc}
0 & \rightarrow & \text{III}(E/\mathbb{Q})[\psi] & \rightarrow & \text{III}(E/\mathbb{Q})[2] & \rightarrow & \text{III}(E/\mathbb{Q})[\phi] & \rightarrow & C & \rightarrow & 0 \\
0 & \rightarrow & \text{III}(E/\mathbb{Q})[\phi] & \rightarrow & \text{III}(E/\mathbb{Q})[2] & \rightarrow & \text{III}(E/\mathbb{Q})[\psi] & \rightarrow & \tilde{C} & \rightarrow & 0
\end{array} \]
where \(C\) and \(\widehat{C}\) are finite groups of square order by results of Cassels [7]. Since they are quotients of groups of order 2, it follows that \(C = \widehat{C} = 0\), and this implies our claim. \(\square\)

4. The case \(k = pl \equiv 1 \mod 8\)

The simplest cases are those where \(p \equiv l \equiv 3, 5, 7 \mod 8\); they were already discussed by Lagrange [10]:

| \(p \mod 8\) | \(l \mod 8\) | \((p/l)\) | \(S^{(\psi)}(\mathbb{E}/\mathbb{Q})\) | \(S^{(\psi)}(E/\mathbb{Q})\) |
|---|---|---|---|---|
| 1 | 1 | +1 | \((-1, p, l)\) | \(\langle 2, p, l \rangle\) |
| 5 | 5 | +1 | \((-1, pl)\) | \(\langle p, l \rangle\) |
| 3 | 3 | +1 | \((-1, pl)\) | \(\langle 2p, 2l \rangle\) |
| 7 | 7 | +1 | \((-1, pl)\) | \(\langle 2 \rangle\) |

He also found necessary criteria for the solvability of certain torsors. Here are the results, reformulated using our notation:

**Proposition 6.** Let \(p\) and \(l\) be distinct primes such that \(p \equiv l \equiv 3, 5, 7 \mod 8\). If the torsors in the table below have a rational point, then the conditions in the last column must be satisfied:

| \(p \mod 8\) | \(l \mod 8\) | \((p/l)\) | torsors | conditions |
|---|---|---|---|---|
| 5 | 5 | +1 | \(T^{(\psi)}(p), T^{(\psi)}(l), T^{(\psi)}(pl)\) | \((p/l)_4 = (l/p)_4\) |
| 5 | 5 | +1 | \(T^{(\psi)}(2p), T^{(\psi)}(2l), T^{(\psi)}(pl)\) | \([1 + i] \pi / \lambda = +1\) |
| 7 | 7 | +1 | \(T^{(\psi)}(2), T^{(\psi)}(p), T^{(\psi)}(l)\) | \([\Lambda/\Pi] = +1\) |

In the last row, \(\Lambda \in \mathbb{Z}[^{\sqrt{2}}]\) is a primary element with norm \(-l\), and \(\Pi \in \mathbb{Z}[\sqrt{2}]\) has norm \(\pm p\). Observe that \([\Lambda/\Pi]\) is well defined since \([\Lambda/\Pi][\overline{\Lambda}/\overline{\Pi}] = [-l/\Pi] = (-l/p) = (p/l) = +1\).

The proofs for \(p \equiv l \equiv 5 \mod 8\) are straightforward and left as an exercise to the reader. Here we give some details for the case \(p \equiv l \equiv 7 \mod 8\): Consider the torsor \(T(p) : pm^a = M^4 - P e^4\). Reduction modulo \(l\) shows immediately that either 1) \(l \mid M\) and \((p/l) = +1\), or 2) \(l \mid M\) and \((p/l) = -1\). Moreover, either A) \(2 \mid Me\) and \(2 \mid n\), or B) \(2 \mid ne\) and \(2 \mid M\). As in the case \(p \equiv l \equiv 1 \mod 8\), we get four equations per case:

| case | \(M^2 + le^2 = 2pa^2\) | \(M^2 - le^2 = 2b^2\) | \(pa^2 + b^2 = M^2\) | \(pa^2 - b^2 = le^2\) |
|---|---|---|---|---|
| 1A) | \(M^2 + le^2 = 2pa^2\) | \(M^2 - le^2 = 2b^2\) | \(pa^2 + b^2 = M^2\) | \(pa^2 - b^2 = le^2\) |
| 1B) | \(M^2 + le^2 = 2pa^2\) | \(M^2 - le^2 = 2b^2\) | \(pa^2 + b^2 = 2M^2\) | \(pa^2 - b^2 = 2le^2\) |
| 2A) | \(lm^2 + e^2 = 2a^2\) | \(lm^2 - e^2 = 2p^2\) | \(a^2 - pb^2 = e^2\) | \(a^2 - pb^2 = lm^2\) |
| 2B) | \(lm^2 + e^2 = a^2\) | \(lm^2 - e^2 = pb^2\) | \(a^2 - pb^2 = 2e^2\) | \(a^2 - pb^2 = 2lm^2\) |

Now we distinguish these four cases:
Proposition 7. Let \( d_i \) denote the density of rank 0 curves among the \( E_{pl} \), where \( p \equiv l \equiv i \mod 8 \) are primes. Then we have \( d_3 = 1 \), \( d_5 \geq \frac{1}{2} \) and \( d_7 \geq \frac{1}{2} \).

The main result of this note is that we also have \( d_1 \geq \frac{1}{2} \) (this is much stronger than the result obtained by Lagrange [17]). Although numerical computations seem
to suggest that $d_i = 1$, it seems that the bounds derived in this article cannot be improved using our methods.

From now on, we will assume that $p$ and $q$ are both primes $\equiv 1 \mod 8$.

4.1. **The case** $(p/l) = -1$. Let $k = pl$ be a product of primes $p \equiv l \equiv 1 \mod 8$ with $(p/l) = -1$. Then (see [17])

$$S^{(\psi)}(\hat{E}/\mathbb{Q}) = (\psi, pl) = W(\hat{E}/\mathbb{Q}), \quad S^{(\phi)}(E/\mathbb{Q}) = (2, pl).$$

In particular, $\text{III}(\hat{E}/\mathbb{Q})[\psi] = 0$, so we only have to discuss the $\phi$-part of $\text{III}(E/\mathbb{Q})$.

**Proposition 8.** If $k = pl$ is a product of primes $p \equiv l \equiv 1 \mod 8$ with $(p/l) = -1$, then $\text{III}(E/\mathbb{Q})[\phi] = (2, pl)$ whenever $(-4/p)s(-4/l)s = -1$. If this condition holds, we have $\#\text{III}(E/\mathbb{Q})[2] = 4$.

**Proof.** Consider $\mathcal{T}^{(\phi)}(2) : N^2 = 2M^4 + 2p^2l^2e^4$.

- Assume first that $(M, pl) = 1$; then $N = 2n$ gives $2n^2 = M^4 + p^2l^2e^4$.
  
  Now $M^2 + ple^2i = 1 + i \mod 8$ and unique factorization in $\mathbb{Z}[i]$ shows that $M^2 + ple^2i = (1 + i)\nu^2$. Write $p = \pi\overline{\pi}$ for primes $\pi, \overline{\pi} \equiv 1 \mod 2 + 2i$; reducing modulo $\pi$ gives $[1 + i/\pi] = +1$, that is, $(-4/p)s = +1$, and similarly $(-4/l)s = +1$.

- If $(M, pl) = pl$ put $M = mp$ and $N = 2pn$; then we get $2n^2 = (pm^2 + le^2i)(pm^2 + le^2i)$, and again $pm^2 + le^2i = (1 + i)\nu^2$. Reducing modulo $\pi$ gives $[1 + i/\pi] = [l/\pi] = (l/p) = -1$, hence $(-4/p)s = (-4/l)s = -1$.

- The cases $(M, pl) = l$ and $(M, pl) = pl$ are treated similarly.

Next take $\mathcal{T}^{(\psi)}(pl) : N^2 = plM^4 + 4ple^4$. With $N = pln$ this gives $pln^2 = M^4 + 4e^4$; since we may switch the roles of $M$ and $e$ we may assume that $M$ is odd and $e$ is even. Reducing modulo $p$ and $l$ shows that $(-4/pl)_s = (Me/p)$. Write $e = 2' e'$ with $e'$ odd: then $(e/p) = (e'/p) = (p/e') = 1$ and $(M/p) = (p/M) = 1$. Thus $(-4/pl)_s = 1$.

Finally look at $\mathcal{T}^{(\phi)}(2pl) : 2pln^2 = M^4 + e^4$. As above, $M^2 + ie^2 = (1 + i)\pi\lambda\overline{\lambda}^2$; adding this equation to its conjugate gives $2M^2 = (1 + i)\pi\lambda\overline{\lambda}^2 + (1 - i)\overline{\pi}\lambda\overline{\lambda}^2$. Reducing modulo $\pi$ gives $1 = (2/p) = [1 + i/\pi][\pi/\overline{\pi}][\lambda/\overline{\lambda}]$. Now $[\pi/\overline{\pi}] = 1$ and $[\lambda/\overline{\lambda}] = [\lambda/\pi]$, hence $(-4/p)s = [\pi/\lambda]$. Similarly, $(-4/l)s = [\pi/\lambda]$ and the claim follows. Note that $[\pi/\lambda]$ depends on the choice of $\pi$ and $\lambda$. \hfill \Box

From Prop. 8 we get by a standard application of Chebotarev’s density theorem the following

**Corollary 9.** The curves of rank 0 among $E_{pl}$, where $p \equiv l \equiv 1 \mod 8$ are primes such that $(p/l) = -1$, have density at least $\frac{1}{9}$.

4.2. **The case** $(p/l) = +1$. Let $k = pl$ be a product of primes $p \equiv l \equiv 1 \mod 8$ with $(p/l) = +1$. Then (see [17])

$$S^{(\psi)}(\hat{E}/\mathbb{Q}) = (-1, p, l), \quad S^{(\phi)}(E/\mathbb{Q}) = (2, p, l).$$

Moreover $(-1, pl) \subseteq W(\hat{E}/\mathbb{Q})$. As above, we will now compute nontrivial elements of $\text{III}(E/\mathbb{Q})[\phi]$ and $\text{III}(\hat{E}/\mathbb{Q})[\psi]$. 
The $\psi$-part

First we observe that $W(\hat{E}/\mathbb{Q})$ always contains $(-1, pl)$. Thus

$$W(\hat{E}/\mathbb{Q}) = (-1, p, l)$$

or $W(\hat{E}/\mathbb{Q}) = (-1, pl)$ and $\text{III}(\hat{E}/\mathbb{Q})[\psi] = \langle p \rangle$,

where $\langle p \rangle$ represents the class of $p\mathbb{Q}^{x^2}$ (which is the same as the class of $l\mathbb{Q}^{x^2}$ in view of $pl\mathbb{Q}^{x^2} \in W(\hat{E}/\mathbb{Q})$) in $\text{III}(\hat{E}/\mathbb{Q})[\psi]$.

It is therefore sufficient to consider the torsor $T^{(\psi)}(p) : N^2 = pM^4 - pl^2e^4$. Here the right hand side factors over $\mathbb{Q}$ as $N^2 = p(M^2 - le^2)(M^2 + le^2)$. We have the following possibilities concerning divisibility

by 2: \[\begin{array}{l}
1) 2 \mid e, 2 \nmid MN \\
2) 2 \mid N, 2 \nmid Me,
\end{array}\]

by $l$: \[\begin{array}{l}
A) l \nmid MN \\
B) l \mid M, l \mid N,
\end{array}\]

and by $p$: \[\begin{array}{l}
a) p \mid (M^2 + le^2) \\
b) p \mid (M^2 - le^2).
\end{array}\]

Thus we have to consider eight different cases. We claim

**Proposition 10.** Let $E$ be the elliptic curve defined by $y^2 = x(x^2 - k^2)$, where $k = pl$ and where $p \equiv l \equiv 1 \mod 8$ are primes such that $(p/l) = 1$. If the torsor

\[T^{(\psi)}(p) : N^2 = pM^4 - pl^2e^4,\]

has a rational solution, then the conditions in Table 1 hold according to the case we are in.

| case  | conditions(*) |
|-------|---------------|
| 1Aa)  | $[\Pi/\Lambda] = (l/p)_4 = (-4/p)_8 = 1$ |
| 1Ab)  | $[\Pi/\Lambda] = (p/l)_4 = (l/p)_4(-4/p)_8 = 1$ |
| 1Ba)  | $[\Pi/\Lambda] = (-4/pl)_8, (l/p)_4 = (p/l)_4(-4/p)_8 = 1$ |
| 1Bb)  | $[\Pi/\Lambda] = (-4/l)_8, (p/l)_4 = (-4/p)_8 = 1$ |
| 2Aa)  | $[\Pi/\Lambda] = (-4/p)_8, (l/p)_4 = (-4/l)_8 = 1$ |
| 2Ab)  | $[\Pi/\Lambda] = (l/p)_4 = (p/l)_4(-4/l)_8 = 1$ |
| 2Ba)  | $[\Pi/\Lambda] = (-4/pl)_8, (p/l)_4 = (l/p)_4(-4/l)_8 = 1$ |
| 2Bb)  | $[\Pi/\Lambda] = (p/l)_4 = (-4/l)_8 = 1$ |

**Table 1.** If $T^{(\psi)}(p)$ has a rational point, then the conditions (*) hold.

If we are in case 1A), then putting $N = pn$ in (1) gives $pn^2 = M^4 - l^2e^4 = (M^2 - le^2)(M^2 + le^2)$. In case 1Aa), these two factors are coprime, hence $M^2 + le^2 = pa^2$ (I) and $M^2 - le^2 = \overline{b}^2$ (II), where $ab = n$. By adding and subtracting (I) and (II) we get $2M^2 = \overline{b}^2 + pa^2$ (III) and $2le^2 = pa^2 - \overline{b}^2$ (IV). In a similar way we find the following table displaying the four equations (I)–(IV) whose solvability follow from the existence of a rational point on $[\mathbb{I}]$:
In order to save some work we prove a general result that may be applied to each of these cases:

**Proposition 11.** Let $A, B, C, D \in \mathbb{N}$ be pairwise coprime integers, each a product of primes $\equiv 1 \mod 4$, and assume that these primes are quadratic residues of each other. If there are $x, y, v, w \in \mathbb{N}$ such that

\[(2) \quad Ax^2 + By^2 = Cv^2,\]
\[(3) \quad Ax^2 - By^2 = Dw^2,\]

then $C \equiv D \mod 8$, and $A, B, C$ and $D$ satisfy the relations

\[(4) \quad \left( \frac{AB}{C} \right)_4 \left( \frac{AD}{B} \right)_4 \left( \frac{BD}{A} \right)_4 = 1\]

and

\[(5) \quad (-1)^{\frac{C-W}{2}} \left( \frac{2}{CD} \right)_4 \left( \frac{BC}{D} \right)_4 \left( \frac{BD}{C} \right)_4 \left( \frac{CD}{A} \right)_4 = 1.\]

**Proof.** Assume that we have a congruence $Ar^2 = Bs^2 \mod D$ with $(r, D) = (s, D) = 1$, and assume moreover that $(AB/p) = (+1$ for all $p \mid D$. Then for each such $p$ we have $Ar^2 = Bs^2 \mod p$, and raising this congruence to the $\frac{p-1}{2}$-th power we find that $(A/p)4(r/p) = (B/p)4(s/p)$; multiplying these relations together shows that $(AB/D)4 = (rs/D)$. We will use this type of reasoning without comment below.

We may (and will) assume that $(x, y) = 1$. From $2y^2 = 2By^2 = Cv^2 - Dw^2 \equiv v^2 - w^2 \mod 4$ we then deduce that $2 \mid y$ and $2 \nmid xyw$.

Reducing \((\frac{2}{C})\) modulo $C$ gives $(-AB/C)4 = (xy/C)$. Writing $y = 2^j y'$ for some odd $y'$ gives $(y/C) = (2/C)4(y'/C) = (2/C)4(y'/C)$. Reducing $\left( \frac{2}{D} \right)_4$ modulo $y'$ we see $(C/y') = (A/y')$. Similarly, we get $(x/C) = (C/x) = (B/x) = (x/B)$ from $\left( \frac{D}{C} \right)_4$, and $(x/B) = (AD/B)4(w/B)$. Since $(w/B) = (B/w) = (A/w) = (w/A) = (-BD/A)4(y/A) = (-BD/A)4(2/A)4(y'/A)$, collecting our results gives $(-AB/C)4 = (AD/B)4(-BD/A)4(2/AC)4$. Next, $(-1/A)4 = (2/A)$ and $(-1/C) = (2/C)$, hence the relations becomes $(AB/C)4(AD/B)4(BD/A)4 = (2/AC)4+1$.

Now there are two cases: if $j = 1$, then $A \equiv C + 4 \mod 8$, hence $(2/AC) = -1$, but $(2/AC)^{j+1} = 1$; if $j \geq 2$, then $A \equiv C \mod 8$, hence $(2/AC) = 1$. In both cases, we arrive at the desired relation.
By adding and subtracting (2) and (3), we get

\[(6) \quad 2Ax^2 = Cv^2 + Dw^2,\]
\[(7) \quad 2By^2 = Cv^2 - Dw^2.\]

From (2) and the fact that \(y\) is even we deduce that \(C \equiv D \mod 8\).

Reducing (2) modulo \(D\) yields \((2BC/D)_4 = (vy/D)\). From (2) we deduce that \((y/D) = (2/D)^j(y/D) = (2/D)^j(D/y') = (2/D)^j(C/y')\) and \((v/D) = (D/v) = (2A/v), so \((2BC/D)_4 = (2A/v)(2/D)^j(C/y')\). Similarly, \((-2BD/C)_4 = (wy/C), (y/C) = (2/C)^j(C/y')\) and \((w/C) = (C/w) = (2A/w)\). Combining these results yields \((2BC/D)_4(−2BD/C)_4 = (2A/vw)(2/CD)^j\). Since \(C \equiv D \mod 8\), we have \((2/CD) = 1\), and using \((-1/C)_4 = (2/C)\) we conclude that

\[\left(\frac{2BC}{D}\right)_4\left(\frac{2BD}{C}\right)_4 = \left(\frac{2A}{vw}\right)\left(\frac{2}{C}\right).\]

Next, \((A/w) = (w/A) = (−BD/A)_4(y/A)\) and \((A/v) = (v/A) = (BC/A)_4(y/A)\), thus \((A/vw) = (−BD/A)_4(BC/A)_4 = (2/A)(CD/A)_4\) since \((B/A) = +1\). This gives us

\[\left(\frac{2}{CD}\right)_4\left(\frac{BC}{D}\right)_4\left(\frac{BD}{C}\right)_4\left(\frac{CD}{A}\right)_4 = \left(\frac{2}{vw}\right)\left(\frac{2}{C}\right).\]

If \(j = 1\), then \(Cv^2 \equiv Dw^2 + 8 \mod 16\), hence \(C \equiv D + 8 \mod 16\) if and only if \((2/v) = (2/w)\), or \((2/vw) = −1\). Moreover, \(2Ax^2 \equiv 2Cv^2 + 8 \mod 16\) implies \((2/AC) = −1\), so we get \((2/vw)(2/AC) = (−1)^{(C−D)/8}\).

If \(j \geq 2\), then \(Cv^2 \equiv Dw^2 \mod 16\), and this shows that \(C \equiv D \mod 16\) if and only if \((2/v) = (2/w)\), hence \((2/vw) = −1\). Moreover, \((\frac{2}{vw})^2 = 2\). This implies that \(A \equiv C \mod 8\), hence \((2/AC) = +1\), and again \((2/vw)(2/AC) = (−1)^{(C−D)/8}\).

In order to apply this result we have to identify the coefficients \(A, B, C, D\).

| case  | (1) | (2) | A | B | C | D | case  | (1) | (2) | A | B | C | D |
|-------|-----|-----|---|---|---|---|-------|-----|-----|---|---|---|---|
| 1Aa   | I   | II  | 1 | l | p | 1 | 2Aa   | III | IV  | p | 1 | 1 | l |
| 1Ab   | I   | II  | 1 | l | 1 | p | 2Ab   | III | IV  | 1 | p | 1 | l |
| 1Ba   | I   | II  | l | 1 | p | 1 | 2Ba   | III | IV  | p | 1 | l | 1 |
| 1Bb   | I   | II  | l | 1 | l | 1 | 2Bb   | III | IV  | p | 1 | l | 1 |

This takes care of all the conditions not involving \([Π/Λ]\). For completing the proof we need the following

**Lemma 12.** Let \(P \equiv L \equiv 1 \mod 8\) be primes such that \((P/L) = +1\). Let \(Π, Λ \in \mathbb{Z}[\sqrt{2}]\) be primary elements of norm \(P\) and \(L\), respectively. If there exist integers \(x, y, z, w \in \mathbb{N}\) such that

\[x^2 − 2y^2 = −Pz^2, \quad \text{and} \quad x^2 − y^2 = εLw^2\]

for some \(ε = ±1\), then \([Π/Λ] = +1\).

**Proof.** Unique factorization gives \(x + y\sqrt{2} = ε_2Πε^2,\) where \(ε_2\) is a fundamental unit of \(\mathbb{Z}[\sqrt{2}]\) and where \(N_{0} = z\). Thus \([Π/Λ] = [ε_2/Λ][x + y\sqrt{2}]/[x/Λ][1 + \sqrt{2}/Λ]\). Now \(y \equiv ±x \mod Λ\) from the second equation, hence \([x + y\sqrt{2}/Λ] = [x/Λ][1 + \sqrt{2}/Λ]. But [1 + \sqrt{2}/Λ] =
$[\varepsilon_2/\Lambda]$ since the expression $[\pm1 \pm \sqrt{2}/\Lambda]$ does not depend on the choice of signs, and we get $[\Pi/\Lambda] = [x/\Lambda] = (x/L)$. If $\epsilon = +1$, then $(x/L) = (y/L) = (L/y) = +1$, and if $\epsilon = -1$, then $(x/L) = (L/x) = +1$. This proves our claim. \hfill \Box

Lemma 13 takes care of four out of our eight cases:

| case | $x$ | $y$ | $z$ | $w$ | $P$ | $L$ | $\epsilon$ |
|------|-----|-----|-----|-----|-----|-----|----------|
| 1Aa  | $b$ | $M$ | $a$ | $e$ | $p$ | $l$ | $-1$     |
| 1Ab  | $a$ | $M$ | $b$ | $e$ | $p$ | $l$ | $+1$     |
| 2Ab  | $M$ | $a$ | $e$ | $b$ | $l$ | $p$ | $+1$     |
| 2Bb  | $e$ | $a$ | $m$ | $b$ | $l$ | $p$ | $-1$     |

For the remaining four cases, the role of Lemma 13 is taken over by

**Lemma 13.** Let $P \equiv L \equiv 1 \mod 8$ be primes such that $(P/L) = +1$. Let $\Pi, \Lambda \in \mathbb{Z}[\sqrt{2}]$ be primary elements of norm $P$ and $L$, respectively. If there exist integers $x, y, z, w \in \mathbb{N}$ such that

$$x^2 + 2\epsilon y^2 = Pz^2, \quad \text{and} \quad x^2 + \epsilon y^2 = Lw^2$$

for some $\epsilon = \pm 1$, then

$$[\Pi/\Lambda] = \left\{ \left( \frac{-1}{L} \right)_L, \left( \frac{L}{\pi} \right)_L \left( \frac{-2}{\pi} \right)_L \right\} \text{ if } \epsilon = -1,$$

$$[\Pi/\Lambda] = \left\{ \left( \frac{2}{L} \right)_L, \left( \frac{L}{\pi} \right)_L \left( \frac{-2}{\pi} \right)_L \right\} \text{ if } \epsilon = +1.$$

**Proof.** Let $\pi, \lambda \in \mathbb{Z}[\sqrt{2}]$ be primary elements of norm $P$ and $L$, respectively. Then from $\pi\alpha^2 = x + y\sqrt{2}$ we get $[\pi/\lambda] = [x + y\sqrt{2}/\lambda]$. The second equation gives $x \equiv \pm y\sqrt{\epsilon} \mod l$, where $l$ denotes a prime ideal above $l$ in $\mathbb{Q}(\zeta)$. Letting $\{ \cdot / \cdot \}$ denote the quadratic residue symbol in $\mathbb{Z}[\zeta]$, we find $[x + y\sqrt{2}/\lambda] = \{x + y\sqrt{2} / l\} = \{(x/L)[1 + \sqrt{2}/\lambda]$. Now if $\epsilon = 1$ then $(x/L) = (L/x) = +1$, whereas if $\epsilon = -1$ then $(x/L) = (y/L) = (y'/L) = (L/y') = +1$. Thus $[\pi/\lambda] = [1 + \sqrt{2}/\lambda] = (-4/L)_L$. If $\epsilon = -1$, then $\pi = \Pi$ and $\lambda = \Lambda$, but if $\epsilon = +1$ then $\pi = \Pi^*$ and $\lambda = \Lambda^*$, $\Pi^*, \Lambda^* \in \mathbb{Z}[\sqrt{2}]$ are primary elements of norm $p$ and $l$, respectively. Thus

$$[\Pi/\Lambda] = [\Pi^*/\Lambda^*] = (P/L)_4(L/P)_4 = (P/L)_4(L/P)_4(-4/L)_S.$$ \hfill \Box

Lemma 13 covers the remaining four cases:

| case | $x$ | $y$ | $z$ | $w$ | $P$ | $L$ | $\epsilon$ |
|------|-----|-----|-----|-----|-----|-----|----------|
| 1Ba  | $b$ | $e$ | $a$ | $m$ | $p$ | $l$ | $+1$     |
| 1Bb  | $a$ | $e$ | $m$ | $b$ | $p$ | $l$ | $-1$     |
| 2Aa  | $M$ | $b$ | $a$ | $e$ | $l$ | $p$ | $-1$     |
| 2Bb  | $e$ | $b$ | $m$ | $a$ | $l$ | $p$ | $+1$     |

Note that, in case 1Ba), Lemma 13 gives $[\Pi/\Lambda] = (-4/l)_S(p/l)_4(l/p)_4$; but since $(p/l)_4(l/p)_4 = (-4/p)_S$ by Lemma 13, we get the relation in the table above.

As a matter of fact, the criteria involving $[\Pi/\Lambda]$ can just as well be obtained using genus theory (compare the discussion of $T^{(2)}(2p)$ below). As the discussion
of the $\phi$-part below shows, however, it seems that arguments from genus theory cannot always be replaced by the direct calculation of residue symbols.

The $\phi$-part

Our aim in this section is to show

**Proposition 14.** If the torsor $T^{(\phi)}(b_1)$ with $1 \neq b_1 \in \langle 2, p, l \rangle$ has a rational point, then the conditions in Table 2 must be satisfied.

| $b_1$ | conditions (*) |
|-------|-----------------|
| 2     | $(-4/p)_8 = (-4/l)_8 = [\Pi/\Lambda] = 1$ |
| $p$   | $(p/l)_4 = (l/p)_4 = (-4/p)_8 = 1$ |
| $2p$  | $(p/l)_4(l/p)_4 = (-4/l)_8, (-4/p)_8 = 1, [\Pi/\Lambda] = (l/p)_4$ |
| $l$   | $(p/l)_4 = (l/p)_4 = (-4/l)_8 = 1$ |
| $2l$  | $(p/l)_4(l/p)_4 = (-4/p)_8, (-4/l)_8 = 1, [\Pi/\Lambda] = (p/l)_4$ |
| $pl$  | $(p/l)_4 = (l/p)_4, (-4/p)_8 = (-4/l)_8 = 1$ |
| $2pl$ | $(p/l)_4(l/p)_4 = (-4/p)_8 = (-4/l)_8, [\Pi/\Lambda] = 1$ |

Table 2. If $T^{(\phi)}(b_1)$ has a rational point, then the conditions (*) must be satisfied.

For the proof of Prop. 14, we need the following proposition dealing with a slightly more general situation:

**Proposition 15.** Let $k$ be a product of pairwise distinct primes $\equiv 1 \pmod{8}$ that are quadratic residues of each other. Let $k = AB$ for $A, B \in \mathbb{N}$; if the torsor $T^{(\phi)}(A)$ of $E_k$ has a nontrivial rational point, then the following conditions hold for any primary $\alpha \in \mathbb{Z}[i]$ with norm $A$:

1. $(-4/A)_8 = +1$;
2. $[\alpha/\pi] = +1$ for all $\pi \mid B$;
3. $(-4/p)_8 = (B/p)_4$ for all $p \mid A$.
4. $[\alpha^* / \pi] = +1$ for all $\pi \mid \alpha$, where $\alpha = \alpha^* \pi$.

**Proof.** We have $T^{(\phi)}(A) : AN^2 = M^4 + 4B^2e^4$; let $b = \gcd(M, B)$ be normalized by $b > 0$. Putting $N = bn$ and $M = bm$, we get $An^2 = b^2m^4 + 4c^2e^4$, where $bc = B$.

We may assume that $m$ is odd; otherwise we switch the roles of $m$ and $e$. Note that $A \equiv 1 \pmod{8}$ implies that $4 \mid e$.

Factoring the right hand side on $\mathbb{Z}[i]$ gives $\alpha \nu^2 = bm^2 + 2cie^2$ for some primary $\alpha \in \mathbb{Z}[i]$ with norm $N\alpha = A$. First observe that we have $\alpha \nu^2 = bm^2 \equiv 1 \pmod{8}$: thus $\alpha$ is congruent to a square modulo 8, and this implies 1. Moreover, $[\alpha/\pi] = [b/\pi] = (b/p) = +1$ for all $\pi \mid c$ with $N\pi = p$, and similarly $[\alpha/\pi] = 1$ for $\pi \mid b$; hence criterion 2.

Reducing the equation modulo some $\pi \mid \alpha$ gives $[1 + i/\pi](c/p)_4 = (-b/p)_4$, hence $(-4/p)_8 = (B/p)_4$ for all $p \mid A$, and this is 3.
Finally, subtracting $\alpha v^2 = bm^2 + 2cic^2$ from its conjugate yields $\alpha v^2 - \overline{\alpha v^2} = 4cie^2$; reducing modulo some $\mathfrak{p} \mid \mathfrak{p}$ we get $[\alpha/\mathfrak{p}] = (2c/p) = +1$. Since $[\pi/\mathfrak{p}] = +1$, this is equivalent to $[\alpha^*/\pi] = +1$, proving 4.

\begin{proof}[Proof of Prop. 14]
In the case $T^{(\phi)}(p)$ we have $A = p$ and $B = l$, so $(-4/p)_8 = 1$ from 1., $(p/l)_4(l/p)_4 = [\pi/\lambda] = 1$ from 2., $(-4/p)_8 = (l/p)_4$ from 3. and no condition from 4. In this way we find all criteria given in Table 3 except those involving $[\Pi/\Lambda]$. These have to be derived in an ad hoc manner:

- $T^{(\phi)}(2) : 2n^2 = M^4 + p^2l^2e^4$. Write the torsor in the form $-p^2l^2e^4 = (M^2 + n\sqrt{2})(M^2 - n\sqrt{2})$. We assume that $(M, pl) = 1$; the other cases are treated similarly. Then $M^2 + n\sqrt{2} = \eta\Pi^2\Lambda^2\alpha^4$ for primes $\Pi, \Lambda \in \mathbb{Z}[\sqrt{2}]$ such that $N\Pi = p$, $N\Lambda = l$ and $\Pi \equiv \Lambda \equiv 1 \text{ mod } 2$. Moreover, $\eta = \varepsilon^{\pm 1}$ with $\varepsilon = 1 + \sqrt{2}$. Adding the last equation to its conjugate gives $2M^2 = (\sqrt{2}\Pi)^2 = \eta\Pi^2\Lambda^2\alpha^4 + \eta\Pi^2\Lambda^2\alpha^4$. Replacing $M$ by $M\varepsilon$ where necessary we may assume without loss of generality that $\eta = \varepsilon$. Thus

$$\varepsilon^{-1}(\sqrt{2}M)^2 = \Pi^2\Lambda^2\alpha^4 - \varepsilon\Pi^2\Lambda^2\alpha^4 = (\Pi\Lambda\alpha^2 + \varepsilon\Pi\Lambda\alpha^2)(\Pi\Lambda\alpha^2 - \varepsilon\Pi\Lambda\alpha^2).$$

Now $\Pi\Lambda\alpha^2 + \varepsilon\Pi\Lambda\alpha^2 \equiv \sqrt{2} \text{ mod } 2$, hence $\Pi\Lambda\alpha^2 + \varepsilon\Pi\Lambda\alpha^2 = \sqrt{2}n^2$, $\Pi\Lambda\alpha^2 - \varepsilon\Pi\Lambda\alpha^2 = \sqrt{2}n^2$. Reducing modulo $\Pi$ and using $[\Pi/\Pi] = (2/p)_4$, $[\varepsilon/\Pi] = (-4/p)_8 = 1$ (in this case), as well as $[\Lambda/\Pi] = [\Lambda/\Pi]$ we find that the solvability of $T^{(\phi)}(2)$ implies $[\Lambda/\Pi] = 1$.

- $T^{(\phi)}(2p)$: Factoring $2pn^2 = M^4 + l^2e^4$ as $2pn^2 = (M^2 + le^2 + Me\sqrt{2})(M^2 + le^2 - Me\sqrt{2})$ and observing that $Me \equiv 1 \text{ mod } 2$ implies that each factor is divisible exactly once by the prime ideal $2$ above 2. Thus $2pn^2 = (M^2 + le^2 + Me\sqrt{2})$, where $n$ is an ideal with norm $n$. Let $h^+$ denote the class number of $\mathbb{Q}(\sqrt{2})$ in the strict sense. We have to distinguish several cases:

1. $h \equiv 2 \text{ mod } 4$, $h^+ \equiv 4 \text{ mod } 8$. By Proposition 3, this holds if and only if $(-4/l)_8 = -1$, and we also know that $N\varepsilon_2l = +1$ and that $2$ is principal in the weak sense. Now $[\Pi/\Lambda] = +1 \iff p \sim 4$ by Lemma 3, and since $2pn^2$ is principal in the strict sense, this happens if and only if $2n^2 \sim 4$. If $(2/l)_4 = -1$, then $2 \sim 4$ is principal in the strict sense, and this happens if and only if $n^2 \sim 4$ thus by genus theory $\iff (2/n) = (l/n) = +1$. But $(2/n) = (2p/l)_4 = -(p/l)_4$. Finally, solvability of $T^{(\phi)}(2p)$ implies $(-4/l)_8 = (p/l)_4(l/p)_4$, so $(p/l)_4 = (-4/l)_8(l/p)_4 = -(l/p)_4$, and we see that $[\Pi/\Lambda] = (l/p)_4$ as claimed. If $(2/l)_4 = +1$, on the other hand, then $2$ is not principal in the strict sense, hence $[\Pi/\Lambda] = +1 \iff n^2 \sim 4$, that is, if $-1 = (2/n) = (p/l)_4$, and as above this gives $[\Pi/\Lambda] = (l/p)_4$.

2. $h \equiv h^+ \equiv 4 \text{ mod } 8$. By Proposition 3, this holds if and only if $(2/l)_4 = -1$ and $l = 9 \text{ mod } 16$. Here $2^2$ is principal in the strict sense and 2 is not, in particular $2 \sim 2$ but $2 \sim 4$. Now $[\Pi/\Lambda] = +1 \iff n \sim 4$ which in turn happens if $-1 = (2/n) = (2p/l)_4 = -(p/l)_4$. Since $1 = (-4/l)_8 = (p/l)_4(l/p)_4$ from earlier solvability results, this gives $[\Pi/\Lambda] = 1 \iff (l/p)_4 = 1$ as claimed.

3. $h^+ \equiv 0 \text{ mod } 8$. By Proposition 3, this holds if and only if $(2/l)_4 = +1$ and $l \equiv 1 \text{ mod } 16$. Here $2^2 = (2)$ is principal, and since the class group $\text{Cl}_{16}^2(k)$ is cyclic, $2 \sim 4$. Thus $[\Pi/\Lambda] = +1 \iff n \sim 4 \iff 1 = (2p/l)_4 = (p/l)_4$, and we conclude as above that $[\Pi/\Lambda] = (l/p)_4$. 

\end{proof}
• $\mathcal{T}(\phi)(2l) : N^2 = 2lM^4 + 2p^2\ell e^4$. Symmetry reduces this to the discussion of $\mathcal{T}(\phi)(2p)$.

• $\mathcal{T}(\phi)(2pl) : N^2 = 2plM^4 + 2ple^4$. We start by factoring the torsor as $2pln^2 = M^4 + e^4 = (M^2 + e^2 + M\sqrt{2})(M^2 + e^2 - M\sqrt{2})$. Unique Factorization in $\mathbb{Z}[(\sqrt{2})$ gives $M^2 + e^2 + M\sqrt{2} = 2\Pi L\nu^2$ and $M^2 + e^2 - M\sqrt{2} = -2\Pi L\nu^2$. Subtracting the second equation from the first gives $2Me = \varepsilon\Pi L\nu^2 + 2\Pi L\nu^2$, which in view of $[\varepsilon/\Pi] = (-4/p)s$ and $[\Pi/\Pi] = (2/p)_4$ gives $[\Lambda/\Pi] = (Me/p)(-1/p)s$.

On the other hand we have $2pln^2 = (M^2 + ie^2)(M^2 - ie^2)$, hence $M^2 + ie^2 = (1+i)\pi L\nu^2$ for some $\nu \in \mathbb{Z}[i]$. This implies $(Me/p) = [Me/\pi] = [-i/\pi]4 = (-1/p)s$, hence our claim that $[\Pi/\Lambda] = 1$ is proved. □

The use of genus theory in this connection was suggested by the proofs of Pépin’s conjectures in [20]. This concludes our discussion of the $\phi$-part of $\mathcal{III}(E/\mathbb{Q})$.

5. The Main Result

The main result of this note is the following theorem:

**Theorem 16.** Let $p \equiv l \equiv 1 \mod 8$ be primes with $(p/l) = 1$. The properties of the Tate-Shafarevich groups $\mathcal{III}(E_k/\mathbb{Q})[\phi]$ and $\mathcal{III}(\hat{E}_k/\mathbb{Q})[\psi]$ corresponding to the 2-isogenies between the elliptic curves $E_k : y^2 = x(x^2 - p^2l^2)$ and $\hat{E}_k : y^2 = x(x^2 + 4p^2l^2)$ are recorded in Table 3. If the rank given there is 0, then the given subgroups actually equal $\mathcal{III}(E_k/\mathbb{Q})[\phi]$ and $\mathcal{III}(\hat{E}_k/\mathbb{Q})[\psi]$, and we have $\mathcal{III}(E/\mathbb{Q})[2] \simeq (\mathbb{Z}/2\mathbb{Z})^4$.

The last two columns in Table 3 give the smallest examples of $p$ and $l$ satisfying the conditions and such that the given inequality for the rank is an equality (assuming the BSD-conjecture, and with the possible exception of the first line with $p = 41$, $l = 2273$, where the rank is 2 or 4). In all cases except one, the given example is the one that occurs first: the exception is $pl = 41 \cdot 1601$, where the example $pl = 41 \cdot 1321$ has the same residue symbols; yet rank $E_{41,1321} = 0$.

Let us sketch the proof by going through one example. Take e.g. the second line; we claim that $\mathcal{T}(\phi)(p)$ is the only possibly trivial torsor in $S(\phi)(E/\mathbb{Q})$ (that means that it is the only one that might have a rational point). In fact, the torsors $\mathcal{T}(\phi)(2), \mathcal{T}(\phi)(l)$, $\mathcal{T}(\phi)(2l)$ and $\mathcal{T}(\phi)(pl)$ are nontrivial since $(-4/l)_8 = -1$, whereas $\mathcal{T}(\phi)(2p)$ and $\mathcal{T}(\phi)(2pl)$ are nontrivial because $(p/l)_4(l/p)_4 \neq (-4/l)_8$. The other claims now follow immediately.

It remains to prove that $\mathcal{III}(E/\mathbb{Q})[2]$ has order 16 if rank $E_{pl} = 0$. Recall the exact sequence

$$0 \rightarrow \mathcal{III}(E/\mathbb{Q})[\phi] \rightarrow \mathcal{III}(E/\mathbb{Q})[2] \rightarrow \mathcal{III}({\hat{E}}/\mathbb{Q})[\psi] \rightarrow \hat{C} \rightarrow 0,$$

where $\hat{C}$ is a finite 2-group of even rank by a result of Cassels. Since $\hat{C}$ is a quotient of the group $\mathcal{III}(\hat{E}/\mathbb{Q})[\psi]$ of order 2 in our case, we must have $\hat{C} = 0$, and in particular we get $\mathcal{III}(E/\mathbb{Q})[2] \simeq \mathcal{III}(E/\mathbb{Q})[\phi] \oplus \mathcal{III}({\hat{E}}/\mathbb{Q})[\psi]$ as claimed.

The formula in [25], p. 30 shows that, assuming BSD, the order of $\mathcal{III}(\hat{E}/\mathbb{Q})[2]$ is 4 in these cases; this will be proved unconditionally in a subsequent paper dealing with a comparison of the method used here and classical 2-descent.

**Corollary 17.** The curves of rank 0 among $E_{pl}$, where $p \equiv l \equiv 1 \mod 8$ are primes such that $(p/l) = +1$, have density at least $\frac{1}{4}$. Those with rank 4 have density at most $\frac{1}{32}$. 


In Table 3, we present the Tate-Shafarevich groups $\Sha[\phi] := \Sha(E_k/k)[\phi]$ and $\Sha[\psi] := \Sha(E_k/k)[\psi]$ corresponding to the 2-isogenies between the elliptic curves $E_k : y^2 = x(x^2 - k^2)$ and $E_k : y^2 = x(x^2 + 4k^2)$ with $k = pl$ having subgroups as indicated. The column labeled by $\text{rk } E$ gives bounds for the rank of $E_k(k)$. The column $W^{(\phi)}$ gives the subgroup of torsors in $S^{(\phi)}(E/k)$ that may have rational points.

**Some Examples.** In [27], Wada and Taira (extending previous calculations of Noda & Wada [23]; see also Nemenzo [24]) computed the rank of most curves $E_k$ for $k < 40,000$. For 20 of these curves, they could only prove that the rank was
between 2 and 4. For 8 out of these 20 numbers, our results show that the rank is in fact 2 in these cases:

| \(k\) | \(p\) | \(l\) | \((l/p)_4\) | \((p/l)_4\) | \((-4/p)_8\) | \((-4/l)_8\) | \(\Pi/\Lambda\) |
|---|---|---|---|---|---|---|---|
| 1513 | 17 | 89 | +1 | −1 | −1 | −1 | +1 |
| 2329 | 17 | 137 | +1 | −1 | −1 | +1 | −1 |
| 4633 | 41 | 113 | +1 | −1 | +1 | +1 | +1 |
| 6001 | 17 | 353 | +1 | +1 | −1 | +1 | −1 |
| 6953 | 17 | 409 | +1 | +1 | −1 | +1 | −1 |
| 7361 | 17 | 433 | −1 | +1 | −1 | −1 | +1 |
| 7769 | 17 | 457 | −1 | +1 | −1 | +1 | −1 |
| 9809 | 37 | 577 | +1 | +1 | +1 | +1 | +1 |

We remark in passing that the inequality rank \(E \leq 2\) in these cases follows already from the criteria not involving \(\Pi/\Lambda\). Moreover, the special case \(k = 1513\) was discussed by Wada \[36\].

The tables of Nemenzo \[25, 26\] contain 70 more values \(k = pl < 100,000\) such that \(E_k\) has analytic rank 2 and Selmer rank 4. For 66 of them, the criteria involving the rational residue symbols suffice to show that the rank is at most 2; the 4 exceptions are \(k = 64297 = 113 \cdot 569, 67009 = 113 \cdot 593, 93193 = 41 \cdot 2273\) and \(94177 = 41 \cdot 2297\). For these values of \(k\) we find \(\Lambda/\Pi = −1\) except when \(k = 93193\).

In \[21\], we will treat the remaining values of \(k\) from \[37\] for which the rank could not be determined there.

References

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

[2] B.J. Birch, H.P.F. Swinnerton-Dyer, *Notes on elliptic curves. II*, J. Reine Angew. Math. 218 (1965), 79–108

[3] R. Bölling, *Die Ordnung der Schafarewitsch-Tate-Gruppe kann beliebig groß werden*, Math. Nachr. 67 (1975), 157–179

[4] J.W.S. Cassels, *Arithmetic on curves of genus 1. VI. The Tate-Safarevic group can be arbitrarily large*, J. Reine Angew. Math. 214/215 (1964), 65–70

[5] J. Cremona, *Higher descents on elliptic curves*, preprint 1998

[6] L. Dirichlet, *Démonstration d’une propriété analogue à la loi de réciprocité qui existe entre deux nombres premiers quelconques*, J. Reine Angew. Math. 9 (1832), 379–389; Werke I, 173–188

[7] K. Feng, *Non-congruent numbers, odd graphs and the Birch-Swinnerton-Dyer conjecture*, Acta Arith. 75 (1996), 71–83

[8] K. Feng, *Non-congruent number, odd graph and the BSD conjecture on \(y^2 = x^3 - n^2x\)*, Singularities and complex geometry (Beijing, 1994), 54–66, 1997; coincides with \[7\]

[9] A. Genocchi, *Sur l’impossibilité de quelques égalités doubles*, C. R. Acad. Sci. Paris 78 (1874), 423–436

[10] R.K. Guy, *Unsolved Problems in Number Theory*, Springer Verlag 1981; Japan. transl. 1983; 2nd Engl. ed. 1994

[11] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Jahresber. D.M.V., Ergänzungsband 6 (1930), 204 pp., Teil II: Reziprozitätsgezet. Reprint: Physica Verlag, Würzburg 1965
[12] B. Iskra, Non-congruent numbers with arbitrarily many prime factors congruent to 3 modulo 8, Proc. Japan Acad. 72 (1996), 168–169
[13] G. Kings, Über Bedingungen für Punkte unendlicher Ordnung über ℚ auf den Kurven $E : y^2 = x^3 + \ell^2 x$, Diplomarbeit Univ. Bonn, 1989
[14] N. Koblitz, Introduction to elliptic curves and modular forms, GTM 97, 2nd ed. Springer-Verlag 1993
[15] K. Kramer, A family of semistable elliptic curves with large Tate-Shafarevitch groups, Proc. Amer. Math. Soc. 89 (1983), 379–386
[16] J. Lagrange, Construction d'une table de nombres congruents, Bull. Soc. Math. France, Suppl., Mem. 49–50 (1977), 125–130
[17] J. Lagrange, Nombres congruents et courbes elliptiques, Sémin. Delange-Pisot-Poitou 1974/75, Fasc. 1, Exposé 16, 17 p. (1975)
[18] F. Lemmermeyer, On Tate-Shafarevich Groups of some Elliptic Curves, Proc. Conf. Graz 1998, (2000), 277–291
[19] F. Lemmermeyer, Reciprocity Laws. From Euler to Eisenstein, Springer-Verlag Heidelberg 2000
[20] F. Lemmermeyer, A note on Pépin’s counter examples to the Hasse Principle for curves of genus 1, Abh. Math. Sem. Hamburg 69 (1999), 335–345
[21] C.-E. Lind, Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins, Diss. Univ. Uppsala 1940
[22] O. McGuinness, The Cassels pairing in a family of elliptic curves, Ph. D. Diss. Brown Univ. 1982
[23] F.R. Nemenzo, On the rank of the elliptic curve $y^2 = x^3 − 2379^2 x$, Proc. Japan Acad. 72 (1996), 206–207
[24] F.R. Nemenzo, All congruent numbers less than 40000, Proc. Japan Acad. 74 (1998), 29–31
[25] F.R. Nemenzo, email February 4, 2002
[26] K. Noda, H. Wada, All congruent numbers less than 10000, Proc. Japan Acad. 69 (1993), 175–178
[27] T. Ono, On the relative Mordell-Weil rank of elliptic quartic curves, J. Math. Soc. Japan 32 (1980), 665–670
[28] M.J. Razar, A relation between the two-component of the Tate-Shafarevich group and $L(1)$ for certain elliptic curves, Amer. J. Math. 96 (1974), 127–144
[29] L. Rédei, Die Diophantische Gleichung $mx^2 + ny^2 = z^4$, Monatsh. Math. Phys. 48 (1939), 43–60
[30] A. Scholz, Über die Lösbarkeit der Gleichung $t^2 − Du^2 = −4$, Math. Z. 39 (1934), 95–111
[31] E.S. Selmer, A conjecture concerning rational points on cubic curves, Math. Scand. 2 (1954), 49–54
[32] P. Serf, Congruent numbers and elliptic curves, Proc. Colloq. Debrecen/Hung. 1989, 227–238 (1991)
[33] J. Silverman, Arithmetic of Elliptic Curves, Springer-Verlag 1986
[34] R.J. Stroeker, J. Top, On the equation $Y^2 = (X + p)(X^2 + p^2)$, Rocky Mt. J. Math. 24 (1994), 1135–1161
[35] H. Wada, On the rank of the elliptic curve $y^2 = x^3 − 1513^2 x$, Proc. Japan Acad. 72 (1996), 34–35
[36] H. Wada, M. Taira, Computations of the rank of elliptic curve $y^2 = x^5 − n^2 x$, Proc. Japan Acad. 70 (1994), 154–157

CSU SAN MARCOS, 333 S TWIN OAKS VALLEY RD, SAN MARCOS, CA 92096-0001, USA
E-mail address: franzl@csusm.edu