Notes on Number Theory and Discrete Mathematics
Vol. 18, 2012, No. 2, 42–55

On Tate-Shafarevich groups of families of elliptic curves

Jerome T. Dimabayao and Fidel R. Nemenzo

Institute of Mathematics, University of the Philippines Diliman
Quezon City, Philippines
e-mails: `jdimabayao@math.upd.edu.ph`, `fidel@math.upd.edu.ph`

Abstract: We explicitly show that for some primes $p \equiv 1 \pmod 8$, the elliptic curves $y^2 = x^3 - p^2x$ and $y^2 = x^3 - 4p^2x$ have Tate-Shafarevich groups with nontrivial elements. This involves obtaining Diophantine equations that violate the local-global principle.
Keywords: Elliptic curve, Congruent number, Rational point, Torsor, Mordell-Weil rank, Selmer group.
AMS Classification: 11G05, 11D09.

1 Introduction

Consider the elliptic curves $E : y^2 = x^3 - k^2x$, where k is a nonzero integer. Elliptic curves with rational point T of order 2 such as E come attached with an isogeny $\phi : E \longrightarrow \widehat{E}$ (which depends on the choice of T). With $T = (0,0)$, we have $\widehat{E} : y^2 = x^3 + 4k^2x$, if k is odd, or $\widehat{E} : y^2 = x^3 + \frac{k^2}{4}x$, if k is even. The isogeny $\widehat{E} \longrightarrow E$ will be denoted by ψ. We are interested in the nontrivial rational points of E. These rational points can be recovered from the nontrivial solutions N, M, e of the torsors

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

and

$$\mathcal{T}^{(\phi)}(b_1) : N^2 = b_1M^4 + b_2e^4, \qquad b_1b_2 = 4k^2 \text{ if } k \text{ is odd or } \frac{k^2}{4} \text{ if } k \text{ is even.}$$

It can be shown that the least solution of the torsors above satisfy $(M,e) = (N,e) = (b_1,e) = (b_2,M) = (M,N) = 1$.

We define the Selmer group $S^{(\psi)}(\widehat{E}/\mathbb{Q})$ as the subgroup of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ containing the cosets $b_1 \pmod{\mathbb{Q}^{\times 2}}$ such that the torsor $\mathcal{T}^{(\psi)}(b_1)$ is locally solvable everywhere. The subgroup of

$S^{(\psi)}(\widehat{E}/\mathbb{Q})$ which consists of $b_1 \pmod{\mathbb{Q}^{\times 2}}$ such that the torsor $\mathcal{T}^{(\psi)}(b_1)$ has a global solution will be denoted by $W(\widehat{E}/\mathbb{Q})$. Similarly, we define $S^{(\phi)}(E/\mathbb{Q})$ and $W(E/\mathbb{Q})$. Finally, the quotient of $S^{(\psi)}(\widehat{E}/\mathbb{Q})$ by $W(\widehat{E}/\mathbb{Q})$ is defined as the ψ-part of the Tate-Shafarevich group $\text{Ш}(\widehat{E}/\mathbb{Q})[\psi]$ of $\widehat{E}$; while that of $S^{(\phi)}(E/\mathbb{Q})$ by $W(E/\mathbb{Q})$ is the ϕ-part of the Tate-Shafarevich group $\text{Ш}(E/\mathbb{Q})[\phi]$ of E. The following exact sequences give a summary of the definitions above:

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

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

In particular, a nontrivial element of $\text{Ш}(\widehat{E}/\mathbb{Q})[\psi]$ is given by a torsor $\mathcal{T}^{(\psi)}(b_1)$ that is everywhere solvable locally but not globally. Similarly for $\text{Ш}(E/\mathbb{Q})[\phi]$. The groups Ш measures the failure of the local-global principle for the elliptic curve E_k.

Determining global solvability of the torsors $\mathcal{T}^{(\psi)}(b_1)$ and $\mathcal{T}^{(\phi)}(b_1)$ is necessary in computing the **Mordell-Weil rank** or **rank** r of E using Tate's formula:

$$2^{r+2} = \#W(\widehat{E}/\mathbb{Q}) \cdot \#W(E/\mathbb{Q}).$$

However, it is generally difficult to determine whether a Diophantine equation is globally solvable or not. Thus making rank computation a tough one. But since $\#W(\widehat{E}/\mathbb{Q}) \mid \#S^{(\psi)}(\widehat{E}/\mathbb{Q})$ and $\#W(E/\mathbb{Q}) \mid \#S^{(\phi)}(E/\mathbb{Q})$, we see that computation of the Selmer groups allows us to obtain an upper bound for r.

In this paper, we look at the elliptic curves E_p for p prime such that

$$\begin{cases} p \equiv 1 \pmod{16} \text{ with } \left(\dfrac{2}{p}\right)_4 \neq 1; \text{ or} \\ p \equiv 9 \pmod{16} \text{ with } \left(\dfrac{2}{p}\right)_4 = 1. \end{cases} \tag{H}$$

These elliptic curves are of interest since they have associated torsors that violates the local-global principle. We give families of equations by elementary means that produce nontrivial elements of the Tate-Shafarevich groups for E_p, thus, showing that E_p have rank zero. We do the same for the elliptic curves $E_{2p} : y^2 = x^3 - 4p^2x$, where $p \equiv 9 \pmod{16}$.

2 The Selmer groups

Determining whether a torsor is locally solvable everywhere is more manageable due to the following result [3]:

Theorem 2.1. *The equation*

$$N^2 = b_1M^4 + b_2e^4$$

has a nontrivial solution in $\mathbb{F}_p$ where $p \nmid 2b_1b_2$.

Thus, the problem of local solvability everywhere reduces to the local solvability modulo a finite set of primes, i.e. modulo the primes dividing the coefficients in the torsor. For the elliptic curves E_p, the associated torsors are given by

$$\mathcal{T}^{(\psi)}(b_1) : N^2 = b_1 M^4 + b_2 e^4, \qquad b_1 b_2 = -p^2$$

and

$$\mathcal{T}^{(\phi)}(b_1) : N^2 = b_1 M^4 + b_2 e^4, \qquad b_1 b_2 = 4p^2.$$

By applying the previous theorem and with the aid of Hensel's Lemma, it is easy to show the following:

Theorem 2.2. *Let* $p \equiv 1 \pmod 8$ *be prime. Then*

$$S^{(\psi)}(\widehat{E}_p/\mathbb{Q}) = \langle -1, p \rangle = W(\widehat{E}_p/\mathbb{Q}) \qquad \textit{and} \qquad S^{(\phi)}(E_p/\mathbb{Q}) = \langle 2, p \rangle \,.$$

Similarly, for the elliptic curves $E_{2p} : y^2 = x^3 - 4p^2 x$, we have

Theorem 2.3. *If* $p \equiv 1 \pmod 8$*, then*

$$S^{(\psi)}(\widehat{E}_{2p}/\mathbb{Q}) = \langle -1, 2, p \rangle \qquad \textit{and} \qquad S^{(\phi)}(E_{2p}/\mathbb{Q}) = \langle p \rangle \,.$$

3 Main results

3.1 The rank of the elliptic curve E_p for $p \equiv 1 \pmod 8$

From Theorem 2.2, we see that the rank of E_p is bounded by 0 and 2. The succeeding results will help us determine the exact rank of E_p for primes p satisfying (H). To be able to get the exact rank, we need to determine the number of elements of $W(E_p/\mathbb{Q})$. This amounts to showing the existence of nontrivial elements of the ϕ-part of the Tate-Shafarevich group $Ш(E_p/\mathbb{Q})[\phi]$.

3.1.1 Some lemmata

Lemma 3.1. *Let* p *be a prime such that* $p \equiv 1 \pmod 8$*. Write* $p = a^2 - 2b^2 = c^2 + d^2$*, with* a, c *odd and* b, d *even. Then*

$$\left(\frac{2}{p}\right)_4 = \left(\frac{-2}{a}\right) = (-1)^{d/4}$$

Proof. See page 156 of [1]. □

Lemma 3.1 says that if $p = a^2 - 2b^2 \equiv 1 \pmod 8$, then

$$\left(\frac{2}{p}\right)_4 = \begin{cases} 1 & \text{if } a \equiv 1, 3 \pmod 8 \\ -1 & \text{if } a \equiv 5, 7 \pmod 8 \end{cases}$$

Also, if we write $p = c^2 + d^2$, then

$$\left(\frac{2}{p}\right)_4 = \begin{cases} 1 & \text{if } d \equiv 0 \pmod 8 \\ -1 & \text{if } d \equiv 4 \pmod 8 \end{cases}$$

The following lemma is the well-known Pythagorean triple theorem. This result allows us to enumerate all the Pythagorean triples. We will use this result to break down the the torsors into degree 2 equations. Solvability of such equations is easier to investigate.

Lemma 3.2. *The solutions of the equation*

$$x^2 + y^2 = z^2$$

with $(x, y, z) = 1$ *and* y *even, are given by the formulas*

$$x = s^2 - t^2, \quad y = 2st, \quad z = s^2 + t^2,$$

where s, t *are integers with* $(s, t) = 1$ *and* $s \not\equiv t \pmod 2$.

Lemma 3.3. *Let* a *be odd,* b *even and* c *squarefree with* $c = a^2 + b^2$*. Moreover, assume that* x *is odd,* y *is even,* $(x, y) = 1$*, and* $z \in \mathbb{Z}$ *such that* $x^2 + y^2 = cz^2 = (a^2 + b^2)z^2$*. Then we have*

$$(ax + by + cz)(ax - by - cz) = -c(y + bz)^2$$

and

$$d = (ax + by + cz, ax - by - cz) = 2\square.$$

As a consequence, there exist integers u, v *such that*

$$\begin{aligned} by + cz \pm ax &= 2cu^2 \\ by + cz \mp ax &= 2v^2 \\ y + bz &= 2uv. \end{aligned}$$

Proof. See [5]. $\square$

We present a similar version of the previous lemma:

Lemma 3.4. *Let* a *be odd,* b *even and* c *squarefree with* $c = a^2 - 2b^2$*. Moreover, assume that* x *is odd,* y *is even,* $(x, y) = 1$*, and* $z \in \mathbb{Z}$ *such that* $x^2 - 2y^2 = cz^2 = (a^2 - 2b^2)z^2$*. Then we have*

$$(ax + 2by + cz)(ax - 2by - cz) = 2c(y - bz)^2$$

and

$$d = (ax + 2by + cz, ax - 2by - cz) = 2\square$$

Proof. Set $A = ax + 2by + cz$ and $B = ax - 2by - cz$. We see that

$$\begin{aligned} AB &= a^2x^2 - 4b^2y^2 - 4bcyz - c^2z^2 \\ &= a^2(cz^2 + 2y^2) - 4b^2y^2 - 4bcyz - c^2z^2 \\ &= ca^2z^2 + (a^2 - 2b^2)(2y^2) - 4bcyz - c^2z^2 \\ &= ca^2z^2 + 2cy^2 - 4bcyz - c^2z^2 \\ &= c(a^2z^2 + 2y^2 - 4byz - cz^2) \\ &= c(a^2z^2 + 2y^2 - 4byz - a^2z^2 + 2b^2z^2) \\ &= 2c(y - bz)^2. \end{aligned}$$

Since A and B are both even, and $d \mid A + B = 2ax$ with ax odd, we have $2 \mid\mid d$. Let q be an odd prime divisor of d. Then $q \mid ax$. Also, $q \mid 2c(y - bz)^2$ which implies $q \mid y - bz$, because $2c$ is squarefree.

If $q \mid a$, then $q \mid 2(y - bz)(y + bz) = 2(y^2 - b^2z^2) = x^2 - a^2z^2$ from which it follows that $q \mid x$. Conversely, $q \mid x$ implies $q \mid az$. But $(x, z) = 1$, so $q \mid a$.

Note that $q \not| \; y + bz$. Otherwise we would get $q \mid y + bz + y - bz = 2y$ and $q \mid y$, which contradicts $(x, y) = 1$.

Now, let $q^k \mid\mid a$ and $q^l \mid\mid x$. So $q^{2k} \mid\mid a^2$ and $q^{2l} \mid\mid x^2$. Consider the following cases:

If $k < l$, we get $q^{2k} \mid\mid (x^2 - a^2z^2) = 2(y + bz)(y - bz)$. Thus, $q^{2k} \mid\mid y - bz$, so $q^{2k} \mid\mid d$.

If $k > l$, we get $q^{2l} \mid\mid d$.

If $k = l$, then $q^{2k} \mid d$, and since $d \mid 2ax$ and $q2k \mid\mid ax$, we obtain $q^{2k} \mid\mid d$.

Therefore, d is twice a square. □

A result of the previous lemma is the existence of integers u, v such that

$$\begin{aligned} ax \pm 2by \pm cz &= 4cu^2 \\ ax \mp 2by \mp cz &= 2v^2 \\ y - bz &= 2uv \end{aligned} \quad \text{or} \quad \begin{aligned} ax \pm 2by \pm cz &= 2cu^2 \\ ax \mp 2by \mp cz &= 4v^2 \\ y - bz &= 2uv \end{aligned}$$

To show $\#W(E_p/\mathbb{Q}) = 1$, we need to show global unsolvability of the following torsors:

$$\begin{aligned} \mathcal{T}^{(\phi)}(2) : N^2 &= 2M^4 + 2p^2e^4 \\ \mathcal{T}^{(\phi)}(p) : N^2 &= pM^4 + 4pe^4 \\ \mathcal{T}^{(\phi)}(2p) : N^2 &= 2pM^4 + 2pe^4 \end{aligned}$$

Theorem 3.1. *The torsor $\mathcal{T}^{(\phi)}(2) : N^2 = 2M^4 + 2p^2e^4$ is not solvable in $\mathbb{Z}$.*

Proof. Suppose $\mathcal{T}^{(\phi)}(2)$ is solvable in $\mathbb{Z}$ with solution (N, M, e), such that $(M, e) = (N, e) = (2, e) = (2p^2, M) = (M, N) = 1$. Then there exists $n \in \mathbb{Z}$ such that

$$2n^2 = M^4 + p^2e^4. \tag{1}$$

Clearly, M and e are both odd. Also note that $p \nmid n$. Reducing (1) modulo 8 shows that n is also odd.

Let q be an odd prime such that $q \mid n$. Reducing (1) modulo q, we get $\left(\frac{-1}{q}\right) = 1$. Thus, $q \equiv 1 \pmod 4$ and consequently, $n \equiv 1 \pmod 4$.

Squaring both sides of (1), we get

$$4n^4 = M^8 + 2p^2M^4e^4 + p^4e^8.$$

We add $-4p^2M^4e^4$ to both sides and work further on the previous equation to derive a Pythagorean equation:

$$\begin{aligned}
4n^4 - 4p^2M^4e^4 &= M^8 + 2p^2M^4e^4 + p^4e^8 - 4p^2M^4e^4 \\
4(n^4 - p^2M^4e^4) &= (M^4 - p^2e^4)^2 \\
(n^2)^2 - (pM^2e^2)^2 &= \left(\frac{M^4 - p^2e^4}{2}\right)^2 \\
(n^2)^2 &= \left(\frac{M^4 - p^2e^4}{2}\right)^2 + (pM^2e^2)^2
\end{aligned}$$

The integers n^2 and pM^2e^2 are relatively prime from the conditions about N, M and e stated above.

Let $d = (M^4 - p^2e^4, pM^2e^2)$. Then d is odd and we have

$$d^2 | (M^4 - p^2e^4)^2 + 4p^2M^4e^4 = (M^4 + p^2e^4)^2.$$

So $d | M^4 + p^2e^4 = 2n^2$. Because d is odd, $d | n^2$, and thus $d = 1$. This shows that $\frac{M^4 - p^2e^4}{2}$ and pM^2e^2 are relatively prime.

If $d_1 = (M^4 - p^2e^4, n^2)$, then $d_1 \mid 2n^2$. Thus,

$$d_1 | 2n^2 + M^4 - p^2e^4 = M^4 + p^2e^4 + M^4 - p^2e^4 = 2M^2.$$

Since n is odd, $d_1 \nmid 2$. So $d_1 \mid M^2$. Because $(M, N) = (M, 2n) = 1$, we must have $d_1 = 1$. Consequently, $\left(\frac{M^4 - p^2e^4}{2}, n^2\right) = 1$.

The above arguments show that the quantities n^2, $\frac{M^4 - p^2e^4}{2}$ and pM^2e^2 are mutually relatively prime.

Since $16 \mid M^4 - p^2e^4$, we see that $\frac{M^4 - p^2e^4}{2}$ is even. Hence, by Lemma 3.2, there exist relatively prime integers s and t such that

$$pM^2e^2 = s^2 - t^2, \qquad M^4 - p^2e^4 = 4st, \qquad n^2 = s^2 + t^2.$$

From the second equation, we have $4st = M^4 - p^2e^4 \equiv 0 \pmod{16}$. So $st \equiv 0 \pmod 4$. Since $s^2 - t^2 \equiv 1 \pmod 8$ from the first equation above, we see that s must be odd and $t \equiv 0 \pmod 4$.

Now, from the first and third equations, we derive $pM^2e^2 = n^2 - 2t^2$. Now writing $p = a^2 - 2b^2$, with a odd, b even, and employing Lemma 3.4, we find integers u and v such that

$$\begin{aligned}
an \pm 2bt \pm pMe &= 4pu^2 \\
an \mp 2bt \mp pMe &= 2v^2 \\
t - bMe &= 2uv
\end{aligned}
\qquad \text{or} \qquad
\begin{aligned}
an \pm 2bt \pm pMe &= 2pu^2 \\
an \mp 2bt \mp pMe &= 4v^2 \\
t - bMe &= 2uv
\end{aligned}$$

Consider the first system of equations. The sum and difference of the first two equations give

$$an = 2pu^2 + v^2 \qquad \text{and} \qquad 2bt + pMe = 2pu^2 - v^2,$$

respectively. Consider the following cases:

1. If $p \equiv 1 \pmod{16}$ such that $\left(\frac{2}{p}\right)_4 = -1$. From the remark succeeding Lemma 3.1, we have $a \equiv 5$ or $7 \pmod 8$.

   If $a \equiv 5 \pmod 8$, then $2 \mid\mid b$. For if $4 \mid b$, we get $p = a^2 - 2b^2 \equiv 9 \pmod{16}$. Now, $2pu^2 + v^2 = an \equiv 1 \pmod 4$ shows that u must be even and v odd. Reducing the third equation modulo 4, we obtain

   $$-bMe \equiv t - bMe = 2uv \equiv 0 \pmod 4,$$

   a contradiction since $2 \mid\mid b$ and Me is odd.

   On the other hand, when $a \equiv 7 \pmod 8$, we see that $2pu^2 + v^2 = an \equiv 3 \pmod 4$. Thus, u and v are both odd in this case. As a result,

   $$Me \equiv 2bt + pMe = 2pu^2 - v^2 \equiv 1 \pmod 8.$$

   Reduction of the equation $pM^2e^2 = n^2 - 2t^2$ modulo 16 gives $n^2 \equiv 1 \pmod{16}$ or $n \equiv \pm 1 \pmod 8$ But since $n \equiv 1 \pmod 4$, we must have $n \equiv 1 \pmod 8$. These give

   $$7 \equiv an = 2pu^2 + v^2 \equiv 3 \pmod 8,$$

   a contradiction.

2. Suppose $p \equiv 9 \pmod{16}$ with $\left(\frac{2}{p}\right)_4 = -1$. So that $a \equiv 1$ or $3 \pmod 8$.

   This time, $a \equiv 1 \pmod 8$ implies $2 \mid\mid b$. Arguing as before, we deduce u is even and v is odd and arrive at a contradiction. If $a \equiv 3 \pmod 8$, then u and v are both odd and $Me \equiv 1 \pmod 8$. Hence, reduction of $pM^2e^2 = n^2 - 2t^2$ modulo 16 and the fact that $n \equiv 1 \pmod 4$ leads us to $n \equiv 5 \pmod 8$. So

   $$7 \equiv an = 2pu^2 + v^2 \equiv 3 \pmod 8,$$

   again a contradiction.

With the same flow of arguments, we can show that the second system of equations will lead us to contradictions. These contradictions show that $\mathcal{T}^{\phi}(2)$ does not admit a solution in $\mathbb{Z}$. $\square$

Theorem 3.2. *The torsor $\mathcal{T}^{(\phi)}(p) : N^2 = pM^4 + 4pe^4$ is not solvable in $\mathbb{Z}$.*

Proof. Assume it has a solution $(N, M, e) \in \mathbb{Z}^3$, with $(M, e) = (N, e) = (p, e) = (4p, M) = (M, N) = 1$. Reduction modulo 8 of $\mathcal{T}^{(\phi)}(p)$ will show that e is even, M and n are odd. Also, there exists an integer n such that

$$pn^2 = (M^2)^2 + (2e^2)^2.$$

Let q be a prime divisor of n. Then $\left(\frac{-1}{q}\right) = 1$ and so $q \equiv 1 \pmod 4$. Hence, $n \equiv 1 \pmod 4$. Write $p = c^2 + d^2$, with c odd and d even. By Lemma 3.3, we can find integers u and v such that

$$\begin{aligned} 2de^2 + pn \pm cM^2 &= 2pu^2 \\ 2de^2 + pn \mp cM^2 &= 2v^2 \\ 2e^2 + dn &= 2uv \end{aligned}$$

Eliminating cM^2, we obtain $2de^2 + pn = pu^2 + v^2$. Consider now the following cases:

1. Assume $p \equiv 1 \pmod{16}$ such that $\left(\frac{2}{p}\right)_4 = -1$, that is $d \equiv 4 \pmod 8$. Since e is even and $n \equiv 1 \pmod 4$, we have

$$\begin{aligned} 2uv = 2e^2 + dn &\equiv 4 \pmod 8 \\ \Longrightarrow uv &\equiv 2 \pmod 4 \end{aligned}$$

So one of u and v is odd and the other is even. The even one is congruent to 2 modulo 4. Thus $2de^2 + pn = pu^2 + v^2 \equiv 5 \pmod 8$, from which it follows that $n \equiv 5 \pmod 8$ and so $n^2 \equiv 9 \pmod{16}$. Hence,

$$9 \equiv pn^2 = M^4 + 4e^4 \equiv 1 \pmod{16},$$

a contradiction.

2. Now suppose $p \equiv 9 \pmod{16}$ such that $\left(\frac{2}{p}\right)_4 = 1$. This time we have $d \equiv 0 \pmod 8$. Then

$$\begin{aligned} 2uv = 2e^2 + dn &\equiv 0 \pmod 8 \\ \Longrightarrow uv &\equiv 0 \pmod 4 \end{aligned}$$

So, at least one of u and v is even. If one is odd, then 4 divides the other one. Thus,

$$n \equiv pn + 2de^2 = pu^2 + v^2 \equiv 0, 1 \text{ or } 4 \pmod 8.$$

Since n is odd, we must have $n \equiv 1 \pmod 8$. So

$$9 \equiv pn^2 = M^4 + 4e^4 \equiv 1 \pmod{16},$$

again a contradiction.

Therefore, $\mathcal{T}^{(\phi)}(p)$ is not solvable in $\mathbb{Z}$. $\square$

Theorem 3.3. *The torsor* $\mathcal{T}^{(\phi)}(2p) : N^2 = 2pM^4 + 2pe^4$ *is not solvable in* $\mathbb{Z}$.

Proof. Again, we proceed by contradiction. Assuming we have a solution $(N, M, e) \in \mathbb{Z}^3$ with $(M, e) = (N, e) = (2p, e) = (2p, M) = (M, N) = 1$, then it is clear that M and e are both odd. We can find an integer n such that $2pn^2 = M^4 + e^4$. It is easy to see that n is odd. Let q be a prime divisor of n then reduction modulo q gives $\left(\frac{-1}{q}\right)_4 = 1$. This means that $q \equiv 1 \pmod 8$ and so $n \equiv 1 \pmod 8$. Note that

$$\begin{aligned}
4p^2n^4 &= M^8 + 2M^4e^4 + e^8 \\
4p^2n^4 - 4M^4e^4 &= M^8 - 2M^4e^4 + e^8 \\
4(p^2n^4 - M^4e^4) &= (M^4 - e^4)^2 \\
(pn^2)^2 &= \left(\frac{M^4 - e^4}{2}\right)^2 + (M^2e^2)^2
\end{aligned}$$

Since M and e are odd, $\frac{M^4 - e^4}{2}$ is even. From the conditions $(N, M) = (2p, e) = (2p, M) = (N, e) = 1$, we see that pn^2 and M^2e^2 are relatively prime.

Let $d = (pn^2, M^4 - e^4)$. Then d is odd and $d | 2pn^2 = M^4 + e^4$. Hence,

$$d | M^4 + e^4 + M^4 - e^4 = 2M^4$$

and

$$d | M^4 + e^4 - (M^4 - e^4) = 2e^4.$$

The fact that d is odd and $(M, e) = 1$ implies that $d = 1$. Thus, $\frac{M^4 - e^4}{2}$ and pn^2 are relatively prime.

Suppose $d_1 = (M^4 - e^4, M^2e^2)$. Again, d_1 is odd and

$$d_1^2 | (M^4 - e^4)^2 + 4M^4e^4 = (M^4 + e^4)^2.$$

So $d_1 | M^4 + e^4$. Arguing as above, we obtain $d_1 = 1$ and thus $(\frac{M^4 - e^4}{2}, M^2e^2) = 1$.

We have shown that the quantities $\frac{M^4 - e^4}{2}$, M^2e^2 and pn^2 are pairwise relatively prime; thus mutually relatively prime. By Lemma 3.2, there exist relatively prime integers s and t, with $s \not\equiv t \pmod 2$ such that

$$M^2e^2 = s^2 - t^2, \qquad M^4 - e^4 = 4st, \qquad pn^2 = s^2 + t^2.$$

Since M and e are odd, we have $s^2 - t^2 = (Me)^2 \equiv 1 \pmod 8$. Thus, s is odd and $4 \mid t$. Again, writing $p = c^2 + d^2$, with c odd and d even, and applying Lemma 3.3 to the third equation above, we can find integers u and v such that

$$\begin{aligned}
pn + dt \pm cs &= 2pu^2 \\
pn + dt \mp cs &= 2v^2 \\
t + dn &= 2uv
\end{aligned}$$

Eliminating cs, we get $pn + dt = pu^2 + v^2$. Reduction modulo 8, we see that

$$u^2 + v^2 \equiv pu^2 + v^2 = pn + dt \equiv 1 \pmod 8.$$

Hence, one of u and v is odd and the other is even. The even one is divisible by 4. In modulo 8, we have

$$t + d \equiv t + dn = 2uv \equiv 0 \pmod 8.$$

So $t \equiv -d \pmod 8$.

Now, because $(Me)^2 = (s+t)(s-t)$ and $(M,e) = (s,t) = 1$ we have

$$g^2 = s + t \qquad \text{and} \qquad h^2 = s - t,$$

where g and r are odd and $gh = Me$.

Finally, we consider the following cases:

1. Suppose $p \equiv 1 \pmod{16}$ with $\left(\dfrac{2}{p}\right)_4 \neq 1$, that is $d \equiv 4 \pmod 8$. Then $t \equiv -d \equiv 4 \pmod 8$. The last two equations that we obtained give $s \equiv 5 \pmod 8$, which implies $s^2 \equiv 9 \pmod{16}$. But

$$s^2 \equiv s^2 + t^2 = pn^2 \equiv 1 \pmod{16}.$$

2. If $p \equiv 9 \pmod{16}$ with $\left(\dfrac{2}{p}\right)_4 = 1$, then $8|t$. This time the last equations give $s \equiv 1 \pmod 8$ and so $s^2 \equiv 1 \pmod{16}$. But

$$s^2 \equiv s^2 + t^2 = pn^2 \equiv 9 \pmod{16}.$$

The two cases in consideration both result to a contradiction. This shows that the torsor $\mathcal{T}^{(\phi)}(2p)$ cannot have a solution in $\mathbb{Z}$.

$\square$

The previous theorems show that $2\mathbb{Q}^{\times 2}, p\mathbb{Q}^{\times 2}, 2p\mathbb{Q}^{\times 2} \notin W(E_p/\mathbb{Q})$ and that the torsors $\mathcal{T}^{(\phi)}(2)$, $\mathcal{T}^{(\phi)}(p)$ and $\mathcal{T}^{(\phi)}(2p)$ all define nontrivial elements of $\text{Ш}(E_p/\mathbb{Q})[\phi]$. Hence, $\#W(E_{2p}/\mathbb{Q}) = 1$.

Finally, Tate's formula for the rank allows us to give the exact rank of E_p for the cases being considered. The following theorem summarizes these:

Theorem 3.4. *Let p be a prime that satisfies condition H. Then the elliptic curve E_p has rank zero. In this case, the Tate-Shafarevich group of E_p has nontrivial elements.*

3.2 The rank of the elliptic curve E_{2p} for $p \equiv 9 \pmod{16}$

From Theorem 2.3, we know that $S^{(\psi)}(\widehat{E}_{2p}/\mathbb{Q}) = \langle -1, 2, p\rangle$ and $S^{(\phi)}(E_{2p}/\mathbb{Q}) = \langle p \rangle$ when $p \equiv 1 \pmod 8$. Thus in this case, the rank of E_{2p} is bounded by 0 and 2. The succeeding results will help us determine the exact rank of E_{2p} for $p \equiv 9 \pmod{16}$. To be able to get the exact rank, we need to determine the number of elements of $W(\widehat{E}_{2p}/\mathbb{Q})$ and $W(E_{2p}/\mathbb{Q})$. We first deal with the order of $W(\widehat{E}_{2p}/\mathbb{Q})$. We will use the following result which enables us to parametrize the solutions of the equation $x^2 + 2y^2 = z^2$, in the same way that we can parametrize the Pythagoren triples.

Lemma 3.5. *The solutions of the equation*

$$x^2 + 2y^2 = z^2 \tag{2}$$

with $(x, y, z) = 1$ are given by the formulas

$$x = \pm(s^2 - 2t^2), \quad y = 2st, \quad z = s^2 + 2t^2,$$

where s, t are integers with $(s, t) = 1$ and s is odd.

Proof. We first note that the solutions x, y and z of (2) are relatively prime in pairs. To show this, let $(x, y) = d > 1$. Then some prime q divides z^2. So that q divides z also, which contradicts the assumption that $(x, y, z) = 1$. Thus, $d = 1$. Similarly, we see that $(x, z) = (y, z) = 1$ also.

Clearly, x and y cannot both be even. We claim that they cannot be both odd either. For if they were, then z is also odd. So

$$3 = 1 + 2 \equiv x^2 + 2y^2 = z^2 \equiv 1 \pmod 8,$$

contradicting (2). Now, if x is even and y is odd, then z is even, contradiction to the fact that $(x, z) = 1$. Thus, x must be odd and y must even. Hence, z is odd.

Write $y = 2u$, for some $u \in \mathbb{Z}$. Substituting this equation in (2) gives

$$x^2 + 8tu^2 = z^2,$$

or

$$8u^2 = z^2 - x^2 = (z + x)(z - x).$$

Since x and z are both odd the two factors $z + x$ and $z - x$ are even, so we can write

$$2u^2 = \left(\frac{z+x}{2}\right) \cdot \left(\frac{z-x}{2}\right),$$

where the factors on the right are integers. Moreover, they are relatively prime. If $\left(\frac{z+x}{2}, \frac{z-x}{2}\right) = d_1 > 1$, then $d_1 \mid \left(\frac{z+x}{2} + \frac{z-x}{2}\right) = z$ and $d_1 \mid \left(\frac{z+x}{2} - \frac{z-x}{2}\right) = x$. But $(x, z) = 1$, so $d_1 = 1$.

So, there exist relatively prime integers s and t such that $st = u$ and

$$2t^2 = \frac{z+x}{2} \text{ and } s^2 = \frac{z-x}{2}$$

or

$$s^2 = \frac{z+x}{2} \text{ and } 2t^2 = \frac{z-x}{2},$$

where we may assume that s and t are positive.

For the first pair of equations, we have $(2s, t) = 1$ and adding those equations gives $z = s^2 + 2t^2$, and subtracting them yields $x = 2t^2 - s^2$.

For the second pair, we have $(2t, s) = 1$ and getting the sum of the equations, we obtain $z = s^2 + 2t^2$. Subtracting the equations gives $x = s^2 - 2t^2$.

In any case, s must be odd. Moreover, we have $y = 2u = 2st$ for both cases. This completes the proof of the lemma. □

Lemma 3.6. *Let* $p \equiv 9 \pmod{16}$. *Then the equation*

$$N^2 = 2M^4 - 2p^2e^4 \tag{3}$$

is not solvable in $\mathbb{Z}$.

Proof. If (3) is solvable in $\mathbb{Z}$ with solution (n, M, e) such that $(N, M) = (N, e) = (M, e) = (2, e) = (2p^2, M) = 1$, then there exists $n \in \mathbb{Z}$ such that

$$2n^2 = M^4 - p^2e^4. \tag{4}$$

Clearly, M and e cannot be both even. From the conditions above, M and e are both odd. Reducing (4) modulo 16 shows that $4 \mid n$.

Let q be an odd prime such that $q \mid e$. Reducing (4) modulo q, we get $\left(\frac{2}{q}\right) = 1$. Thus, $q \equiv \pm 1 \pmod 8$ and consequently, $e \equiv \pm 1 \pmod 8$. If r is an odd prime dividing M, then we have $\left(\frac{-2}{r}\right) = 1$ by reducing (4) modulo r. This shows that every prime divisor of M is congruent to 1 or 3 modulo 8. As a result, $M \equiv 1$ or $3 \pmod 8$.

We write (4) as

$$(pe^2)^2 + 2n^2 = (M^2)^2.$$

Clearly, n and M^2 are relatively prime. Since $(2p^2, M) = (M, e) = 1$, we must have $(pe^2, M^2) = 1$. If d is the greatest common divisor of pe^2 and n then d^2 is a divisor of $(pe^2)^2+2n^2$. Thus $d^2|M^4$ and $d|M^2$. Since $(M, N) = (M, n) = 1$, we get $d = 1$. This shows that pe^2, n and M^2 are mutually relatively prime.

By Lemma 3.5, there exists relatively prime integers s and t, with s odd such that

$$\begin{aligned} pe^2 &= \pm(s^2 - 2t^2), \\ n &= 2st, \\ M^2 &= s^2 + 2t^2. \end{aligned}$$

Since $4 \mid n$, we see that t is even.

The third equation can be written as $s^2 = M^2 - 2t^2$. Plugging this into the first equation gives

$$pe^2 = \pm(M^2 - 4t^2).$$

The equation $pe^2 = -M^2 + 4t^2$ does not hold. If it did, then

$$1 \equiv pe^2 = -M^2 + 4t^2 \equiv -1 + 0 = -1 \pmod 8,$$

contradiction.

Consider $pe^2 = M^2 - 4t^2$. Reducing modulo 16, we see that

$$9 = 9 \cdot 1 \equiv pe^2\ M^2 - 4t^2 \equiv \begin{cases} 1 & \text{if } M \equiv 1 \pmod 8 \\ 9 & \text{if } M \equiv 3 \pmod 8). \end{cases}$$

So, in order for the equation to hold, $M \equiv 3 \pmod 8$.

Now write the equation as $pe^2 = (M+2t)(M-2t)$. Let $d_2 = (M+2t, M-2t)$. Then $d_2 \mid (M+2t+M-2t) = 2M$ and $d_2 = (M+2t-(M-2t)) = 4t$. Since the factors $M+2t$ and $M-2t$ are both odd, $d_2 \not\mid 2$. It follows that $d_2 \mid M$ and $d_2 \mid t$. But $t \mid n$ and $(M,n) = 1$. Hence, $d_2 = 1$. As a result, there exist relatively prime integers e_1 and e_2 with $e_1 e_2 = e$ such that

$$pe_1^2 = M + 2t \text{ and } e_2^2 = M - 2t$$

or

$$e_1^2 = M + 2t \text{ and } pe_2^2 = M - 2t$$

Consider the first pair. Reducing modulo 4, we see that

$$1 \equiv pe_1^2 = M + 2t \equiv 3 + 0 = 3 \pmod 4$$

and

$$1 \equiv e_1^2 = M - 2t \equiv 3 - 0 = 3 \pmod 8.$$

A similar argument shows that the second pair will also lead us to contradiction. These contradictions show that there are no integers N,M and e that satisfy (3).

□

We now count the elements of the group $W(E_{2p}/\mathbb{Q})$. There is only one torsor to consider, $\mathcal{T}^{(\phi)}(p)$. The following lemma shows global nonsolvability of this torsor.

Lemma 3.7. *If* $p \equiv 9 \pmod{16}$, *then the equation*

$$N^2 = pM^4 + pe^4 \tag{5}$$

has no solution in $\mathbb{Z}$.

Proof. Suppose the triple $(N, M, e) \in \mathbb{Z}$ satisfies (5) with $(M, e) = 1$. Then there exists an integer n such that $pn^2 = M^4 + e^4$.

Clearly, M and e cannot be both even. If M and e are both odd, then n must be even and we have

$$2 \equiv M^4 + e^4 = pn^2 \equiv 0 \text{ or } 4 \pmod{16},$$

which leads to a contradiction.

Thus, M and e must be of different parities. By symmetry, assume M is odd and e is even. So that n is odd. Meanwhile, note that $n \neq 1$. Otherwise, we get

$$9 \equiv p = M^4 + e^4 \equiv 1 + 0 = 1 \pmod{16}.$$

Let q be an odd prime dividing n. As $q \mid M \Leftrightarrow q \mid e$ and M is relatively prime to e, $q \nmid Me$. Reducing the equation modulo q, we obtain

$$M^4 + e^4 = pn^2 \equiv 0 \pmod q.$$

Hence, $\left(\frac{-1}{q}\right)_4 = 1$, which implies that $q \equiv 1 \pmod 8$.

This means that every prime divisor of n is 1 modulo 8. Thus, $n \equiv 1 \pmod 8$ and $pn^2 \equiv 9 \pmod{16}$. But this contradicts $M^4 + e^4 \equiv 1 \pmod{16}$ which completes the proof of our assertion. $\square$

Theorem 3.5. *If* $p \equiv 9 \pmod{16}$*, the elliptic curve* E_{2p} *has rank zero with nontrivial element in the Tate-Shafarevich group.*

Proof. Lemma 3.6 shows that $2 \notin W(\widehat{E}_{2p}/\mathbb{Q})$ and that the torsor $\mathcal{T}^{(\psi)}(2)$ defines a nontrivial element of $\text{Ш}(\widehat{E}_{2p}/\mathbb{Q})[\psi]$. Since -1 and $2p$ are in the group $W(\widehat{E}_{2p}/\mathbb{Q})$, we can see that $-2, \pm p \notin W(\widehat{E}_{2p}/\mathbb{Q})$. Hence, $\#W(\widehat{E}_{2p}/\mathbb{Q}) = 4$. With Lemma 3.7, we obtain a nontrivial element of $\text{Ш}(E_{2p}/\mathbb{Q})[\phi]$ and $\#W(E_{2p}/\mathbb{Q}) = 1$. Applying Tate's formula for the rank, we get a zero rank for E_{2p} as stated. $\square$

References

[1] Lemmermeyer, F., *Reciprocity Laws: From Euler to Eisenstein*, Springer Verlag, Berlin, 2000.

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

[3] Nemenzo, F.R., *Congruent Numbers and the Tate-Shafarevich Group of the Elliptic Curve* $y^2 = x^3 - n^2x$. D.Sc. dissertation, Sophia University, 1997.

[4] Silverman, J.H. and Tate, J., *Rational Points on Elliptic Curves*, Springer Verlag, New York, 1992.

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