On the Rank of the Elliptic Curve $y^2 = x^3 - 1513^2x$

By Hideo WADA

Department of Mathematics, Sophia University

(Communicated by Shokichi IYANAGA, M. J. A., Feb. 13, 1996)

§1. Method to be used. Let r_n be the rank of the elliptic curve $y^2 = x^3 - n^2x$. We will prove in this paper r_n is two for $n = 1513 = 17 \cdot 89$ using Tate's method (cf. [3]).

If $x/y = u^2$ for some rational number u, we write $x \sim y$. Consider the diophantine equations:

(1) $dX^4 - (n^2/d)Y^4 = Z^2,\ d \mid n^2,\ d \neq \pm 1,\ d \neq \pm n$

(2) $dX^4 + (4n^2/d)Y^4 = Z^2,\ d \mid 4n^2,\ d \neq 1$

Let $\{d_1, \dots, d_\mu\}$ be the set of d's for which (1) is solvable in X, Y, Z with $(X, (n^2/d)YZ) = (Y, dXZ) = 1$ and $\{d_{\mu+1}, \dots, d_{\mu+\nu}\}$ be the set of d's for which (2) is solvable in X, Y, Z with $(X, (4n^2/d)YZ) = (Y, dXZ) = 1$ (we assume $d_i \neq d_j$ for $1 \leq i < j \leq \mu$ and for $\mu + 1 \leq i < j \leq \mu + \nu$). Then $2^{r_n+2} = (4+\mu)(1+\nu)$ which gives r_n.

For $n = 17 \cdot 89$, we have a solution of (1): $17^2 \cdot 89 \cdot 3^4 - 89 \cdot 5^4 = 1424^2$ and a solution of(2): $2 \cdot 17 \cdot 89 \cdot 7^4 + 2 \cdot 17 \cdot 89 \cdot 5^4 = 3026^2$. Therefore we get $r_n \geq 2$. For proving $r_n = 2$, we must show that the next five diophantine equations have no solutions.

(3) $17 \cdot 89X^4 + 4 \cdot 17 \cdot 89Y^4 = Z^2$

(4) $17X^4 + 4 \cdot 17 \cdot 89^2Y^4 = Z^2$

(5) $17 \cdot 89^2X^4 + 4 \cdot 17Y^4 = Z^2$

(6) $89X^4 + 4 \cdot 17^2 \cdot 89Y^4 = Z^2$

(7) $89 \cdot 17^2X^4 + 4 \cdot 89Y^4 = Z^2$

§2. Non solvability of (3)–(7). If (3) is solvable then $Z = 17 \cdot 89W$ for some integer W and we get $X^4 + 4Y^4 = 17 \cdot 89W^2$. This equation can be written as $(X^2)^2 + (2Y^2)^2 = (27^2 + 28^2)W^2$. We need next lemma (cf. [2] p. 317).

Lemma. When $a =$ odd, $b =$ even, $c = a^2 + b^2 =$ square free, $(x, y) = 1$, $x =$ odd, $y =$ even and $x^2 + y^2 = cz^2 = (a^2 + b^2)z^2$. Then we have

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

$$d = (ax + by + cz, ax - by - cz) = \text{twice a square}$$

Proof. Put $A = ax + by + cz$, $B = ax - by - cz$. Then

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

As $A \equiv B \equiv 0 \pmod 2$ and $d \mid A + B = 2ax$, we have $2 \parallel d$. Let p be an odd prime divisor of d. Then $p \mid ax$ and $p \mid y + bz$ because c is square free. If $p \mid a$ then $p \mid (y + bz)(y - bz) = a^2z^2 - x^2$. So we have $p \mid x$. If $p \mid x$ then $p \mid az$. But $(x, z) = 1$, so we have $p \mid a$. If $p \mid y - bz$ then $p \mid (y + bz) + (y - bz) = 2y$. But $(x, y) = 1$, so we have $p \nmid y - bz$. Let $p^k \parallel a$, $p^l \parallel x$. When $k < l$ then $p^{2k} \parallel y + bz$. So we have $p^{2k} \parallel d$. When $k > l$ we have $p^{2l} \parallel d$. When $k = l$, we have $p^{2k} \mid d$. But $d \mid A + B = 2ax$, so we have $p^{2k} \parallel d$. Therefore d is twice a square.

From this lemma, we can find c_1, c_2, u, v such that

$$ax = c_1u^2 - c_2v^2,\ c_1c_2 = c,\ 2uv = y + bz$$

When $x = X^2$, $y = 2Y^2$, $z = W$, $a = 27$, $b = 28$ then $x =$ odd because of $(X, 4 \cdot 17 \cdot 89YZ) = 1$ and we have

$$27X^2 = c_1u^2 - c_2v^2,\ c_1c_2 = 17 \cdot 89$$

Using $17 \equiv 1 \pmod 4$, $\left(\frac{27}{17}\right) = -1$, $\left(\frac{89}{17}\right) = 1$, we have a contradiction. So (3) has no solution.

If (4) is solvable, then $Z = 17W$ for some integer W and we get

$$(X^2)^2 + (2 \cdot 89Y^2)^2 = (1^2 + 4^2)W^2$$

As X is odd, we have $W =$ odd, $Y =$ even and

$$X^2 = c_1u^2 - c_2v^2,\ c_1c_2 = 17,$$

$$2uv = 2 \cdot 89Y^2 + 4W \equiv 4 \pmod 8$$

From this we have $c_1u^2 - c_2v^2 \equiv \pm 3 \pmod 8$. This is a contradiction. So (4) had no solution. In the same way, (5) has no solution.

If (6) is solvable, then $Z = 89W$ for some integer W and we get

$$(X^2)^2 + (2 \cdot 17Y^2)^2 = (5^2 + 8^2)W^2$$

As X is odd, we have $W =$ odd, $Y =$ even and

$$5X^2 = c_1u^2 - c_2v^2,\ c_1c_2 = 89,$$

$$2uv = 2 \cdot 17Y^2 + 8W \equiv 0 \pmod 8$$

Therefore $c_1u^2 - c_2v^2 \equiv \pm 1 \pmod 8$. This is a contradiction. So (6) has no solution. In the same way, (7) has no solution. Therefore we get $r_{1513} = 2$. Similarly we can get $r_{7361} = 2$.

References

[1] K. Noda and H. Wada: All congruent numbers less than 10000. Proc. Japan Acad., **69A**, 175–178 (1993).

[2] J. H. Silverman: The Arithmetic of Elliptic Curves. GTM106, Springer-Verlag (1986).

[3] J. H. Silverman and J. Tate: Rational Points on Elliptic Curves. Springer-Verlag (1992).

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