On the Rank of the Elliptic Curve $y^2=x^3-2379^2x$

By Fidel R. NEMENZO

Department of Mathematics, Sophia University

(Communicated by Shokichi IYANAGA, M. J. A., Nov. 12, 1996)

Let n be a positive square-free integer and r_n be the rank of the elliptic curve $C: y^2 = x^3 - n^2x$. When $n = 2379$, the zero at $s = 1$ of the Hasse-Weil L-function of C has order 2, which is conjectured by Birch and Swinnerton-Dyer to be the rank r_{2379}. We will use Tate's method to show that r_{2379} is effectively equal to 2.

We write $x \sim y$ whenever $x/y = u^2$ for some rational number u. Consider two types of Diophantine equations:

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

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

Now let $D = (d_1, d_2, \ldots, d_\mu\}$ be the set of distinct (i.e. inequivalent pairwise) d's such that (1) is solvable in integers X, Y, and Z with $(X, (4n^2/d)YZ) = (Y, dXZ) = 1$ and $D' = \{d_{\mu+1}, \ldots, d_{\mu+\nu}\}$ be the set of d's such that (2) is solvable in integers X, Y, and Z with $(X, (n^2/d)YZ) = (Y, dXZ) = 1$. Then $2^{r_n+2} = (1+\mu)(4+\nu)$. See Silverman and Tate [5].

Let $n = 2379 = 3\cdot 13\cdot 61$. We first consider the Diophantine equations of the first type and determine μ. We have

$13(6)^4 + 2^2\cdot 3^2\cdot 13\cdot 61^2(1)^4 = (1326)^2$ and

$61(2)^4 + 2^2\cdot 3^2\cdot 13^2\cdot 61(1)^4 = (610)^2$

so $d = 13$, $d = 61$ and $d = 13\cdot 61$ are in D. The equations (1) for $d = 2$, 3 and 6 can be shown to have no solutions by, say, considering them modulo 3. Hence $\mu = 3$.

In order to show that $r_{2379} = 2$, it will suffice to show that the following equations do not have solutions under the conditions stated above.

(3) $3\cdot 13X^4 - 3\cdot 13\cdot 61^2Y^4 = -Z^2$

(4) $3\cdot 13\cdot 61^2X^4 - 3\cdot 13Y^4 = -Z^2$

(5) $13\cdot 61X^4 - 3^2\cdot 13\cdot 61Y^4 = Z^2$

(6) $13\cdot 61\cdot 3^2X^4 - 13\cdot 61Y^4 = Z^2$

(7) $3\cdot 61X^4 - 3\cdot 61\cdot 13^2Y^4 = -Z^2$

(8) $3\cdot 61\cdot 13^2X^4 - 3\cdot 61Y^4 = -Z^2$

Lemma. *Let a be odd, b even, $c = a^2 - b^2$ square-free, and x odd, y even, $(x, y) = 1$ and $x^2 - y^2 = cz^2$. Then*

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

and

$$(ax + by + cz, ax - by - cz) = 2e^2$$

for some integer e, so that we can find integers c_1, c_2, u and v such that $ax = c_1u^2 + c_2v^2$ and $c = c_1c_2$.

Proof. See Wada [3].

Suppose (3) is solvable. Then for some integer W,

$$X^4 - 61^2Y^4 = -3\cdot 13W^2 \text{ or}$$
$$(X^2)^2 - (61Y^2)^2 = (5^2 - 8^2)W^2.$$

Letting $x = X^2$, $y = 61Y^2$, $z = W^2$, $a = 5$ and $b = 8$, we see that $(x, y) = 1$. If both x and y are odd, or if x is even and y odd, the two sides of the equation above will not be congruent modulo 16. Hence we can apply the lemma and get

$$5X^2 = c_1u^2 + c_2v^2 \text{ and } c_1c_2 = -3\cdot 13.$$

Since $(5/13) = -1$ and $(3/13) = 1$, we have contradiction. Hence (3) is not solvable.

If (4) is solvable, then $(61X)^2 - (Y^2)^2 = (5^2 - 8^2)W^2$. Thus we have $5\cdot 61X^2 = c_1u^2 + c_2v^2$ and $c_1c_2 = -3\cdot 13$. In modulo 13, the right side of the equation is a square while left is not. Hence, (4) is not solvable.

If (5) has solutions X, Y and Z, then for some integer W,

$$(X^2)^2 - (3Y^2)^2 = 13\cdot 61W^2$$
$$= (37^2 - 24^2)W^2.$$

The two sides of the equation are not congruent modulo 16 unless X is odd and Y is even. Applying the lemma, we have

$$37X^2 = c_1u^2 + c_2v^2 \text{ and}$$
$$c_1c_2 = 13\cdot 61.$$

Since $(37/13) = -1$ and $(61/13) = 1$, we have a contradiction, and hence (5) has no solution. Similarly, (6) has no solution.

Lastly, we show that (7) and (8) are not solvable. If (7) has solutions X, Y and Z, then for some integer W,

$$(X^2)^2 - (13Y^2)^2 = -3\cdot 61W^2$$
$$= (29^2 - 32^2)W^2.$$

X is odd and Y is even, so we can apply the lemma once more to get

$$29X^2 = c_1 u^2 + c_2 v^2 \text{ and}$$
$$c_1 c_2 = -3 \cdot 61.$$

Now $(29/61) = -1$ but $(3/61) = 1$, a contradiction. Hence (7) has no solution. Similarly, (8) has no solution. This shows that $\nu = 0$ and $r_{2379} = 2$.

References

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

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

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

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

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