25. *Triangles and Elliptic Curves**)

By Takashi ONO

Department of Mathematics, The Johns Hopkins University, U. S. A.

(Communicated by Shokichi IYANAGA, M. J. A., April 12, 1994)

In this paper, we shall obtain a family of infinitely many elliptic curves defined over an algebraic number field k so that every curve in it has positive Mordell-Weil rank with respect to k. The construction of curves is very easy: we have only to replace *right* triangles in the antique congruent number problem by *arbitrary* triangles.

§1. Arbitrary field. Let k be a field of characteristic $\neq 2$ and let $\bar{k}$ be an algebraic closure of k, fixed once for all. For three elements a, b, c in $\bar{k}$, we shall put

$$P = \frac{1}{2}(a^2 + b^2 - c^2), \tag{1.1}$$

$$Q = \frac{1}{16}(a+b+c)(a+b-c)(a-b+c)(a-b-c) \tag{1.2}$$

$$= \frac{1}{16}(a^4 + b^4 + c^4 - 2a^2b^2 - 2b^2c^2 - 2c^2a^2).$$

One verifies easily that

$$P^2 - 4Q = a^2b^2. \tag{1.3}$$

Now consider the plane cubic:

$$y^2 = x^3 + Px^2 + Qx = x\left(x + \frac{P+ab}{2}\right)\left(x + \frac{P-ab}{2}\right). \tag{1.4}$$

From (1.3), (1.4), one finds that the cubic is non-singular if and only if

$$abQ \neq 0. \tag{1.5}$$

We shall call E the elliptic curve given by (1.4) with the condition (1.5). Referring to standard definitions on Weierstrass equations ([1] p. 46), we find the values of the discriminant and the j-invariant of E in terms of a, b, c, P, Q:

(1.6) $\Delta = (4abQ)^2 = 16D$, D being the discriminant of $x^3 + Px^2 + Qx$,

(1.7) $j = 2^8(P^2 - 3Q)^3/(abQ)^2 = 2^8(Q + a^2b^2)^3/(abQ)^2$.

(1.8) **Remark.** Although not neccesary in this paper, we mention here a basic fact. A simple calculation shows that if (a, b, c) and (a', b', c') are triples in $\bar{k}$ with (1.5) such that $a' = ra$, $b' = rb$, $c' = rc$ with $r \in \bar{k}^\times$, then they have the same j-invariant. Consequently, our construction $(a, b, c) \mapsto E$ induces a map:

(1.9) $P^2(\bar{k}) - H \rightarrow \bar{k}$ (moduli space of elliptic curves over $\bar{k}$),

where H is the union of six lines $a = 0$, $b = 0$, $a + b + c = 0$, $a + b - c = 0$, $a - b + c = 0$ and $a - b - c = 0$.

(1.10) **Lemma.** *Let E be the elliptic curve defined by $a, b, c \in \bar{k}$ with* (1.5).

*) Dedicated to Professor S. Iyanaga on his 88th birthday.

Then the point $P_0 = (x_0, y_0)$ *with* $x_0 = \left(\frac{1}{2}c\right)^2$, $y_0 = \frac{1}{8}c(b^2 - a^2)$ *belongs to* E.

In fact, since $(0, 0) \in E$, we can assume that $c \neq 0$, and we are reduced to check that $(b^2 - a^2)^2 = c^4 + 4Pc^2 + 16Q$.

§2. Number field. Let k be a finite extension of $\boldsymbol{Q}$ and $\mathfrak{o}$ be the ring of integers of k. For a prime ideal $\mathfrak{p}$ of $\mathfrak{o}$, we denote by $\nu_{\mathfrak{p}}$ the order function on k at $\mathfrak{p}$. Let a, b, c be numbers in $\mathfrak{o}$ satisfying, in addition to (1.5), the following conditions:

(2.1) $a + b \equiv c \mod 2$,

(2.2) $c \not\equiv 0 \mod \mathfrak{p}$ for some $\mathfrak{p} \mid 2$.

By (2.1), one sees that P, Q in (1.1), (1.2), respectively, are both in $\mathfrak{o}$. Let E be the elliptic curve (1.4) defined by a, b, c, P, Q. By the Mordell-Weil theorem the group $E(k)$ of rational points on E is finitely generated and hence the rank of $E(k)$ makes sense.

(2.3) **Theorem.** *Notation and assumptions being as above, the rank of* $E(k)$ *is positive, i.e., the elliptic curve* E *contains infinitely many rational points over* k.

Proof. Let $P_0 = (x_0, y_0)$ be the point of E in (1.10). Clearly, P_0 belongs to $E(k)$, and we are going to show that the order of P_0 is not finite. So assume, on the contrary, that P_0 is a point of order $m \geq 2$. From this point on, we need extensively the help of a generalization of the Nagell-Lutz theorem for number fields ([1] p. 220, Theorem 7.1). This theorem, when applied to our $P_0 = (x_0, y_0)$, says:

(a) *If* m *is not a prime power, then* $x_0, y_0 \in \mathfrak{o}$.

(b) *If* $m = \ell^n$ *is a prime power, for each prime ideal* $\mathfrak{q}$ *of* $\mathfrak{o}$ *let*

$$r_{\mathfrak{q}} = [\nu_{\mathfrak{q}}(\ell) / (\ell^n - \ell^{n-1})] \quad ([\ \ ] = \textit{the integral part}).$$

Then $\nu_{\mathfrak{q}}(x_0) \geq -2r_{\mathfrak{q}}$ *and* $\nu_{\mathfrak{q}}(y_0) \geq -3r_{\mathfrak{q}}$.

In particular, x_0 *and* y_0 *are* $\mathfrak{q}$*-integral if* $\nu_{\mathfrak{q}}(\ell) = 0$.

Now the assumption (2.2) implies that $\nu_{\mathfrak{p}}(c) = 0$ for a $\mathfrak{p}$ dividing 2 and so $\nu_{\mathfrak{p}}(x_0) = -2\,\nu_{\mathfrak{p}}(2) < 0$; hence $x_0 \notin \mathfrak{o}$, which shows that the case (a) does not occur. As for the case (b), assume first that $\ell \neq 2$. Take a prime $\mathfrak{p} \mid 2$ with (2.2). Then since $\nu_{\mathfrak{p}}(\ell) = 0$ we have, by the last italicized statement in (b), $0 \leq \nu_{\mathfrak{p}}(x_0) = -2\nu_{\mathfrak{p}}(2) < 0$, and the case $\ell \neq 2$ does not occur also. Therefore it remains to consider the case where $m = 2^n$, $n \geq 1$. For a prime $\mathfrak{p} \mid 2$ with (2.2), put $e = \nu_{\mathfrak{p}}(2)$. If we write $e = s2^{n-1} + r$, with $0 \leq r < 2^{n-1}$, we have $r_{\mathfrak{p}} = s$. Hence (b) implies that $-2s \leq \nu_{\mathfrak{p}}(x_0) = 2\nu_{\mathfrak{p}}(c) - 2\nu_{\mathfrak{p}}(2) = -2\nu_{\mathfrak{p}}(2) = -2e$; so $s \geq e \geq s2^{n-1}$ which is impossible unless $n = 1$. In this case, however, $m = 2$, i.e., $P_0 = (x_0, y_0)$ is of order 2 and so $0 = y_0 = \frac{1}{8}c(b^2 - a^2)$. Therefore $b = \pm a$ and, by (2.1), $c \equiv a + b \equiv 0 \mod 2$, which contradicts (2.2). Thus the last case does not occur, too, Q.E.D.

§3. $\boldsymbol{Q}$ (Comments). (3.1) Right triangles. Let $k = \boldsymbol{Q}$ (so $\mathfrak{o} = \boldsymbol{Z}$) and a, b, c be integers $\neq 0$ such that $gcd(a, b, c) = 1$ and $a^2 + b^2 = c^2$. Then one verifies (1.5), (2.1), (2.2). We have $P = 0$ and $Q = -\frac{1}{4}a^2b^2 = -A^2$, where A is the area of the right triangle with integral sides. The corresponding E is $y^2 = x^3 - A^2x$ with $\Delta = (ab)^6 = 2^6A^6$, $j = 2^63^3 = 1728$.

(3.2) Search of E such that $j(E) = 1728$. To be more precise, let T be a set of $t = (a, b, c) \in \boldsymbol{Z}^3$ such that $gcd(a, b, c) = 1$, $a + b \equiv c \bmod 2$ and $abQ \neq 0$. Let E_t be the elliptic curve (1.4) defined by t. Then, in view of (1.7), finding t such that $j(E_t) = 1728$ amounts to solve the equation

$$(*) \qquad 4(P^2 - 3Q)^3 - 27(abQ)^2 = 0, \quad t = (a, b, c) \in T.$$

Eliminating $(ab)^2$ from $(*)$ and (1.3), we get, after a simple calculation,

$$(**) \qquad 2P^2 = 9Q \quad \text{if } P \neq 0.$$

(Case $P = 0$ was taken care of in (3.1).) From $(**)$ and (1.3), we get

$$(***) \qquad P = \pm 3ab, \quad Q = 2a^2b^2.$$

Hence E_t is isomorphic over $\boldsymbol{Q}$ to the elliptic curve

$$(\#) \qquad y^2 = x^3 - (ab)^2x.$$

(3.3) Case c is even. Let T be the same as in (3.2). Since we do not assume the condition (2.2) (i.e., c is odd) here, we can not use (2.3) to decide whether rank $E_t(\boldsymbol{Q})$, $t = (a, b, c) \in T$, is positive or not when c is even. In this case, however, one finds, using notation in (1.10), that $P_0 = (x_0, y_0) \in \boldsymbol{Z}^2$, and so one has again rank $E_t(\boldsymbol{Q}) > 0$ when

$$(\#\#) \qquad y_0 \nmid \sqrt{D}, \quad D = (abQ)^2.$$

(Cf. the stronger form of the Nagell-Lutz theorem, [2] p. 56.)

By machine computation one obtains lots of curves with positive rank for c even. It would be nice if one could get rid of the assumption (2.2) in (2.3), at least in the case $k = \boldsymbol{Q}$, except isosceles triangles $(a = b)$.

References

[1] Silverman, J. H.: The Arithmetic of Elliptic Curves. Springer-Verlag, New York (1986).

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

[3] Tunnell, J.: A classical diophantine problem and modular forms of weight 3/2. Inventiones Math., **72**, 323–334 (1983).