Elliptic Curves Related with Triangles

By Soonhak KWON

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

(Communicated by Shokichi IYANAGA, M. J. A., June 11, 1996)

In a series of papers [4] [5] [6], T. Ono associated an elliptic curve E to a triangle with sides a, b and c as follows:

$$E : y^2 = x^3 + Px^2 + Qx,$$

where

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

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

We assume $abQ \neq 0$ so that this cubic is non-singular. Then one verifies that the elliptic curve has a point $P_0 = (x_0, y_0) = \left(\frac{c^2}{4}, \frac{c(b^2 - a^2)}{8}\right)$. Assuming that a, b and c belong to an algebraic number field k, T. Ono obtained a certain condition under which the point P_0 has an infinite order, and asked whether this condition can be improved (cf. [4,(I)]). In this paper, we assume that a, b and c belong to $\boldsymbol{Q}$. So the elliptic curve is defined over $\boldsymbol{Q}$ and P_0 is a rational point. In this case, we will get more precise condition so that P_0 has an infinite order.

Following another setting of T. Ono [4,(II)], we define l, m and n as follows:

$$l = \frac{b + a}{2},\ m = \frac{b - a}{2},\ n = \frac{c}{2}.$$

Then, we have

$$E : y^2 = x(x + l^2 - n^2)(x + m^2 - n^2),$$

and $P_0 = (n^2, lmn)$.

Since rational multiples of l, m, n (etc. a, b, c) give isomorphic elliptic curves, we may assume that l, m, n are integers with $(l, m, n) = 1$. Further we assume $lmn \neq 0$, because in case $lmn = 0$ P_0 becomes a 2-torsion point. (i.e. we exclude isosceles triangles.)

Theorem. *Let E be an elliptic curve*

$$y^2 = x(x + l^2 - n^2)(x + m^2 - n^2),$$

where l, m, n are nonzero integers for which

$$(l, m, n) = 1, \quad (l^2 - n^2)(m^2 - n^2)(l^2 - m^2) \neq 0.$$

Suppose that E does not satisfy the following two conditions.

(i) *There exist integers α, β with $(\alpha, \beta) = 1$ such that*

$$l^2 = \alpha^2(\alpha + \beta)^2,\ m^2 = \beta^2(\alpha + \beta)^2,\ n^2 = \alpha^2\beta^2.$$

(ii) *There is a relation among l, m, n as follows*:

$$\frac{1}{n^2} = \frac{1}{l^2} + \frac{1}{m^2} \text{ or } \frac{1}{l^2} = \frac{1}{m^2} + \frac{1}{n^2} \text{ or } \frac{1}{m^2} = \frac{1}{n^2} + \frac{1}{l^2}.$$

Then, $P_0 = (n^2, lmn) \in E(\boldsymbol{Q})$ is of infinite order. If E satisfies (i), *P_0 becomes a 3-torsion point, and if E satisfies* (ii), *P_0 becomes a 4-torsion point.*

Proof. In view of the equation of E there exists a point P in $E(\boldsymbol{Q})$ such that $2P = P_0$ (cf. [2, Th. 4.2]). Suppose that P_0 is a torsion point. Then by Mazur's classification of torsion subgroups of elliptic curves over $\boldsymbol{Q}$, we have

$$P_0 = 2P \in 2 \cdot (\boldsymbol{Z}/2\boldsymbol{Z} \oplus \boldsymbol{Z}/\nu\boldsymbol{Z}), \quad \nu = 2,4,6,8.$$

From the above relation and since $lmn \neq 0$, we easily conclude that P_0 is either a 3-torsion point or a 4-torsion point. Now suppose that P_0 is a point of order 3, then the torsion subgroup of E is isomorphic to $\boldsymbol{Z}/2\boldsymbol{Z} \oplus \boldsymbol{Z}/6\boldsymbol{Z}$ and the theorem of K. Ono [3] implies that there exist a positive integer d and relatively prime integers α, β such that

$$l^2 - n^2 = d^2\alpha^3(\alpha + 2\beta), \quad m^2 - n^2 = d^2\beta^3(\beta + 2\alpha).$$

Since $(d^2\alpha^2\beta^2, \pm d^3\alpha^2\beta^2(\alpha + \beta)^2)$ are points of order 3 (as a simple computation shows) and these are the only 3-torsion points in $\boldsymbol{Q}$, we have $n^2 = d^2\alpha^2\beta^2$. Thus we get

$$l^2 = n^2 + d^2\alpha^3(\alpha + 2\beta) = d^2\alpha^2(\alpha + \beta)^2,$$
$$m^2 = n^2 + d^2\alpha^3(\beta + 2\alpha) = d^2\beta^2(\alpha + \beta)^2.$$

Since we assumed $(l, m, n) = 1$,we get $d = 1$, and

$$l^2 = \alpha^2(\alpha + \beta)^2,\ m^2 = \beta^2(\alpha + \beta)^2,\ n^2 = \alpha^2\beta^2,$$

where α and β are relatively prime integers. Conversely if l, m, n satisfy above conditions, then P_0 must be a 3-torsion point. Next we suppose that P_0 is a 4-torsion point. Then, since $2P_0$ is a point of order 2, we have

$$2P_0 = (0,0), \text{ or } (n^2 - l^2, 0), \text{ or } (n^2 - m^2, 0).$$

Note that, if (x_0, y_0) is a point of $y^2 = x(x + M)$ ·

$(x+N)$, then using the addition law of elliptic curves, the x-coordinate of $2(x_0, y_0)$ becomes $\left(\frac{x_0^2 - MN}{2y_0}\right)^2$. Therefore $2P_0 = (0,0)$ implies $n^4 - (l^2 - n^2)(m^2 - n^2) = 0$, which can be written as $\frac{1}{n^2} = \frac{1}{l^2} + \frac{1}{m^2}$. If $2P_0 = (n^2 - l^2, 0)$, we may use the following isomorphism

$$E : y^2 = x(x + l^2 - n^2)(x + m^2 - n^2) \xrightarrow{\sim} E' : y^2 = x(x + n^2 - l^2)(x + m^2 - l^2)$$
$$(x, y) \mapsto (x + l^2 - n^2, y)$$
$$P_0 = (n^2, lmn) \mapsto (l^2, lmn)$$

Thus $2P_0 = (n^2 - l^2, 0)$ in E is equivalent to $2(l^2, lmn) = (0,0)$ in E'. Therefore we get $\frac{1}{l^2} = \frac{1}{m^2} + \frac{1}{n^2}$ in this case. If $2P_0 = (n^2 - m^2, 0)$, in the same way we get $\frac{1}{m^2} = \frac{1}{n^2} + \frac{1}{l^2}$. Note that converse arguments also hold. □

If we further assume that at least two of l, m, n are odd integers in the above theorem, it is trivial to verify that corresponding elliptic curve does not satisfy the conditions (i) and (ii). Thus we have the following improved version of the theorem of T. Ono [4,(I)] in the special case of the rational field.

Corollary 1. *Let a, b and c be integers with $(a, b, c) = 1$. Then the following elliptic curve*

$$E : y^2 = x^3 + Px^2 + Qx, \quad abQ \neq 0,$$

where

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

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

has infinitely many rational points if $a + b \equiv 1 \pmod 2$.

Proof. By defining $l = b + a$, $m = b - a$, $n = c$ it is clear that E is isomorphic to the elliptic curve $E' : y^2 = x(x + l^2 - n^2)(x + m^2 - n^2)$. Since $(l, m, n) = 1$ and l, m are both odd integers, the point $(n^2, lmn) \in E'(\boldsymbol{Q})$ or equivalently, $\left(\frac{c^2}{4}, \frac{c(b^2 - a^2)}{8}\right) \in E(\boldsymbol{Q})$ is of infinite order. □

Remark 1. Note that we do not need to assume that c is odd as in [4,(I)]. If $a + b \equiv 0 \pmod 2$, then there are plenty of cases where the point $P_0 = \left(\frac{c^2}{4}, \frac{c(b^2 - a^2)}{8}\right)$ becomes a torsion point. For example, when $a = 2$, $b = 4$ and $c = 3$, then P_0 becomes a 3-torsion point and when $a = 4$, $b = 16$ and $c = 15$, then P_0 becomes a 4-torsion point.

Remark 2. If we consider a right triangle a, b, c with $a^2 + b^2 = c^2$ and $(a, b, c) = 1$, then the corresponding elliptic curve is

$$E : y^2 = x^3 - \frac{1}{4}a^2b^2x.$$

Since $a + b \equiv 1 \pmod 2$, the point P_0 is of infinite order and all such elliptic curves have positive rank. Let us consider the easiest case where $a = 3$, $b = 4$ and $c = 5$. Then the corresponding elliptic curve is

$$E : y^2 = x^3 - 36x = x(x + 6)(x - 6),$$

and the point $P_0 = (25/4, 35/8) \in E(\boldsymbol{Q})$. This is an elliptic curve of conductor $N = 576 = 2^6 \cdot 3^2$ and has rank one over $\boldsymbol{Q}$. Therefore it is natural to try to find the relation between the generator and the point P_0 (modulo torsion). Here we can use the table of Cremona [1], where the generators are given for every strong Weil curves of each isogeny classes of elliptic curves of conductor N less than 1000. Since $E : y^2 = x^3 - 36x$ is not a strong Weil curve, we cannot use the table directly but we know that the strong Weil curve of this isogeny class is $E' : y^2 = x^3 + 9x$ and there is a 2-isogeny map $\varphi : E' \to E$. Cremona's table lists (4,10) as a generator of $E'(\boldsymbol{Q})$. By the following simple lemma, we have an information on the generator of $E(\boldsymbol{Q})$.

Lemma. *Let E and E' be elliptic curves over $\boldsymbol{Q}$. Assume that there is a p-isogeny over $\boldsymbol{Q}$, $\varphi : E \to E'$ where p is a prime number. Assume further that the rank of E over $\boldsymbol{Q}$ (hence of E') is one. Let P be a generator of $E(\boldsymbol{Q})$. Then $\varphi(P) = Q$ or pQ* (modulo torsion) *for some generator Q of $E'(\boldsymbol{Q})$.*

Proof. Let $\psi : E' \to E$ be a dual isogeny such that $\psi \circ \varphi = p$. Choose a generator Q of $E'(\boldsymbol{Q})$ such that $\varphi(P) = mQ$ (modulo torsion) where m is a positive integer. Then modulo torsion, we have the following

$$pP = \psi(mQ) = m\psi(Q) = mnP,$$

which implies $mn = p$. Hence $m = 1$ or p. □

Note that $\varphi((4,10)) = (25/4, 35/8) = P_0$ where φ is a 2-isogeny from $E' : y^2 = x^3 + 9x$ to $E : y^2 = x^3 - 36x$ (as for an explicit form of φ, see [8, Ch. III .4]). Thus by the Lemma P_0 is either a generator or twice of a generator. Since P_0 is divisible by 2, it should be twice of a

generator.

Now suppose that we have an elliptic curve $y^2 = x(x + l^2 - n^2)(x + m^2 - n^2)$ and the point (n^2, lmn). Then there is an easy way of finding a point P such that $2P = (n^2, lmn)$ due to T. Ono. Namely, one defines l', m', n' as follows:
$l'^2 = (l + m)(l + n)$, $m'^2 = (m + l)(m + n)$, $n'^2 = (n + l)(n + m)$.

Then it is clear that $l'^2 - n'^2 = l^2 - n^2$ and $m'^2 - n'^2 = m^2 - n^2$. Thus $(n'^2, l'm'n')$ is again a point on the curve and it is trivial to verify $2(n'^2, l'm'n') = (n^2, lmn)$. Since $(25/4, 35/8) = \left(\left(\frac{5}{2}\right)^2, \frac{7}{2}\cdot\frac{1}{2}\cdot\frac{5}{2}\right)$ in $E : y^2 = x(x + 6)(x - 6)$, by applying above method, we easily find a generator (18,72) such that $2(18, 72) = (25/4, 35/8) = P_0$. (End of Remark 2)

Here we have two more corollaries of our theorem.

Corollary 2. *Let E be an elliptic curve*
$E : y^2 = x(x + l^2 - n^2)(x + m^2 - n^2)$,
where $(l^2 - n^2)(m^2 - n^2)(l^2 - m^2) \neq 0$, $lmn \neq 0$. If l, m, n are pairwise prime, i.e. $(l, m) = (m, n) = (n, l) = 1$, then E has a positive rank over $\boldsymbol{Q}$.

Proof. Obvious. □

Corollary 3. *If l, m, n are pairwise prime integers for which $l^2 + m^2 = n^2$. Then the following elliptic curve*
$$E : y^2 = x(x - l^2)(x - m^2)$$
has a positive rank over $\boldsymbol{Q}$.

Proof. $-l^2 = m^2 - n^2$ and $-m^2 = l^2 - n^2$. □

Example. Let $l = 3$ and $m = 4$. Then we have the following elliptic curve $E : y^2 = x(x - 9)(x - 16)$ and the point $P_0 = (25, 60)$ in $E(\boldsymbol{Q})$. This elliptic curve has rank one and the conductor $N = 336 = 2^4 \cdot 3 \cdot 7$. The strong Weil curve of this isogeny class is $E' : y^2 = x(x^2 - x + 16)$ and Cremona's table gives a generator (2,6) for this curve. It is trivial to verify that E' is 2-isogenous to E via tha map
$$\varphi : E' \to E, \quad \text{where } \varphi((x, y)) = \left(\frac{y^2}{x^2} + 9, \frac{y(x^2 - 16)}{x^2}\right).$$
Since $\varphi((2,6)) = (18, -18)$ is not divisible by 2, it is a generator for $E(\boldsymbol{Q})$. Now it is routine to check $2(18, -18) = P_0$, therefore again P_0 is twice of generator.

References

[1] J. E. Cremona: Algorithms for Modular Elliptic Curves. Cambridge Univ. Press, Cambridge (1992).

[2] A. Knapp: Elliptic Curves. Princeton Univ. Press, Princeton (1992).

[3] K. Ono: Euler's concordant forms (preprint).

[4] T. Ono: Triangles and elliptic curves 1-III. Proc. Japan Acad., **70A**, 106–108, 223–225, 311–314 (1994).

[5] T. Ono: Triangles and elliptic curves Ⅳ -VI. Proc. Japan Acad., **71A**, 104–106, 137–139, 184–186 (1995).

[6] T. Ono: Triangles and elliptic curves VII. Proc. Japan Acad., **72A**, 31–33 (1996).

[7] T. Ono: Variations on a Theme of Euler. Plenum Press, New York (1994).

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