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 $y^2 = x(x + M)\cdot$