# 52. On Pythagorean Elliptic Curves

By Norio ADACHI

School of Science and Engineering, Waseda University

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

For any primitive Pythagorean triple $(a, b, c)$, namely, for any relatively prime natural numbers $a, b, c$ which satisfy $a^2 + b^2 = c^2$ with $a$ even, we define an elliptic curve $E = E(a, b, c)$ by the equation

(1) $$y^2 = x(x - a^2)(x - c^2),$$

which will be called the Pythagorean elliptic curve associated with the triple $(a, b, c)$. The curve $E$ is known to be stable with discriminant $\Delta = (abc/4)^4$ and conductor $N = \Pi_{p|abc/4}\, p$ (cf. [1]). We denote by $E(\boldsymbol{Q})$ the group of rational points on the curve $E$, which is a finitely generated abelian group. For simplicity we will adopt the term "a Pythagorean elliptic curve" for $E(\boldsymbol{Q})$. In the present paper, we are going to prove there exist infinitely many Pythagorean elliptic curves $E(\boldsymbol{Q})$ whose rank is positive.

First of all, we note the following:

**Proposition 1.** *Let $T$ be the torsion subgroup of $E(\boldsymbol{Q})$. Then we have*

(2) $$T \simeq \boldsymbol{Z}/2\boldsymbol{Z} \oplus \boldsymbol{Z}/4\boldsymbol{Z}.$$

For the proof, see [2], pp. 96-98.

We paraphrase having a positive rank in the following way:

**Proposition 2.** *Let $r$ denote the rank of $E(\boldsymbol{Q})$. Then we have the inequality $r \geq 1$ if and only if there exists a rational number $x$ such that*

(3) $$x = \square,\ x - a^2 = \square,\ x - c^2 = \square.$$

*Here, and in what follows, $\square$ represents a square of any rational number different from* 0.

*Proof.* The rank $r$ is positive if and only if the rank of the subgroup $2E(\boldsymbol{Q})$ is positive. On the other hand, Proposition 1 states that the torsion subgroup of $2E(\boldsymbol{Q})$ consists of the point at infinity $O$ and the point $P = (c^2, 0)$. If $Q = (x, y)$ is a torsion-free point on $2E(\boldsymbol{Q})$, then $x$ satisfies (3) (cf. [3], p. 47, or [2], p. 37). Since the point $Q$ is not a torsion, none of these $\square$'s are 0.

Conversely, suppose that a rational number $x$ different from 0 satisfies (3). Then the point $Q = (x, y)$, where $y = \sqrt{x(x - a^2)(x - c^2)} \neq 0$ lies on $2E(\boldsymbol{Q})$ and is torsion-free. Hence we have $r \geq 1$. **Q.E.D.**

Since $x$ is a square in (3), it can be expressed as $x^2$ itself. We then write the second and the third $\square$ as $y^2$ and $z^2$, respectively. Then the condition (3) is equivalent to the condition that there exist rational numbers $x, y, z$ different from 0 which satisfy

$$x^2 = a^2 + y^2 = c^2 + z^2.$$

Equivalently, that there exist integers $k, x, y, z$ different from 0 which satisfy

(4) $$x^2=(ka)^2+y^2=(kc)^2+z^2.$$

**Lemma 3.** *The complete solution in integers of the Diophantine equation*
$$x^2+y^2=z^2+w^2$$
*is given by*
$$2x=UX+VY,\ 2z=UX-VY,\ 2w=UY+VX,\ 2y=UY-VX,$$
*where $U$, $V$, $X$, $Y$ are arbitrary integers which make $x$, $y$, $z$, $w$ integral.*

The proof is straightforward (cf. [4], p. 15).

Applying Lemma 3 to (4), we have

(5) $$2ka=UX+VY,\ 2kc=UX-VY$$

(6) $$2y=UY-VX,\ 2z=UY+VX.$$

Since $c+a$, $c-a$ are both square numbers, we express them as $u^2$, $v^2$, respectively:

(7) $$c+a=u^2,\ c-a=v^2.$$

Here, since $a$ is supposed to be even, we have $u\equiv v\equiv 1 \pmod 2$.

Then, from (5), we obtain
$$ku^2=UX,\ kv^2=-VY.$$

Since we have
$$\square=4(ka)^2+4y^2=(UX+VY)^2+(UY-VX)^2=(U^2+V^2)(X^2+Y^2),$$
substituting $U=ku^2/X$, $V=-kv^2/Y$, we see that in order to have $r\geq 1$, it is necessary and sufficient that the equation

(8) $$(u^4Y^2+v^4X^2)(X^2+Y^2)=\square$$

has solutions $X$, $Y$ in integers different from 0 satisfying $X:Y\neq u:v$, which corresponds to the condition that none of the $\square$'s in (3) is equal to 0.

On the other hand, since the torsion subgroup of the rational points of the elliptic curve defined by the equation
$$y^2=x(x+1)(x+(v/u)^4)$$
is isomorphic to the group $\boldsymbol{Z}/2\boldsymbol{Z}\oplus\boldsymbol{Z}/4\boldsymbol{Z}$ (cf. [2], p. 97), the condition that (8) has nonzero solutions in integers is equivalent to the condition that
$$X^2+Y^2=\square,\quad u^4Y^2+v^4X^2=\square$$
has nonzero solutions in integers. The last equation cannot have such solutions $X$, $Y$ as $X:Y=u:v$, because it holds that $u^2+v^2=2c\neq\square$, since $c$ is odd. We thus completed the proof of the following:

**Proposition 4.** *Let $r$ be the rank of $E(\boldsymbol{Q})$. Then $r\geq 1$ if and only if the system of equations*

(9) $$x^2+y^2=\square,\quad v^4x^2+u^4y^2=\square$$

*has solutions in integers different from* 0.

Next, we study how to generate Pythagorean elliptic curves with positive rank. For the purpose we first give a solution $x$, $y$ to the first equation of (9), and then find $u$, $v$ for which the second equation of (9) holds.

Any solution to the first equation of (9) is given by
$$x=2pq,\ y=p^2-q^2,$$
where $p$, $q$ are arbitrary integers with odd parity. Putting $n=pq(p^2-q^2)$, we get
$$(u(p^2-q^2))^4+4n^2v^4=\square$$
from the second equation. If this equation has a solution $(u,v)$ with $u$, $v$

odd, we can determine $a$, $c$ by (7). Then the elliptic curve defined by (1) with these $a$, $c$ has a positive rank. In other words, it is enough that the equation

(10) $$C_n : V^2 = U^4 + 4n^2$$

has a rational point $(U, V)$ with $U \neq \pm(p^2 - q^2)$ and with $U$ 2-free, that is to say, the numerator and the denominator are both odd when $U$ is expressed in the lowest term.

The curve $C_n$ is birationally equivalent to

$$E_n : y^2 = x^3 - n^2 x$$

by the transformation

$$x = (V + U^2)/2,\ y = U(V + U^2)/2;$$
$$V = 2x - (y/x)^2,\ U = y/x.$$

It is necessary and sufficient for $U$ to be 2-free that it holds that $v_2(x) = v_2(y)$. Here, and in what follows, $v_2(x)$ denotes the order of $x$ at 2.

Incidentally, the elliptic curve $E_n$ is known to be related to the congruent number problem (cf. [3]).

$E_n(\boldsymbol{Q})$ has the point

$$P_0 = (x_0, y_0) = (p^2(p^2 - q^2),\ p^2(p^2 - q^2)^2)$$

which is torsion-free. We note that $x_0/y_0$ is 2-free. Since $p$ and $q$ have odd parity, we assume that $p$ is odd. When we deal with $E_n(\boldsymbol{Q})$, this assumption does not damage generality.

For a point $P = (x, y)$ we let $t = t(P) = x/y$ and $s = s(P) = 1/y$. Then we have the following result:

**Proposition 5.** *Let $C$ be the set of rational points $(x, y)$ on the curve $E_n$ for which $v_2(s) \geq 0$ (and hence $v_2(t) \geq 0$), plus the point at infinity $O$. Then the set $C$ is a subgroup of $E_n(\boldsymbol{Q})$, and the map*

$$C \to \boldsymbol{Z}/8\boldsymbol{Z},\quad P = (x, y) \mapsto t(P) = x/y$$

*is a homomorphism, namely, if $P_1, P_2 \in C$, then*

(11) $$t(P_1 + P_2) \equiv t(P_1) + t(P_2) \pmod 8.$$

*Proof.* Since

$$t = \frac{x}{y} \text{ and } s = \frac{1}{y},$$

$y^2 = x^3 - n^2 x$ becomes

(12) $$s = t^3 - n^2 t s^2.$$

Let $P_1 = (t_1, s_1)$ and $P_2 = (t_2, s_2)$ be two rational points on the curve (12). And let $\alpha$ be the slope of the straight line connecting $P_1$ with $P_2$; if $P_1 = P_2$, let $\alpha$ denote the slope of the tangent line to the curve (12) at $P_1$. Then we find

$$\alpha = \frac{t_1^2 + t_1 t_2 + t_2^2 - n^2 s_2^2}{1 + n^2 t_1(s_1 + s_2)}.$$

Let $P_3 = (t_3, s_3)$ be the third point of intersection of the line $s = \alpha t + \beta$ with the curve (12): $\beta = s_1 - \alpha t_1$. Then we get

$$t_1 + t_2 + t_3 = \frac{2n^2\alpha\beta}{1 - n^2\alpha^2};$$

cf. [6], pp. 50-55 for the detailed calculation.

Since $v_2(\alpha)$ and $v_2(\beta)$ are nonnegative and since $n$ is even, we see

$$t_1 + t_2 + t_3 \equiv 0 \pmod 8,$$

from which follows the assertion of the proposition. **Q.E.D.**

Repeated application of the congruence (11) gives the formula

$$t(mP) \equiv mt(P) \pmod 8$$

for a point $P \in C$. On the other hand, the point $P_0$ defined before is in the group $C$, because $p$ is odd. Hence for any odd positive integer $m(\neq 1)$ the point $mP_0 = (x, y)$ has the property that $x/y$ is 2-free. From the preceding consideration we know that this implies the existence of an infinite number of Pythagorean elliptic curves whose rank is positive.

## References

[ 1 ] Frey, G.: Links between stable elliptic curves and certain diophantine equations. Annales Universitatis Saraviensis, Series Mathematicae, **1**, 1-40 (1986).

[ 2 ] Hüsemöller, D.: Elliptic Curves. GTM 111, Springer (1987).

[ 3 ] Koblitz, N.: Introduction to Elliptic Curves and Modular Forms. GTM 97, Springer (1984).

[ 4 ] Mordell, L. J.: Diophantine Equations. Academic Press (1969).

[ 5 ] Silverman, J.: The Arithmetic of Elliptic Curves. GTM 106, Springer (1986).

[ 6 ] Silverman, J., and Tate, J.: Rational Points on Elliptic Curves. UTM, Springer (1992).