Congruent numbers over real quadratic fields

Masatomo Tada
(Received November 6, 2000)
(Revised January 18, 2001)

Abstract. Let \( m \neq 1 \) be a square-free positive integer. We say that a positive integer \( n \) is a congruent number over \( \mathbb{Q}(\sqrt{m}) \) if it is the area of a right triangle with three sides in \( \mathbb{Q}(\sqrt{m}) \). We put \( K = \mathbb{Q}(\sqrt{m}) \). We prove that if \( m \neq 2 \), then \( n \) is a congruent number over \( K \) if and only if \( E_n(K) \) has a positive rank, where \( E_n(K) \) denotes the group of \( K \)-rational points on the elliptic curve \( E_n \) defined by \( y^2 = x^3 - n^2x \). Moreover, we classify right triangles with area \( n \) and three sides in \( K \).

1. Introduction

A positive integer \( n \) is called a congruent number if it is the area of a right triangle whose three sides have rational lengths. For each positive integer \( n \), let \( E_n \) be the elliptic curve over \( \mathbb{Q} \) defined by \( y^2 = x^3 - n^2x \), and \( E_n(k) \) the group of \( k \)-rational points on \( E_n \) for a number field \( k \). By the following well-known theorem, we have a condition such that \( n \) is a congruent number in terms of \( E_n(\mathbb{Q}) \).

**Theorem A** (cf. [4, p. 46]). A positive integer \( n \) is a congruent number if and only if \( E_n(\mathbb{Q}) \) has a point of infinite order.

Let \( \infty \) be the point at infinity of \( E_n(\mathbb{Q}) \) which is regarded as the identity for the group structure on \( E_n \). We note that, in the proof of Theorem A, we use that the torsion subgroup of \( E_n(\mathbb{Q}) \) consists of four elements \( \infty \), \((0,0)\), and \((\pm n,0)\) of order 1 or 2.

For any positive integer \( n \), determining whether it is a congruent number or not is a classical problem. In relation to Theorem A, some important results are known. By the result of J. Coates and A. Wiles [2] for elliptic curves \( E \) over \( \mathbb{Q} \) with complex multiplication, if the rank of \( E_n(\mathbb{Q}) \) is positive, then \( L(E_n, 1) = 0 \), where \( L(E_n, s) \) is the Hasse-Weil \( L \)-function of \( E_n(\mathbb{Q}) \). Assuming the weak Birch and Swinnerton-Dyer conjecture [1], it is known that if \( L(E_n, 1) = 0 \), then the rank of \( E_n(\mathbb{Q}) \) is positive. F. R. Nemenzo [7] showed that for \( n < 42553 \), the weak Birch and Swinnerton-Dyer conjecture holds for \( E_n \), i.e.,

---

2000 Mathematics Subject Classification. 11G05.

Key words and phrases. congruent number, elliptic curve, torsion subgroup.
the rank of $E_n(\mathbb{Q})$ is positive if and only if $L(E_n, 1) = 0$. Moreover, J. B. Tunnell [9] gave a necessary and sufficient condition for $n$ such that $L(E_n, 1) = 0$. And hence, assuming the weak Birch and Swinnerton-Dyer conjecture, it gives a simple criterion to determine whether or not $n$ is a congruent number.

When $n$ is a non-congruent number, one can ask if $n$ is the area of a right triangle with three sides in a real quadratic field. The first aim of this paper is to study an analogy to Theorem A in the case of real quadratic fields, so we will consider congruent numbers over real quadratic fields. Let $m (\neq 1)$ be a square-free positive integer, and put $K = \mathbb{Q}(\sqrt{m})$. We say that $n$ is a congruent number over $K$ if it is the area of a right triangle with three sides consisting of elements in $K$. For the sake of avoiding confusion, when $n$ is the area of a right triangle whose three sides have rational lengths, in this paper, we say that $n$ is a congruent number over $\mathbb{Q}$.

Using the result of Kwon [6, Theorem 1 and Proposition 1] which classify the torsion subgroup of $E : y^2 = x(x + M)(x + N)$, with $M, N \in \mathbb{Z}$, one can determine the torsion subgroup of $E_n(K)$ and prove the following theorem.

**Theorem 1.** Let $n$ be a positive integer. Assume that $m \neq 2$. Then $n$ is a congruent number over $K = \mathbb{Q}(\sqrt{m})$ if and only if $E_n(K)$ has a point of infinite order.

When $m = 2$, Theorem 1 does not hold. For example, when $m = 2$ and $n = 1$, there is the right triangle with three sides $(\sqrt{2}, \sqrt{2}, 2)$ and area 1. However, by using Theorem B which will be reviewed in §2, one can see that the rank of $E_1(\mathbb{Q}(\sqrt{2}))$ is 0.

Combining Theorem 1 with Theorem B, we have the following corollary.

**Corollary 1.** Let $n$ be a positive integer. Assume that $m \neq 2$. Then $n$ is a congruent number over $K = \mathbb{Q}(\sqrt{m})$ if and only if either $n$ or $nm$ is a congruent number over $\mathbb{Q}$.

We assume that $n$ is a non-congruent number over $\mathbb{Q}$. The second aim of this paper is to classify right triangles with three sides in $K$ and area $n$. By using a correspondence between the set of points $2P \in 2E_n(K) \setminus \{\infty\}$ and the set of three sides $(X, Y, Z) \in K^3$ of right triangles with area $n$, and by studying $P + \sigma(P)$, where $\sigma$ is the generator of $\text{Gal}(K/\mathbb{Q})$, we can classify the right triangles with area $n$ and three sides in $K$ as follows.

**Theorem 2.** We assume that $n$ is a non-congruent number over $\mathbb{Q}$. Then we have:
1. Any right triangles with area $n$ and three sides $X, Y, Z \in K = \mathbb{Q}(\sqrt{m})$ ($X \leq Y < Z$) is necessarily one of the following types:
   Type 1. $X \sqrt{m}, Y \sqrt{m}, Z \sqrt{m} \in \mathbb{Q}$. 

Type 2. \( X, Y, Z/\sqrt{m} \in \mathbb{Q} \),
Type 3. \( X, Y \in K \setminus \mathbb{Q} \) such that \( \sigma(X) = Y, Z \in \mathbb{Q} \),
Type 4. \( X, Y \in K \setminus \mathbb{Q} \) such that \( \sigma(X) = -Y, Z \in \mathbb{Q} \),
where \( \sigma \) is the generator of \( \text{Gal}(K/\mathbb{Q}) \).

(2) If \( m \equiv 3, 6, 7 \pmod{8} \) or \( m \) has a prime factor \( q \equiv 3 \pmod{4} \), then there is no right triangle of Type 2. Moreover, there is no right triangle of Type 3 or no right triangle of Type 4.

(3) If \( m \equiv 3, 5, 6, 10, 11, 13 \pmod{16} \) or \( m \) has a prime factor \( q \equiv 3, 5 \pmod{8} \), then there is no right triangle of Type 3 nor that of Type 4.

Remark. Suppose that \( m = 2 \). If \( n = c^2 \) for some \( c \in \mathbb{N} \), then there is a right triangle with \( X = Y = cv/2 \) and area \( n \), which is of Type 4. And if \( n = 2c^2 \) for some \( c' \in \mathbb{N} \), then there is a right triangle with \( X = Y = 2c' \) and area \( n \), which is of Type 2.

The third aim of this paper is to give a condition on types of right triangles with area \( n \) and three sides in \( \mathbb{Q}(\sqrt{m}) \) which is equivalent that \( n \) and \( mn \) are congruent numbers over \( \mathbb{Q} \) as follows.

**Theorem 3.** A positive integer \( n \) is the area of a right triangle with three sides \( X, Y, Z \in \mathbb{Q}(\sqrt{m}) \) such that \( X < Y < Z, Z \notin \mathbb{Q} \) and \( Z/\sqrt{m} \notin \mathbb{Q} \) if and only if \( n \) and \( mn \) are congruent numbers over \( \mathbb{Q} \).

2. Known results

For any real quadratic field \( K \), we need to know the rank of \( E_n(K) \) to prove Theorems 1, 2 and Corollary 1. And hence, we recall the following result.

**Theorem B** (cf. [8, p. 63]). Let \( E \) be an elliptic curve over a number field \( k \) which is given by
\[
E : y^2 = x^3 + ax^2 + bx + c, \quad a, b, c \in k.
\]
And let \( D \) be an element of \( k \setminus \{x^2 | x \in k\} \). Then
\[
\text{rank}(E(k(\sqrt{D}))) = \text{rank}(E(k)) + \text{rank}(E_D(k)),
\]
where \( E_D \) is the twist of \( E \) over \( k(\sqrt{D}) \) which is defined by
\[
E_D : y^2 = x^3 + aDx^2 + bDx + cD^3.
\]

The following theorem allows us to recognize elements of \( 2E_n(K) \).
THEOREM C (cf. [3, p. 85]). Let \(k\) be a field of characteristic not equal to 2 nor 3, and \(E\) an elliptic curve over \(k\). Suppose \(E\) is given by
\[
E : y^2 = (x - \alpha)(x - \beta)(x - \gamma)
\]
with \(\alpha, \beta, \gamma\) in \(k\). Let \((x_0, y_0)\) be a \(k\)-rational point of \(E \setminus \{\infty\}\). Then there exists a \(k\)-rational point \((x_1, y_1)\) of \(E\) with \(2(x_1, y_1) = (x_0, y_0)\) if and only if \(x_0 - \alpha, x_0 - \beta, \) and \(x_0 - \gamma\) are squares in \(k\).

3. Proof of Theorem 1

We first describe the torsion subgroup of \(E_n(\mathbb{Q}(\sqrt{m}))\) in Proposition 1. In the proof of Proposition 1, we use a result of Kwon [6, Theorem 1 and Proposition 1].

PROPOSITION 1. Let \(n\) be either 1 or a square-free positive integer. Let \(T(E_n,k)\) be the torsion subgroup of \(E_n(k)\) over a number field \(k\), and \(E_n[2]\) the 2-torsion subgroup of \(E_n\). If \(n = 1, m = 2,\) then
\[
T(E_1, \mathbb{Q}(\sqrt{2})) = \{ \infty, (0, 0), (\pm 1, 0), (1 + \sqrt{2}, \pm (2 + \sqrt{2})), (1 - \sqrt{2}, \pm (2 - \sqrt{2})) \}.
\]
If \(n = 2, m = 2,\) then
\[
T(E_2, \mathbb{Q}(\sqrt{2})) = \{ \infty, (0, 0), (\pm 2, 0), (2 + 2\sqrt{2}, \pm 4(1 + \sqrt{2})), (2 - 2\sqrt{2}, \pm 4(1 - \sqrt{2})) \}.
\]
Otherwise, \(T(E_n, \mathbb{Q}(\sqrt{m})) = E_n[2] = \{ \infty, (0, 0), (\pm n, 0) \} \).

PROOF. First, note that the 2-torsion subgroup \(E_n[2]\) consists of four elements \((0, 0), (\pm n, 0)\), the point at infinity \(\infty\), i.e.,
\[
T(E_n, \mathbb{Q}(\sqrt{m})) \supseteq E_n[2] \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.
\]
Here, \(E_n^n\) is the twist of \(E_n\) over \(\mathbb{Q}(\sqrt{m})\) and defined by \(y^2 = x^3 - (nm)^2x\), hence \(E_n^n\) is \(E_{nm}\). Therefore, \(T(E_n^n, \mathbb{Q}) = T(E_{nm}, \mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}\). And because \(T(E_n, \mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}\), by using the result of Kwon [6, Theorem 1 and Proposition 1], we have
\[
T(E_n, \mathbb{Q}(\sqrt{m})) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \quad \text{or} \quad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.
\]
Suppose that \(T(E_n, \mathbb{Q}(\sqrt{m})) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}\). Then there exists a point \(P\) of order 4 in \(T(E_n, \mathbb{Q}(\sqrt{m}))\). Therefore, \(2P\) must be \((0, 0)\) or \((\pm n, 0)\). By Theorem C, if \(2P = (0, 0)\) or \((-n, 0)\), then \(-n\) must be a square in \(\mathbb{Q}(\sqrt{m})\) which is a contradiction. If \(2P = (n, 0)\), by Theorem C, then \(n\) and \(2n\) must be squares in \(\mathbb{Q}(\sqrt{m})\). Since \(n\) is a square-free integer, one can see that \(n = 1,\)
m = 2 or n = m = 2. By solving equations obtained by the duplication formula on elliptic curves, we can describe \( T(E_n, \mathbb{Q}(\sqrt{m})) \) concretely. Otherwise, \( T(E_n, \mathbb{Q}(\sqrt{m})) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \). We have completed the proof of Proposition 1.

\[ \square \]

**Proof of Theorem 1.** Let \( k \) be a subfield of \( \mathbb{R} \). For a positive integer \( n \), let \( S \) be the set which consists of \((X, Y, Z) \in k^3\) satisfying that \( 0 < X \leq Y < Z \), \( X^2 + Y^2 = Z^2 \) and \( XY = 2n \), and put

\[
T = \{(u, v) \in 2E_n(k) \setminus \{\infty\} | v \geq 0\}.
\]

Then the map \( \varphi : S \to T \) is defined by

\[
\varphi((X, Y, Z)) = \left( \frac{Z^2}{2}, \frac{Z(Y^2 - X^2)}{8} \right) \quad ((X, Y, Z) \in S).
\]

By Theorem C, one can define a map \( \psi : T \to S \) by

\[
\psi((u, v)) = (\sqrt{u + n} - \sqrt{u - n}, \sqrt{u + n} + \sqrt{u - n}, 2\sqrt{u}) \quad ((u, v) \in T).
\]

Then it is easy to see that \( \psi \) gives the inverse map \( \varphi^{-1} \) of \( \varphi \).

We shall prove that \( S \neq \emptyset \) if and only if \( E_n(k) \setminus E_n[2] \neq \emptyset \). First, we assume that \( S \neq \emptyset \). For \((X, Y, Z) \in S \), we put \( Q = \varphi((X, Y, Z)) \). Because \( Q \) is the point on \( T \), there is a point \( P \in E_n(k) \setminus E_n[2] \) such that \( Q = 2P \). Therefore, we see that \( E_n(k) \setminus E_n[2] \neq \emptyset \). Conversely, we assume that \( E_n(k) \setminus E_n[2] \neq \emptyset \). We take \( P \in E_n(k) \setminus E_n[2] \), and put \( 2P = (x_0, y_0) \). By Theorem C, \( x_0, x_0 \pm n \) are squares in \( k \). Therefore, by the map \( \psi \), we obtain a right triangle with three sides in \( k \).

Here we take a quadratic field \( K = \mathbb{Q}(\sqrt{m}) \) as \( k \). Assume that \( m \neq 2 \). Then we have \( T(E_n, K) = E_n[2] \) by Proposition 1. Therefore, \( E_n(K) \) has a positive rank if and only if \( E_n(K) \setminus E_n[2] \neq \emptyset \). We have completed the proof of Theorem 1.

\[ \square \]

**Proof of Corollary 1.** By Theorem B, \( \text{rank}(E_n(K)) > 0 \) if and only if \( \text{rank}(E_n(Q)) > 0 \) or \( \text{rank}(E_n^m(Q)) > 0 \). Here, \( E_n^m \) is the twist of \( E_n \) over \( K \) and defined by \( y^2 = x^3 - (nm)^2x \). Hence \( E_n^m \) is \( E_{nm} \), which implies that \( \text{rank}(E_n^m(Q)) > 0 \) if and only if \( nm \) is a congruent number. This completes the proof of Corollary 1.

\[ \square \]

**4. Proof of Theorem 2**

First, we describe a formula for the additive law on \( E_n \). For two points \( P_1, P_2 \in E_n(R) \) such that \( P_1 + P_2 \neq \infty \), we put \( P_1 = (x_1, y_1), P_2 = (x_2, y_2) \) and \( P_1 + P_2 = (x_3, y_3) \), where \( x_1, x_2, x_3, y_1, y_2, y_3 \in R \). If \( P_1 \neq P_2 \), then

\[
x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda(x_1 - x_3) - y_1,
\]
where \( \lambda = \frac{y_2 - y_1}{x_2 - x_1} \). If \( P_1 = P_2 \), then we have
\[
x_3 = \left( \frac{x_1^2 + n^2}{2y_1} \right)^2,
\]
which is called the duplication formula.

Now we prove (1) in Theorem 2. Assume that \( n \) is a congruent number over \( K = \mathbb{Q}(\sqrt{m}) \), and let \( X, Y, Z \) (\( 0 < X \leq Y < Z \)) be the three sides of a right triangle with area \( n \) and three sides in \( K \). Then, as is seen in the proof of Theorem 1, there is a point \( P \in E_n(K) \setminus E_n[2] \) such that \( \psi(2P) = (X, Y, Z) \). Further, by the geometric interpretation of the group law on \( E_n(\mathbb{R}) \), we may assume that \( x, y \) satisfies that \( x \geq (1 + \sqrt{2})n \) by replacing \( P \) with \( P + (0, 0) \), \( P + (n, 0) \) or \( P + (-n, 0) \) if necessary. We put \( 2P = (u, v) \), and let \( | \cdot | \) be the usual absolute value which is induced from the embedding \( i : K \hookrightarrow \mathbb{R} \) such that \( i(\sqrt{m}) \) is positive. Then, by the duplication formula on elliptic curves, we have
\[
u = \left( \frac{x^2 + n^2}{2y} \right)^2,
\]
and hence,
\[
\sqrt{u + n} = \frac{x^2 + 2nx - n^2}{2|y|},
\]
\[
\sqrt{u - n} = \frac{x^2 - 2nx - n^2}{2|y|},
\]
\[
\sqrt{u} = \frac{x^2 + n^2}{2|y|}.
\]
Therefore, using the map \( \psi \) in Section 3, we have
\[
X = \frac{2nx}{|y|}, \quad Y = \frac{x^2 - n^2}{|y|}, \quad Z = \frac{x^2 + n^2}{|y|}.
\]
Let \( \sigma \) be the generator of \( \operatorname{Gal}(K/\mathbb{Q}) \), and put \( \sigma(P) = (\sigma(x), \sigma(y)) \). Because \( P + \sigma(P) \) is an element in \( E_n(\mathbb{Q}) \) and \( n \) is a non-congruent number over \( \mathbb{Q} \), we have
\[
P + \sigma(P) \in T(E_n, \mathbb{Q}) = \{ \infty, (0, 0), (\pm n, 0) \}.
\]
Therefore, one of the following cases necessarily happens:

**Case 1.** \( P + \sigma(P) = \infty \). In this case, by the geometric interpretation of the group law on \( E_n(\mathbb{R}) \), \( \sigma(x) = x \) and \( \sigma(y) = -y \). So, \( x \) and \( y \sqrt{m} \) are rational. Therefore, \( X \sqrt{m}, Y \sqrt{m} \) and \( Z \sqrt{m} \) are rational, and so we obtain a right triangle of Type 1.
Case 2. \(P + \sigma(P) = (0,0)\). In this case, by the geometric interpretation of the group law on \(E_n(R)\), we have \(\sigma(x)/x = \sigma(y)/y\), which we denote by \(\lambda\). Then we have
\[
\sigma(y)^2 = x^2y^2 = x^2x^3 - x^2n^2x.
\]
And since \(\sigma(P)\) is a point on \(E_n\), we have
\[
\sigma(y)^2 = \sigma(x)^3 - n^2\sigma(x) = x^3x^3 - n^2x^2x.
\]
Because we easily see that \(x \neq 0, 1\) and \(x \neq 0\), by these equations, we have
\[
ax^2 = -n^2.
\]
Substituting this for \(Y\) and \(Z\), we have \(Y = x(x + \sigma(x))/|y|\) and \(Z\sqrt{m} = x(x - \sigma(x))/\sqrt{m}/|y|\). Since \(x/y = \sigma(x/y)\) and \(x \geq (1 + \sqrt{2})n > 0, x/|y|\) is rational. Therefore, \(X = 2nx/|y|\), \(Y\) and \(Z\sqrt{m}\) are rational, and so we obtain a right triangle with two rational sides including a right angle, which is of Type 2.

Case 3. \(P + \sigma(P) = (n,0)\). In this case, by the geometric interpretation of the group law on \(E_n(R)\), we have \(\sigma(x-n)/(x-n) = \sigma(y)/y\), which we denote by \(\beta\). And we put \(z = x-n\). Then we have
\[
\sigma(y)^2 = \beta^2z^3 + 3\beta^2z^2n + 2\beta^2zn^2.
\]
And since \(\sigma(P)\) is a point on \(E_n\), we have
\[
\sigma(y)^2 = \beta^3z^3 + 3\beta^2z^2n + 2\beta zn^2.
\]
Because we easily see that \(\beta \neq 0, 1\) and \(z \neq 0\), by these equations, we have
\[
\beta z^2 = 2n^2.
\]
Substituting this equation and \(x = z+n\) for three sides \(X, Y,\) and \(Z\), we have \(X = z(\sigma(z) + 2n)/|y|\), \(Y = z(z + 2n)/|y|\) and \(Z = z(z + 2n + \sigma(z))/|y|\). Since \(z/y = \sigma(z/y)\) and \(z > 0, z/|y|\) is rational. Therefore, \(Z\) is rational and \(\sigma(X) = Y\), and so we obtain a right triangle with one rational side and two conjugate sides, which is of Type 3.

Case 4. \(P + \sigma(P) = (-n,0)\). In this case, we put \(w = x + n\). Then one can show, as in the case of Type 3, that \(w/|y|\) and \(Z\) are rational and that \(X = w(\sigma(w) + 2n)/|y|\), \(Y = w(w + 2n)/|y|\), which implies that \(\sigma(X) = -Y\). Hence, we obtain a right triangle with one rational side \(Z\) and two sides \(X, Y\) such that \(\sigma(X) = -Y\), which is of Type 4.
Second, we prove (3) in Theorem 2. Suppose that there is a right triangle of Type 3 (resp. Type 4), and let $a - b\sqrt{m}$ (resp. $-a + b\sqrt{m}$), $a + b\sqrt{m}$ be two sides including a right angle and $c$ the hypotenuse, where $a, b, c$ are positive rational numbers. Then $(x, y, z) = (a, b, c)$ is a non-zero solution of the following equation

$$2x^2 + 2my^2 = z^2.$$  

By the Hasse principle, the above equation has a solution in $\mathbb{Q}$ if and only if it has a solution in $\mathbb{Q}_p$ for every prime $p$, where $\mathbb{Q}_p$ is the field of $p$-adic numbers. Using Hilbert symbols, one can see that it has a solution in $\mathbb{Q}_2$ if and only if $m \equiv 1, 7, 9, 14, 15 \pmod{16}$, and that, when $p = q$ for prime factor $q \neq 2$ of $m$, the above equation has a solution in $\mathbb{Q}_q$ if and only if $2$ is a quadratic residue mod $q$, i.e., $q \equiv 1, 7 \pmod{8}$.

Third, we prove (2) in Theorem 2. Using Hilbert symbols as in the case of (3), one can prove that if $m \equiv 3, 6, 7 \pmod{8}$ or $m$ has a prime factor $q \equiv 3 \pmod{4}$, then there is no right triangle of Type 2. And since a set $\{P \in \sigma(P)\}$ becomes a subgroup of $E_n[2]$, the number of different types of right triangles with area $n$ must not be 3. Therefore, one can see that if there is no right triangle of Type 2, then there is not the right triangle of Type 3 or not the right triangle of Type 4. This completes the proof of Theorem 2.

5. Proof of Theorem 3

First, suppose that $n$ and $nm$ are congruent numbers over $\mathbb{Q}$. By definition, there are rational numbers $a, b, c$ such that $a^2 + b^2 = c^2$, $ab = 2n$, and $a < b < c$. Similarly, there are rational numbers $d, e, f$ such that $d^2 + e^2 = f^2$, $de = 2nm$ and $d < e < f$. Hence, $n$ is also the area of a right triangle

$$\left(\frac{d}{\sqrt{m}}, \frac{e}{\sqrt{m}}, \frac{f}{\sqrt{m}}\right).$$

We recall the maps $\varphi : S \to T$ and $\psi : T \to S$ in §3, and put $P = (u, v) = \varphi((a, b, c)) + \varphi((d/\sqrt{m}, e/\sqrt{m}, f/\sqrt{m}))$. Then

$$u = \frac{f^2(e^2 - d^2)^2 + m^3c^2(b^2 - a^2)^2 - (f^2 + mc^2)(f^2 - mc^2)^2}{4m(f^2 - mc^2)^2} - \frac{cf(b^2 - a^2)(e^2 - d^2)\sqrt{m}}{2(f^2 - mc^2)^2}.$$  

We may assume that $P = (u, v)$ satisfies that $v \geq 0$ by replacing $P$ with $-P$ if necessary. Because $(u, v) \in T$, we have $\psi((u, v)) \in S$, which denotes a system of
three sides of a right triangle with area $n$. Let $(X, Y, Z)$ be the system of three sides of the right triangle with area $n$ obtained above. By Theorem C and the additive law to the points on the elliptic curve, one can see that $X, Y, Z \in \mathbb{Q}(\sqrt{m})$, $Z \notin \mathbb{Q}$ and $Z\sqrt{m} \notin \mathbb{Q}$.

Conversely, suppose to the contrary that either $n$ or $nm$ is non-congruent number over $\mathbb{Q}$. Assuming that $n$ is a non-congruent number over $\mathbb{Q}$ and $nm$ is a congruent number over $\mathbb{Q}$, by Theorem 2 (1), $n$ is not the area of a right triangle with three sides $X, Y, Z \in \mathbb{Q}(\sqrt{m})$ such that $X \leq Y < Z$, $Z \notin \mathbb{Q}$ and $Z\sqrt{m} \notin \mathbb{Q}$. Second, we assume that $nm$ is a non-congruent number over $\mathbb{Q}$ and $n$ is a congruent number over $K = \mathbb{Q}(\sqrt{m})$, and let $(a, b, c) \in K^3$ be a system of three sides of right triangles with area $n$. By multiplying the three sides by $\sqrt{m}$, we have a right triangle with area $nm$ and three sides $(a\sqrt{m}, b\sqrt{m}, c\sqrt{m}) \in K^3$.

For a positive integer $nm$, we define the map $\phi'$ in the same way as for $\phi$. Then one can put $2P' = \phi'((a\sqrt{m}, b\sqrt{m}, c\sqrt{m}))$ for a point $P' \in E_{nm}(K)$. For the generator $\sigma$ of $\text{Gal}(K/\mathbb{Q})$, because $P' + \sigma(P')$ is an element in $E_{nm}(\mathbb{Q})$ and $nm$ is a non-congruent number over $\mathbb{Q}$, we have

$$P' + \sigma(P') \in T(E_{nm}, \mathbb{Q}) = \{ \infty, (0, 0), (\pm nm, 0) \}.$$ 

Therefore, by the same way as in the proof of Theorem 2 (1), one can see that one of the following cases necessarily happens:

Case 1. $a, b, c \in \mathbb{Q}$.
Case 2. $a\sqrt{m}, b\sqrt{m}, c \in \mathbb{Q}$.
Case 3. $a, b \in K \setminus \mathbb{Q}$ such that $\sigma(a) = -b$, $c\sqrt{m} \in \mathbb{Q}$.
Case 4. $a, b \in K \setminus \mathbb{Q}$ such that $\sigma(a) = b$, $c\sqrt{m} \in \mathbb{Q}$.

Hence, $n$ is not the area of a right triangle with hypotenuse $Z = c$ such that $Z \notin \mathbb{Q}$ and $Z\sqrt{m} \notin \mathbb{Q}$. Third, we assume that $n$ and $nm$ are non-congruent numbers over $\mathbb{Q}$. When $m \neq 2$, by Corollary 1, $n$ is not a congruent number over $K$. When $m = 2$ and $n$ is a congruent number over $K$, the right triangle with area $n$ has three sides such that $X = Y$. Hence, one can see that $n$ is not the area of a right triangle with hypotenuse $Z$ such that $Z \notin \mathbb{Q}$ and $Z\sqrt{m} \notin \mathbb{Q}$. We have completed the proof of Theorem 3.

6. Examples

In this section, we give some examples of right triangles. For a positive integer $n$ and a square-free positive integer $m$, let $X, Y, Z \in K = \mathbb{Q}(\sqrt{m})$ ($X \leq Y < Z$) be three sides of right triangles with area $n$, and, using the map $\phi$ in §3, put $Q = \phi((X, Y, Z)) \in 2E_n(K) \setminus \{ \infty \}$.

Example 1. $n = 2$, $m = 17$; We have the following right triangle of Type 1, that of Type 2, that of Type 3 and that of Type 4 in Theorem 2 (1) and the corresponding points of $2E_n(K) \setminus \{ \infty \}$. 

\[\text{Example 1.} \quad n = 2, \ m = 17; \text{ We have the following right triangle of Type 1, that of Type 2, that of Type 3 and that of Type 4 in Theorem 2 (1) and the corresponding points of } 2E_n(K) \setminus \{ \infty \}.\]
Type 1. $34 (= 2 \times 17)$ is a congruent number over $\mathbb{Q}$, and there is a right triangle with three rational sides $(15/2, 136/15, 353/30)$ and area 34. By dividing the three sides by $\sqrt{17}$, we obtain the following right triangle:

$$(X, Y, Z) = \left(\frac{15\sqrt{17}}{34}, \frac{8\sqrt{17}}{15}, \frac{353\sqrt{17}}{510}\right),$$

and we have the corresponding point

$$Q = \left(\frac{2118353}{1040400}, \pm \frac{8245727\sqrt{17}}{6242400}\right) \in 2E_2(\mathbb{Q}(\sqrt{17})) \setminus \{\infty\}.$$

Type 2. We have the following right triangle such that two sides including a right angle are rational:

$$(X, Y, Z) = (1, 4, \sqrt{17}),$$

and the corresponding point

$$Q = \left(\frac{17}{4}, \pm \frac{15\sqrt{17}}{8}\right) \in 2E_2(\mathbb{Q}(\sqrt{17})) \setminus \{\infty\}.$$

Type 3. First, we put $X = x - y\sqrt{17}$, $Y = x + y\sqrt{17}$, and $Z = z$, where $x, y, z \in \mathbb{Q} \setminus \{0\}$. Then $(x, y)$ satisfies that $x^2 - 17y^2 = 4$. For example, $(13/2, 3/2)$ is a solution of this equation. Representing $x$ and $y$ in terms of $t \in \mathbb{Q}$ by using the above solution, we obtain

$$x = \frac{13 - 102t + 221t^2}{2(-1 + 17t^2)}, \quad y = \frac{-3 + 26t - 51t^2}{2(-1 + 17t^2)}.$$

Substituting them for $2x^2 + 34y^2$, by using MATHEMATICA, we find out that if $t = 1$, then $2x^2 + 34y^2$ is a square in $\mathbb{Q}$. Hence, we obtain the following right triangle:

$$(X, Y, Z) = \left(\frac{33 - 7\sqrt{17}}{8}, \frac{33 + 7\sqrt{17}}{8}, \frac{31}{4}\right),$$

and we have the corresponding point

$$Q = \left(\frac{961}{64}, \pm \frac{7161\sqrt{17}}{512}\right) \in 2E_2(\mathbb{Q}(\sqrt{17})) \setminus \{\infty\}.$$
Type 4. The following example is obtained as in the case of Type 3. We have the following right triangle;

\[(X, Y, Z) = \left(\frac{-1 + \sqrt{17}}{2}, \frac{1 + \sqrt{17}}{2}, 3\right),\]

and we have the corresponding point

\[Q = \left(\frac{9}{4}, \pm \frac{3\sqrt{17}}{8}\right) \in 2E_2(Q(\sqrt{17})) \setminus \{\infty\}.\]

We put \(K = Q(\sqrt{17})\). In the same way as in K. Kume’s paper [5, 4-3], using the above examples, one can see that the rank of \(E_{34}(Q)\) is not less than 2 as follows. We define a homomorphism \(\phi : E_2(K) \to E_2(Q)\) by \(\phi(P) = P + \sigma(P)\), \(P \in E_2(K)\) and \(\sigma\) is the generator of \(Gal(K/Q)\). Because 2 is a non-congruent number over \(Q\), we have \(E_2(Q) = E_2[2]\). By the existence of four types of right triangles with area 2, \(\phi\) is surjective, i.e.,

\[E_2(K)/\text{Ker}(\phi) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.\]

Here note that \(\text{Ker}(\phi) \supseteq 2E_2(K)\). Let \(P_1, P_2 \in E_2(K)\) be a point such that \(2P_1 = (17/4, 15\sqrt{17}/8)\), \(2P_2 = (961/64, 7161\sqrt{17}/512)\). Then, by the proof of Theorem 2 (1), \(\phi(P_1) = (0, 0)\), \(\phi(P_2) = (2, 0)\). Hence, we have \(P_1, P_2 \notin 2E_2(K)\) and \(P_1 + P_2 \notin 2E_2(K)\). If we assume that the rank of \(E_2(K)\) is 1, then \(P_1 + P_2 \in 2E_2(K)\), which is a contradiction. Hence, by Theorem B, the rank of \(E_{34}(Q)\) is greater than 1.

It is known that the rank of \(E_{34}(Q)\) is 2 (for example, see [10]).

**Example 2.** \(n = 3, m = 7\); We have the following right triangle of Type 1 and that of Type 4 in Theorem 2 (1), and the corresponding points of \(2E_n(K)\) \(\setminus \{\infty\}\). By Theorem 2 (2), there is no right triangle of Type 2 nor that of Type 3.

Type 1. \(21 (=3 \times 7)\) is a congruent number over \(Q\), and there is a right triangle with area 21 and three rational sides \((7/2, 12, 25/2)\). By dividing the three sides by \(\sqrt{7}\), we obtain the following right triangle;

\[(X, Y, Z) = \left(\frac{\sqrt{7}}{2}, \frac{12\sqrt{7}}{7}, \frac{25\sqrt{7}}{14}\right),\]

and we have the corresponding point

\[Q = \left(\frac{4375}{784}, \pm \frac{13175\sqrt{7}}{3136}\right) \in 2E_3(Q(\sqrt{7})) \setminus \{\infty\}.\]
Type 4. The following example is obtained as in the case of Type 3 in Example 1:

\[ (X, Y, Z) = (-1 + \sqrt{7}, 1 + \sqrt{7}, 4), \]

and we have the corresponding point

\[ Q = (4, \pm 2\sqrt{7}) \in 2E_3(Q(\sqrt{7}))\setminus \{ \infty \}. \]

**Example 3.** \( n = 2, m = 3; \) We have the following right triangle of Type 1 in Theorem 2 (1) and the corresponding point of \( 2E_n(K)\setminus \{ \infty \}. \) By Theorem 2 (2) and (3), there is no right triangle of Type 2, that of Type 3 and that of Type 4.

Type 1. 6 \((= 2 \times 3)\) is a congruent number over \( \mathbb{Q} \), and there is a right triangle with area 6 and three rational sides \((3, 4, 5)\). By dividing the three sides by \( \sqrt{3} \), we obtain the following three sides of a right triangle:

\[ (X, Y, Z) = \left( \sqrt{3}, \frac{4\sqrt{3}}{3}, \frac{5\sqrt{3}}{3} \right), \]

and we have the corresponding point

\[ Q = \left( \frac{25}{12}, \pm \frac{35\sqrt{3}}{72} \right) \in 2E_2(Q(\sqrt{3}))\setminus \{ \infty \}. \]

**Example 4.** \( n = 6, m = 5; \) 6 is a congruent number over \( \mathbb{Q} \), and there is a right triangle with area 6 and three rational sides \((3, 4, 5)\). Further, \( 30 \ ((= 6 \times 5)\) is a congruent number over \( \mathbb{Q} \), and there is a right triangle with area 30 and three rational sides \((5, 12, 13)\). By dividing the three sides by \( \sqrt{5} \), we obtain the right triangle:

\[ \left( \sqrt{5}, \frac{12\sqrt{5}}{5}, \frac{13\sqrt{5}}{5} \right). \]

By the calculation in the proof of Theorem 3, we obtain the right triangle with area 6:

\[ (X, Y, Z) = \left( \frac{33(13 - 5\sqrt{5})}{44}, \frac{4(13 + 5\sqrt{5})}{11}, \frac{7(85 - 13\sqrt{5})}{44} \right). \]

**Acknowledgements**

I am grateful to Professor T. Ichikawa for his valuable suggestions and comments on this research. Actually he suggested me his idea on the classifi-
cation of right triangles by observing $P + \sigma(P)$ and $P' + \sigma(P')$ in the proof of Theorems 2 and 3 respectively. I also thanks to Professor N. Terai and Mr. H. Sekiguchi for their advice. Furthermore, I would like to thank the referee for his many useful comments.

References


Department of Mathematics
Faculty of Science and Engineering
Saga University
Saga, 840-8502 Japan
E-mail: tada@ms.saga-u.ac.jp