On Congruent Numbers and Their Generalizations over Number Fields

Shamik Das

Department of Mathematics
Indian Institute of Technology Guwahati
Guwahati-781039

Nov 06, 2020

Table of Contents

1 Preliminaries
- Congruent number
- Elliptic Curves
- θ-Congruent Number
- Complete 2-descent

2 Our work
- Families of non-congruent numbers
- Criterion of θ-congruent number over number field

3 Publication

4 References

Congruent Number

Congruent number

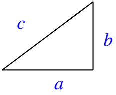
- A natural number $n \in \mathbb{N}$ is called a *congruent number* if it occurs as the area of a rational right triangle, i.e., there exist rational numbers a, b and c such that

$$a^2 + b^2 = c^2, \quad ab = 2n. \tag{1}$$

Congruent number

- A natural number $n \in \mathbb{N}$ is called a *congruent number* if it occurs as the area of a rational right triangle, i.e., there exist rational numbers a, b and c such that

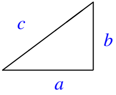
$$a^2 + b^2 = c^2, \quad ab = 2n. \tag{1}$$



Congruent number

- A natural number $n \in \mathbb{N}$ is called a *congruent number* if it occurs as the area of a rational right triangle, i.e., there exist rational numbers a, b and c such that

$$a^2 + b^2 = c^2, \quad ab = 2n. \tag{1}$$

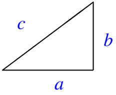


$a, b, c \in \mathbb{Q}$

Congruent number

- A natural number $n \in \mathbb{N}$ is called a *congruent number* if it occurs as the area of a rational right triangle, i.e., there exist rational numbers a, b and c such that

$$a^2 + b^2 = c^2, \quad ab = 2n. \tag{1}$$



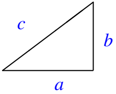
$a, b, c \in \mathbb{Q}$

$n = Area = \frac{1}{2} \times a \times b$

Congruent number

- A natural number $n \in \mathbb{N}$ is called a *congruent number* if it occurs as the area of a rational right triangle, i.e., there exist rational numbers a, b and c such that

$$a^2 + b^2 = c^2, \quad ab = 2n. \tag{1}$$



$a, b, c \in \mathbb{Q}$

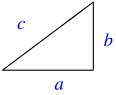
$n = Area = \frac{1}{2} \times a \times b$

- For example, 6 is a congruent number given by the Pythagorean triple $(3, 4, 5)$.

Congruent number

- A natural number $n \in \mathbb{N}$ is called a *congruent number* if it occurs as the area of a rational right triangle, i.e., there exist rational numbers a, b and c such that

$$a^2 + b^2 = c^2, \quad ab = 2n. \tag{1}$$



$a, b, c \in \mathbb{Q}$

$n = Area = \frac{1}{2} \times a \times b$

- For example, 6 is a congruent number given by the Pythagorean triple $(3, 4, 5)$.

- The classical problem of determining whether a given natural number is congruent or not is known as the *congruent number problem*.

The Congruent Number Problem

- It seems that the congruent number problem was first discussed systematically by Arab scholars of tenth century.

The Congruent Number Problem

- It seems that the congruent number problem was first discussed systematically by Arab scholars of tenth century.
- Euler was the first mathematician to show that $n = 7$ is a congruent number.

The Congruent Number Problem

- It seems that the congruent number problem was first discussed systematically by Arab scholars of tenth century.
- Euler was the first mathematician to show that $n = 7$ is a congruent number. Fermat showed that $n = 1$ is not; this result is essentially equivalent to Fermat's Last Theorem for the exponent 4.

The Congruent Number Problem

- It seems that the congruent number problem was first discussed systematically by Arab scholars of tenth century.
- Euler was the first mathematician to show that $n = 7$ is a congruent number. Fermat showed that $n = 1$ is not; this result is essentially equivalent to Fermat's Last Theorem for the exponent 4.
- Nowadays, the Congruent Number Problem can be thought of as the oldest manifestation of a famous conjecture known as the Birch and Swinnerton-Dyer (BSD) Conjecture.

Elliptic Curve

- Elliptic curve appeared first in the book "Arithmetica" by the Greek mathematician Diophantus in the third century A.D..

Elliptic Curve

- Elliptic curve appeared first in the book "Arithmetica" by the Greek mathematician Diophantus in the third century A.D..
- An elliptic curve over a *field* K is a 'non-singular curve' defined by an equation of the form

$$y^2 = x^3 + ax + b, \quad a, \ b \in K.$$

Elliptic Curve

- Elliptic curve appeared first in the book "Arithmetica" by the Greek mathematician Diophantus in the third century A.D..
- An elliptic curve over a *field* K is a 'non-singular curve' defined by an equation of the form
$$y^2 = x^3 + ax + b, \quad a, \ b \in K.$$
- In our case, we take K as number field.

The Point at Infinity on an Elliptic Curve

- A non-vertical line will have three real points of intersection or one real and two complex points of intersection, which is also clear form the substitution $y = mx + c$ in $y^2 = x^3 + ax + b$.

The Point at Infinity on an Elliptic Curve

- A non-vertical line will have three real points of intersection or one real and two complex points of intersection, which is also clear form the substitution $y = mx + c$ in $y^2 = x^3 + ax + b$.
- However, the vertical lines $x = x_0$ will have either two real or two complex points of intersection.

The Point at Infinity on an Elliptic Curve

- A non-vertical line will have three real points of intersection or one real and two complex points of intersection, which is also clear form the substitution $y = mx + c$ in $y^2 = x^3 + ax + b$.

- However, the vertical lines $x = x_0$ will have either two real or two complex points of intersection. For a consistent theory, we need a third point of intersection. We adjoin an additional 'point at infinity' to the curve.

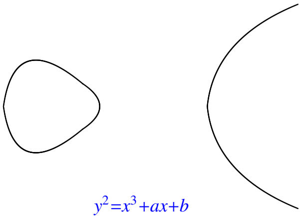
The Point at Infinity on an Elliptic Curve

- A non-vertical line will have three real points of intersection or one real and two complex points of intersection, which is also clear form the substitution $y = mx + c$ in $y^2 = x^3 + ax + b$.
- However, the vertical lines $x = x_0$ will have either two real or two complex points of intersection. For a consistent theory, we need a third point of intersection. We adjoin an additional 'point at infinity' to the curve.
- This point can be visualized as lying on the top (and the bottom) of the xy-plane at infinity.

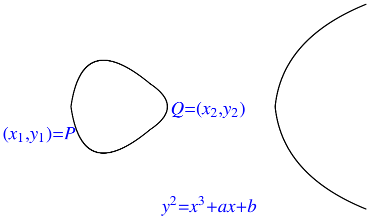
The Point at Infinity on an Elliptic Curve

- A non-vertical line will have three real points of intersection or one real and two complex points of intersection, which is also clear form the substitution $y = mx + c$ in $y^2 = x^3 + ax + b$.
- However, the vertical lines $x = x_0$ will have either two real or two complex points of intersection. For a consistent theory, we need a third point of intersection. We adjoin an additional 'point at infinity' to the curve.
- This point can be visualized as lying on the top (and the bottom) of the xy-plane at infinity.
- Any two vertical lines intersect at the point at infinity, which we denote by $\mathcal{O}$.

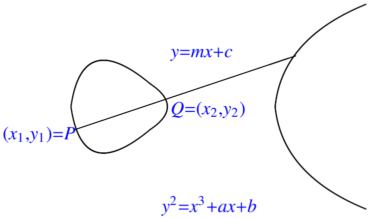
Addition on Elliptic Curve: A Diagram



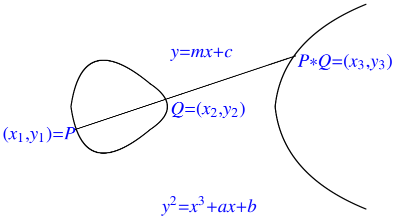
Addition on Elliptic Curve: A Diagram



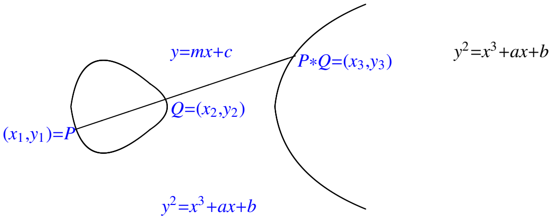
Addition on Elliptic Curve: A Diagram



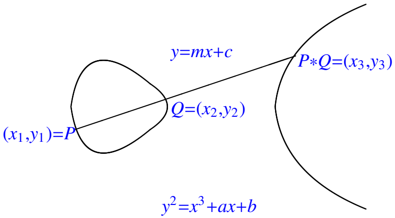
Addition on Elliptic Curve: A Diagram



Addition on Elliptic Curve: A Diagram



Addition on Elliptic Curve: A Diagram

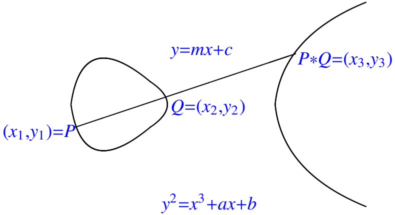


$y^2=x^3+ax+b$

$\Rightarrow (mx+c)^2=x^3+ax+b$

$\Rightarrow x_1+x_2+x_3=m^2$

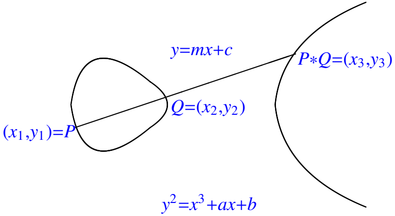
Addition on Elliptic Curve: A Diagram



$$y^2=x^3+ax+b$$
$$\Rightarrow (mx+c)^2=x^3+ax+b$$
$$\Rightarrow x_1+x_2+x_3=m^2$$
$$\Rightarrow x_3=m^2-x_1-x_2.$$

Addition on Elliptic Curve: A Diagram

O: the point at infinity



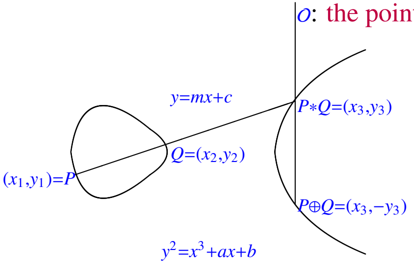
$y^2=x^3+ax+b$

$\Rightarrow(mx+c)^2=x^3+ax+b$

$\Rightarrow x_1+x_2+x_3=m^2$

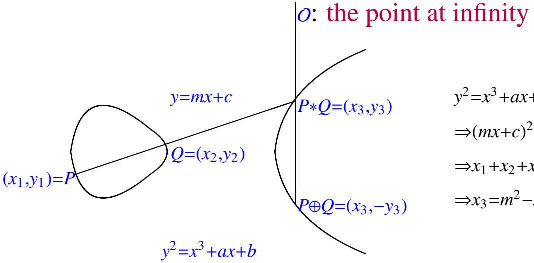
$\Rightarrow x_3=m^2-x_1-x_2.$

Addition on Elliptic Curve: A Diagram



$$y^2=x^3+ax+b$$
$$\Rightarrow (mx+c)^2=x^3+ax+b$$
$$\Rightarrow x_1+x_2+x_3=m^2$$
$$\Rightarrow x_3=m^2-x_1-x_2.$$

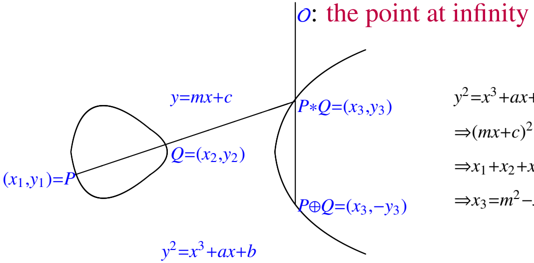
Addition on Elliptic Curve: A Diagram



$$y^2=x^3+ax+b$$
$$\Rightarrow (mx+c)^2=x^3+ax+b$$
$$\Rightarrow x_1+x_2+x_3=m^2$$
$$\Rightarrow x_3=m^2-x_1-x_2.$$

- Any two points P and Q on E can be added to obtain a third point $P \oplus Q$ on E.

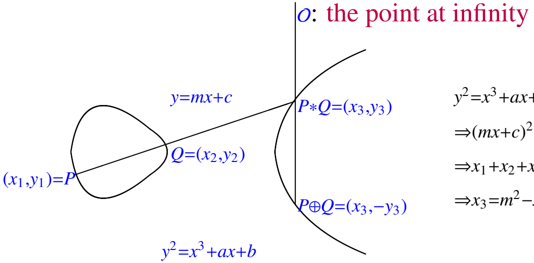
Addition on Elliptic Curve: A Diagram



$$
\begin{aligned}
& y^2=x^3+ax+b \\
& \Rightarrow (mx+c)^2=x^3+ax+b \\
& \Rightarrow x_1+x_2+x_3=m^2 \\
& \Rightarrow x_3=m^2-x_1-x_2.
\end{aligned}
$$

- Any two points P and Q on E can be added to obtain a third point $P \oplus Q$ on E.
- For this addition of points, we have
- an identity, which is $\mathcal{O}$,

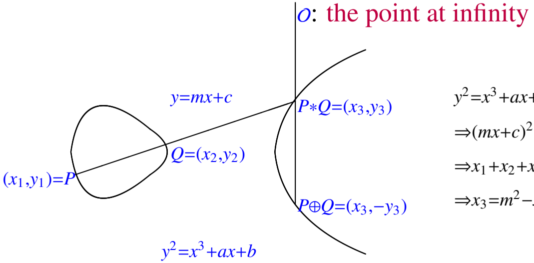
Addition on Elliptic Curve: A Diagram



$$y^2=x^3+ax+b$$
$$\Rightarrow (mx+c)^2=x^3+ax+b$$
$$\Rightarrow x_1+x_2+x_3=m^2$$
$$\Rightarrow x_3=m^2-x_1-x_2.$$

- Any two points P and Q on E can be added to obtain a third point $P \oplus Q$ on E.
- For this addition of points, we have
- an identity, which is $\mathcal{O}$,
- an inverse for each point,

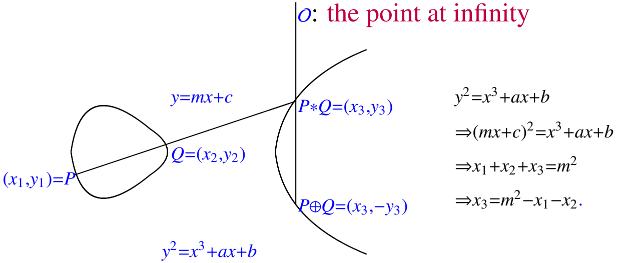
Addition on Elliptic Curve: A Diagram



$$y^2=x^3+ax+b$$
$$\Rightarrow (mx+c)^2=x^3+ax+b$$
$$\Rightarrow x_1+x_2+x_3=m^2$$
$$\Rightarrow x_3=m^2-x_1-x_2.$$

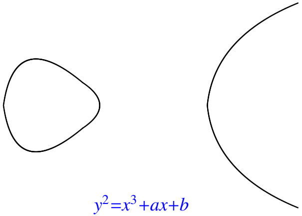
- Any two points P and Q on E can be added to obtain a third point $P \oplus Q$ on E.
- For this addition of points, we have
- an identity, which is $\mathcal{O}$,
- an inverse for each point,
- associativity and

Addition on Elliptic Curve: A Diagram

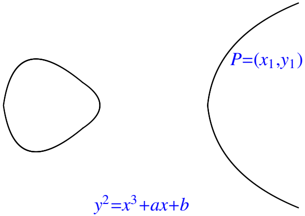


- Any two points P and Q on E can be added to obtain a third point $P \oplus Q$ on E.
- For this addition of points, we have
- an identity, which is $\mathcal{O}$,
- an inverse for each point,
- associativity and
- commutativity.

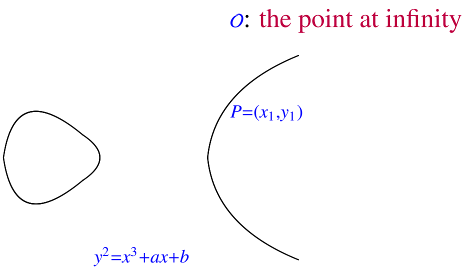
O is the Identity



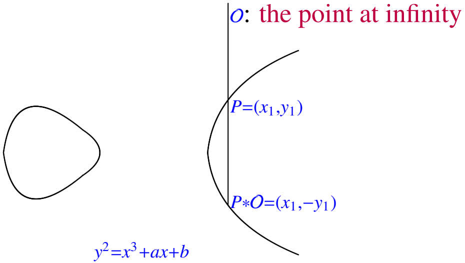
$\mathcal{O}$ is the Identity



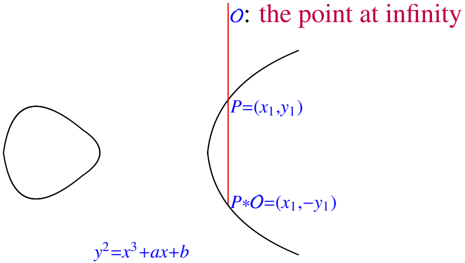
O is the Identity



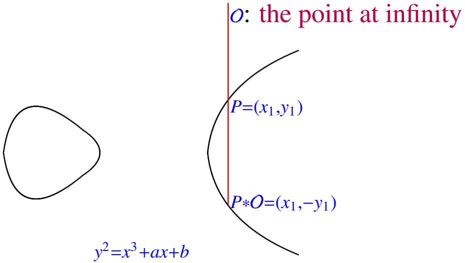
$\mathcal{O}$ is the Identity



$\mathcal{O}$ is the Identity

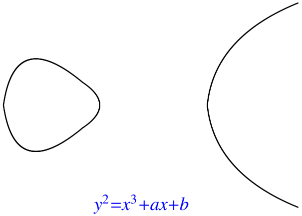


$\mathcal{O}$ is the Identity

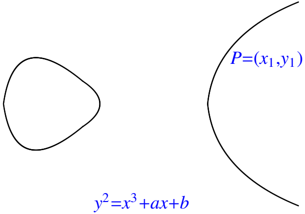


- The point $\mathcal{O}$ serves as the identity for addition on elliptic curve.

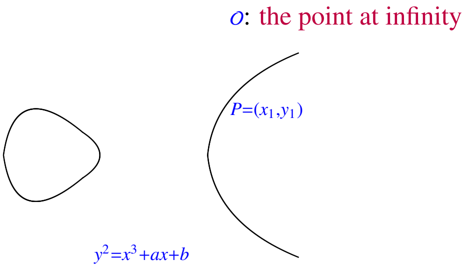
The Inverse of a Point



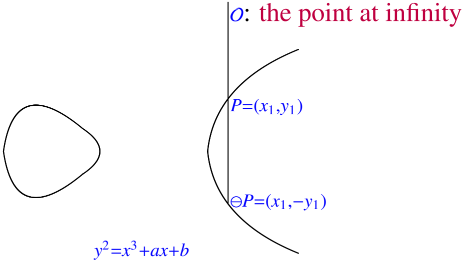
The Inverse of a Point



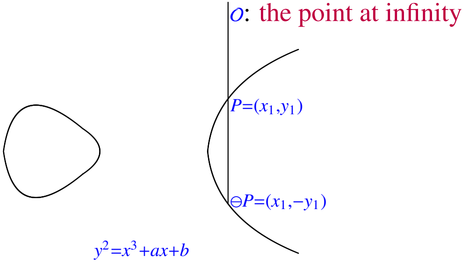
The Inverse of a Point



The Inverse of a Point



The Inverse of a Point



- The additive inverse of the point $P = (x_1, y_1)$ is given by $\ominus P = (x_1, -y_1)$.

The Mordell-Weil Theorem

E is elliptic curve defined over a number field K, then the group $E(K)$ of K-rational point of E, is a finitely generated abelian group.

The Mordell-Weil Theorem

E is elliptic curve defined over a number field K, then the group $E(K)$ of K-rational point of E, is a finitely generated abelian group.

Structure theorem says that

$$E(K) \cong \mathbb{Z}^r \times E(K)_{tors},$$

where r is known as rank of E over K and $E(K)_{tors}$ is torsion part of $E(K)$.

Congruent Number Elliptic Curve

$$E_n : y^2 = x(x^2 - n^2). \tag{2}$$

Congruent Number Elliptic Curve

$$E_n : y^2 = x(x^2 - n^2). \tag{2}$$

Here, E_n is called the *congruent number elliptic curve*.

Congruent Number Elliptic Curve

$$E_n : y^2 = x(x^2 - n^2). \tag{2}$$

Here, E_n is called the *congruent number elliptic curve*.

Now here,

$$E_n(\mathbb{Q})_{tors} = E_n(\mathbb{Q})[2] = \{\mathcal{O}, (0,0), (\pm n, 0)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Congruent number elliptic curve

Consider the two sets

$$S = \left\{(a, b, c) \in \mathbb{Q}^3 : 0 < a < b < c, \quad ab = 2n, \quad a^2 + b^2 = c^2\right\},$$

and

$$T = \left\{(x, y) \in 2E_n(\mathbb{Q}) \setminus \{\mathcal{O}\} : y \geq 0\right\}.$$

Congruent number elliptic curve

Consider the two sets

$$S = \left\{(a, b, c) \in \mathbb{Q}^3 : 0 < a < b < c, \quad ab = 2n, \quad a^2 + b^2 = c^2\right\},$$

and

$$T = \left\{(x, y) \in 2E_n(\mathbb{Q}) \setminus \{\mathcal{O}\} : y \geq 0\right\}.$$

Define

$$\phi : S \to T, \qquad (a, b, c) \mapsto \left(\frac{c^2}{4}, \frac{c(b^2 - a^2)}{8}\right),$$

$$\psi : T \to S \qquad (x, y) \mapsto (\sqrt{x+n} - \sqrt{x-n}, \ \sqrt{x+n} + \sqrt{x-n}, \ 2\sqrt{x}).$$

Congruent number elliptic curve

Consider the two sets

$$S = \left\{(a, b, c) \in \mathbb{Q}^3 : 0 < a < b < c, \quad ab = 2n, \quad a^2 + b^2 = c^2\right\},$$

and

$$T = \left\{(x, y) \in 2E_n(\mathbb{Q}) \setminus \{O\} : y \geq 0\right\}.$$

Define

$$\phi : S \to T, \qquad (a, b, c) \mapsto \left(\frac{c^2}{4}, \frac{c(b^2 - a^2)}{8}\right),$$

$$\psi : T \to S \qquad (x, y) \mapsto (\sqrt{x+n} - \sqrt{x-n},\ \sqrt{x+n} + \sqrt{x-n},\ 2\sqrt{x}).$$

Proposition 1

Let E be an elliptic curve over a field k (of characteristic $\neq 2, 3$) given by

$$E : y^2 = (x - a_1)(x - a_2)(x - a_3) \text{ with } a_1, a_2, a_3 \in k.$$

Let (x_0, y_0) be a k-rational point of $E \setminus \{O\}$. 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 $x_0 - a_1,\ x_0 - a_2$ and $x_0 - a_3$ are squares in k.

Congruent number elliptic curve

Consider the two sets

$$S = \left\{(a,b,c) \in \mathbb{Q}^3 : 0 < a < b < c, \quad ab = 2n, \quad a^2 + b^2 = c^2\right\},$$

and

$$T = \left\{(x,y) \in 2E_n(\mathbb{Q}) \setminus \{\mathcal{O}\} : y \geq 0\right\}.$$

Define

$$\phi : S \to T, \qquad (a,b,c) \mapsto \left(\frac{c^2}{4}, \frac{c(b^2 - a^2)}{8}\right),$$
$$\psi : T \to S \qquad (x,y) \mapsto (\sqrt{x+n} - \sqrt{x-n}, \ \sqrt{x+n} + \sqrt{x-n}, \ 2\sqrt{x}).$$

Proposition 1

Let E be an elliptic curve over a field k (of characteristic $\neq 2, 3$) given by

$$E : y^2 = (x - a_1)(x - a_2)(x - a_3) \text{ with } a_1, a_2, a_3 \in k.$$

Let (x_0, y_0) be a k-rational point of $E \setminus \{\mathcal{O}\}$. 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 $x_0 - a_1$, $x_0 - a_2$ and $x_0 - a_3$ are squares in k.

Using Proposition 1 it is easy to observe that the maps ϕ and ψ are well defined and inverses to each other.

Criterion 1

A positive integer n is a congruent number if and only if $E_n(\mathbb{Q})$ has a point of infinite order.

θ-Congruent Number

A positive integer n is called a congruent number over a number field K (or in short, a K-*congruent number*) if there exist $a, b, c \in K$ such that (1) holds.

θ-Congruent Number

A positive integer n is called a congruent number over a number field K (or in short, a K-*congruent number*) if there exist $a, \ b, \ c \in K$ such that (1) holds.

Definition 2

Let $0 < \theta < \pi$ be an angle with rational cosine $cos(\theta) = \frac{s}{r}$ with $0 < |s| < r$ and $gcd(r, s) = 1$. Let $(u, v, w)_\theta$ denote a triangle with an angle θ between the sides u and v. A positive integer n is called a θ-congruent number if there exists a triangle $(u, v, w)_\theta$ with sides in $\mathbb{Q}$ having area $n\alpha_\theta$, where $\alpha_\theta = \sqrt{r^2 - s^2}$. In other words, n is a θ-congruent number if it satisfies

$$2rn = uv, \quad w^2 = u^2 + v^2 - 2uv \cdot \frac{s}{r}. \tag{3}$$

θ-Congruent Number

A positive integer n is called a congruent number over a number field K (or in short, a *K-congruent number*) if there exist $a, b, c \in K$ such that (1) holds.

Definition 2

Let $0 < \theta < \pi$ be an angle with rational cosine $cos(\theta) = \frac{s}{r}$ with $0 < |s| < r$ and $gcd(r, s) = 1$. Let $(u, v, w)_\theta$ denote a triangle with an angle θ between the sides u and v. A positive integer n is called a θ-congruent number if there exists a triangle $(u, v, w)_\theta$ with sides in $\mathbb{Q}$ having area $n\alpha_\theta$, where $\alpha_\theta = \sqrt{r^2 - s^2}$. In other words, n is a θ-congruent number if it satisfies

$$2rn = uv, \quad w^2 = u^2 + v^2 - 2uv \cdot \frac{s}{r}. \tag{3}$$

θ-congruent number elliptic curve given by

$$E_{n,\theta} : y^2 = x(x + (r + s)n)(x - (r - s)n), \tag{4}$$

θ-Congruent Number

A positive integer n is called a congruent number over a number field K (or in short, a K-*congruent number*) if there exist $a,\ b,\ c \in K$ such that (1) holds.

Definition 2

Let $0 < \theta < \pi$ be an angle with rational cosine $cos(\theta) = \frac{s}{r}$ with $0 < |s| < r$ and $gcd(r, s) = 1$. Let $(u, v, w)_\theta$ denote a triangle with an angle θ between the sides u and v. A positive integer n is called a θ-congruent number if there exists a triangle $(u, v, w)_\theta$ with sides in $\mathbb{Q}$ having area $n\alpha_\theta$, where $\alpha_\theta = \sqrt{r^2 - s^2}$. In other words, n is a θ-congruent number if it satisfies

$$2rn = uv, \quad w^2 = u^2 + v^2 - 2uv \cdot \frac{s}{r}. \tag{3}$$

θ-congruent number elliptic curve given by

$$E_{n,\theta} : y^2 = x(x + (r + s)n)(x - (r - s)n), \tag{4}$$

Criterion 3

Let $\theta \in (0, \pi)$ be an angle such that $\cos\theta$ is rational.

1. *A positive integer n is θ-congruent if and only if $E_{n,\theta}$ has a point of order greater than 2;*
2. *If $n \neq 1, 2, 3, 6$, then n is θ-congruent if and only if $E_{n,\theta}$ has positive rank.*

- Tunnel ([28]), Monsky ([18]) and Tian ([27]) are some of the eminent mathematicians who have made significant contribution toward identifying congruent numbers.

- Tunnel ([28]), Monsky ([18]) and Tian ([27]) are some of the eminent mathematicians who have made significant contribution toward identifying congruent numbers.
- For the known results on the construction of non-congruent numbers with arbitrarily many prime factors of the form $8k + 3$, one can refer to [10] and [22] for instance.

- Tunnel ([28]), Monsky ([18]) and Tian ([27]) are some of the eminent mathematicians who have made significant contribution toward identifying congruent numbers.
- For the known results on the construction of non-congruent numbers with arbitrarily many prime factors of the form $8k+3$, one can refer to [10] and [22] for instance.
- Study of congruent number problem over algebraic extensions dates back at least to Tada ([26]) who considered real quadratic fields.

- Tunnel ([28]), Monsky ([18]) and Tian ([27]) are some of the eminent mathematicians who have made significant contribution toward identifying congruent numbers.
- For the known results on the construction of non-congruent numbers with arbitrarily many prime factors of the form $8k + 3$, one can refer to [10] and [22] for instance.
- Study of congruent number problem over algebraic extensions dates back at least to Tada ([26]) who considered real quadratic fields.Some results were given by Jędrzejak in [13] for congruent number over certain other real number fields.

Complete 2-descent

Complete 2-descent

Let E/K is an elliptic curve given by a Weierstrass equation

$$y^2 = (x - e_1)(x - e_2)(x - e_3) \qquad \text{with } e_1, e_2, e_3 \in K,$$

where K is a number field.

Complete 2-descent

Let E/K is an elliptic curve given by a Weierstrass equation

$$y^2 = (x - e_1)(x - e_2)(x - e_3) \qquad \text{with } e_1, e_2, e_3 \in K,$$

where K is a number field.

Let S be a finite set of places of K includes all archimedean places, all places dividing 2, and all places at which E has bad reduction.

Complete 2-descent

Let E/K is an elliptic curve given by a Weierstrass equation

$$y^2 = (x - e_1)(x - e_2)(x - e_3) \qquad \text{with } e_1, e_2, e_3 \in K,$$

where K is a number field.

Let S be a finite set of places of K includes all archimedean places, all places dividing 2, and all places at which E has bad reduction.

Further let,

$$K(S,2) := \{c \in K^*/(K^*)^2 \mid ord_v(c) \equiv 0 \pmod 2 \quad \forall\, v \in M_K \setminus S\},$$

where $ord_v(c)$ is the v-adic valuation of c.

Complete 2-descent

Proposition 2 (Complete 2-Descent)

There exists an injective homomorphism

$$b : E(K)/2E(K) \hookrightarrow K(S,2) \times K(S,2) \tag{5}$$

defined by

Proposition 2 (Complete 2-Descent)

There exists an injective homomorphism

$$b : E(K)/2E(K) \hookrightarrow K(S,2) \times K(S,2) \tag{5}$$

defined by

$$P = (x,y) \longmapsto \begin{cases} (1,1), & \text{if } P = O \\ \left(\frac{e_1 - e_3}{e_1 - e_2}, e_1 - e_2\right), & \text{if } P = (e_1, 0) \\ \left(e_2 - e_1, \frac{e_2 - e_3}{e_2 - e_1}\right), & \text{if } P = (e_2, 0) \\ (x - e_1, x - e_2), & \text{if } P \neq O, (e_1, 0), (e_2, 0). \end{cases}$$

Proposition 2 (Complete 2-Descent)

There exists an injective homomorphism

$$b : E(K)/2E(K) \hookrightarrow K(S,2) \times K(S,2) \tag{5}$$

defined by

$$P = (x,y) \longmapsto \begin{cases} (1,1), & \text{if } P = \mathcal{O} \\ \left(\frac{e_1-e_3}{e_1-e_2}, e_1 - e_2\right), & \text{if } P = (e_1,0) \\ \left(e_2 - e_1, \frac{e_2-e_3}{e_2-e_1}\right), & \text{if } P = (e_2,0) \\ (x-e_1, x-e_2), & \text{if } P \neq \mathcal{O}, (e_1,0), (e_2,0). \end{cases}$$

Let $(b_1,b_2) \in K(S,2) \times K(S,2)$ *be a pair that is not the image of one of three points* $\mathcal{O}, (e_1,0), (e_2,0)$. *Then* (b_1,b_2) *is the image of a point*

$$P = (x,y) \in E(K)/2E(K)$$

if and only if the equations

$$b_1 z_1^2 - b_2 z_2^2 = e_2 - e_1, \tag{6}$$

$$b_1 z_1^2 - b_1 b_2 z_3^2 = e_3 - e_1. \tag{7}$$

have a solution $(z_1,z_2,z_3) \in K^* \times K^* \times K$.

Proposition 2 (Complete 2-Descent)

There exists an injective homomorphism

$$b : E(K)/2E(K) \hookrightarrow K(S,2) \times K(S,2) \tag{5}$$

defined by

$$P = (x,y) \longmapsto \begin{cases} (1,1), & \text{if } P = \mathcal{O} \\ \left(\frac{e_1-e_3}{e_1-e_2}, e_1 - e_2\right), & \text{if } P = (e_1, 0) \\ \left(e_2 - e_1, \frac{e_2-e_3}{e_2-e_1}\right), & \text{if } P = (e_2, 0) \\ (x - e_1, x - e_2), & \text{if } P \neq \mathcal{O}, (e_1, 0), (e_2, 0). \end{cases}$$

Let $(b_1, b_2) \in K(S,2) \times K(S,2)$ *be a pair that is not the image of one of three points* $\mathcal{O}, (e_1, 0), (e_2, 0)$. *Then* (b_1, b_2) *is the image of a point*

$$P = (x,y) \in E(K)/2E(K)$$

if and only if the equations

$$b_1 z_1^2 - b_2 z_2^2 = e_2 - e_1, \tag{6}$$

$$b_1 z_1^2 - b_1 b_2 z_3^2 = e_3 - e_1. \tag{7}$$

have a solution $(z_1, z_2, z_3) \in K^* \times K^* \times K$.*If such a solution exists,*

$$P = (x,y) = (b_1 z_1^2 + e_1, b_1 b_2 z_1 z_2 z_3).$$

Families of non-congruent numbers

Theorem 4

Let t be a positive integer. Suppose $p_1, p_2, \ldots, p_t$ and $q_1, q_2, \ldots, q_t$ are distinct primes such that all pairs (p_j, q_j) are equivalent either to $(1,3)$ or to $(5,7)$ modulo 8. Suppose

$$\begin{aligned} &\left(\frac{q_j}{q_i}\right) = -1 \quad \text{if } i > j, \qquad \left(\frac{p_i}{p_j}\right) = 1 \quad \forall\, i \neq j, \quad \text{and} \\ &\left(\frac{p_i}{q_j}\right) = \begin{cases} 1 & \text{if } i \neq j \\ -1 & \text{if } i = j, \end{cases} \end{aligned} \tag{8}$$

where $\left(\frac{\cdot}{\cdot}\right)$ denotes the Legendre symbol. Then

$$n = (p_1q_1)(p_2q_2)\cdots(p_tq_t)$$

is a non-congruent number.

Our results concerning continued fraction

Theorem 4

Let t be a positive integer. Suppose $p_1, p_2, \ldots, p_t$ and $q_1, q_2, \ldots, q_t$ are distinct primes such that all pairs (p_j, q_j) are equivalent either to $(1,3)$ or to $(5,7)$ modulo 8. Suppose

$$\begin{aligned} &\left(\frac{q_j}{q_i}\right) = -1 \quad \text{if } i > j, \qquad \left(\frac{p_i}{p_j}\right) = 1 \quad \forall\ i \neq j, \quad \text{and} \\ &\left(\frac{p_i}{q_j}\right) = \begin{cases} 1 & \text{if } i \neq j \\ -1 & \text{if } i = j, \end{cases} \end{aligned} \tag{8}$$

where $\left(\frac{\cdot}{\cdot}\right)$ denotes the Legendre symbol. Then

$$n = (p_1 q_1)(p_2 q_2) \cdots (p_t q_t)$$

is a non-congruent number.

Example. Consider $n = (17.3)(409.19)(3697.859)$ where each pair of prime factors is equivalent to $(1,3)$ modulo 8, and satisfy the hypotheses (8). Using MAGMA ([1]), we verify that the rank of the elliptic curve $y^2 = x^3 - n^2 x$ is 0, hence n is non-congruent.

Remark 5

For n, defined in Theorem 4, a system of representatives of classes in $\mathbb{Q}(S,2)$ is given by

$$R = \{\pm 2^{\epsilon} p_1^{\epsilon_1} \ldots p_t^{\epsilon_t} q_1^{\mu_1} \cdots q_t^{\mu_t} \mid \epsilon, \epsilon_1, \ldots, \epsilon_t, \mu_1, \ldots, \mu_t \in \{0,1\}\}.$$

Our results concerning continued fraction

Remark 5

For n, defined in Theorem 4, a system of representatives of classes in $\mathbb{Q}(S, 2)$ is given by

$$R = \{\pm 2^{\epsilon} p_1^{\epsilon_1} \ldots p_t^{\epsilon_t} q_1^{\mu_1} \cdots q_t^{\mu_t} \mid \epsilon, \epsilon_1, \ldots, \epsilon_t, \mu_1, \ldots, \mu_t \in \{0, 1\}\}.$$

Let r be the rank of the Mordell-weil group $E_n(\mathbb{Q})$ of rational points on the elliptic curve E_n. Then $E_n(\mathbb{Q})$ is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}^r$, and consequently,

$$E_n(\mathbb{Q})/2E_n(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^{r+2}.$$

Remark 5

For n*, defined in Theorem 4, a system of representatives of classes in* $\mathbb{Q}(S,2)$ *is given by*

$$R = \{\pm 2^{\epsilon} p_1^{\epsilon_1} \dots p_t^{\epsilon_t} q_1^{\mu_1} \cdots q_t^{\mu_t} \mid \epsilon, \epsilon_1, \dots, \epsilon_t, \mu_1, \dots, \mu_t \in \{0,1\}\}.$$

Let r *be the rank of the Mordell-weil group* $E_n(\mathbb{Q})$ *of rational points on the elliptic curve* E_n*. Then* $E_n(\mathbb{Q})$ *is isomorphic to* $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}^r$*, and consequently,*

$$E_n(\mathbb{Q})/2E_n(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^{r+2}.$$

For n *to be a non-congruent number, we require that* $r = 0$*. In other words, we need to show that the system of equations given by*

$$b_1 z_1^2 - b_2 z_2^2 = n, \tag{9}$$

$$b_1 z_1^2 - b_1 b_2 z_3^2 = -n. \tag{10}$$

does not have a solution for any pair

$$(b_1, b_2) \in R \times R \setminus \{(1,1),\ (-1,-n),\ (n,2),\ (-n,-2n)\}, \tag{11}$$

where $(z_1, z_2, z_3) \in \mathbb{Q}^* \times \mathbb{Q}^* \times \mathbb{Q}^*$.

Proposition 3 (Unsolvability Condition)

Let

$$n = 2^{\epsilon} r_1 r_2 \cdots r_k$$

be a square-free positive integer where $\epsilon \in \{0, 1\}$, k *is a natural number and* $r_1, \ r_2, \ \ldots, \ r_k$ *are odd primes. Let* $(b_1, b_2) \in R \times R$, *where*

$$R = \{(-1)^{\alpha} 2^{\beta} r_1^{\epsilon_1} \cdots r_k^{\epsilon_k} \mid \quad \alpha, \ \beta, \ \epsilon_1, \ \ldots, \ \epsilon_k = 0 \text{ or } 1\}.$$

The system of equations given by (9) and (10) has no solution $(z_1, z_2, z_3) \in \mathbb{Q}^* \times \mathbb{Q}^* \times \mathbb{Q}^*$ *in the following cases:*

(a) $b_1 b_2 < 0$ *or*

(b) $2 \nmid n$ *and* $2 \mid b_1$.

Proposition 3 (Unsolvability Condition)

Let

$$n = 2^{\epsilon} r_1 r_2 \cdots r_k$$

be a square-free positive integer where $\epsilon \in \{0, 1\}$, k *is a natural number and* $r_1,\ r_2,\ \ldots,\ r_k$ *are odd primes. Let* $(b_1, b_2) \in R \times R$, *where*

$$R = \{(-1)^{\alpha} 2^{\beta} r_1^{\epsilon_1} \cdots r_k^{\epsilon_k} \mid \quad \alpha,\ \beta,\ \epsilon_1,\ \ldots,\ \epsilon_k = 0 \text{ or } 1\}.$$

The system of equations given by (9) and (10) has no solution $(z_1, z_2, z_3) \in \mathbb{Q}^* \times \mathbb{Q}^* \times \mathbb{Q}^*$ *in the following cases:*

(a) $b_1 b_2 < 0$ *or*

(b) $2 \nmid n$ *and* $2 \mid b_1$.

Lemma 6

Let $(b_1, b_2) \in D$ *represent an element in the image of the map* b *given by (5). Then, there is a pair* (b_1^*, b_2^*) *in* D *representing an element in* $Im(b)$ *such that* b_2^* *is positive and odd.*

Lemma 7

Let (b_1, b_2) *be an element of* $R \times R$ *such that* b_2 *is odd and positive. If* $(b_1, b_2) \in Im(b)$, *then* q_j *does not divide* $b_1 b_2$ *for* $j = 1,\ 2,\ \cdots, t$.

Lemma 7

Let (b_1, b_2) *be an element of* $R \times R$ *such that* b_2 *is odd and positive. If* $(b_1, b_2) \in Im(b)$, *then* q_j *does not divide* $b_1 b_2$ *for* $j = 1,\ 2,\ \cdots, t$.

Lemma 8

Let (b_1, b_2) *be an element of* $R \times R$ *such that* b_2 *is odd and positive. If* $(b_1, b_2) \in Im(b)$, *then* p_j *does not divide* $b_1 b_2$ *for* $j = 1,\ 2,\ \cdots,\ t$.

Lemma 7

Let (b_1, b_2) be an element of $R \times R$ such that b_2 is odd and positive. If $(b_1, b_2) \in Im(b)$, then q_j does not divide $b_1 b_2$ for $j = 1,\ 2,\ \cdots, t$.

Lemma 8

Let (b_1, b_2) be an element of $R \times R$ such that b_2 is odd and positive. If $(b_1, b_2) \in Im(b)$, then p_j does not divide $b_1 b_2$ for $j = 1,\ 2,\ \cdots,\ t$.

Theorem 9

Let H_t denote the collection of positive integers with prime factorization $(p_1 q_1)(p_2 q_2) \cdots (p_t q_t)$, where all the pairs (p_j, q_j) are equivalent to $(1, 3)$ modulo 8 and satisfy the conditions (8). For any natural number t, the set H_t is contains infinitely many elements. The analogous statement for pairs $(p_j, q_j) \equiv (5, 7) \pmod 8$ holds as well.

Criterion of θ-congruent number over number field

Theorem 10

Consider the number field $K_{2,d} = \mathbb{Q}(\sqrt{m_1}, \ldots, \sqrt{m_d})$ *of type* $(2, \ldots, 2)$. *Assume that*

1. n *and* $\mathrm{Sqf}(nm_i)$ *do not divide* 6 *for all* $i \in \{1, 2, \ldots, d\}$;
2. $2r(r - s)$ *is not a square in* $K_{2,d}$.

Then n *is* θ*-congruent number over* $K_{2,d}$ *if and only if* $E_{n,\theta}(K_{2,d})$ *has a point of infinite order.*

Theorem 10

Consider the number field $K_{2,d} = \mathbb{Q}(\sqrt{m_1}, \ldots, \sqrt{m_d})$ *of type* $(2, \ldots, 2)$*. Assume that*

1. n *and* $\mathrm{Sqf}(nm_i)$ *do not divide* 6 *for all* $i \in \{1, 2, \ldots, d\}$*;*
2. $2r(r - s)$ *is not a square in* $K_{2,d}$*.*

Then n *is* θ*-congruent number over* $K_{2,d}$ *if and only if* $E_{n,\theta}(K_{2,d})$ *has a point of infinite order.*

Proposition 4

The θ*-congruent number elliptic curve* $E_{n,\theta}$ *does not have complex multiplication for* $\theta \neq \frac{\pi}{2}$*.*

Theorem 10

Consider the number field $K_{2,d} = \mathbb{Q}(\sqrt{m_1}, \ldots, \sqrt{m_d})$ of type $(2, \ldots, 2)$. Assume that

1. *n and $\mathrm{Sqf}(nm_i)$ do not divide 6 for all $i \in \{1, 2, \ldots, d\}$;*
2. *$2r(r-s)$ is not a square in $K_{2,d}$.*

Then n is θ-congruent number over $K_{2,d}$ if and only if $E_{n,\theta}(K_{2,d})$ has a point of infinite order.

Proposition 4

The θ-congruent number elliptic curve $E_{n,\theta}$ does not have complex multiplication for $\theta \neq \frac{\pi}{2}$.

Theorem 11

Suppose n is a square free natural number other than $1,\ 2,\ 3$ or 6. Let K be a real number field such that $[K:\mathbb{Q}]$ is coprime to 6 and not divisible by 55. Then n is a θ-congruent number over K if and only if $E_{n,\theta}(K)$ has a point of infinite order.

Proposition 5

Let B be a positive integer. Let $E/\mathbb{Q}$ be an elliptic curves and $K/\mathbb{Q}$ a number field of degree d, where the smallest prime divisor of d is $\geq B$. Let $E(K)[p^\infty]$ denote the p-primary torsion subgroup of $E(K)_{tors}$, that is, the p-Sylow subgroup of $E(K)$. Then

(i) *If $B \geq 11$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes. In particular, $E(K)_{tors} = E(\mathbb{Q})_{tors}$.*

Proposition 5

Let B be a positive integer. Let $E/\mathbb{Q}$ be an elliptic curves and $K/\mathbb{Q}$ a number field of degree d, where the smallest prime divisor of d is $\geq B$. Let $E(K)[p^\infty]$ denote the p-primary torsion subgroup of $E(K)_{tors}$, that is, the p-Sylow subgroup of $E(K)$. Then

(i) *If $B \geq 11$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes. In particular, $E(K)_{tors} = E(\mathbb{Q})_{tors}$.*

(ii) *If $B \geq 7$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes $p \neq 7$.*

Proposition 5

Let B be a positive integer. Let $E/\mathbb{Q}$ be an elliptic curves and $K/\mathbb{Q}$ a number field of degree d, where the smallest prime divisor of d is $\geq B$. Let $E(K)[p^\infty]$ denote the p-primary torsion subgroup of $E(K)_{tors}$, that is, the p-Sylow subgroup of $E(K)$. Then

(i) *If $B \geq 11$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes. In particular, $E(K)_{tors} = E(\mathbb{Q})_{tors}$.*

(ii) *If $B \geq 7$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes $p \neq 7$.*

(iii) *If $B \geq 5$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes $p \neq 5,\ 7,\ 11$.*

Proposition 5

Let B be a positive integer. Let $E/\mathbb{Q}$ be an elliptic curves and $K/\mathbb{Q}$ a number field of degree d, where the smallest prime divisor of d is $\geq B$. Let $E(K)[p^\infty]$ denote the p-primary torsion subgroup of $E(K)_{tors}$, that is, the p-Sylow subgroup of $E(K)$. Then

(i) *If $B \geq 11$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes. In particular, $E(K)_{tors} = E(\mathbb{Q})_{tors}$.*

(ii) *If $B \geq 7$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes $p \neq 7$.*

(iii) *If $B \geq 5$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes $p \neq 5,\ 7,\ 11$.*

(iv) *If $B > 2$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes $p \neq 2, 3, 5, 7, 11, 13, 19, 43, 67, 163$.*

Proposition 5

Let B be a positive integer. Let $E/\mathbb{Q}$ be an elliptic curves and $K/\mathbb{Q}$ a number field of degree d, where the smallest prime divisor of d is $\geq B$. Let $E(K)[p^\infty]$ denote the p-primary torsion subgroup of $E(K)_{tors}$, that is, the p-Sylow subgroup of $E(K)$. Then

(i) *If $B \geq 11$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes. In particular, $E(K)_{tors} = E(\mathbb{Q})_{tors}$.*

(ii) *If $B \geq 7$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes $p \neq 7$.*

(iii) *If $B \geq 5$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes $p \neq 5, 7, 11$.*

(iv) *If $B > 2$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes $p \neq 2, 3, 5, 7, 11, 13, 19, 43, 67, 163$.*

Theorem 12

Suppose n is a square free natural number other than $1, 2, 3$ or 6. Let K be a real cubic number field. Suppose s is divisible by 5 or $(r, s) \equiv (\pm 2, \pm 1)$ or $\equiv (\pm 1, \pm 2)$ mod 5. Then n is a θ-congruent number over K if and only if $E_{n,\theta}(K)$ has a point of infinite order.

Example

To illustrate the theorem above, let us take $\cos\theta = \frac{5}{6}$ where $r = 6$ and $s = 5 \equiv 0 \pmod 5$. The corresponding θ-congruent number curve with $n = 7$ is

$$E_{7,\theta} : y^2 = x^3 + 70x^2 - 539x.$$

Example

To illustrate the theorem above, let us take $\cos\theta = \frac{5}{6}$ where $r = 6$ and $s = 5 \equiv 0 \pmod 5$. The corresponding θ-congruent number curve with $n = 7$ is

$$E_{7,\theta} : y^2 = x^3 + 70x^2 - 539x.$$

We can verify by using MAGMA that the rank of $E_{7,\theta}(\mathbb{Q})$ is 0, therefore 7 is not a θ-congruent number over $\mathbb{Q}$.

Example

To illustrate the theorem above, let us take $\cos\theta = \frac{5}{6}$ where $r = 6$ and $s = 5 \equiv 0 \pmod 5$. The corresponding θ-congruent number curve with $n = 7$ is

$$E_{7,\theta} : y^2 = x^3 + 70x^2 - 539x.$$

We can verify by using MAGMA that the rank of $E_{7,\theta}(\mathbb{Q})$ is 0, therefore 7 is not a θ-congruent number over $\mathbb{Q}$.
Consider the polynomial $x^3 + 70x^2 - 539x - 1$. We denote the largest real root by α, then $K = \mathbb{Q}(\alpha)$ is a real cubic field. The point $(\alpha, 1) \in E_{7,\theta}(K)$ is clearly not a 2-torsion point, and hence 7 is θ-congruent over K.

Publication

- Das, S., Saikia, A.: *Families of non-congruent numbers with arbitrarily many pairs of prime factors*, to appear in *Integers*.

- Das, S., Saikia, A.: *On θ-congruent numbers over real number fields*, to appear in *Bulletin of the Autralian Mathematical Society*.

References I

W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput., 24 (1997), pp. 235–265.

J. E. Cremona and P. Serf, *Computing the rank of elliptic curves over real quadratic number fields of class number* 1, Math. Comp., 68 (1999), pp. 1187–1200.

H. B. Daniels and E. González-Jiménez, *On the torsion of rational elliptic curves over sextic fields*, arXiv e-prints, (2018), p. arXiv:1808.02887.

M. Fujiwara, *θ-congruent numbers*, in Number theory (Eger, 1996), de Gruyter, Berlin, 1998, pp. 235–241.

V. Girard, M. N. Lalín, and S. C. Nair, *Families of non-θ-congruent numbers with arbitrarily many prime factors*, Colloq. Math., 152 (2018), pp. 255–271.

E. Girondo, G. González-Diez, E. González-Jiménez, R. Steuding, and J. Steuding, *Right triangles with algebraic sides and elliptic curves over number fields*, Math. Slovaca, 59 (2009), pp. 299–306.

References II

E. González-Jiménez, *Complete classification of the torsion structures of rational elliptic curves over quintic number fields*, J. Algebra, 478 (2017), pp. 484–505.

E. González-Jiménez and F. Najman, *Growth of torsion groups of elliptic curves upon base change*, arXiv e-prints, (2016), p. arXiv:1609.02515.

E. González-Jiménez, F. Najman, and J. M. Tornero, *Torsion of rational elliptic curves over cubic fields*, Rocky Mountain J. Math., 46 (2016), pp. 1899–1917.

B. Iskra, *Non-congruent numbers with arbitrarily many prime factors congruent to 3 modulo 8*, Proc. Japan Acad. Ser. A Math. Sci., 72 (1996), pp. 168–169.

A. S. Janfada and S. Salami, *On θ-congruent numbers on real quadratic number fields*, Kodai Math. J., 38 (2015), pp. 352–364.

A. S. Janfada, S. Salami, A. Dujella, and J. C. Peral, *On high rank $\pi/3$ and $2\pi/3$-congruent number elliptic curves*, Rocky Mountain J. Math., 44 (2014), pp. 1867–1880.

- T. Jędrzejak, *Congruent numbers over real number fields*, Colloq. Math., 128 (2012), pp. 179–186.
- M. Kan, *θ-congruent numbers and elliptic curves*, Acta Arith., 94 (2000), pp. 153–160.
- A. W. Knapp, *Elliptic curves*, vol. 40 of Mathematical Notes, Princeton University Press, Princeton, NJ, 1992.
- N. Koblitz, *Introduction to elliptic curves and modular forms*, vol. 97 of Graduate Texts in Mathematics, Springer-Verlag, New York, 1984.
- J. Lagrange, *Nombres congruents et courbes elliptiques*, in Séminaire Delange-Pisot-Poitou (16e année: 1974/75), Théorie des nombres, Fasc. 1, Exp. No. 16, 1975, p. 17.
- P. Monsky, *Mock Heegner points and congruent numbers*, Math. Z., 204 (1990), pp. 45–67.

References IV

F. Najman, *Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$*, Math. Res. Lett., 23 (2016), pp. 245–272.

D. Prasad and C. S. Yogananda, *Bounding the torsion in CM elliptic curves*, C. R. Math. Acad. Sci. Soc. R. Can., 23 (2001), pp. 1–5.

D. Qiu and X. Zhang, *Elliptic curves and their torsion subgroups over number fields of type $(2, 2, \ldots, 2)$*, Sci. China Ser. A, 44 (2001), pp. 159–167.

L. Reinholz, B. K. Spearman, and Q. Yang, *Families of even non-congruent numbers with prime factors in each odd congruence class modulo eight*, Int. J. Number Theory, 14 (2018), pp. 669–692.

P. Serf, *Congruent numbers and elliptic curves*, in Computational number theory (Debrecen, 1989), de Gruyter, Berlin, 1991, pp. 227–238.

A. Silverberg, *Points of finite order on abelian varieties*, in p-adic methods in number theory and algebraic geometry, vol. 133 of Contemp. Math., Amer. Math. Soc., Providence, RI, 1992, pp. 175–193.

References V

J. H. SILVERMAN, *The arithmetic of elliptic curves*, vol. 106 of Graduate Texts in Mathematics, Springer, Dordrecht, second ed., 2009.

M. TADA, *Congruent numbers over real quadratic fields*, Hiroshima Math. J., 31 (2001), pp. 331–343.

Y. TIAN, *Congruent numbers and Heegner points*, Camb. J. Math., 2 (2014), pp. 117–161.

J. B. TUNNELL, *A classical Diophantine problem and modular forms of weight* $3/2$, Invent. Math., 72 (1983), pp. 323–334.

THANK YOU