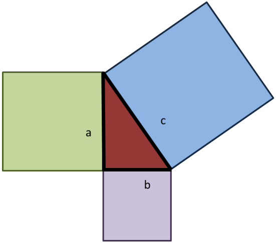
Congruent Numbers and Elliptic Curves

Jennifer Li

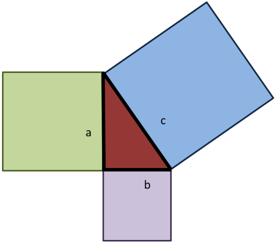
Department of Mathematics
Louisiana State University
Baton Rouge

Pythagorean Theorem



$$a^2 + b^2 = c^2$$

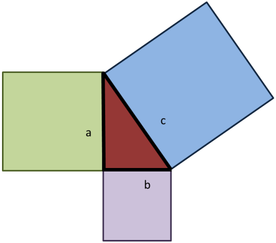
Pythagorean Theorem



$$a^2 + b^2 = c^2$$

Then (a, b, c) is a Pythagorean Triple.

Pythagorean Theorem



$$a^2 + b^2 = c^2$$

Then (a, b, c) is a Pythagorean Triple.

Introduction to Irrational Numbers.

Rational and Irrational Numbers

A positive number n is rational if $n = \dfrac{a}{b}$, where $a, b \in \mathbb{Z}^+$

Rational and Irrational Numbers

A positive number n is rational if $n = \dfrac{a}{b}$, where $a, b \in \mathbb{Z}^+$

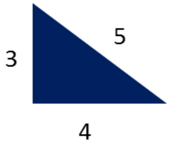
Not rational: irrational.

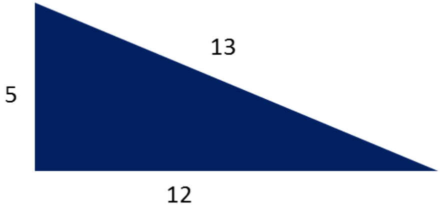
Rational Right Triangles

Some right triangles have all rational sides: Rational Triangles

Rational Right Triangles

Some right triangles have all rational sides: Rational Triangles





Area of a triangle

$$A = \frac{1}{2}bh$$

Congruent Numbers

Area of a triangle

$$A = \frac{1}{2}bh$$

Question: Given a number n, is there a rational triangle with area n?

Area of a triangle

$$A = \frac{1}{2}bh$$

Question: Given a number n, is there a rational triangle with area n?

If so, then we say n is a congruent number (or simply congruent).

The Congruent Number Problem

The Congruent Number Problem Given a number n, is it congruent?

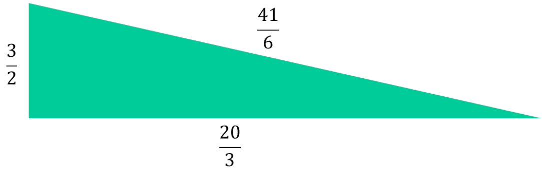
The Congruent Number Problem Given a number n, is it congruent?

Example: $n = 5$ is congruent.

The Congruent Number Problem

The Congruent Number Problem Given a number n, is it congruent?

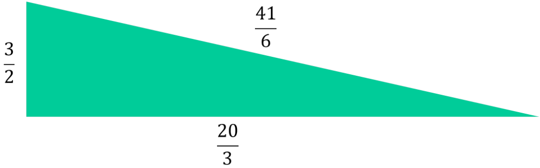
Example: $n = 5$ is congruent.



$$\frac{1}{2}bh = \frac{1}{2} \cdot \frac{20}{3} \cdot \frac{3}{2} = 5$$

The Congruent Number Problem Given a number n, is it congruent?

Example: $n = 5$ is congruent.

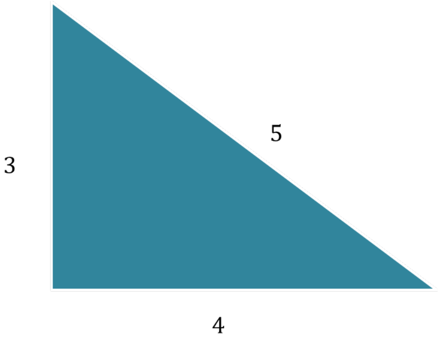


$$\frac{1}{2}bh = \frac{1}{2} \cdot \frac{20}{3} \cdot \frac{3}{2} = 5$$

Can you think of another example?

The Congruent Number Problem

$n = 6$ is a congruent number!



Proposition

An integer n is square-free if no divisor is a perfect square.

Proposition

An integer n is square-free if no divisor is a perfect square.

Proposition. If n is a square-free positive integer, then the following are equivalent:

Proposition

An integer n is square-free if no divisor is a perfect square.

Proposition. If n is a square-free positive integer, then the following are equivalent:

(1) n is congruent.

Proposition

An integer n is square-free if no divisor is a perfect square.

Proposition. If n is a square-free positive integer, then the following are equivalent:

(1) n is congruent. i.e., $n = \frac{1}{2}ab$, where (a, b, c) is a Pythagorean triple.

Proposition

An integer n is square-free if no divisor is a perfect square.

Proposition. If n is a square-free positive integer, then the following are equivalent:

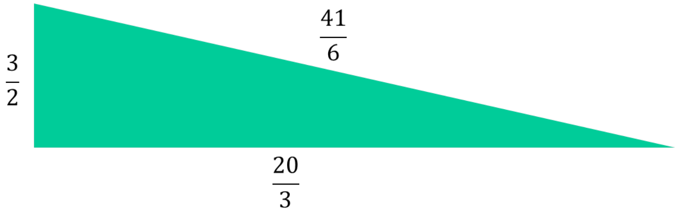
(1) n is congruent. i.e., $n = \frac{1}{2}ab$, where (a, b, c) is a Pythagorean triple.

(2) There exist three rational squares in arithmetic progression with common difference n.

Arithmetic Progression Example

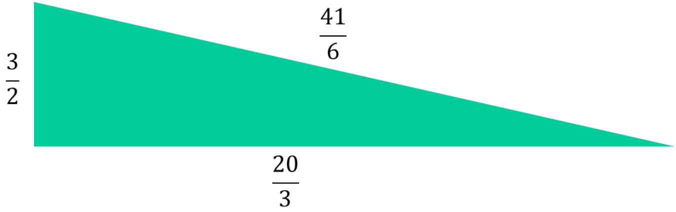
Example: $n = 5$

Example: $n = 5$



Arithmetic Progression Example

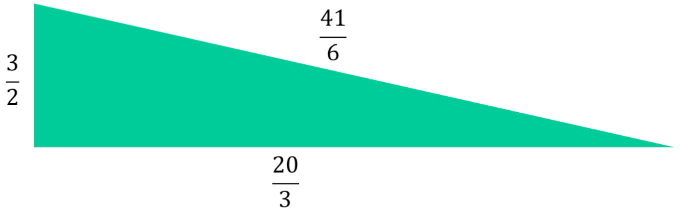
Example: $n = 5$



$$\left(\frac{961}{144}\right) \qquad \left(\frac{1681}{144}\right) \qquad \left(\frac{2401}{144}\right)$$

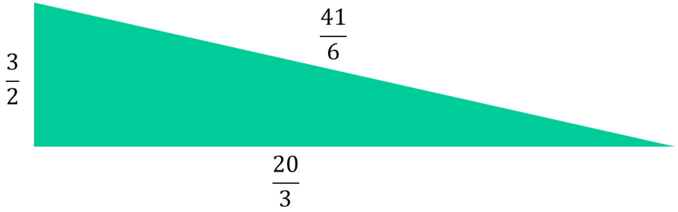
Arithmetic Progression Example

Example: $n = 5$



$$\left(\frac{961}{144}\right) = \left(\frac{31}{12}\right)^2 \qquad \left(\frac{1681}{144}\right) = \left(\frac{41}{12}\right)^2 \qquad \left(\frac{2401}{144}\right) = \left(\frac{49}{12}\right)^2$$

Example: $n = 5$



$$\left(\frac{961}{144}\right) = \left(\frac{31}{12}\right)^2 \qquad \left(\frac{1681}{144}\right) = \left(\frac{41}{12}\right)^2 \qquad \left(\frac{2401}{144}\right) = \left(\frac{49}{12}\right)^2$$

$$5 \qquad\qquad 5$$

Proof (Proposition)

n: square-free integer.

Proof (Proposition)

n: square-free integer.

(1) $\Rightarrow$ (2).

Proof (Proposition)

n: square-free integer.

$(1) \Rightarrow (2)$.

Suppose n is congruent.

Proof (Proposition)

n: square-free integer.

$(1) \Rightarrow (2)$.

Suppose n is congruent.

Then $n = \frac{1}{2}ab$, where (a, b, c) Pythagorean triple.

Proof (Proposition)

n: square-free integer.

$(1) \Rightarrow (2)$.

Suppose n is congruent.

Then $n = \frac{1}{2}ab$, where (a, b, c) Pythagorean triple.

WTS:

Proof (Proposition)

n: square-free integer.

$(1) \Rightarrow (2)$.

Suppose n is congruent.

Then $n = \frac{1}{2}ab$, where (a, b, c) Pythagorean triple.

WTS:

- three rational squares

Proof (Proposition)

n: square-free integer.

$(1) \Rightarrow (2)$.

Suppose n is congruent.

Then $n = \frac{1}{2}ab$, where (a, b, c) Pythagorean triple.

WTS:

- three rational squares
- arithmetic progression of common difference n

Proof (Proposition)

Let $x = \dfrac{c^2}{4}$.

Proof (Proposition)

Let $x = \frac{c^2}{4}$.

$$\frac{(a-b)^2}{4} = \frac{a^2 - 2ab + b^2}{4}$$

Proof (Proposition)

Let $x = \frac{c^2}{4}$.

$$\frac{(a-b)^2}{4} = \frac{a^2 - 2ab + b^2}{4}$$
$$= \frac{a^2 - 4n + b^2}{4} \qquad \text{since } n = \frac{1}{2}ab$$

Proof (Proposition)

Let $x = \frac{c^2}{4}$.

$$\begin{aligned} \frac{(a-b)^2}{4} &= \frac{a^2 - 2ab + b^2}{4} \\ &= \frac{a^2 - 4n + b^2}{4} && \text{since } n = \frac{1}{2}ab \\ &= \frac{(c^2 - 4n)}{4} && \text{since } a^2 + b^2 = c^2 \end{aligned}$$

Proof (Proposition)

Let $x = \frac{c^2}{4}$.

$$\begin{aligned}
\frac{(a-b)^2}{4} &= \frac{a^2 - 2ab + b^2}{4} \\
&= \frac{a^2 - 4n + b^2}{4} && \text{since } n = \frac{1}{2}ab \\
&= \frac{(c^2 - 4n)}{4} && \text{since } a^2 + b^2 = c^2 \\
&= \frac{c^2}{4} - n
\end{aligned}$$

Proof (Proposition)

Let $x = \frac{c^2}{4}$.

$$\begin{aligned}
\frac{(a-b)^2}{4} &= \frac{a^2 - 2ab + b^2}{4} \\
&= \frac{a^2 - 4n + b^2}{4} && \text{since } n = \frac{1}{2}ab \\
&= \frac{(c^2 - 4n)}{4} && \text{since } a^2 + b^2 = c^2 \\
&= \frac{c^2}{4} - n \\
&= x - n
\end{aligned}$$

Proof (Proposition)

Also,

$$\frac{(a+b)^2}{4} = \frac{a^2 + 2ab + b^2}{4}$$

Proof (Proposition)

Also,

$$\begin{aligned}\frac{(a+b)^2}{4} &= \frac{a^2+2ab+b^2}{4} \\ &= \frac{(a^2+b^2)+4n}{4} \qquad \text{since } n = \frac{1}{2}ab\end{aligned}$$

Proof (Proposition)

Also,

$$\begin{aligned}\frac{(a+b)^2}{4} &= \frac{a^2+2ab+b^2}{4} \\ &= \frac{(a^2+b^2)+4n}{4} && \text{since } n = \frac{1}{2}ab \\ &= \frac{(c^2+4n)}{4} && \text{since } a^2+b^2=c^2\end{aligned}$$

Proof (Proposition)

Also,

$$
\begin{aligned}
\frac{(a+b)^2}{4} &= \frac{a^2+2ab+b^2}{4} & \\
&= \frac{(a^2+b^2)+4n}{4} & \text{since } n = \frac{1}{2}ab \\
&= \frac{(c^2+4n)}{4} & \text{since } a^2+b^2=c^2 \\
&= \frac{c^2}{4}+n & \text{since } x = \frac{c^2}{4}
\end{aligned}
$$

Proof (Proposition)

Also,

$$\begin{aligned}
\frac{(a+b)^2}{4} &= \frac{a^2+2ab+b^2}{4} \\
&= \frac{(a^2+b^2)+4n}{4} && \text{since } n = \frac{1}{2}ab \\
&= \frac{(c^2+4n)}{4} && \text{since } a^2+b^2=c^2 \\
&= \frac{c^2}{4}+n && \text{since } x = \frac{c^2}{4} \\
&= x+n
\end{aligned}$$

Proof (Proposition)

Proof (Proposition)

$$\frac{(c^2 - 4n)}{4} = \left(\frac{a-b}{2}\right)^2 = x - n$$

$$\frac{c^2}{4} = \left(\frac{c}{2}\right)^2 = x$$

$$\frac{(c^2 + 4n)}{4} = \left(\frac{a+b}{2}\right)^2 = x + n$$

Proof (Proposition)

$$\frac{(c^2 - 4n)}{4} = \left(\frac{a-b}{2}\right)^2 = x - n$$

$$\frac{c^2}{4} = \left(\frac{c}{2}\right)^2 = x$$

$$\frac{(c^2 + 4n)}{4} = \left(\frac{a+b}{2}\right)^2 = x + n$$

Rational square

Arithmetic progression with common difference n

Proof (Proposition)

$(2) \Rightarrow (1)$.

Proof (Proposition)

$(2) \Rightarrow (1)$.

Suppose $x - n$, x, and $x + n$ are rational squares.

(2) $\Rightarrow$ (1).

Suppose $x - n$, x, and $x + n$ are rational squares.

Choose:

Proof (Proposition)

(2) $\Rightarrow$ (1).

Suppose $x - n$, x, and $x + n$ are rational squares.

Choose:

$$a = \sqrt{x+n} + \sqrt{x-n} \qquad \in \mathbb{Q}$$

Proof (Proposition)

(2) $\Rightarrow$ (1).

Suppose $x - n$, x, and $x + n$ are rational squares.

Choose:

$$
\begin{aligned}
a &= \sqrt{x+n} + \sqrt{x-n} && \in \mathbb{Q} \\
b &= \sqrt{x+n} - \sqrt{x-n} && \in \mathbb{Q}
\end{aligned}
$$

Proof (Proposition)

$(2) \Rightarrow (1)$.

Suppose $x - n$, x, and $x + n$ are rational squares.

Choose:

$$\begin{aligned} a &= \sqrt{x+n} + \sqrt{x-n} && \in \mathbb{Q} \\ b &= \sqrt{x+n} - \sqrt{x-n} && \in \mathbb{Q} \\ c &= 2\sqrt{x} && \in \mathbb{Q} \end{aligned}$$

Proof (Proposition)

(2) $\Rightarrow$ (1).

Suppose $x - n$, x, and $x + n$ are rational squares.

Choose:

$$\begin{aligned} a &= \sqrt{x+n} + \sqrt{x-n} && \in \mathbb{Q} \\ b &= \sqrt{x+n} - \sqrt{x-n} && \in \mathbb{Q} \\ c &= 2\sqrt{x} && \in \mathbb{Q} \end{aligned}$$

Then:

Proof (Proposition)

(2) $\Rightarrow$ (1).

Suppose $x - n$, x, and $x + n$ are rational squares.

Choose:

$$\begin{aligned} a &= \sqrt{x+n} + \sqrt{x-n} && \in \mathbb{Q} \\ b &= \sqrt{x+n} - \sqrt{x-n} && \in \mathbb{Q} \\ c &= 2\sqrt{x} && \in \mathbb{Q} \end{aligned}$$

Then:

$$a^2 + b^2 = c^2$$

(2) $\Rightarrow$ (1).

Suppose $x - n$, x, and $x + n$ are rational squares.

Choose:

$$\begin{aligned} a &= \sqrt{x+n} + \sqrt{x-n} && \in \mathbb{Q} \\ b &= \sqrt{x+n} - \sqrt{x-n} && \in \mathbb{Q} \\ c &= 2\sqrt{x} && \in \mathbb{Q} \end{aligned}$$

Then:

$$a^2 + b^2 = c^2$$

$\therefore$ (1) $\equiv$ (2)

Moreover...

(1) and (2) $\Rightarrow$ (3):

Moreover...

(1) and (2) $\Rightarrow$ (3):

(3) There exists a rational solution (x, y) on $y^2 = x^3 - n^2x$ other than $(-n, 0), (0, 0), (n, 0)$, and ∞.

Proof Continued

Proof.

Proof Continued

Proof.

Suppose n is a congruent number. From previous slides:

Proof Continued

Proof.

Suppose n is a congruent number. From previous slides:

(A) $$\left(\frac{a+b}{2}\right)^2 = \left(\frac{c}{2}\right)^2 + n$$

(B) $$\left(\frac{a-b}{2}\right)^2 = \left(\frac{c}{2}\right)^2 - n$$

Proof Continued

Proof.

Suppose n is a congruent number. From previous slides:

(A) $$\left(\frac{a+b}{2}\right)^2 = \left(\frac{c}{2}\right)^2 + n$$

(B) $$\left(\frac{a-b}{2}\right)^2 = \left(\frac{c}{2}\right)^2 - n$$

Multiplying (A) and (B):

Proof Continued

Proof.

Suppose n is a congruent number. From previous slides:

(A) $\left(\frac{a+b}{2}\right)^2 = \left(\frac{c}{2}\right)^2 + n$

(B) $\left(\frac{a-b}{2}\right)^2 = \left(\frac{c}{2}\right)^2 - n$

Multiplying (A) and (B):

$$\left(\frac{a^2-b^2}{4}\right)^2 = \left(\frac{c}{2}\right)^4 - n^2$$

Proof Continued

$$\left(\frac{a^2 - b^2}{4}\right)^2 = \left(\frac{c}{2}\right)^4 - n^2$$

Proof Continued

$$\left(\frac{a^2 - b^2}{4}\right)^2 = \left(\frac{c}{2}\right)^4 - n^2$$

$$v = \frac{a^2 - b^2}{4} \text{ and } u = \frac{c}{2}$$

Proof Continued

$$\left(\frac{a^2-b^2}{4}\right)^2 = \left(\frac{c}{2}\right)^4 - n^2$$

$$v = \frac{a^2-b^2}{4} \text{ and } u = \frac{c}{2}$$

Rational solution to the equation $v^2 = u^4 - n^2$.

Proof Continued

$$\left(\frac{a^2-b^2}{4}\right)^2 = \left(\frac{c}{2}\right)^4 - n^2$$

$$v = \frac{a^2-b^2}{4} \text{ and } u = \frac{c}{2}$$

Rational solution to the equation $v^2 = u^4 - n^2$.
Multiply:

Proof Continued

$$\left(\frac{a^2-b^2}{4}\right)^2 = \left(\frac{c}{2}\right)^4 - n^2$$

$$v = \frac{a^2-b^2}{4} \text{ and } u = \frac{c}{2}$$

Rational solution to the equation $v^2 = u^4 - n^2$.
Multiply:

$$u^2(v^2) = u^2(u^4 - n^2)$$

Proof Continued

$$\left(\frac{a^2 - b^2}{4}\right)^2 = \left(\frac{c}{2}\right)^4 - n^2$$

$$v = \frac{a^2 - b^2}{4} \quad \text{and} \quad u = \frac{c}{2}$$

Rational solution to the equation $v^2 = u^4 - n^2$.

Multiply:

$$u^2(v^2) = u^2(u^4 - n^2)$$
$$(uv)^2 = (u^2)^3 - n^2 u^2$$

Proof Continued

$$\left(\frac{a^2 - b^2}{4}\right)^2 = \left(\frac{c}{2}\right)^4 - n^2$$

$$v = \frac{a^2 - b^2}{4} \text{ and } u = \frac{c}{2}$$

Rational solution to the equation $v^2 = u^4 - n^2$.

Multiply:

$$u^2(v^2) = u^2(u^4 - n^2)$$
$$(uv)^2 = (u^2)^3 - n^2 u^2$$

Setting $x = u^2$ and $y = uv$:

Proof Continued

$$\left(\frac{a^2-b^2}{4}\right)^2 = \left(\frac{c}{2}\right)^4 - n^2$$

$$v = \frac{a^2-b^2}{4} \quad \text{and} \quad u = \frac{c}{2}$$

Rational solution to the equation $v^2 = u^4 - n^2$.

Multiply:

$$u^2(v^2) = u^2(u^4 - n^2)$$
$$(uv)^2 = (u^2)^3 - n^2u^2$$

Setting $x = u^2$ and $y = uv$:

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

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

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

Elliptic Curve over field $\mathbb{K}$

Elliptic Curves

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

Elliptic Curve over field $\mathbb{K}$

For $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$:

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

where $a, b \in \mathbb{K}$

Field $\mathbb{K}$

Field $\mathbb{K}$

$\mathbb{K}$: Set

Field $\mathbb{K}$

$\mathbb{K}$: Set

$+ \qquad \star$

Field $\mathbb{K}$

$\mathbb{K}$: Set

$+$ $\quad\star$

1. Commutative

Field $\mathbb{K}$

$\mathbb{K}$: Set

$+$ $\star$

1. Commutative
2. Associative

Field $\mathbb{K}$

$\mathbb{K}$: Set

$+ \qquad \star$

1. Commutative
2. Associative
3. Every nonzero $a \longleftrightarrow a^{-1}$

Field $\mathbb{K}$

$\mathbb{K}$: Set

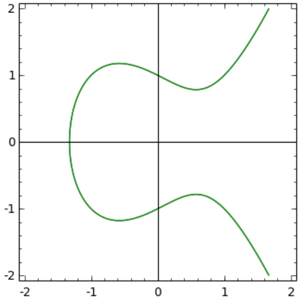
$+$ $\star$

1. Commutative
2. Associative
3. Every nonzero $a \longleftrightarrow a^{-1}$

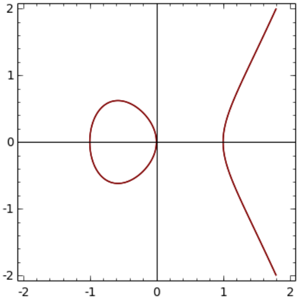
$(\mathbb{K}, +)$ Abelian Group

$(\mathbb{K} - \{0\}, \star)$ Multiplicative Group

Elliptic Curves over $\mathbb{R}$



(a) One Component



(b) Two Components

Singularities

Elliptic Curves: No singularities!

Singularities

Elliptic Curves: No singularities!

Singularity or Singular Point: point where tangent cannot be defined

Singularities

Elliptic Curves: No singularities!

Singularity or Singular Point: point where tangent cannot be defined

How to tell?

Singularities

Elliptic Curves: No singularities!

Singularity or Singular Point: point where tangent cannot be defined

How to tell? No roots are the same.

Singularities

Elliptic Curves: No singularities!

Singularity or Singular Point: point where tangent cannot be defined

How to tell? No roots are the same.
Example ($n \neq 0$):

Singularities

Elliptic Curves: No singularities!

Singularity or Singular Point: point where tangent cannot be defined

How to tell? No roots are the same.
Example ($n \neq 0$):

$$y^2 = x^3 - nx$$

Singularities

Elliptic Curves: No singularities!

Singularity or Singular Point: point where tangent cannot be defined

How to tell? No roots are the same.
Example ($n \neq 0$):

$$\begin{aligned} y^2 &= x^3 - nx \\ &= x(x^2 - n) \end{aligned}$$

Singularities

Elliptic Curves: No singularities!

Singularity or Singular Point: point where tangent cannot be defined

How to tell? No roots are the same.
Example ($n \neq 0$):

$$\begin{aligned} y^2 &= x^3 - nx \\ &= x(x^2 - n) \end{aligned}$$

The roots are $x = 0$ and $x = \pm\sqrt{n}$.

Example:

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

Singularities

Example:

$$\begin{aligned} y^2 &= x^3 + x^2 \\ &= x^2(x+1) \end{aligned}$$

Singularities

Example:

$$\begin{aligned} y^2 &= x^3 + x^2 \\ &= x^2(x+1) \end{aligned}$$

The roots are $x = 0$ (double root) and $x = -1$.

Example:

$$\begin{aligned} y^2 &= x^3 + x^2 \\ &= x^2(x+1) \end{aligned}$$

The roots are $x = 0$ (double root) and $x = -1$. Node

Singularities

Example:

$$\begin{aligned} y^2 &= x^3 + x^2 \\ &= x^2(x+1) \end{aligned}$$

The roots are $x = 0$ (double root) and $x = -1$. Node

Example:

Singularities

Example:

$$\begin{aligned} y^2 &= x^3 + x^2 \\ &= x^2(x+1) \end{aligned}$$

The roots are $x = 0$ (double root) and $x = -1$. Node

Example:

$$y^2 = x^3$$

Example:

$$\begin{aligned} y^2 &= x^3 + x^2 \\ &= x^2(x+1) \end{aligned}$$

The roots are $x = 0$ (double root) and $x = -1$. Node

Example:

$$y^2 = x^3$$

The roots are $x = 0$ (triple root).

Singularities

Example:

$$\begin{aligned} y^2 &= x^3 + x^2 \\ &= x^2(x+1) \end{aligned}$$

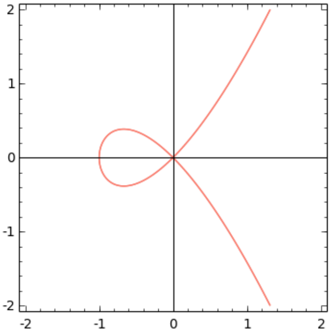
The roots are $x = 0$ (double root) and $x = -1$. Node

Example:

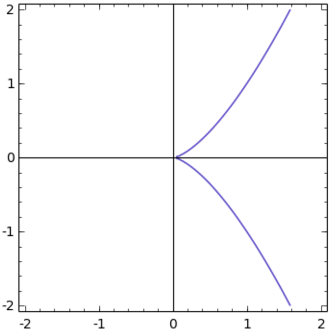
$$y^2 = x^3$$

The roots are $x = 0$ (triple root). Cusp

Singularities



(a) Node: 2 roots same



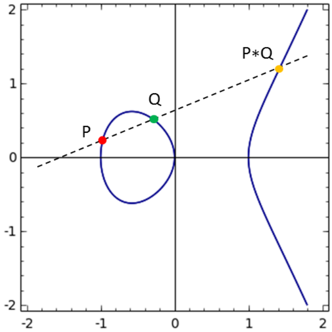
(b) Cusp: 3 roots same

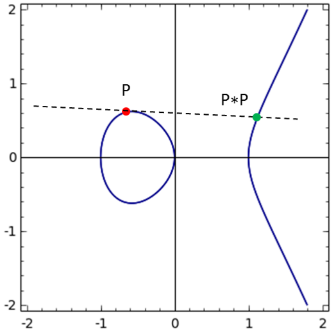
The Binary Operation $\star$

Let P, Q be points on elliptic curve.
Find P $\star$ Q.

The Binary Operation $\star$

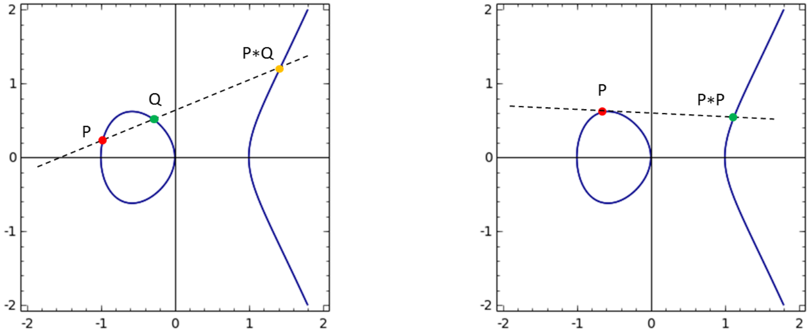
Let P, Q be points on elliptic curve.
Find P $\star$ Q.





The Binary Operation $\star$

Let P, Q be points on elliptic curve.
Find $P \star Q$.



$$P \star Q = Q \star P$$

The Binary Operation $\oplus$

Define $\oplus$ in terms of $\star$.

The Binary Operation $\oplus$

Define $\oplus$ in terms of $\star$.

Projective space: The point at infinity, denoted $\mathcal{O}$

The Binary Operation $\oplus$

Define $\oplus$ in terms of $\star$.

Projective space: The point at infinity, denoted $\mathcal{O}$

$\mathcal{O}$ on every vertical line.

The Binary Operation $\oplus$

Define $\oplus$ in terms of $\star$.

Projective space: The point at infinity, denoted $\mathcal{O}$

$\mathcal{O}$ on every vertical line.

To define P $\oplus$ Q:

1. Draw a vertical line ℓ through P $\star$ Q and $\mathcal{O}$

The Binary Operation $\oplus$

Define $\oplus$ in terms of $\star$.

Projective space: The point at infinity, denoted $\mathcal{O}$

$\mathcal{O}$ on every vertical line.

To define $P \oplus Q$:

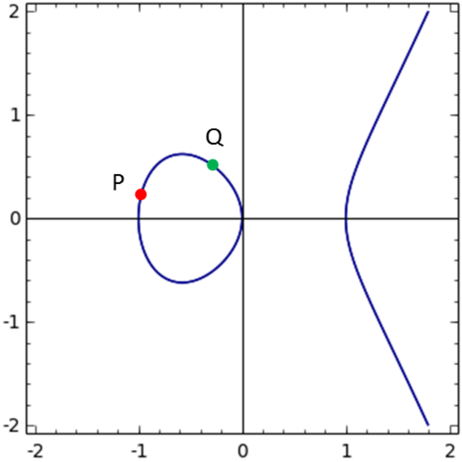
1. Draw a vertical line ℓ through $P \star Q$ and $\mathcal{O}$
2. $P \oplus Q$ is the third intersection of ℓ with elliptic curve

Finding P $\oplus$ Q Geometrically

Case 1: $P \neq Q$

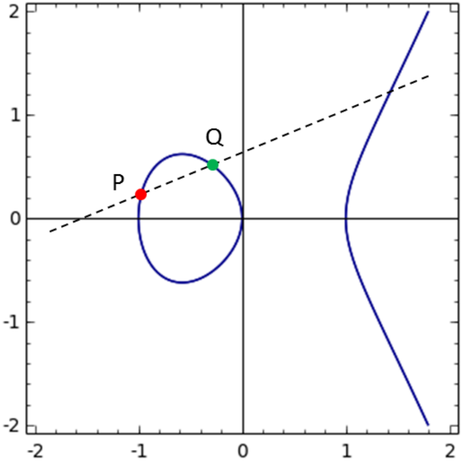
Finding P $\oplus$ Q Geometrically

Case 1: $P \neq Q$



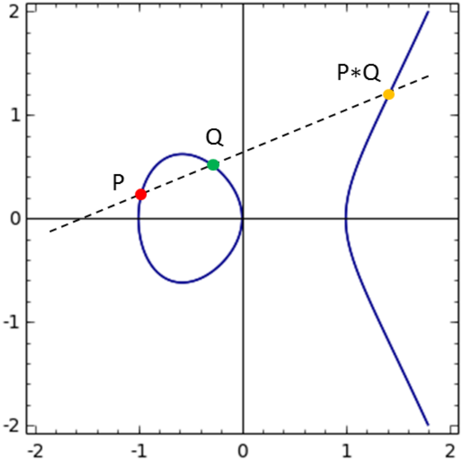
Finding P $\oplus$ Q Geometrically

Case 1: $P \neq Q$



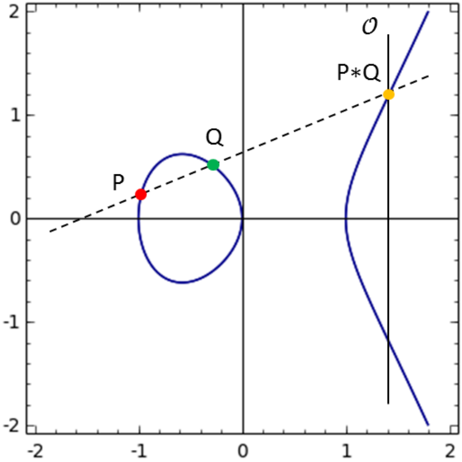
Finding P $\oplus$ Q Geometrically

Case 1: $P \neq Q$



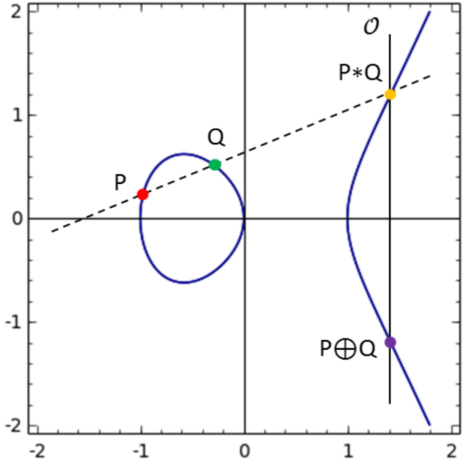
Finding P $\oplus$ Q Geometrically

Case 1: $P \neq Q$



Finding P $\oplus$ Q Geometrically

Case 1: $P \neq Q$

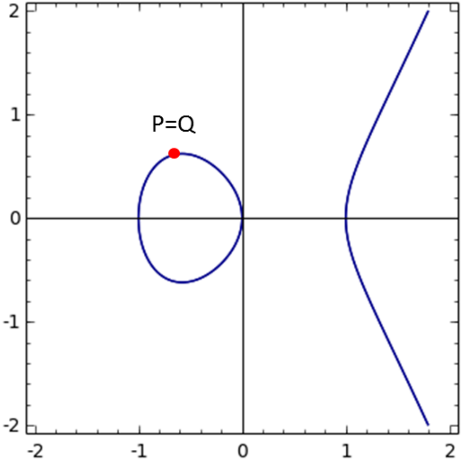


Finding P $\oplus$ Q Geometrically

Case 2: $P = Q$

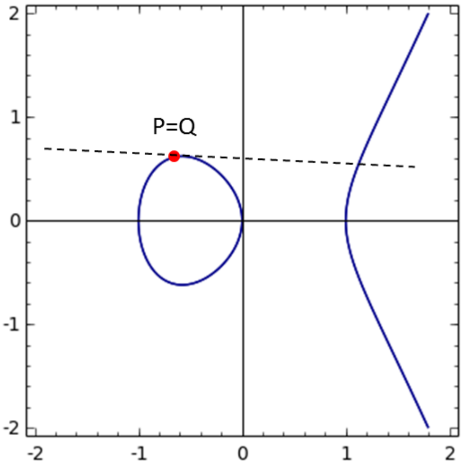
Finding P $\oplus$ Q Geometrically

Case 2: $P = Q$



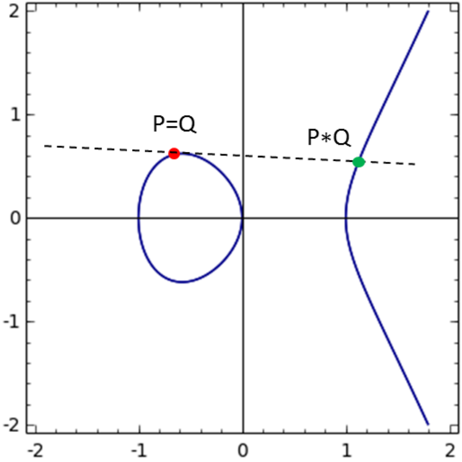
Finding P ⊕ Q Geometrically

Case 2: $P = Q$



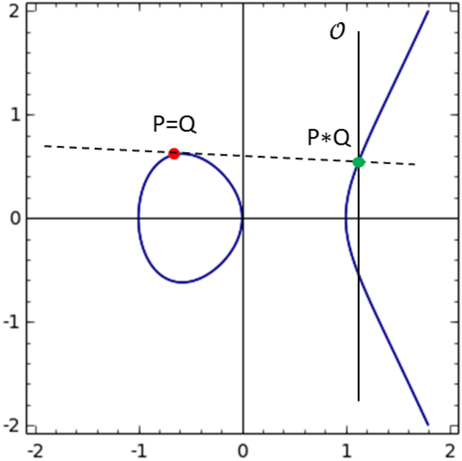
Finding P $\oplus$ Q Geometrically

Case 2: $P = Q$



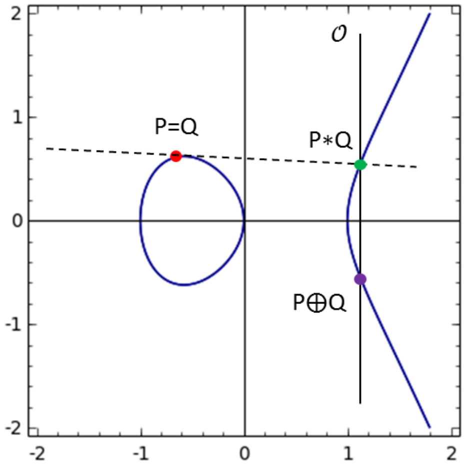
Finding P $\oplus$ Q Geometrically

Case 2: $P = Q$



Finding P $\oplus$ Q Geometrically

Case 2: $P = Q$



Group Structure under $\oplus$

Points on an elliptic curve with operation $\oplus$ form an abelian group.

The Identity Element

The Identity Element

The Identity Element is $\mathcal{O}$.

The Identity Element

The Identity Element is $\mathcal{O}$.

For any points P, Q on the elliptic curve,

The Identity Element

The Identity Element is $\mathcal{O}$.
For any points P, Q on the elliptic curve,

$$P \oplus Q = \mathcal{O} \star (P \star Q)$$

The Identity Element

The Identity Element is $\mathcal{O}$.
For any points P, Q on the elliptic curve,

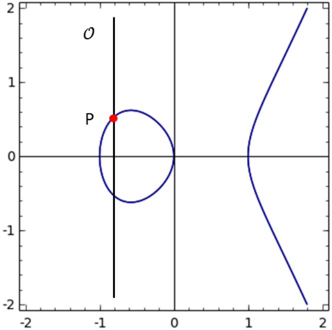
$$\mathrm{P} \oplus \mathrm{Q} = \mathcal{O} \star (\mathrm{P} \star \mathrm{Q})$$

$$\mathcal{O} \oplus \mathrm{P} = \mathcal{O} \star (\mathcal{O} \star \mathrm{P})$$

The Identity Element is $\mathcal{O}$.
For any points P, Q on the elliptic curve,

$$P \oplus Q = \mathcal{O} \star (P \star Q)$$

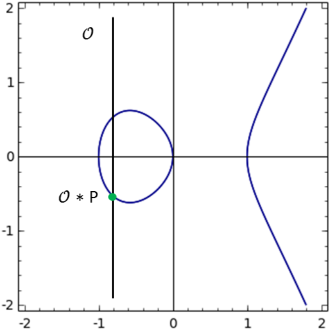
$$\mathcal{O} \oplus P = \mathcal{O} \star (\mathcal{O} \star P)$$



The Identity Element is $\mathcal{O}$.
For any points P, Q on the elliptic curve,

$$P \oplus Q = \mathcal{O} \star (P \star Q)$$

$$\mathcal{O} \oplus P = \mathcal{O} \star (\mathcal{O} \star P)$$

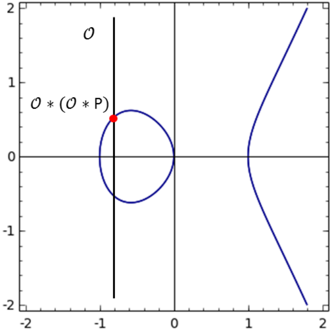


The Identity Element

The Identity Element is $\mathcal{O}$.
For any points P, Q on the elliptic curve,

$$P \oplus Q = \mathcal{O} \star (P \star Q)$$

$$\mathcal{O} \oplus P = \mathcal{O} \star (\mathcal{O} \star P)$$



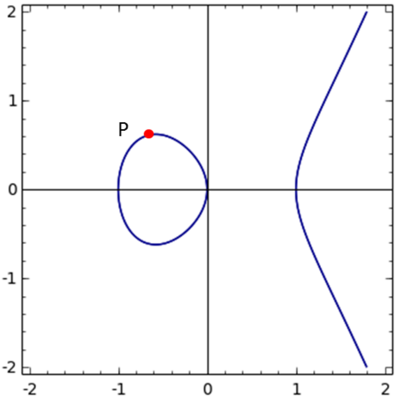
The Additive Inverse

The Additive Inverse

The additive inverse of P is P reflected over x-axis.

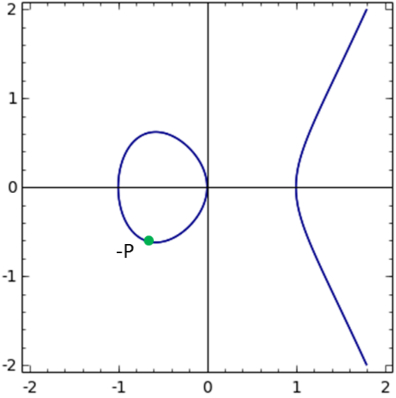
The Additive Inverse

The additive inverse of P is P reflected over x-axis.



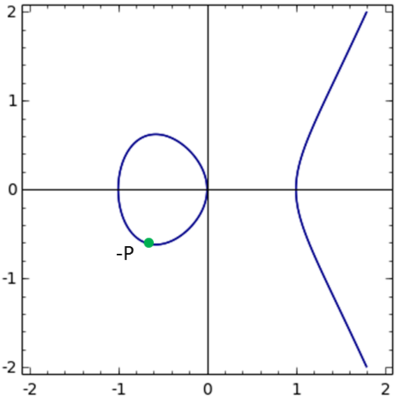
The Additive Inverse

The additive inverse of P is P reflected over x-axis.



The Additive Inverse

The additive inverse of P is P reflected over x-axis.



Then, $\mathrm{P} \star (-\mathrm{P}) = \mathcal{O}$, so (reflection over x-axis) $\mathrm{P} \oplus (-\mathrm{P}) = \mathcal{O}$

Bezout's Theorem

Bezout's Theorem.

Bezout's Theorem.

Let $\mathcal{A}$ be a polynomial of degree n and

Bezout's Theorem.

Let $\mathcal{A}$ be a polynomial of degree n and $\mathcal{B}$ a polynomial of degree m.

Bezout's Theorem.

Let $\mathcal{A}$ be a polynomial of degree n and
$\mathcal{B}$ a polynomial of degree m.
Also, suppose the polynomials do not have any common components.

Bezout's Theorem.

Let $\mathcal{A}$ be a polynomial of degree n and
$\mathcal{B}$ a polynomial of degree m.
Also, suppose the polynomials do not have any common components.
Then $\mathcal{A}$ and $\mathcal{B}$ intersect at nm distinct points.

Cayley-Bacharach Theorem.

Cayley-Bacharach Theorem

Cayley-Bacharach Theorem.

Let $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$ be polynomials of degree three.

Cayley-Bacharach Theorem.
Let $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$ be polynomials of degree three.
Suppose that $\mathcal{A}$ and $\mathcal{B}$ do not have common components.

Cayley-Bacharach Theorem.
Let $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$ be polynomials of degree three.
Suppose that $\mathcal{A}$ and $\mathcal{B}$ do not have common components.
So by Bezout's Theorem, $\mathcal{A}$ and $\mathcal{B}$ intersect at nine points.

Cayley-Bacharach Theorem

Cayley-Bacharach Theorem.

Let $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$ be polynomials of degree three.

Suppose that $\mathcal{A}$ and $\mathcal{B}$ do not have common components.

So by Bezout's Theorem, $\mathcal{A}$ and $\mathcal{B}$ intersect at nine points.

Suppose $\mathcal{C}$ passes through eight of the intersections of $\mathcal{A}$ and $\mathcal{B}$.

Cayley-Bacharach Theorem

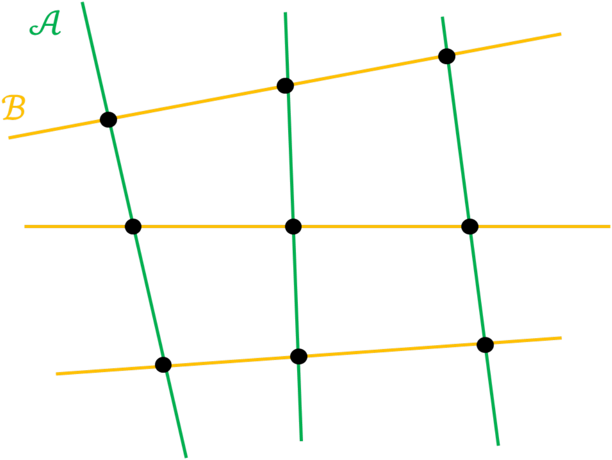
Cayley-Bacharach Theorem.

Let $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$ be polynomials of degree three.
Suppose that $\mathcal{A}$ and $\mathcal{B}$ do not have common components.
So by Bezout's Theorem, $\mathcal{A}$ and $\mathcal{B}$ intersect at nine points.
Suppose $\mathcal{C}$ passes through eight of the intersections of $\mathcal{A}$ and $\mathcal{B}$.
Then $\mathcal{C}$ must also pass through the ninth intersection.

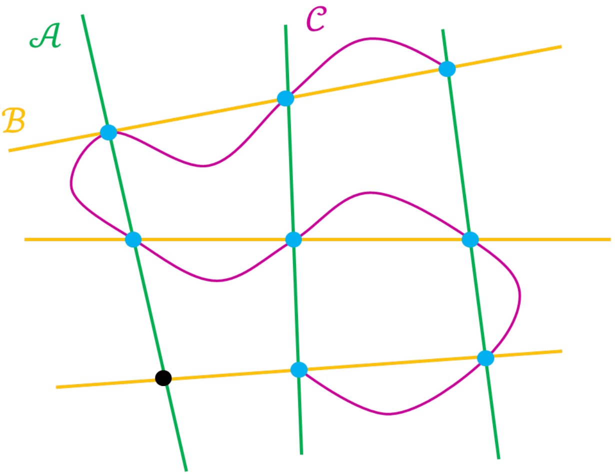
Cayley-Bacharach Theorem.
Let $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$ be polynomials of degree three.
Suppose that $\mathcal{A}$ and $\mathcal{B}$ do not have common components.
So by Bezout's Theorem, $\mathcal{A}$ and $\mathcal{B}$ intersect at nine points.
Suppose $\mathcal{C}$ passes through eight of the intersections of $\mathcal{A}$ and $\mathcal{B}$.
Then $\mathcal{C}$ must also pass through the ninth intersection.

Note: Projective Space

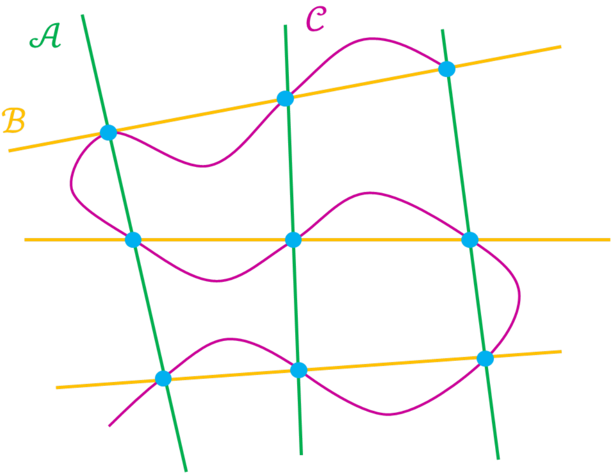
Cayley-Bacharach Theorem



Cayley-Bacharach Theorem



Cayley-Bacharach Theorem



Associative Property

Want to show the associative property of $\oplus$:

$$P \oplus (Q \oplus R) = (P \oplus Q) \oplus R$$

Want to show the associative property of $\oplus$:

$$P \oplus (Q \oplus R) = (P \oplus Q) \oplus R$$

Sufficient to show

$$P \star (Q \oplus R) = (P \oplus Q) \star R$$

Associative Property

Want to show the associative property of $\oplus$:

$$P \oplus (Q \oplus R) = (P \oplus Q) \oplus R$$

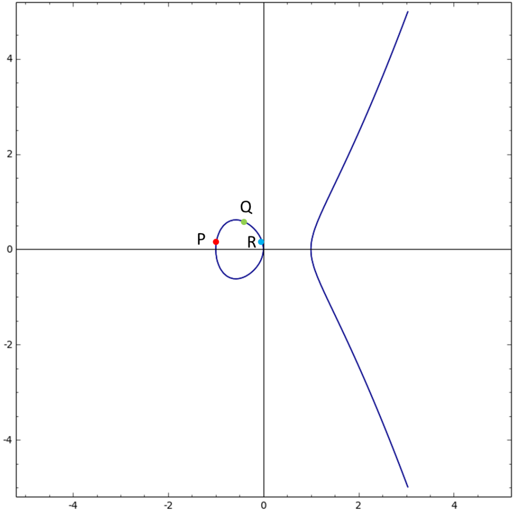
Sufficient to show

$$P \star (Q \oplus R) = (P \oplus Q) \star R$$

By reflection across the x-axis, the associative property holds.

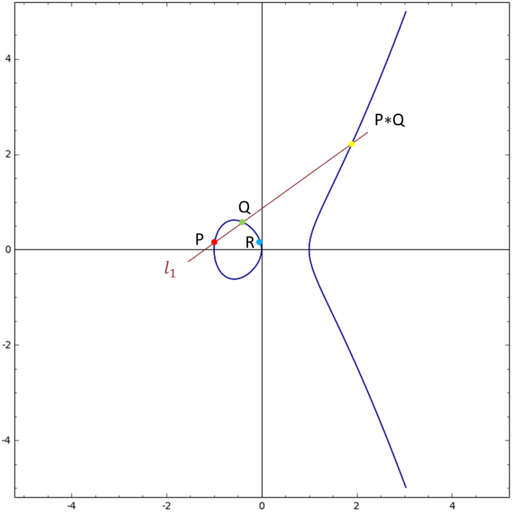
Associative Property

Let $\mathcal{E}$ be an elliptic curve, and suppose P, Q, R are points on $\mathcal{E}$.

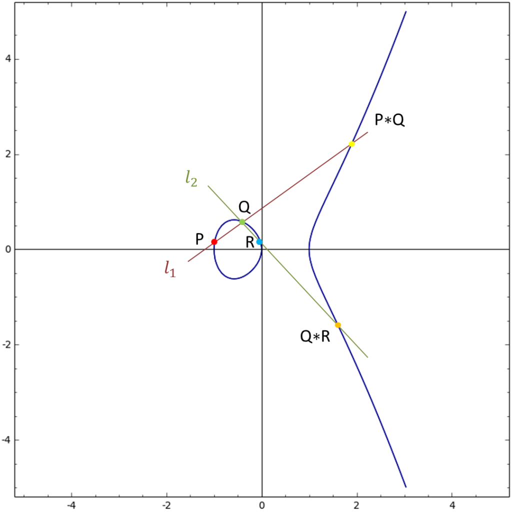


Associative Property

Let l_1 be the line passing through points P, Q, and P $\star$ Q.

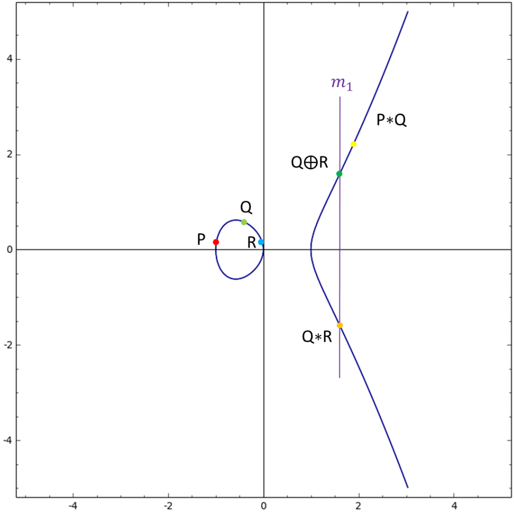


Let l_2 be the line passing through points Q, R, and Q $\star$ R.



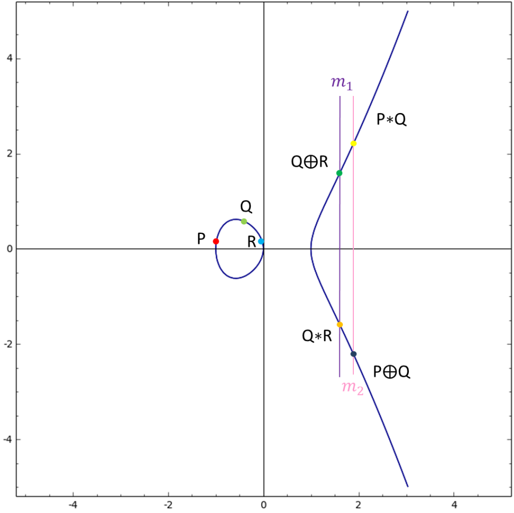
Associative Property

Let m_1 be the line passing through points Q $\star$ R and Q $\oplus$ R.



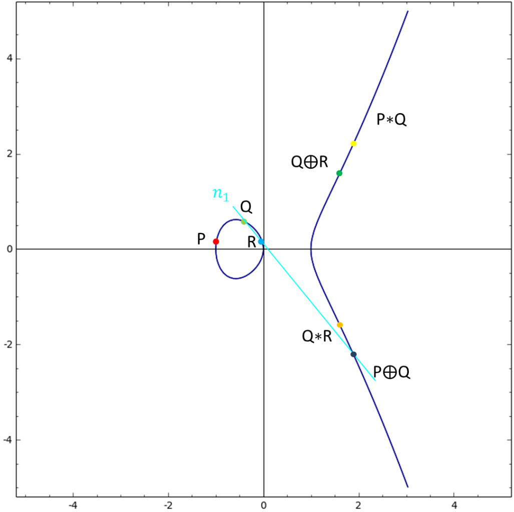
Associative Property

Let m_2 be the line passing through points P $\star$ Q and P $\oplus$ Q.



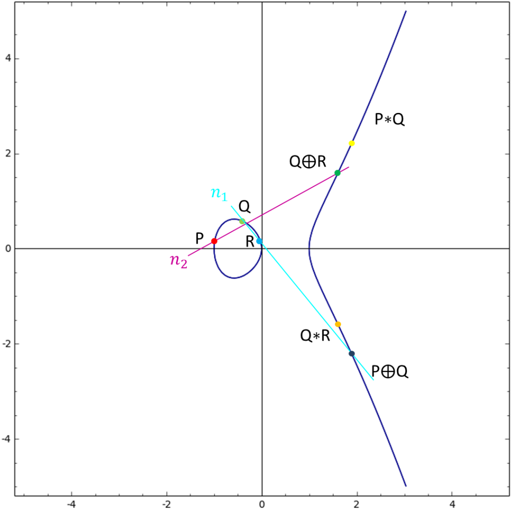
Associative Property

Let n_1 be the line passing through points P $\oplus$ Q and R.



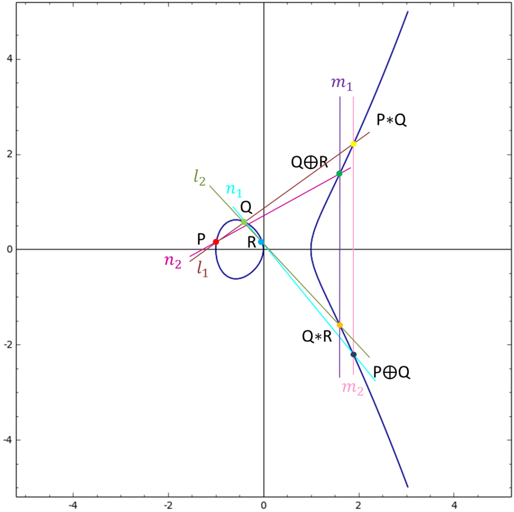
Associative Property

Let n_2 be the line passing through points Q $\oplus$ R and P.



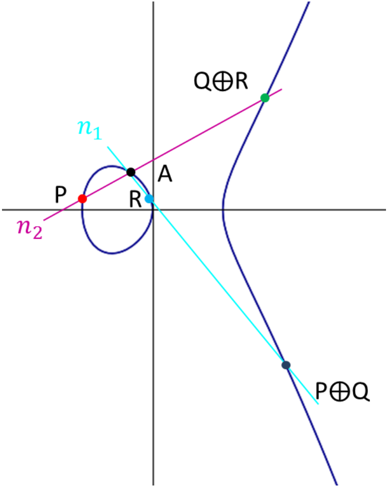
Associative Property

Now we have defined the following lines:

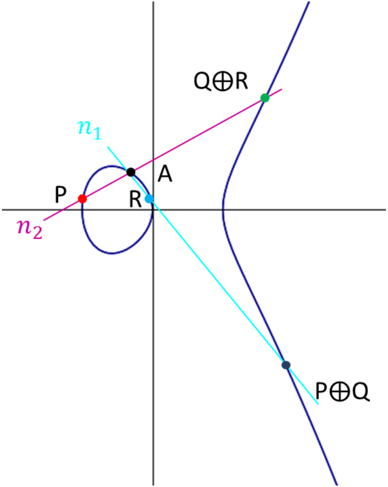


Associative Property

Lines n_1 and n_2 intersect at A.



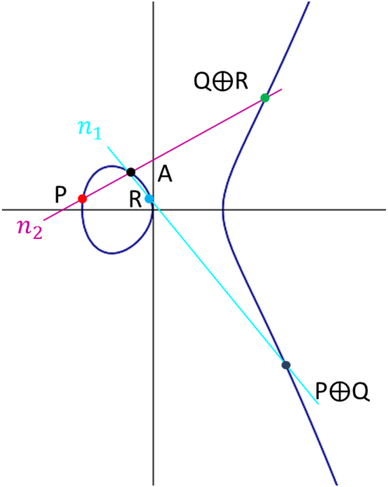
Lines n_1 and n_2 intersect at A.
Case (i): Suppose A lies on $\mathcal{E}$.
Then,



Associative Property

Lines n_1 and n_2 intersect at A.
Case (i): Suppose A lies on $\mathcal{E}$.
Then,

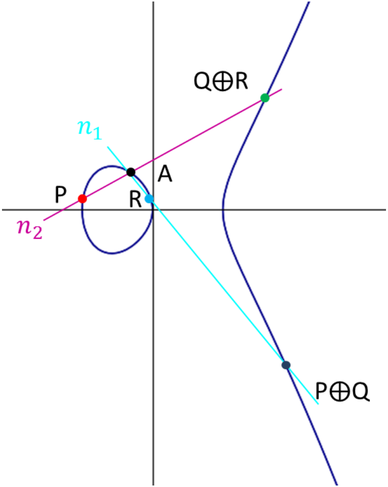
$$A = P \star (Q \oplus R)$$



Associative Property

Lines n_1 and n_2 intersect at A.
Case (i): Suppose A lies on $\mathcal{E}$.
Then,

$$\begin{aligned} A &= P \star (Q \oplus R) \\ &= (P \oplus Q) \star R \end{aligned}$$

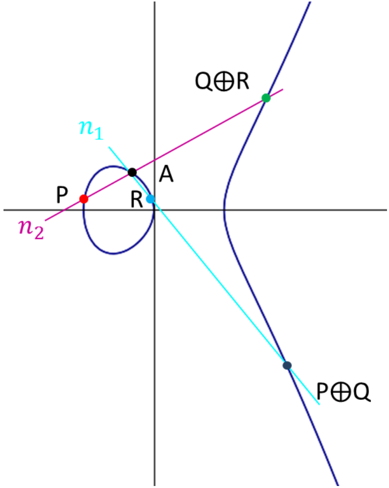


Associative Property

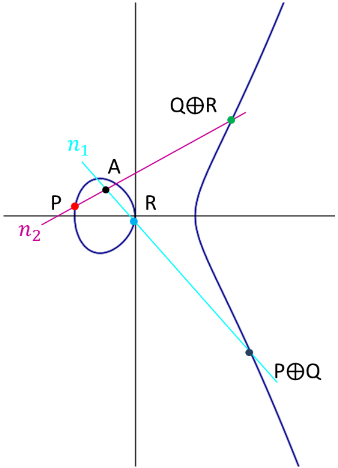
Lines n_1 and n_2 intersect at A.
Case (i): Suppose A lies on $\mathcal{E}$.
Then,

$$\begin{aligned} A &= P \star (Q \oplus R) \\ &= (P \oplus Q) \star R \end{aligned}$$

$\therefore$ the associative property holds.



Case (ii): Suppose A does not lie on $\mathcal{E}$.



Associative Property

Define: $S = \{ P, Q, R, P{\star}Q, Q{\star}R, P{\oplus}Q, Q{\oplus}R, A, \mathcal{O} \}$

Associative Property

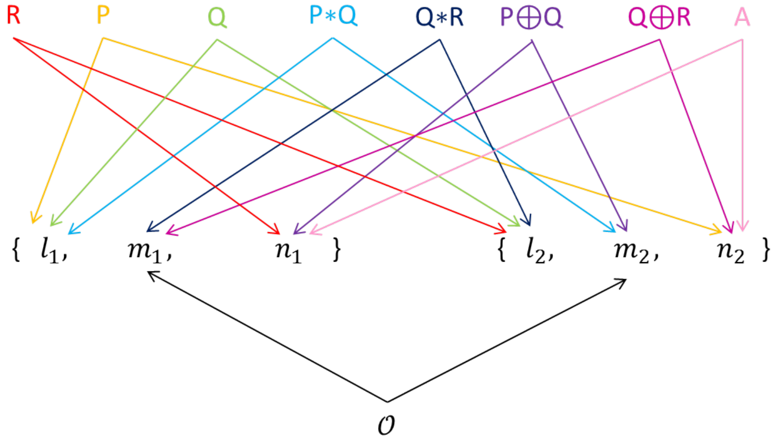
Define: S = { P, Q, R, P$\star$Q, Q$\star$R, P$\oplus$Q, Q$\oplus$R, A, $\mathcal{O}$ }

$\{l_1, m_1, n_1\}$ and $\{l_2, m_2, n_2\}$

Associative Property

Define: S = { P, Q, R, P⋆Q, Q⋆R, P⊕Q, Q⊕R, A, $\mathcal{O}$ }

$\{l_1, m_1, n_1\}$ and $\{l_2, m_2, n_2\}$



Associative Property

Define two curves: $\mathcal{A} = l_1 \cdot m_1 \cdot n_1$ and $\mathcal{B} = l_2 \cdot m_2 \cdot n_2$

Define two curves: $\mathcal{A} = l_1 \cdot m_1 \cdot n_1$ and $\mathcal{B} = l_2 \cdot m_2 \cdot n_2$

Now, curves $\mathcal{A}$ and $\mathcal{B}$ both pass through all nine points in S.

Associative Property

Define two curves: $\mathcal{A} = l_1 \cdot m_1 \cdot n_1$ and $\mathcal{B} = l_2 \cdot m_2 \cdot n_2$

Now, curves $\mathcal{A}$ and $\mathcal{B}$ both pass through all nine points in S.

Elliptic curve $\mathcal{E}$ intersects eight points in S (all except A).

Associative Property

Define two curves: $\mathcal{A} = l_1 \cdot m_1 \cdot n_1$ and $\mathcal{B} = l_2 \cdot m_2 \cdot n_2$

Now, curves $\mathcal{A}$ and $\mathcal{B}$ both pass through all nine points in S.

Elliptic curve $\mathcal{E}$ intersects eight points in S (all except A).

By Cayley-Bacharach Theorem, curve $\mathcal{E}$ must pass through A.

Associative Property

Define two curves: $\mathcal{A} = l_1 \cdot m_1 \cdot n_1$ and $\mathcal{B} = l_2 \cdot m_2 \cdot n_2$

Now, curves $\mathcal{A}$ and $\mathcal{B}$ both pass through all nine points in S.

Elliptic curve $\mathcal{E}$ intersects eight points in S (all except A).

By Cayley-Bacharach Theorem, curve $\mathcal{E}$ must pass through A.

Now we have *reduced* Case (ii) to Case (i).

Associative Property

Define two curves: $\mathcal{A} = l_1 \cdot m_1 \cdot n_1$ and $\mathcal{B} = l_2 \cdot m_2 \cdot n_2$

Now, curves $\mathcal{A}$ and $\mathcal{B}$ both pass through all nine points in S.

Elliptic curve $\mathcal{E}$ intersects eight points in S (all except A).

By Cayley-Bacharach Theorem, curve $\mathcal{E}$ must pass through A.

Now we have *reduced* Case (ii) to Case (i).

$\therefore$ the associative property holds.

Proposition The composition law $\oplus$ has the following properties:

(1) $P \oplus \mathcal{O} = P$

(2) $P \oplus Q = Q \oplus P$

(3) For every $P \longleftrightarrow -P$ such that $P \oplus (-P) = \mathcal{O}$

(4) $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$

Proposition The composition law $\oplus$ has the following properties:

(1) $P \oplus \mathcal{O} = P$

(2) $P \oplus Q = Q \oplus P$

(3) For every $P \longleftrightarrow -P$ such that $P \oplus (-P) = \mathcal{O}$

(4) $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$

Points on elliptic curve with $\oplus$ form an abelian group!

Finding P $\oplus$ Q Algebraically

Geometric addition translates to algebra.

Finding P $\oplus$ Q Algebraically

Geometric addition translates to algebra.

Example 1. Consider elliptic curve $\mathcal{E} : y^2 = x^3 + 17$

Finding P $\oplus$ Q Algebraically

Geometric addition translates to algebra.

Example 1. Consider elliptic curve $\mathcal{E} : y^2 = x^3 + 17$

The point $P = (2, 5)$ lies on this curve.

Finding P $\oplus$ Q Algebraically

Geometric addition translates to algebra.

Example 1. Consider elliptic curve $\mathcal{E} : y^2 = x^3 + 17$

The point $P = (2, 5)$ lies on this curve.

P = (2,5)
2P = (-64/25, 59/125)
3P = (5023/3249, -842480/185193)
4P = (38194304/87025, -236046706033/25672375)
5P = (279124379042/111229587121, 212464088270704525/37096290830311831)
6P = (-22792283822695031/9224204064998400, 1225613646951190271274203/885917648237503131648000)

Finding P $\oplus$ Q Algebraically

Example 2. Consider elliptic curve $\mathcal{E} : y^2 - y = x^3 - x^2$

Finding P $\oplus$ Q Algebraically

Example 2. Consider elliptic curve $\mathcal{E} : y^2 - y = x^3 - x^2$

The point $Q = (0, 0)$ lies on this curve.

Example 2. Consider elliptic curve $\mathcal{E} : y^2 - y = x^3 - x^2$

The point $Q = (0, 0)$ lies on this curve.

Q = (0, 0)
2Q = (1, 1)
3Q = (1, 0)
4Q = (0, 1)
5Q = $\mathcal{O}$

Torsion Points

Torsion Points

$P + P = 2P$

Torsion Points

$P + P = 2P$
$2P + P = 3P$
$\vdots$

Torsion Points

$P + P = 2P$
$2P + P = 3P$
$\vdots$

If $\underbrace{P + P + \cdots + P}_{n} = \mathcal{O}$, then P is an n-torsion point.

Torsion Points

$P + P = 2P$
$2P + P = 3P$
$\vdots$

If $\underbrace{P + P + \cdots + P}_{n} = \mathcal{O}$, then P is an n-torsion point.

Otherwise, P has infinite order.

Torsion Points

$P + P = 2P$
$2P + P = 3P$
$\vdots$

If $\underbrace{P + P + \cdots + P}_{n} = \mathcal{O}$, then P is an n-torsion point.

Otherwise, P has infinite order.

Previously:

(Ex. 1) P is of infinite order on $\mathcal{E}$

(Ex. 2) Q is of order 5 on $\mathcal{E}$

Mordell's Theorem

Mordell's Theorem. The group of rational points of an elliptic curve over $\mathbb{Q}$ is finitely generated. Hence, it is $\mathbb{Z}^r \oplus F$ with F finite abelian.

Mordell's Theorem. The group of rational points of an elliptic curve over $\mathbb{Q}$ is finitely generated. Hence, it is $\mathbb{Z}^r \oplus F$ with F finite abelian.

Given a few points on a curve, can I obtain from these points the point P?

Mordell's Theorem. The group of rational points of an elliptic curve over $\mathbb{Q}$ is finitely generated. Hence, it is $\mathbb{Z}^r \oplus F$ with F finite abelian.

Given a few points on a curve, can I obtain from these points the point P?

r: rank of $E(\mathbb{Q})$

Mordell's Theorem

Mordell's Theorem. The group of rational points of an elliptic curve over $\mathbb{Q}$ is finitely generated. Hence, it is $\mathbb{Z}^r \oplus F$ with F finite abelian.

Given a few points on a curve, can I obtain from these points the point P?

r: rank of $E(\mathbb{Q})$

r $= 0 \Rightarrow$ every point is a torsion point.
larger r $\Rightarrow$ more generators needed to obtain point P.

Proposition

For a fixed integer n,

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

Proposition

For a fixed integer n,

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

Proposition. A square-free integer n fails to be congruent if and only if the elliptic curve E_n has the property that $E_n(\mathbb{Q})$ has rank 0.

A Million Dollar Conjecture

Birch-Swinnerton-Dyer Conjecture: Consider two formal power series:

$$x\prod_{n=1}^{\infty} g(x) = (1-x^{8n})(1-x^{16n})$$

$$\theta_j(x) = 1 + 2\sum_{n=1}^{\infty} x^{2jn^2}$$

where $j = 1$ or $j = 2$.

A Million Dollar Conjecture

Birch-Swinnerton-Dyer Conjecture: Consider two formal power series:

$$x \prod_{n=1}^{\infty} g(x) = (1 - x^{8n})(1 - x^{16n})$$

$$\theta_j(x) = 1 + 2 \sum_{n=1}^{\infty} x^{2jn^2}$$

where $j = 1$ or $j = 2$. Then consider their products:

$$g(x)\theta_1(x) = \sum_{n=1}^{\infty} a(n)x^n$$

$$g(x)\theta_2(x) = \sum_{n=1}^{\infty} b(n)x^n$$

Connection to Congruent Numbers

Connection to Congruent Numbers

a(1) = 1	b(1) = 1
a(3) = 2	b(3) = 0
a(5) = 0	b(5) = 2
a(7) = 0	b(7) = 0
a(11) = -2	b(11) = 0
a(13) = 0	b(13) = -2
a(15) = 0	b(15) = 0
a(17) = -4	b(17) = 0
a(19) = -2	b(19) = 0
a(21) = 0	b(21) = -4

Connection to Congruent Numbers

a(1) = 1	b(1) = 1
a(3) = 2	b(3) = 0
a(5) = 0	b(5) = 2
a(7) = 0	b(7) = 0
a(11) = -2	b(11) = 0
a(13) = 0	b(13) = -2
a(15) = 0	b(15) = 0
a(17) = -4	b(17) = 0
a(19) = -2	b(19) = 0
a(21) = 0	b(21) = -4

Corollary (of Birch-Swinnerton-Dyer Conjecture). Let n be any odd square-free positive integer. Then

(i) n is congruent if and only if $a(n) = 0$,

(ii) $2n$ is congruent if and only if $b(n) = 0$.

Conclusion

Conclusion

Study of congruent numbers $\Longrightarrow$ motivation for study of elliptic curves.

Conclusion

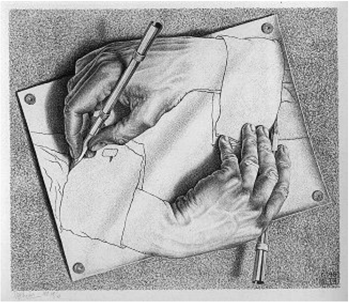
Study of congruent numbers $\Longrightarrow$ motivation for study of elliptic curves.

Discoveries in elliptic curves $\Longrightarrow$ progress on congruent number problem.

Conclusion

Study of congruent numbers $\Longrightarrow$ motivation for study of elliptic curves.

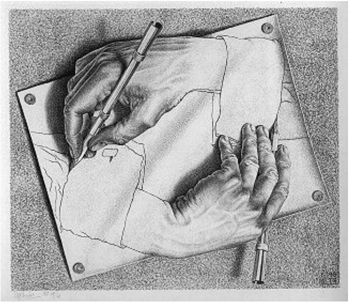
Discoveries in elliptic curves $\Longrightarrow$ progress on congruent number problem.



Conclusion

Study of congruent numbers $\Longrightarrow$ motivation for study of elliptic curves.

Discoveries in elliptic curves $\Longrightarrow$ progress on congruent number problem.

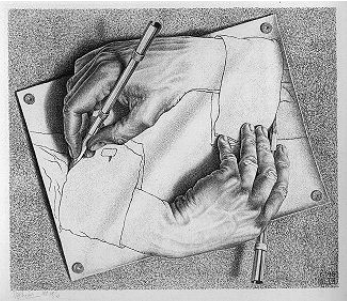


Theoretically Interesting.

Conclusion

Study of congruent numbers $\Longrightarrow$ motivation for study of elliptic curves.

Discoveries in elliptic curves $\Longrightarrow$ progress on congruent number problem.



Theoretically Interesting.

Also very useful in cryptography.

Thanks to Professor Long and Professor Hoffman!