https://research.reading.ac.uk/lms-women-in-maths-2022/

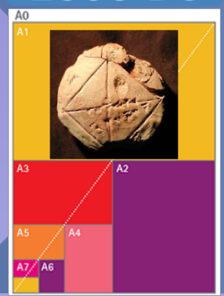
Elliptic curves and the Birch — Swinnerton-Dyer conjecture

Céline Maistret
University of Bristol

May 11, 2022

Number theory

1600 BC

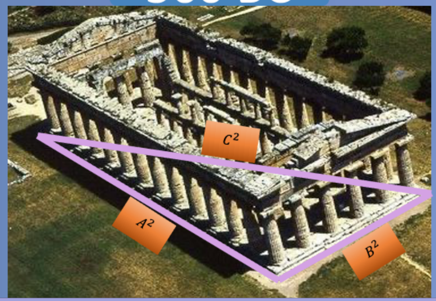


$\sqrt{2}$

Area

x^2-2=0

500 BC



Pythagorean Triples

Architecture

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

1572

Imaginary Numbers

Electricity

$x^2 + 1$=0

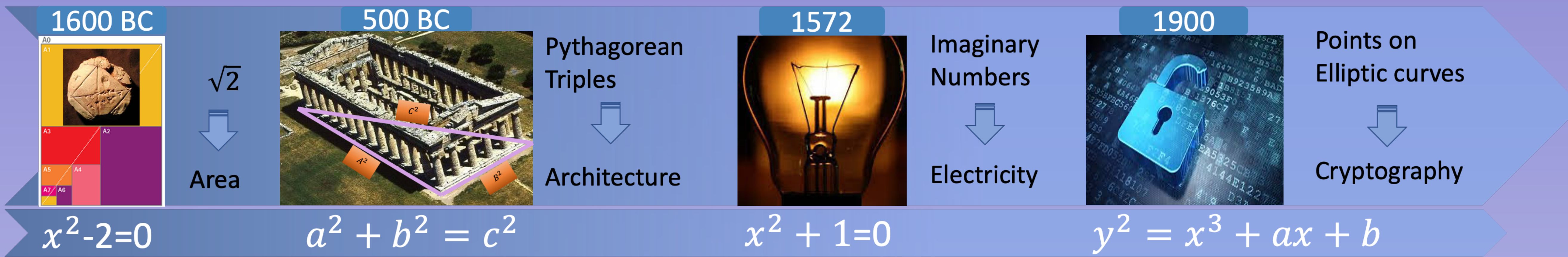
1900

Points on Elliptic curves

Cryptography

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

Number theory



Diophantine equations

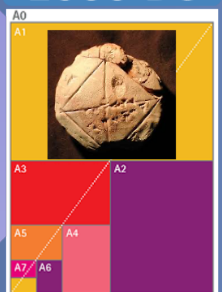
Polynomial equations with integer coefficients for which only rational solutions are sought.

Diophantus of Alexandria
~AD 200

$$x^2 + 5x + y^4 = 0$$

Number theory

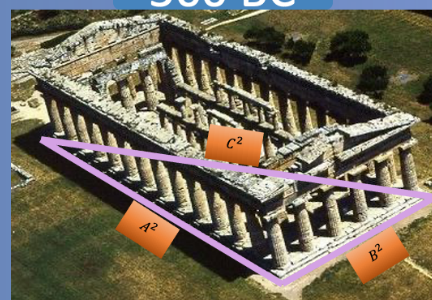
1600 BC



$\sqrt{2}$

Area

500 BC



Pythagorean Triples

Architecture

1572

Imaginary Numbers

Electricity

1900

Points on Elliptic curves

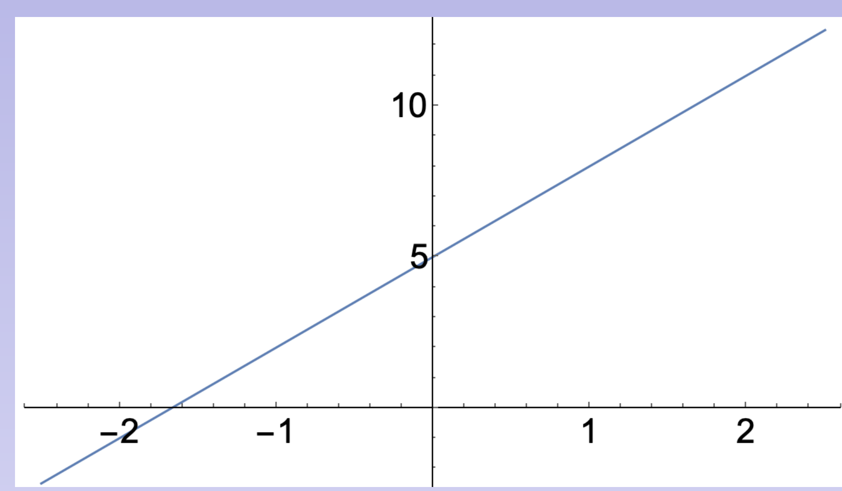
Cryptography

x^2-2=0 $\quad a^2 + b^2 = c^2 \quad x^2 + 1$=0 $\quad y^2 = x^3 + ax + b$

Diophantine equations

Linear equations

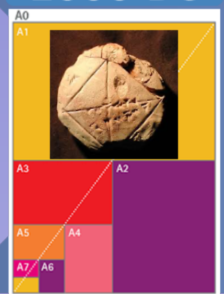
$$y = 3x + 5$$



Parametrised by
$x \in \mathbb{Q}$:
$(x\ ,\ 3x + 5)$

Number theory

1600 BC

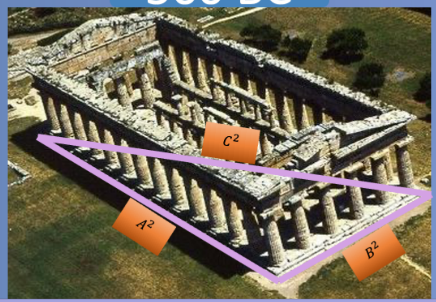


$\sqrt{2}$

Area

x^2-2=0

500 BC



Pythagorean Triples

Architecture

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

1572

Imaginary Numbers

Electricity

$x^2 + 1$=0

1900

Points on Elliptic curves

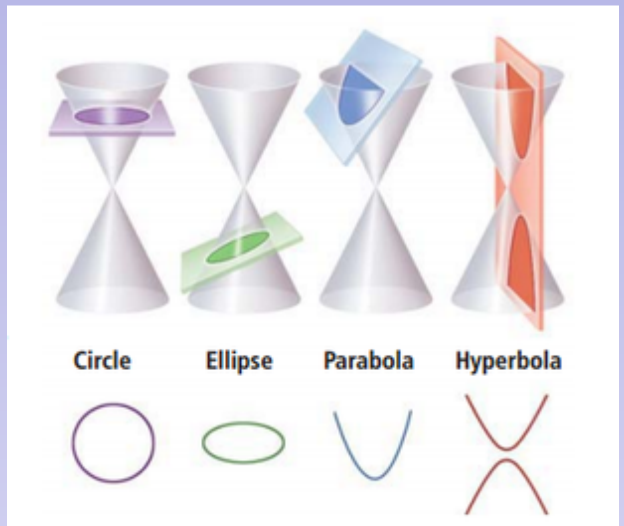
Cryptography

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

Diophantine equations

Conic sections

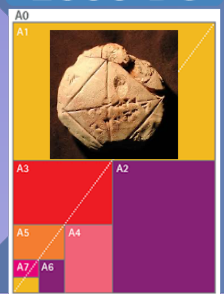
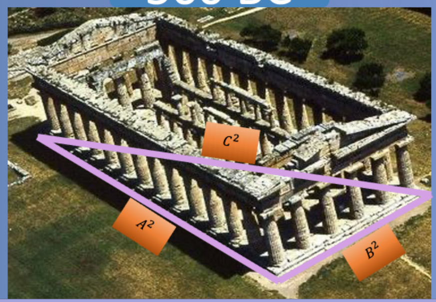
$$x^2 + y^2 = 1$$



Parametrised by $t \in \mathbb{Q}$:

$$\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$$

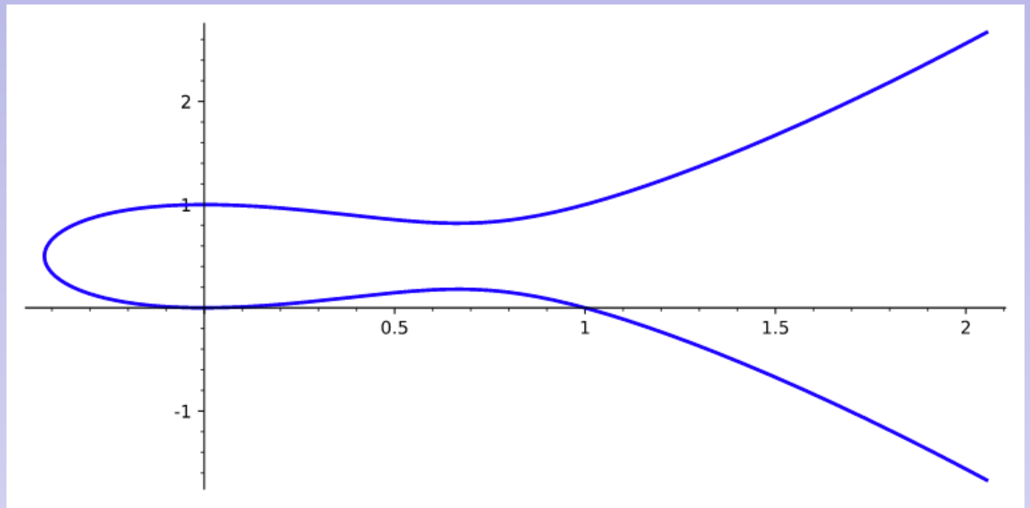
Number theory

1600 BC	500 BC	1572	1900
 $\sqrt{2}$ ⇩ Area	 Pythagorean Triples ⇩ Architecture	 Imaginary Numbers ⇩ Electricity	 Points on Elliptic curves ⇩ Cryptography
x^2-2=0	$a^2 + b^2 = c^2$	$x^2 + 1$=0	$y^2 = x^3 + ax + b$

Diophantine equations

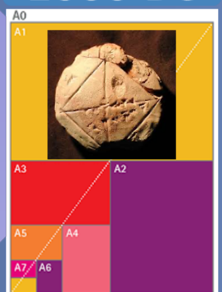
Elliptic curves

$$E : y^2 - y = x^3 - x^2$$



Number theory

1600 BC

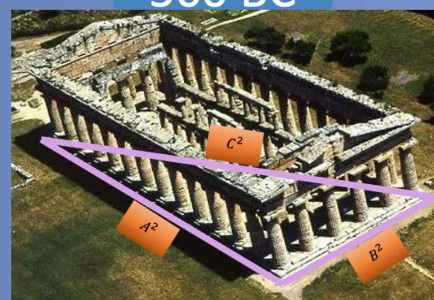


$\sqrt{2}$

Area

x^2-2=0

500 BC



Pythagorean Triples

Architecture

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

1572

Imaginary Numbers

Electricity

$x^2 + 1$=0

1900

Points on Elliptic curves

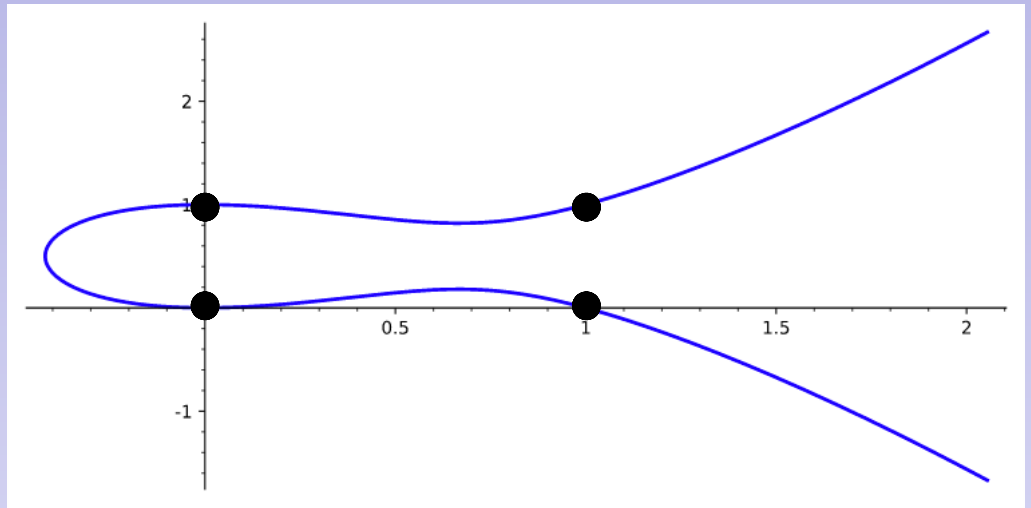
Cryptography

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

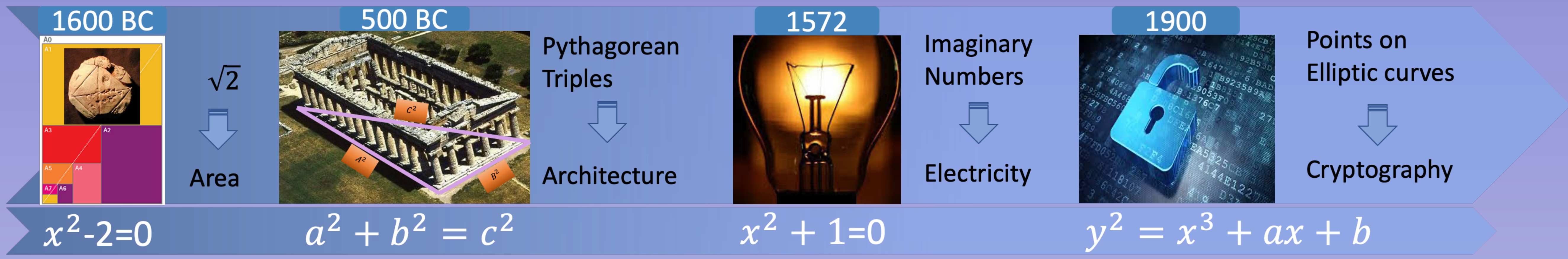
Diophantine equations

Elliptic curves

$$E : y^2 - y = x^3 - x^2$$



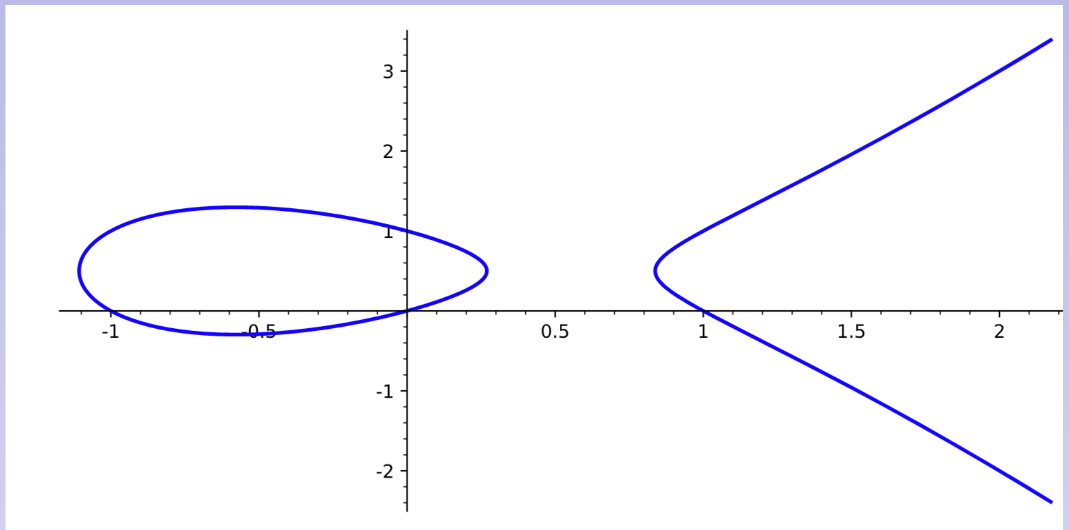
Number theory



Diophantine equations

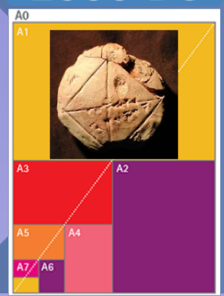
Elliptic curves

$$E : y^2 - y = x^3 - x$$



Number theory

1600 BC

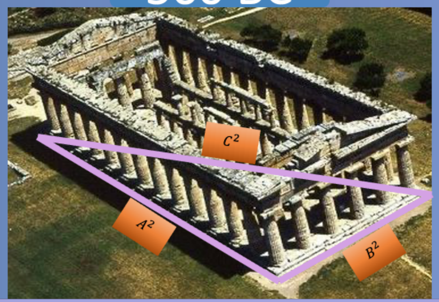


$\sqrt{2}$

Area

x^2-2=0

500 BC



Pythagorean Triples

Architecture

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

1572

Imaginary Numbers

Electricity

$x^2 + 1$=0

1900

Points on Elliptic curves

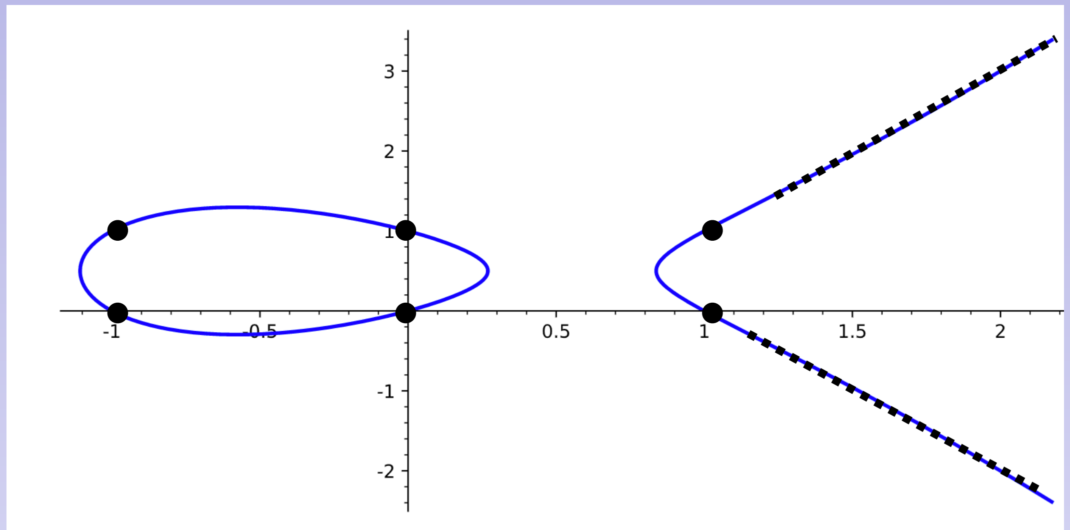
Cryptography

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

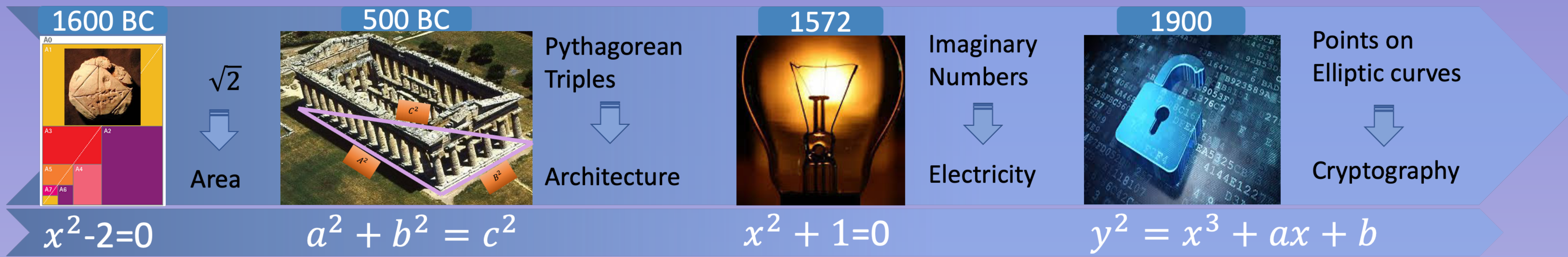
Diophantine equations

Elliptic curves

$$E : y^2 - y = x^3 - x$$



Number theory



Diophantine equations

Elliptic curves

$$E : y^2 - y = x^3 - x$$

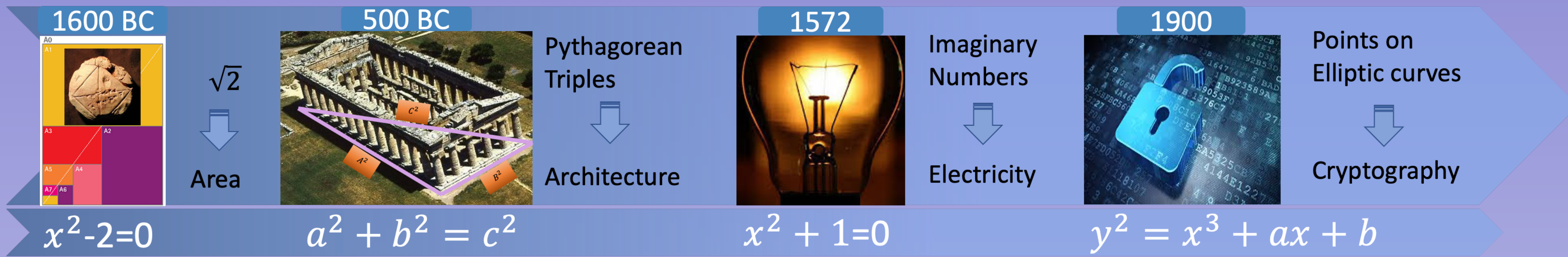
Elliptic curves

$$E : y^2 - y = x^3 - x^2$$

Parametrised by $t \in \mathbb{Q}$:

$$\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$$

Number theory



Diophantine equations

Elliptic curves

$$E : y^2 - y = x^3 - x$$

Elliptic curves

$$E : y^2 - y = x^3 - x^2$$

~~Para ... ed ... $\mathbb{Q}$:~~

$$\cancel{\left(\frac{1}{\ } \ldots \frac{2t}{\ t^2}\right)}$$

Integers

$\ldots,-10,-9,-8,-7,-6,-5,-4,-3,-2,-1,0,1,2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ldots$

$$2 = 1+1$$

$$3 = 1+1+1$$

$$\vdots$$

$$N = 1 + \ldots + 1$$

Integers

…,-10,-9,-8,-7,-6,-5,-4,-3,-2,-1,0,1,2, 3, 4, 5, 6, 7, 8, 9, 10,…

2 = 1+1

3 = 1+1+1

.

.

.

N = 1 + … + 1

The integers form a group under addition

Integers

...,-10,-9,-8,-7,-6,-5,-4,-3,-2,-1,0,1,2, 3, 4, 5, 6, 7, 8, 9, 10,...

2 = 1+1

3 = 1+1+1

.

.

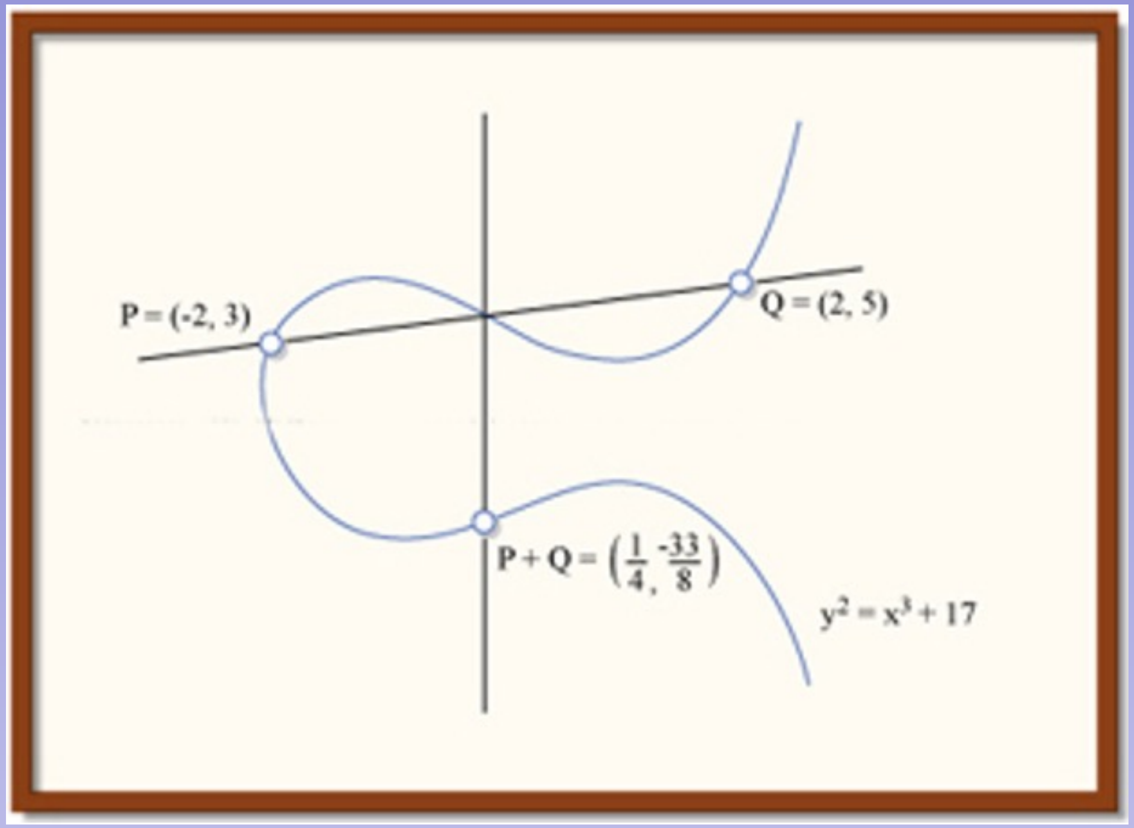
.

N = 1 + ... + 1

The integers form a group under addition

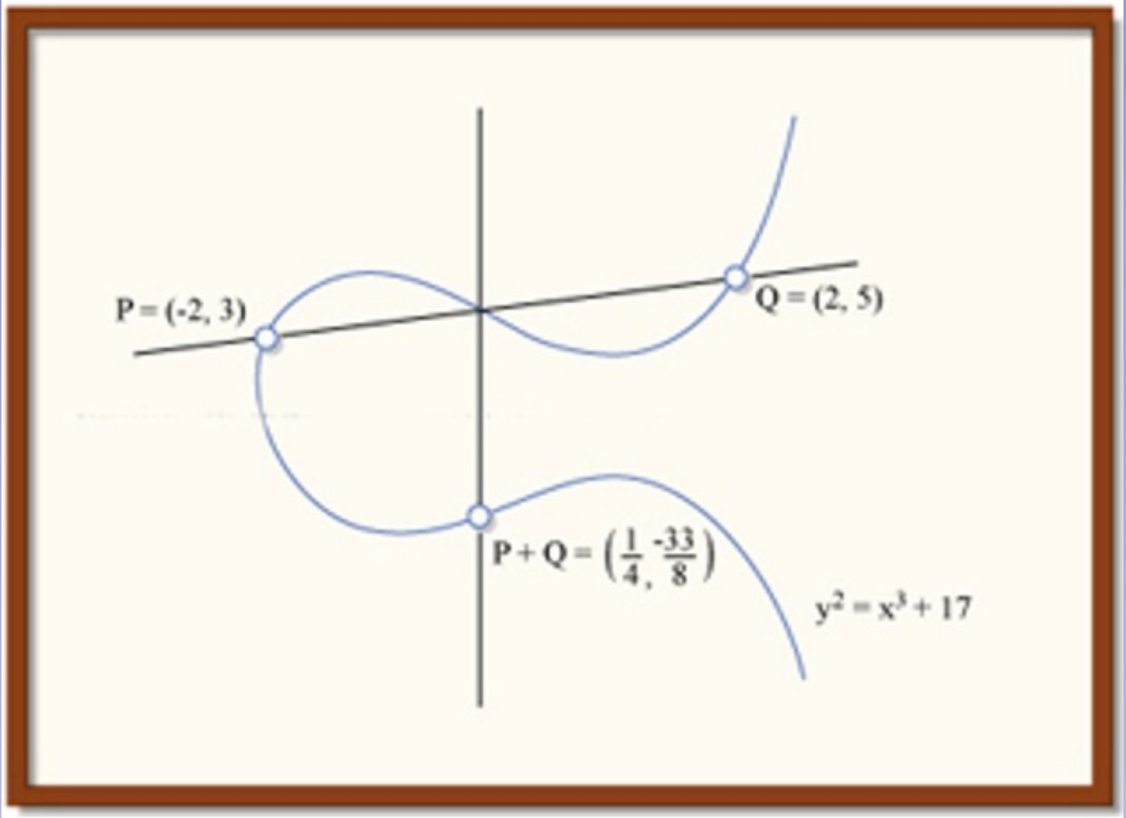
1 is a generator for the integers

Elliptic curve : $y^2 = x^3 + 17$



The rational points form a group under this addition

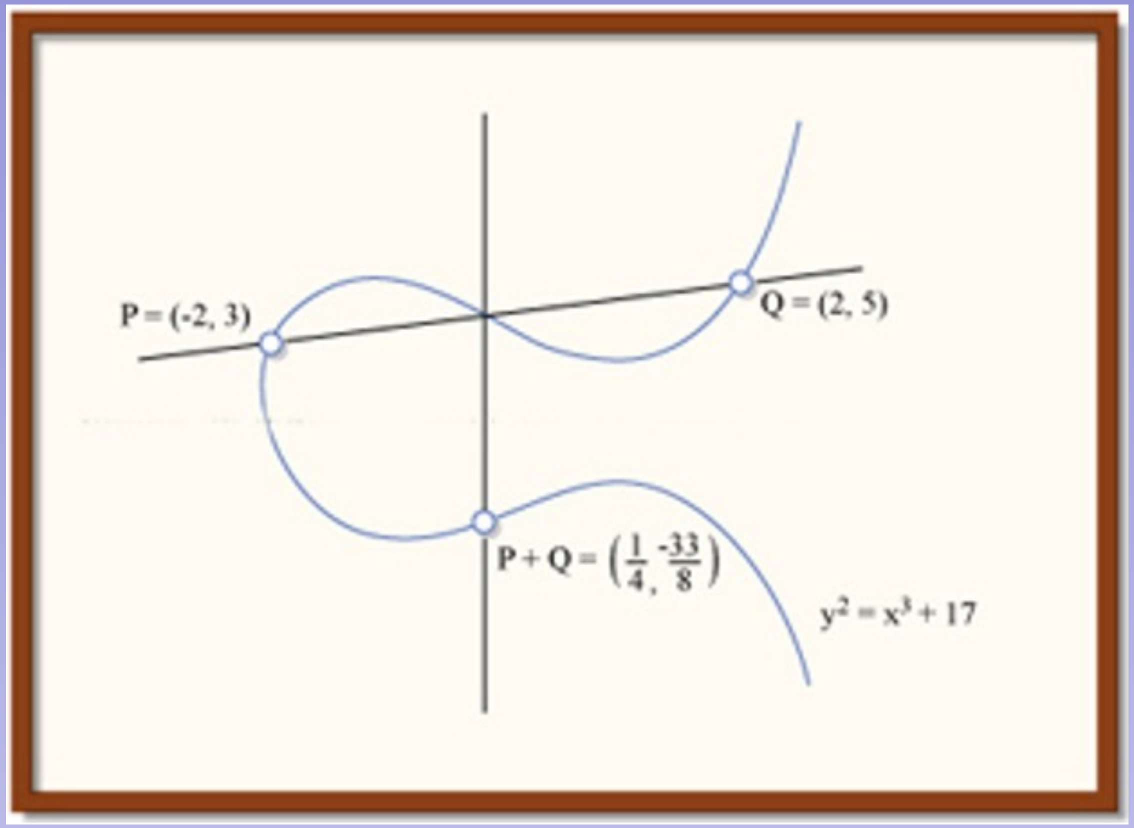
Elliptic curve : $y^2 = x^3 + 17$



The rational points form a group under this addition

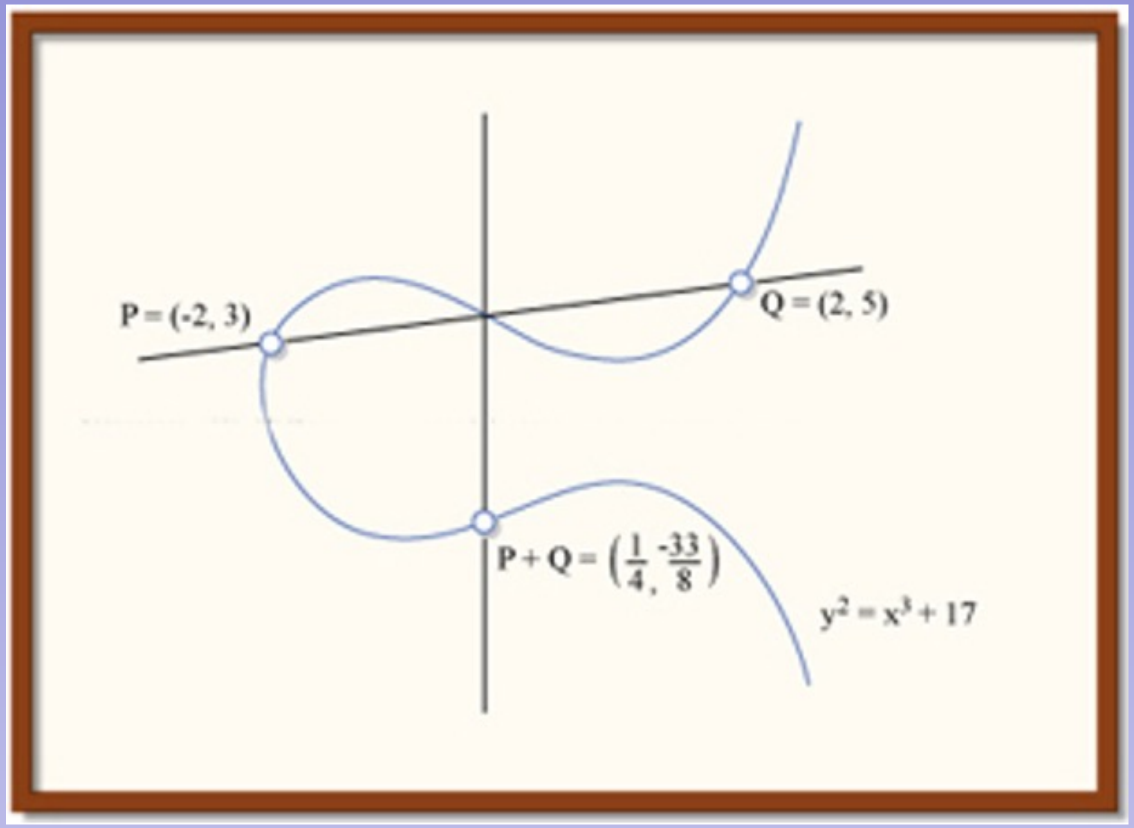
Find generator(s) and done!

Elliptic curve : $y^2 = x^3 + 17$



Any point R = nP + mQ

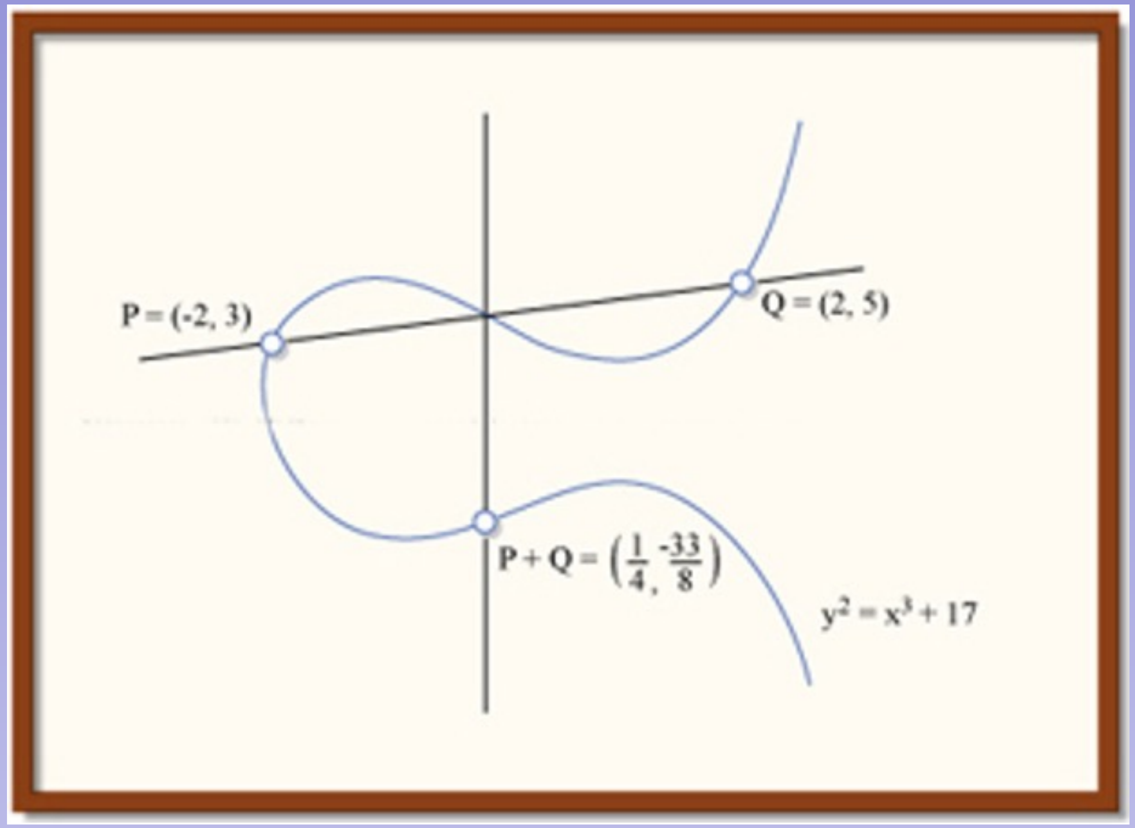
Elliptic curve : $y^2 = x^3 + 17$



Any point R = nP + mQ

P and Q generate all rational points

Elliptic curve : $y^2 = x^3 + 17$

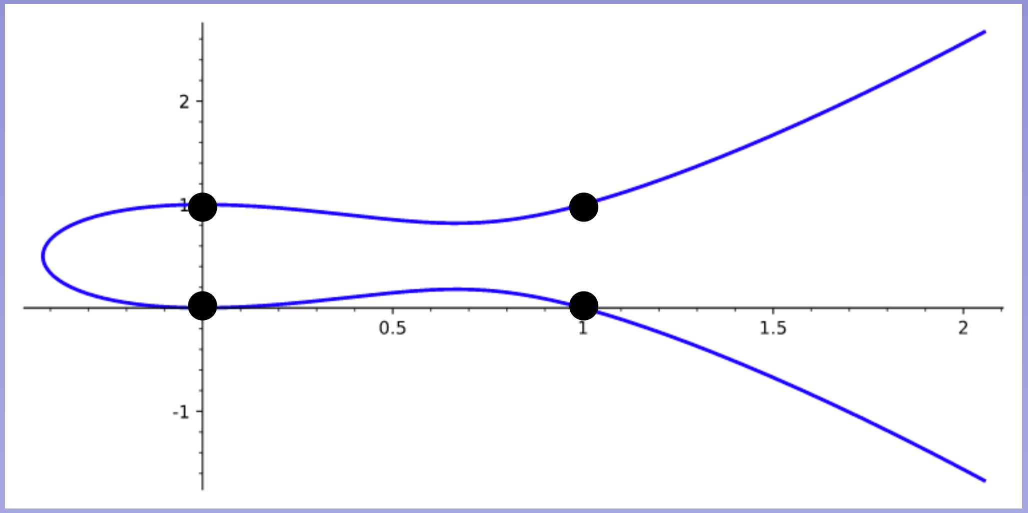


Any point R = nP + mQ

P and Q generate all rational points

This curve has rank 2

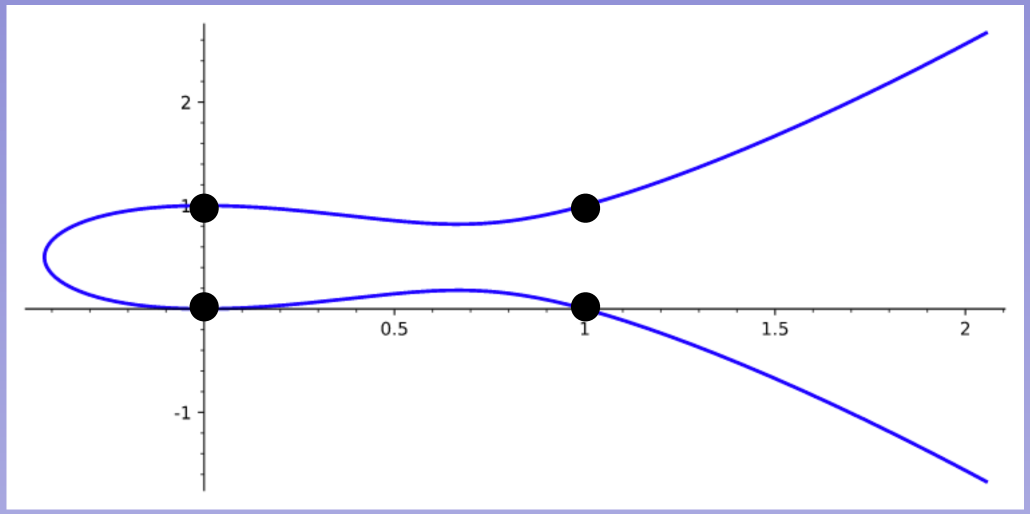
Elliptic curves



$$E : y^2 - y = x^3 - x^2$$

No point on this curve generates infinitely many other points

Elliptic curves

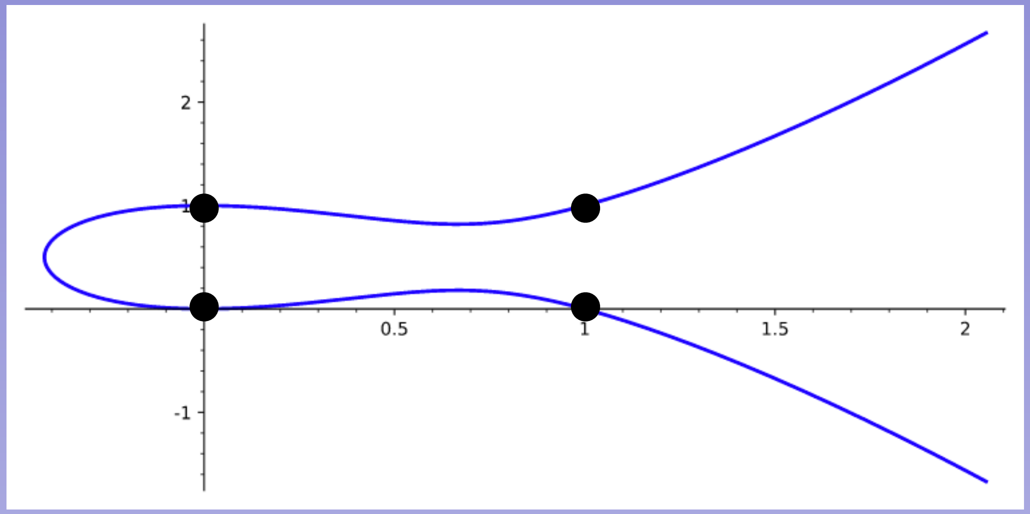


$$E : y^2 - y = x^3 - x^2$$

No point on this curve generates infinitely many other points

This curve has rank 0

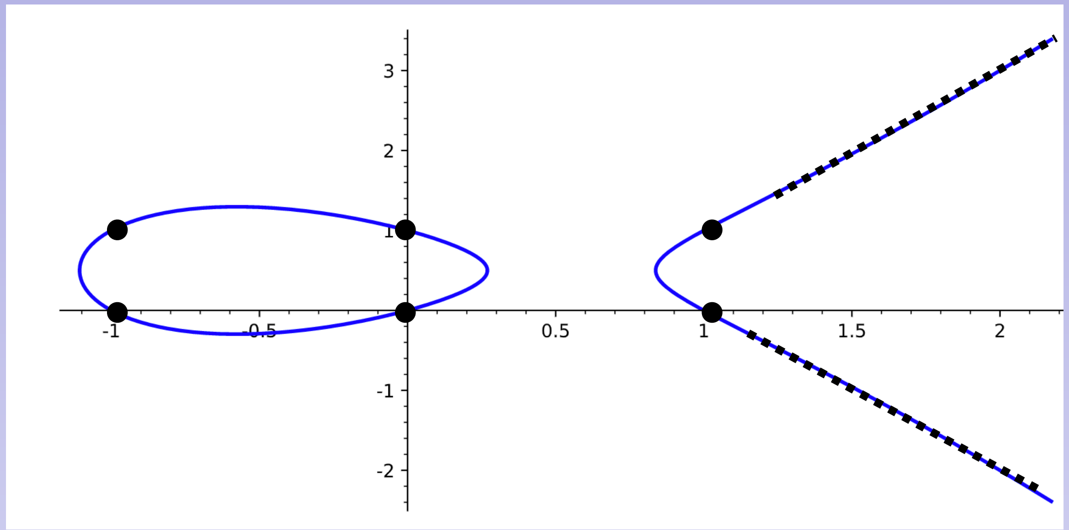
Elliptic curves



$$E : y^2 - y = x^3 - x^2$$

No point on this curve generates infinitely many other points

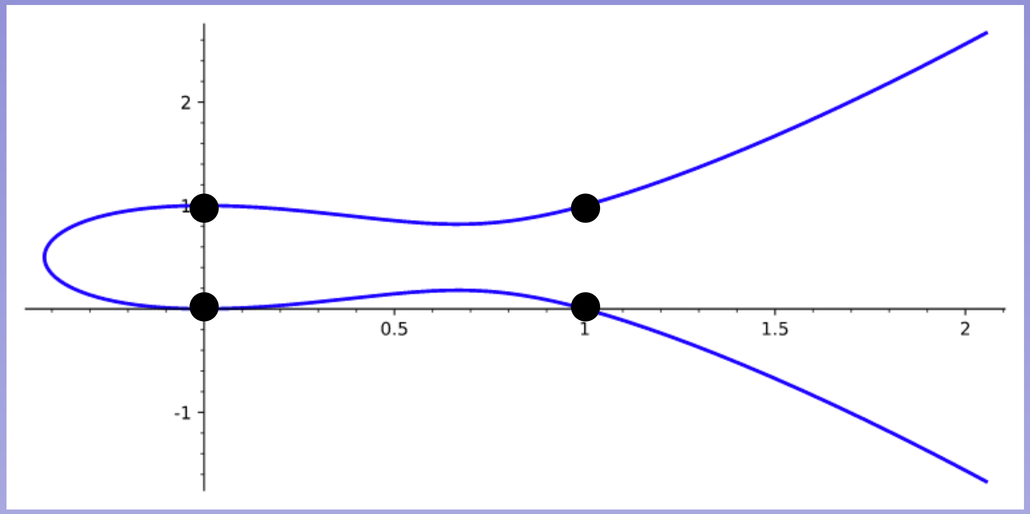
This curve has rank 0



$$E : y^2 - y = x^3 - x$$

One point on this curve generates all rational points

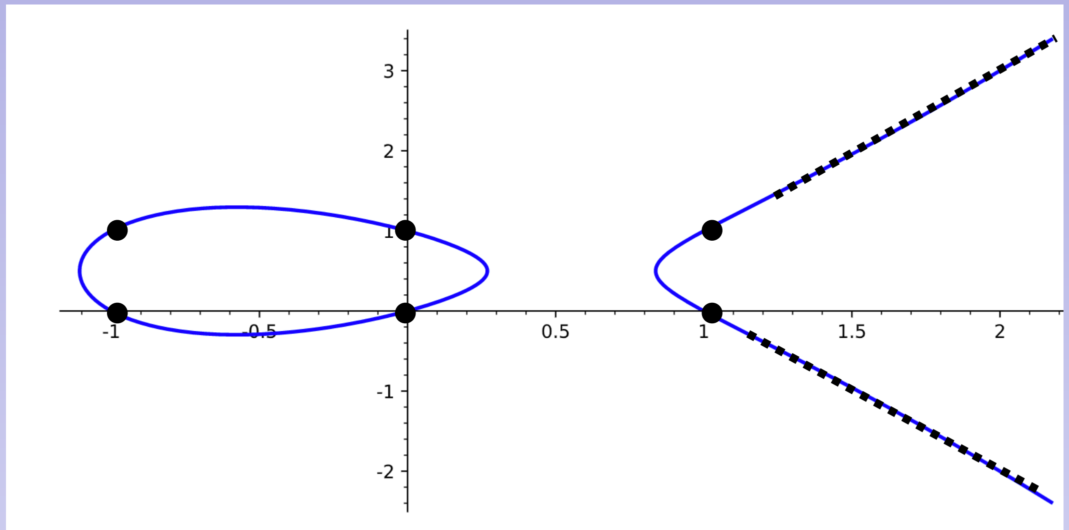
Elliptic curves



$$E : y^2 - y = x^3 - x^2$$

No point on this curve generates infinitely many other points

This curve has rank 0

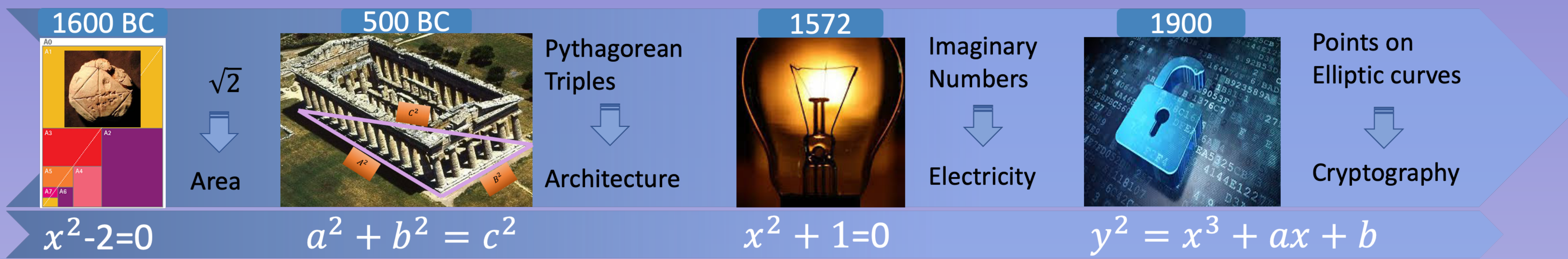


$$E : y^2 - y = x^3 - x$$

One point on this curve generates all rational points

This curve has rank 1

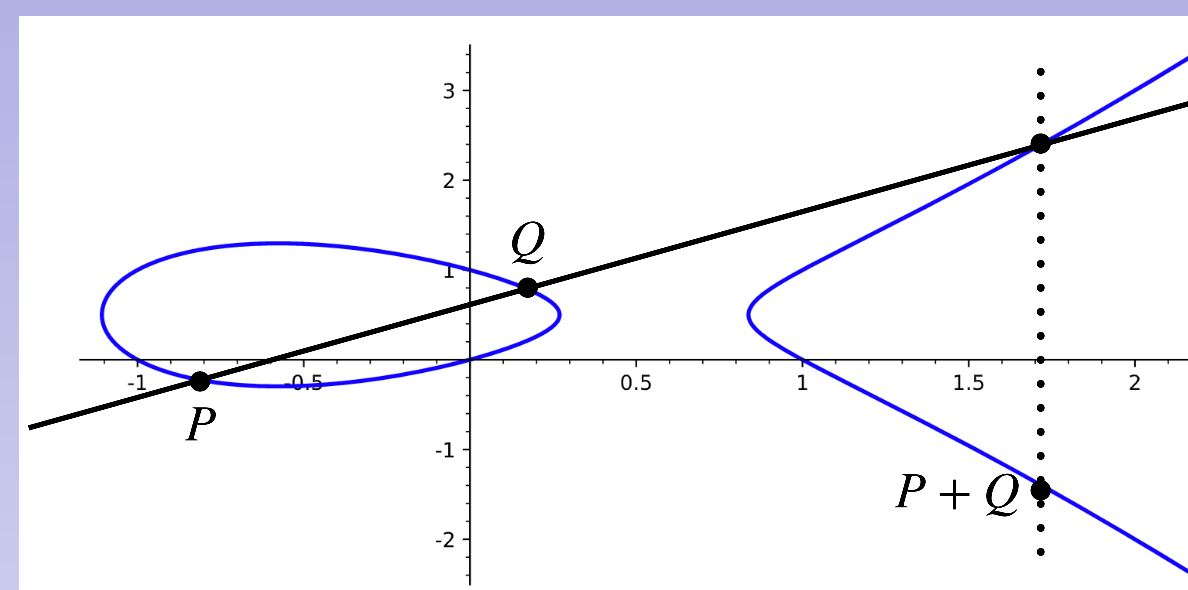
Number theory



Diophantine equations

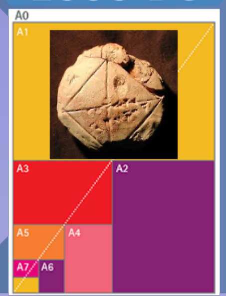
Elliptic curves

$$E : y^2 - y = x^3 - x$$



Number theory

1600 BC

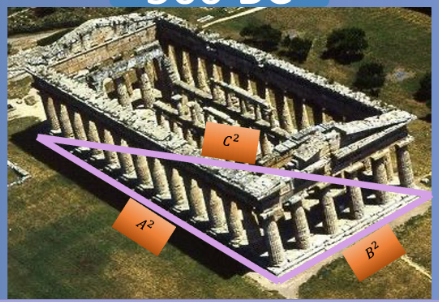


$\sqrt{2}$

Area

x^2-2=0

500 BC



Pythagorean Triples

Architecture

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

1572

Imaginary Numbers

Electricity

$x^2 + 1$=0

1900

Points on Elliptic curves

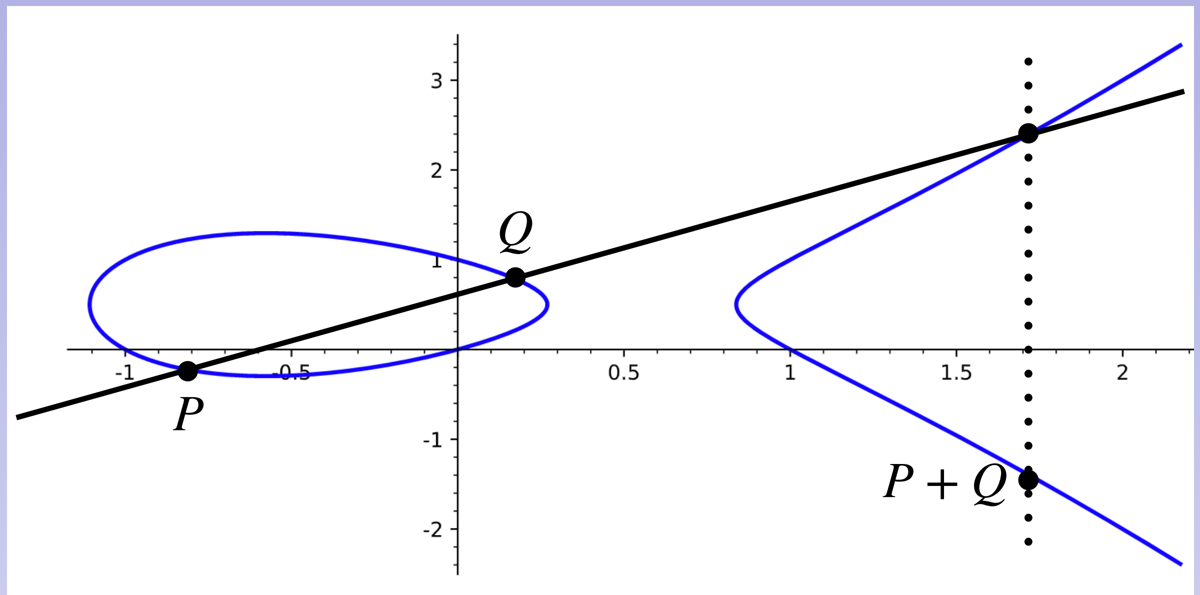
Cryptography

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

Diophantine equations

Elliptic curves

$$E : y^2 - y = x^3 - x$$

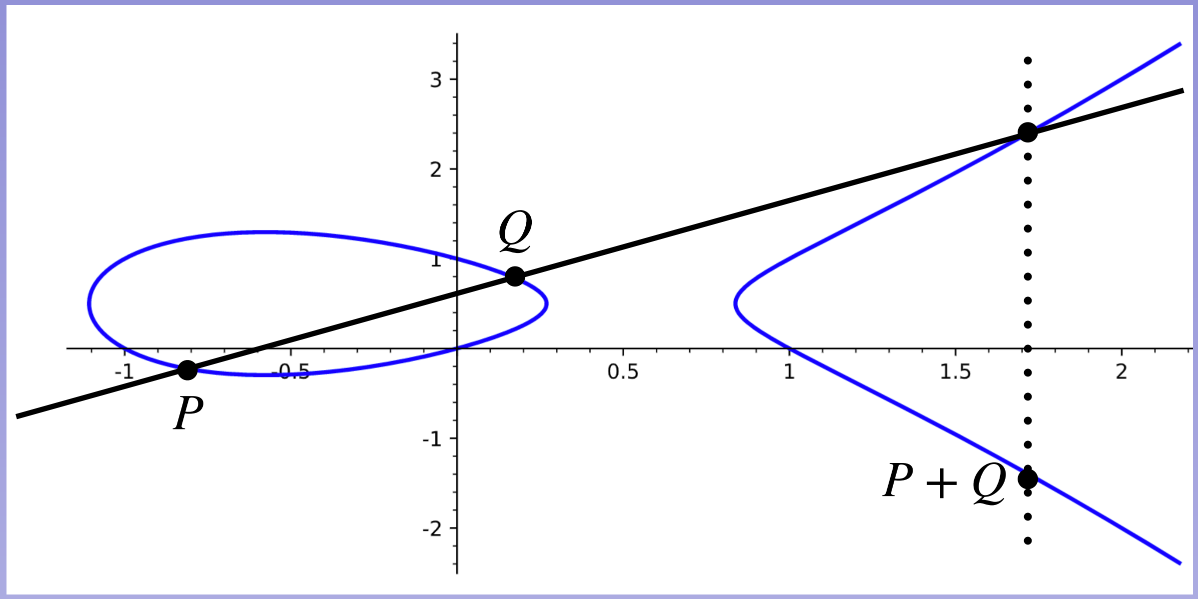


Rank of E is the number of generators

Elliptic curve

Elliptic curves

$$E : y^2 - y = x^3 - x$$

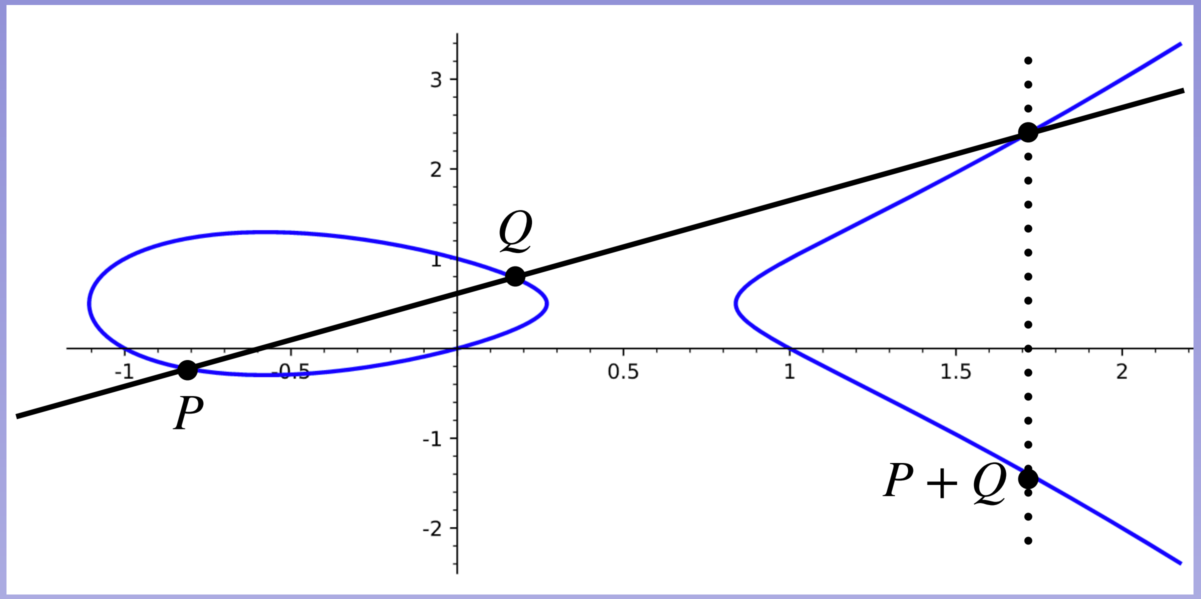


How to compute the rank?

Elliptic curve

Elliptic curves

$$E : y^2 - y = x^3 - x$$



How to compute the rank?

ABOUT PROGRAMS MILLENNIUM PROBLEMS PEOPLE PUBLICATIONS EVENTS EUCLID

Birch and Swinnerton-Dyer Conjecture

Mathematicians have always been fascinated by the problem of describing all solutions in whole numbers x,y,z to algebraic equations like

$$x^2 + y^2 = z^2$$

Euclid gave the complete solution for that equation, but for more complicated equations this becomes extremely difficult. Indeed, in 1970 Yu. V. Matiyasevich showed that Hilbert's tenth problem is unsolvable, i.e., there is no general method for determining when such equations have a solution in whole numbers. But in special cases one can hope to say something. When the solutions are the points of an abelian variety, the Birch and Swinnerton-Dyer conjecture asserts that the size of the group of rational points is related to the behavior of an associated zeta function ζ(s) near the point s=1. In particular this amazing conjecture asserts that if ζ(1) is equal to 0, then there are an infinite number of rational points (solutions), and conversely, if ζ(1) is not equal to 0, then there is only a finite number of such points.

This problem is: Unsolved

Rules:

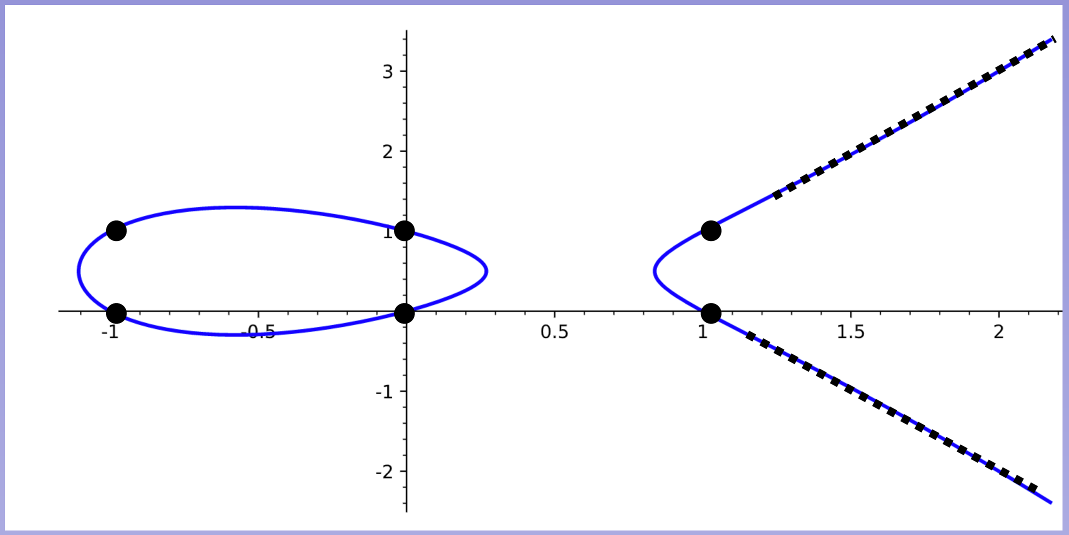
Rules for the Millennium Prizes

Related Documents:

Official Problem Description

Elliptic curve

$$E : y^2 - y = x^3 - x$$

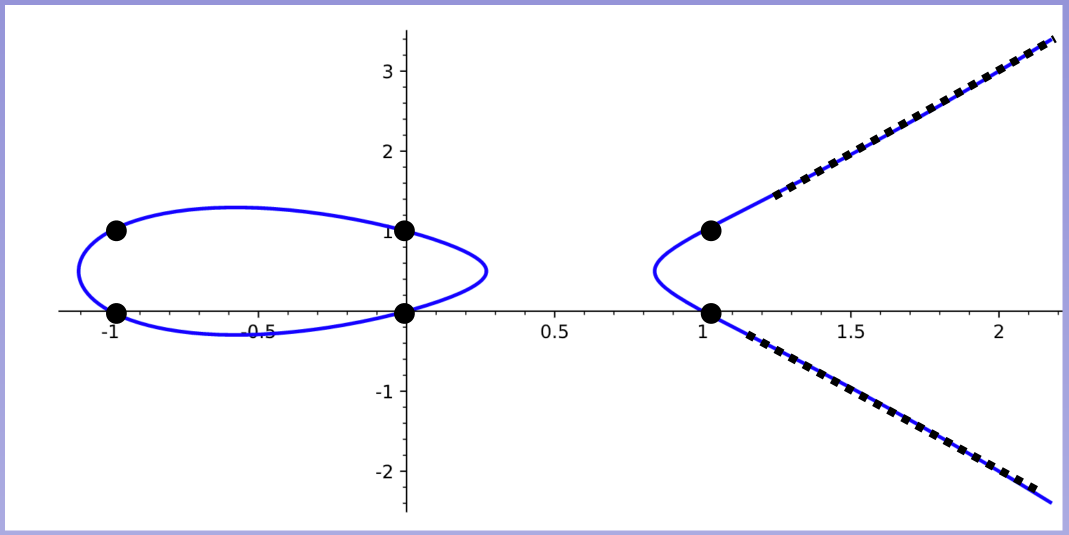


Try all possible values

...,-10,-9,-8,-7,-6,-5,-4,-3,-2,-1,0,1,2,3,4,5,6,7,8,9,10,...

Elliptic curve

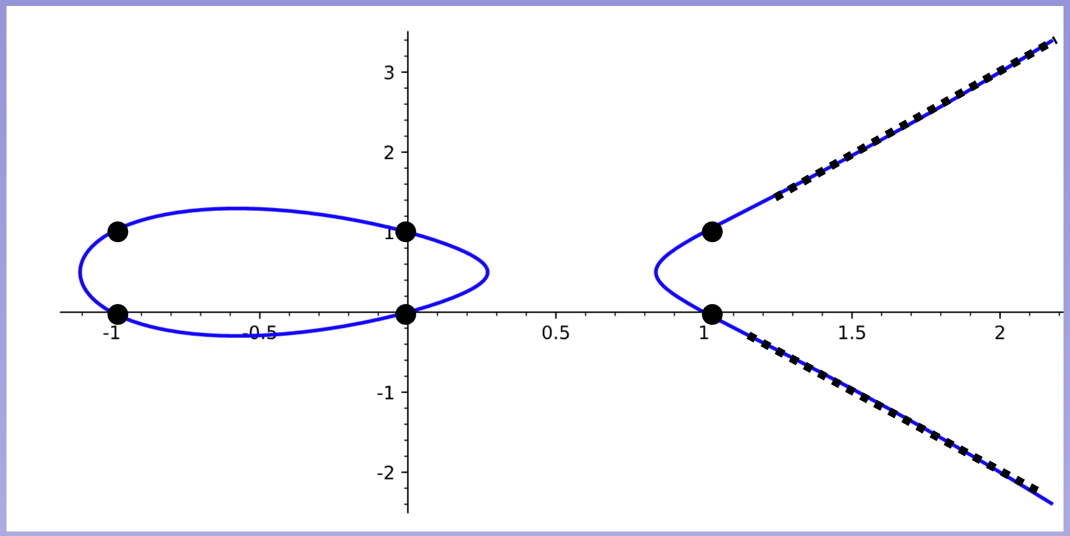
$$E : y^2 - y = x^3 - x$$



Modular arithmetic

Elliptic curve

$$E : y^2 - y = x^3 - x$$

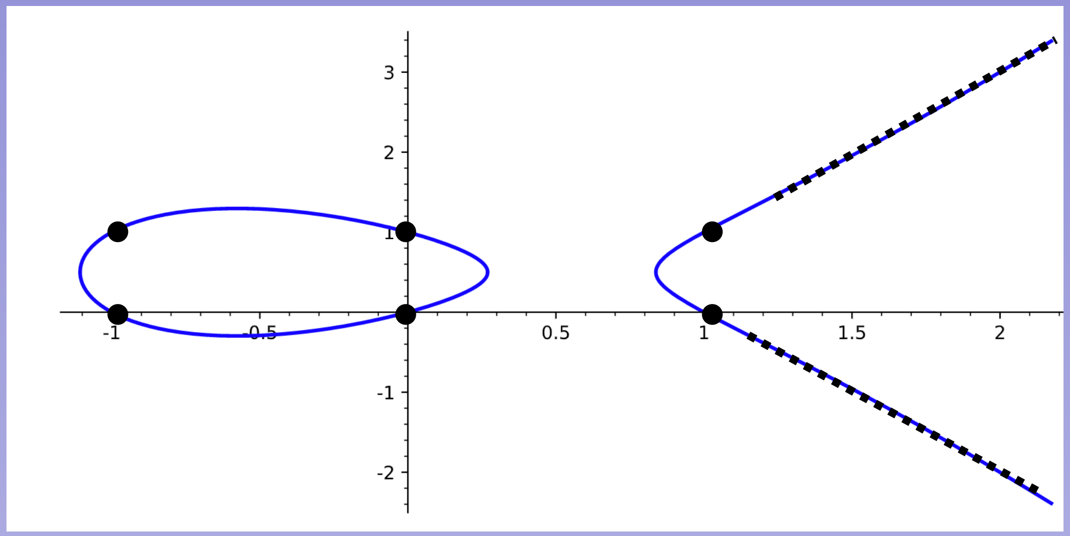


Modular arithmetic

0,1,2,3,4,5,6,7,8,9,10,11

Elliptic curve

$$E : y^2 - y = x^3 - x$$



Modular arithmetic

$p = 3 \quad \{0,1,2\}$

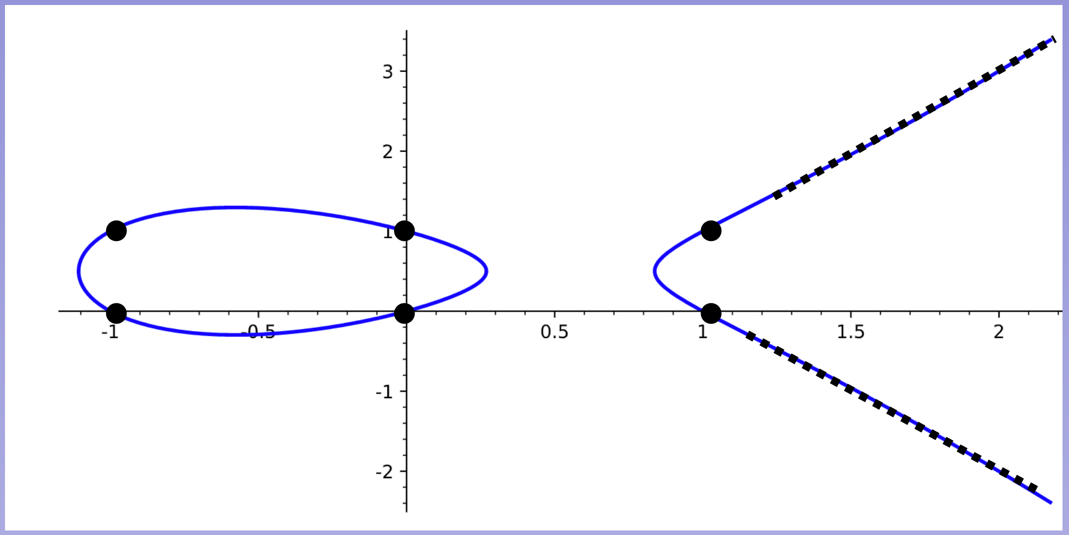
$p = 5 \quad \{0,1,2,3,4\}$

$p = 11 \quad \{0,1,2,3,4,5,6,7,8,9,-1\}$

$\vdots$

Elliptic curve

$$E : y^2 - y = x^3 - x$$



Modulo 3

$p = 3 \quad \{0,1,2\}$

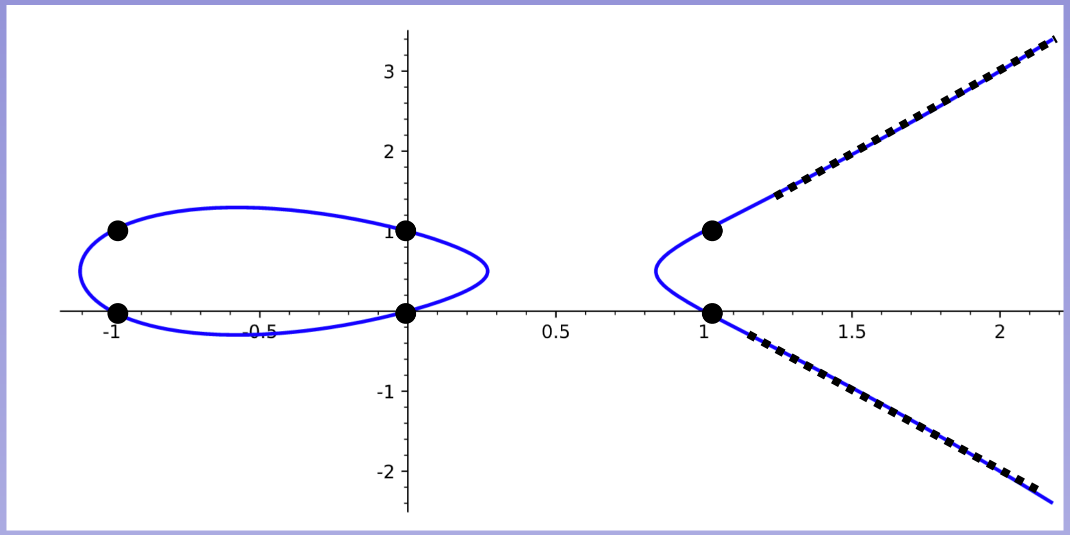
$x \in \{0,1,2\}, y \in \{0,1,2\}$

$$(0,0), (0,1), (1,0), (1,1), (2,0), (2,1)$$

6 points modulo 3

Elliptic curve

$$E : y^2 - y = x^3 - x$$



Modulo p

$$x \in \{0,1,2..p-1\}, y \in \{0,1,2..p-1\}$$

Np points modulo p

Birch and Swinnerton-Dyer

Consider all p up to X

$$\prod_{p \leq X} \frac{Np}{p}$$

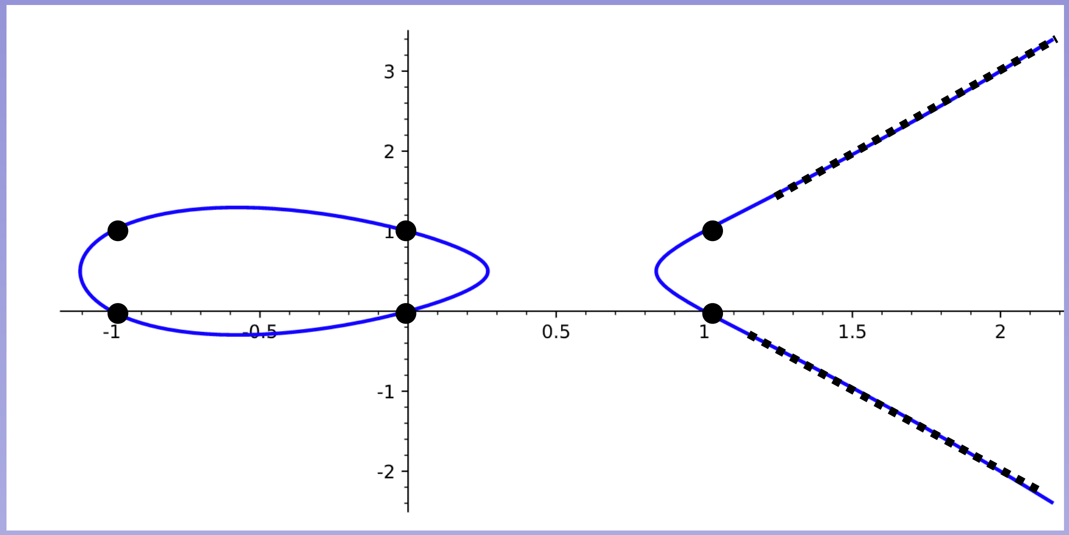
Birch and Swinnerton-Dyer

Consider all p up to X

$$\prod_{p \leq X} \frac{Np}{p} \simeq C \cdot log(X)^{Rk}$$

Birch and Swinnerton-Dyer

$$E : y^2 - y = x^3 - x$$



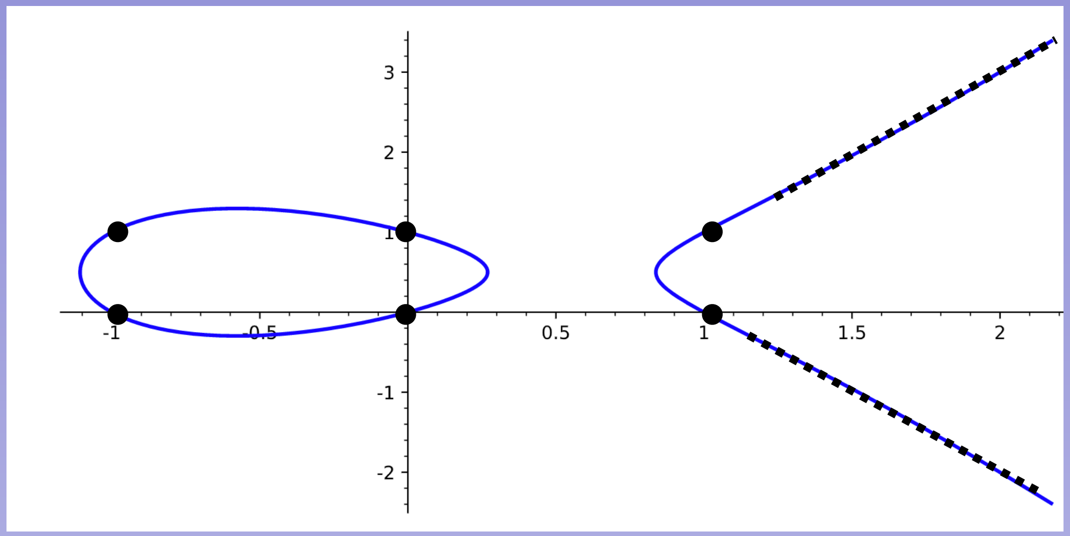
Consider all p up to X

$$\prod_{p \leq X} \frac{Np}{p} \simeq C \cdot log(X)^{Rk}$$

Rk is the rank of the curve

Elliptic curve

$$E : y^2 - y = x^3 - x$$

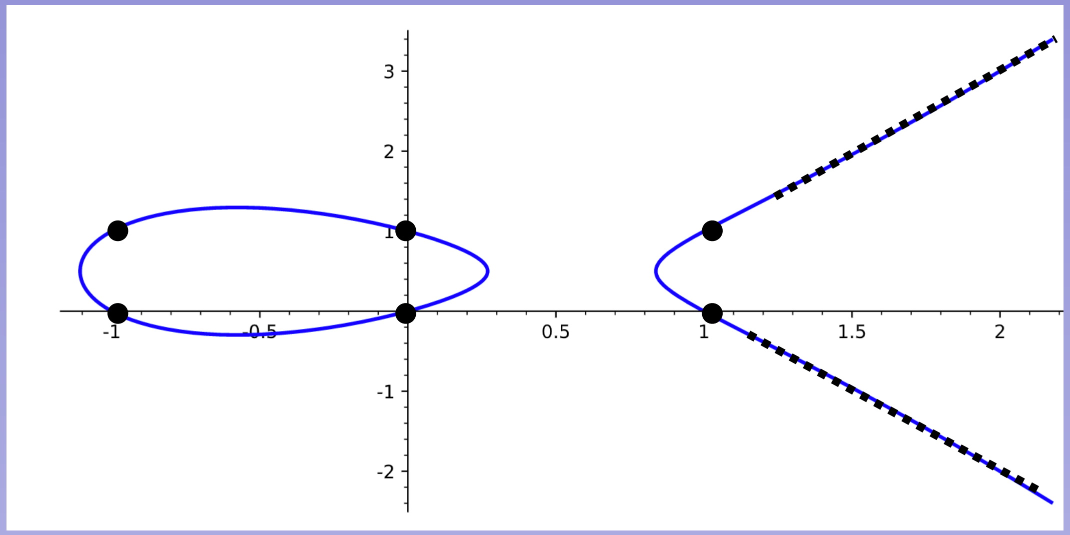


L-function

$$L(E,s)^* = \prod_p \frac{1}{1 - a\,.\,p^{-s} + p^{1-2s}}, \quad a = p + 1 - Np$$

Elliptic curve

$$E : y^2 - y = x^3 - x$$



L-function

$$L(E,s)^* = \prod_p \frac{1}{1 - a\,.\,p^{-s} + p^{1-2s}}, \quad a = p + 1 - Np$$

$$L(E,1)'' ='' \prod_p \frac{p}{Np}$$

Birch and Swinnerton-Dyer conjecture (1966):

Let E be an elliptic curve over $\mathbb{Q}$. Then the rank of $E(\mathbb{Q})$ is equal to the order of vanishing of $L(E, s)$ at $s = 1$.

$$E : y^2 - y = x^3 - x$$

$$L(E, s)^* = \prod_p \frac{1}{1 - a \,.\, p^{-s} + p^{1-2s}}, \quad a = p + 1 - Np$$

ABOUT PROGRAMS MILLENNIUM PROBLEMS PEOPLE PUBLICATIONS EVENTS EUCLID

Birch and Swinnerton-Dyer Conjecture

Mathematicians have always been fascinated by the problem of describing all solutions in whole numbers x,y,z to algebraic equations like

$$x^2 + y^2 = z^2$$

Euclid gave the complete solution for that equation, but for more complicated equations this becomes extremely difficult. Indeed, in 1970 Yu. V. Matiyasevich showed that Hilbert's tenth problem is unsolvable, i.e., there is no general method for determining when such equations have a solution in whole numbers. But in special cases one can hope to say something. When the solutions are the points of an abelian variety, the Birch and Swinnerton-Dyer conjecture asserts that the size of the group of rational points is related to the behavior of an associated zeta function ζ(s) near the point s=1. In particular this amazing conjecture asserts that if ζ(1) is equal to 0, then there are an infinite number of rational points (solutions), and conversely, if ζ(1) is not equal to 0, then there is only a finite number of such points.

This problem is: Unsolved

Rules:

Rules for the Millennium Prizes

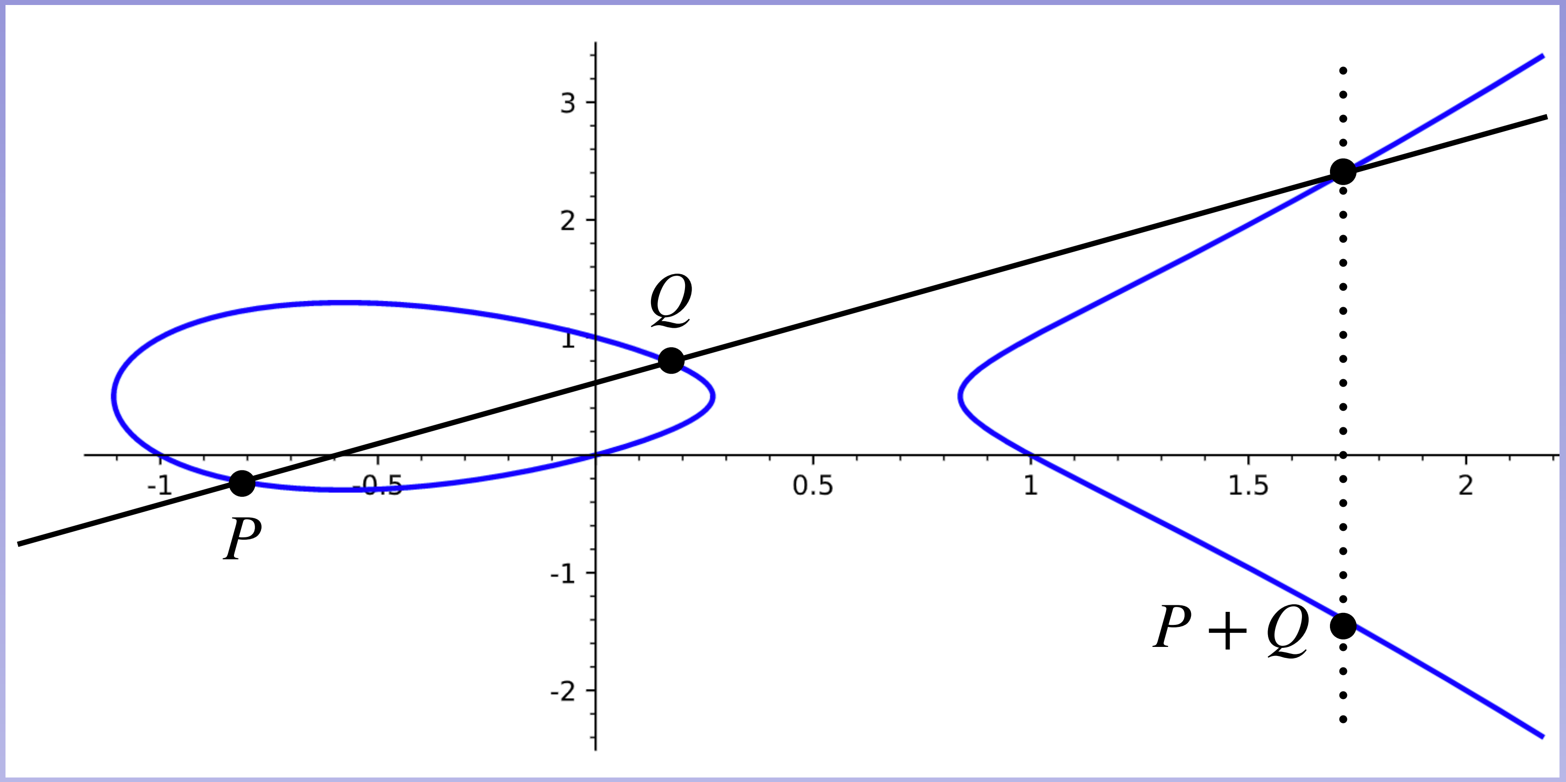
Related Documents:

Official Problem Description

https://research.reading.ac.uk/lms-women-in-maths-2022/

Thank you !

Ranks of elliptic curves



Mordell's Theorem (1922):

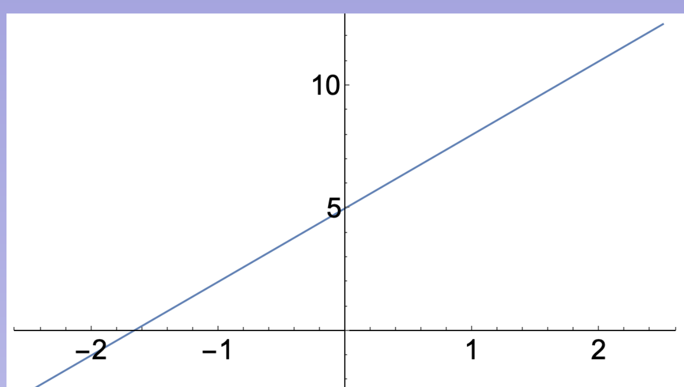
The set of rational points on an elliptic curve $E/\mathbb{Q}$ is a finitely generated group:

$$E(\mathbb{Q}) \simeq \mathbb{Z}^{rk_E} \times T, \text{ where } |T| < \infty.$$

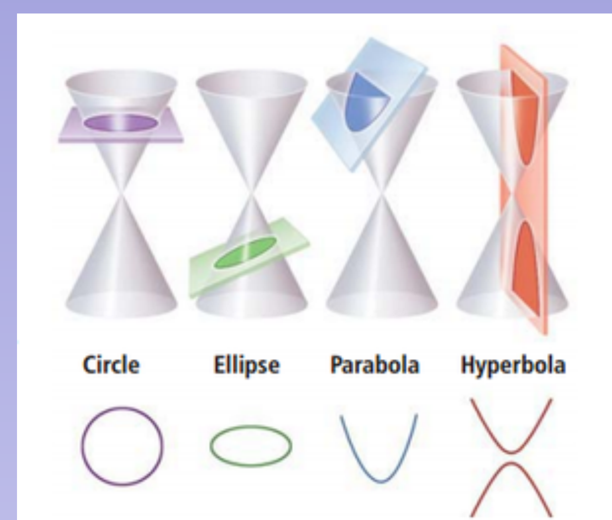
Why Elliptic curves ?

Faltings' Theorem (1983)

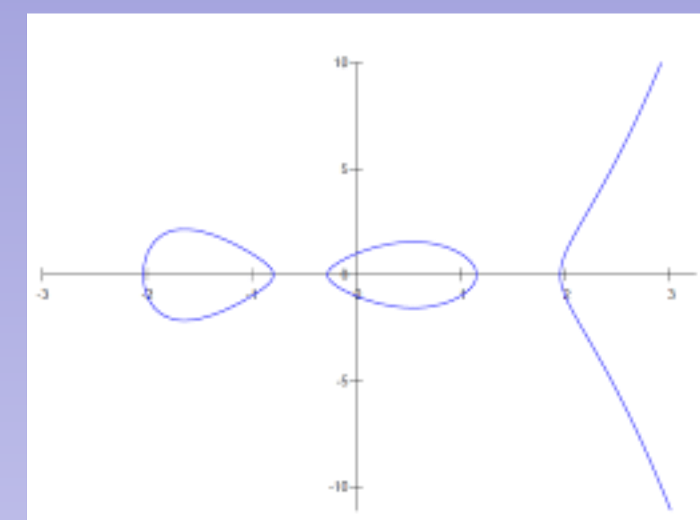
Except for linear equations, conic sections and elliptic curves, all other curves have **finitely many rational solutions**.



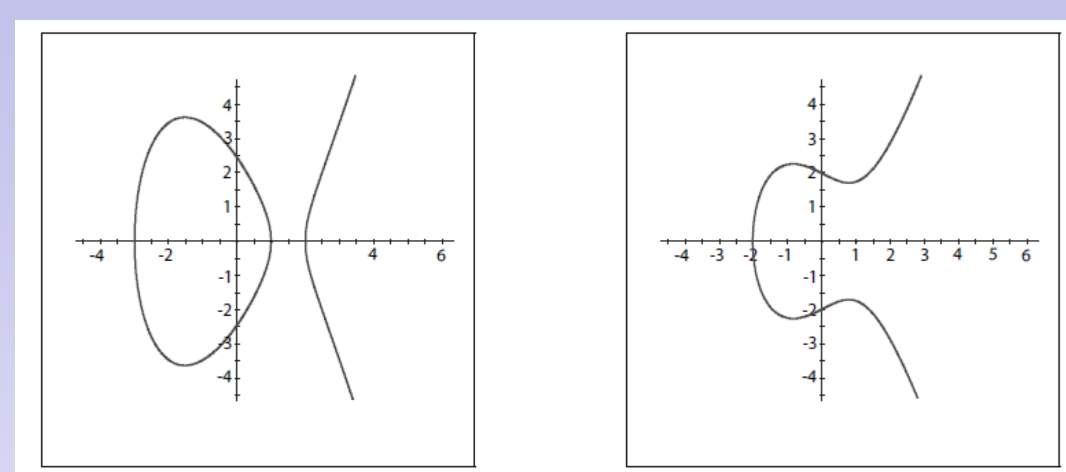
✓



✓



$|C(\mathbb{Q})| < \infty$



$E(\mathbb{Q})$?