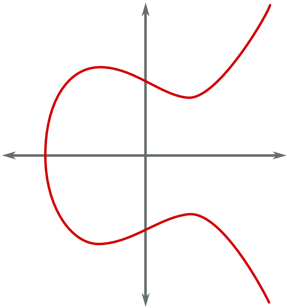
Kummer theory for elliptic curves

Sebastiano Tronto

UNIVERSITÉ DU LUXEMBOURG

Universiteit Leiden

Elliptic curves



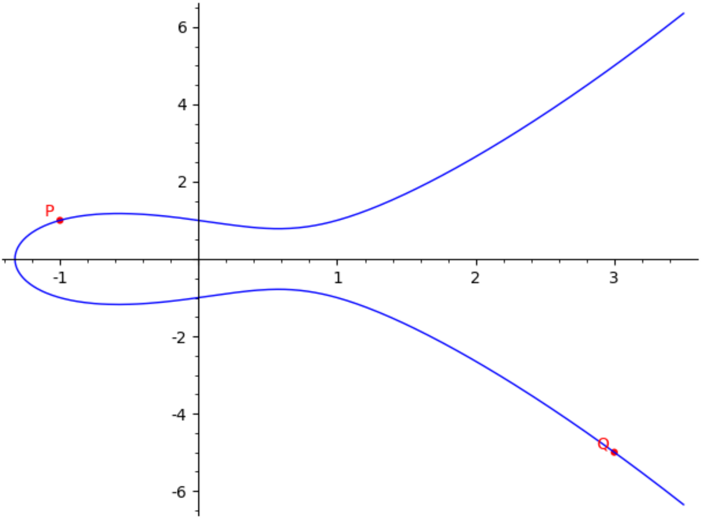
$$y^2 = x^3 - x + 1$$

Figure: An elliptic curve with its defining equation

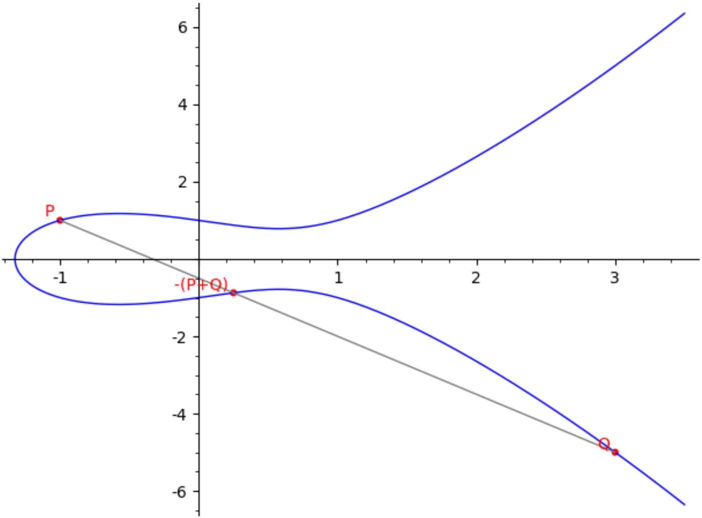
Elliptic curves: applications

- Elliptic curve cryptography
- Post-quantum cryptography
- Prime factorization and primality testing algorithms

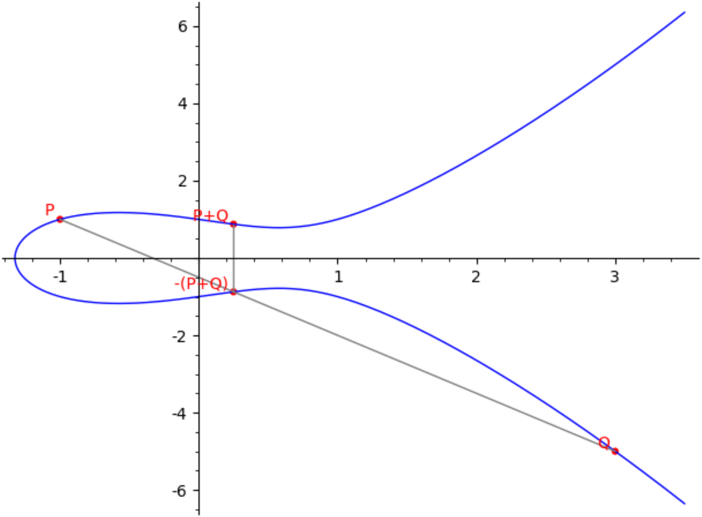
Adding points on elliptic curves



Adding points on elliptic curves

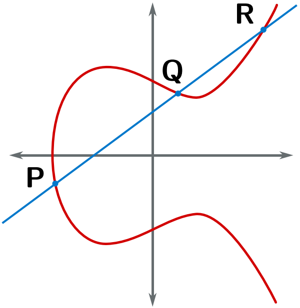


Adding points on elliptic curves



Summing points on elliptic curves

- More complex than “normal” numbers, simple enough to apply
- ECDH: *discrete logarithm problem*
- Smaller keys, same security



$$\mathbf{P} + \mathbf{Q} + \mathbf{R} = \mathbf{0}$$

Equations

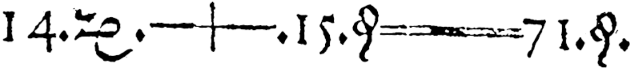
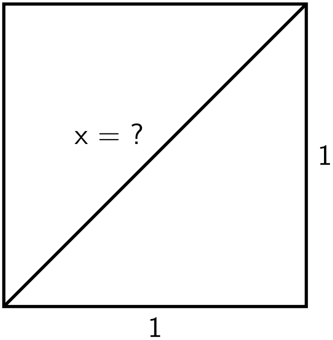


Figure: The first use of the equals sign (1557) [*Source: Wikipedia*]

Pythagora's secret

Equation: $x^2 = 2$

- Solution:
  $x = \sqrt{2} = 1.4142135\ldots$
- But $\sqrt{2}$ is *irrational*



Inventing new numbers

We extend the rational numbers $\mathbb{Q}$ to:

$$\mathbb{Q}[\sqrt{2}] = \{a + b \cdot \boxed{\sqrt{2}} \text{ for } a, b \in \mathbb{Q}\}$$

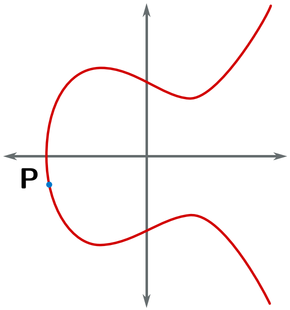
With the rule: $\boxed{\sqrt{2}}^2 = 2$

Example:

$$(1 + 2 \cdot \boxed{\sqrt{2}}) \cdot (3 \cdot \boxed{\sqrt{2}}) = 3 \cdot \boxed{\sqrt{2}} + 6 \cdot \boxed{\sqrt{2}}^2 = 12 + \boxed{\sqrt{2}}$$

Elliptic curves and equations

Equation (unknown Q): $\quad Q + Q = P$



- Does a solution exist?
- If not, how expensive is it to "invent"?

Degree of extensions

- Rational numbers: $\mathbb{Q}[\sqrt[n]{2}]$ has degree n or less
- Elliptic curves: $\mathbb{Q}[\frac{1}{n}P]$ has degree n^2 or less

In both cases, the degree cannot be *much* less... but *how much?*

Kummer theory for elliptic curves

Theorem (Ribet, 1971)

The degree of $\mathbb{Q}[\frac{1}{n}P]$ *is greater than* $\frac{1}{c}n^2$*, for some constant* c *depending on the chose curve.*

Theorem (Lombardo and Tronto, 2021)

The degree of $\mathbb{Q}[\frac{1}{n}P]$ *is greater than* $\frac{1}{c}n^2$*, where*

$$c = 2^{28} \cdot 3^{18} \cdot 5^8 \cdot 7^7 \cdot 11^5 \cdot 13 \cdot 17 \cdot 19 \cdot 37 \cdot 43 \cdot 67 \cdot 163$$

(Remark: both theorems require some restrictions on P*)*

Further results

- Similar results for base fields other than $\mathbb{Q}$
- A *general framework* (Tronto, 2022) unifying our results with those of Javan Peykar
- Possible future work on higher-dimensional *abelian varieties*

Thank you for your attention