Arithmetic of elliptic curves

Brendan Creutz
University of Canterbury
NZMRI Summer Meeting 2021

The Motivating Problem

Problem

Given polynomials $f_1, \ldots, f_m \in \mathbb{Q}[x_1, \ldots, x_n]$ (how) can we

- decide if there exists $\mathbf{a} \in \mathbb{Q}^n$ such that $f_i(\mathbf{a}) = 0$ for all i?
- describe/determine the set of all such rational solutions?

Remarks

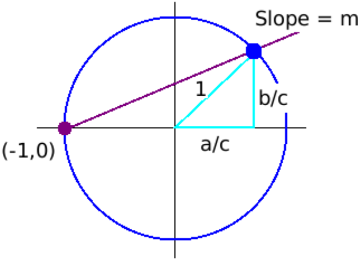
- There is no proven algorithm for answering these questions, already in the case of a single polyomial of degree 3 in 2 variables.
- Can replace $\mathbb{Q}$ with other rings, e.g., $\mathbb{C}$, $\mathbb{F}_p$, $\mathbb{Z}$, $\mathbb{Q}_p$, $\ldots$

Equations of degree 2

Example

Pythagorean triples correspond to rational solutions to
$x^2 + y^2 - 1 = 0$

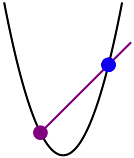
Plimpton Tablet 1800BC



- If we have one rational point, then we can parameterize all others. In particular, there will be infinitely many.

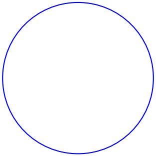
Equations of degree 2

This works for any conic...



$y = x^2$

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



$x^2 + y^2 = 3$

... provided you can find a rational point to get things going.

Local obstructions to rational points

Example

The curve $C : x^2 + y^2 - 3 = 0$ has no rational points because there is a local obstruction at the prime $p = 3$ (i.e., $C(\mathbb{Q}_3) = \emptyset$).

1. Suppose there is a rational solution.
2. Clearing denominators gives an integral solution to

$$X^2 + Y^2 = 3Z^2$$

   which implies X, Y, Z are all divisible by 3.
3. Remove this common factor and repeat...

Theorem (Legendre, Minkowski, Hasse)

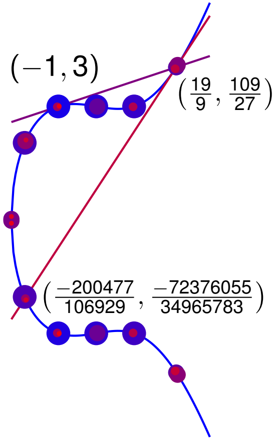
A quadric hypersurface has $\mathbb{Q}$-rational points if and only if there is no local obstruction.

Equations of degree 3

Example (Diophantus, ca 300AD)

There are infinitely many rational points on the curve

$$C : y^2 = x^3 - x + 9$$

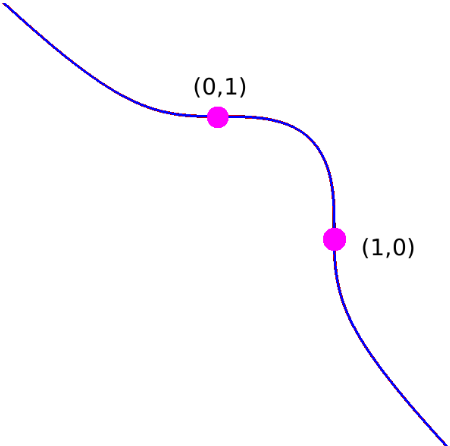


Equations of degree 3

Example (Fermat, 1637)

There are only finitely many rational points on the curve

$$C : x^3 + y^3 = 1$$



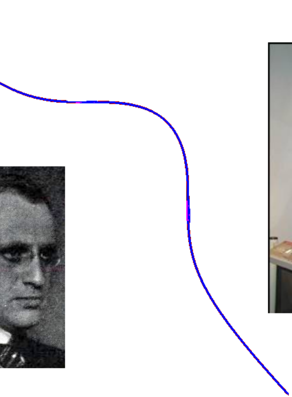
Equations of degree 3

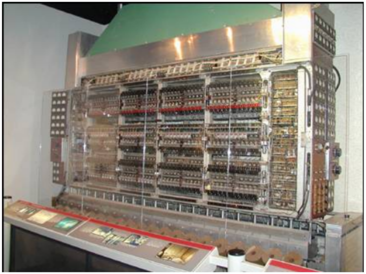
Example (Failure of the Hasse Principle, Selmer 1951)

The curve

$$C : 3x^3 + 4y^3 = 5$$

has no local obstruction, but also no rational points.

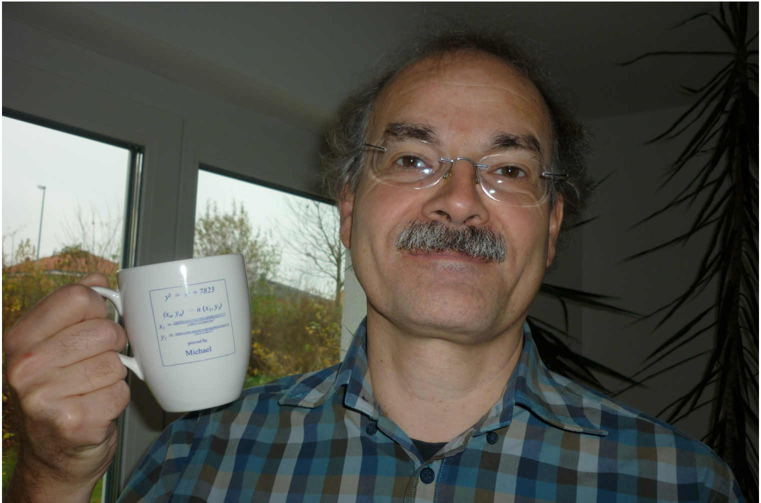




Equations of degree 3

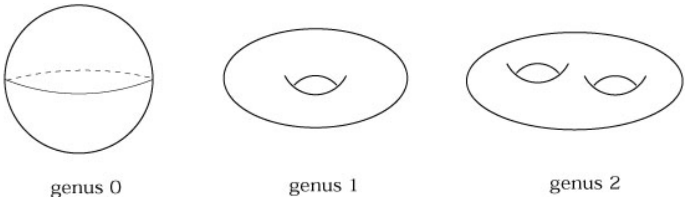
Example (Stoll, 2002)

The curve $C : y^2 = x^3 + 7823$ has infinitely many rational points.



Geometry Determines Arithmetic

Over $\mathbb{C}$ algebraic curves are classified topologically by their genus:



Degree	1 or 2	3	≥ 4
Genus	0	1	≥ 2
$\mathbb{Q}$-points	$C(\mathbb{Q}) = \emptyset$ or $C(\mathbb{Q}) \simeq \mathbb{P}^1(\mathbb{Q})$	$0 \leq \#C(\mathbb{Q}) \leq \infty$	$C(\mathbb{Q})$ is finite (Faltings 1984)
Algorithm?	Known < 1800	Conjectured ca. 1960	Conjectured Poonen/Stoll '06

Genus 1 Curves With Rational Points

Definition

An elliptic curve is a genus one curve with a rational point.

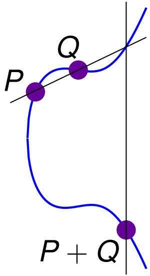
Every elliptic curve can be defined by an equation of the form

$$E : y^2 = x^3 + ax + b \quad \text{with } a, b \in \mathbb{Q} \text{ such that } 4a^3 - 27b^2 \neq 0.$$

Theorem (Mordell 1922)

The set $E(\mathbb{Q})$ of rational points on an elliptic curve forms a finitely generated abelian group. Hence,

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \times T, \text{ with } T \text{ finite.}$$



Proof of Mordell's Theorem

Theorem

For any elliptic curve $E/\mathbb{Q}$, the abelian group $E(\mathbb{Q})$ is finitely generated.

The proof has two steps:

1. Reduce to proving that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.
   - Uses the theory of heights
   - This step is effective: given $\#E(\mathbb{Q})/2E(\mathbb{Q})$ there is an algorithm to determine $E(\mathbb{Q})$ and find generators.
2. Prove that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.
   - It is an open question whether this step can be made effective. There is a procedure which is conjectured to always work.

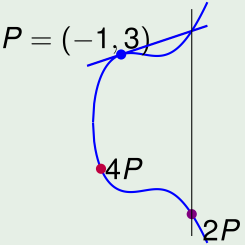
Height of a point

The height of a point $P \in E(\mathbb{Q})$ is (roughly) the number of digits required to write down its x-coordinate.

$$\text{If } P = \left(\frac{p}{q}, y\right), \text{ then } H(P) = \log(\max\{|p|, |q|\}).$$

Example (Diophantus' curve)

n	$x(nP)$	$H(nP)$
1	-1	0
2	$19/9$	2.94
3	$785/196$	6.67
4	$-200477/106929$	12.21



- $H : E(\mathbb{Q}) \to \mathbb{R}$ behaves like a quadratic form:
  1. $H(mP) \sim m^2 H(P)$
  2. $H(P + Q) + H(P - Q) \sim 2H(P) + 2H(Q)$

Step 1 of the proof

Claim: If $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite, then $E(\mathbb{Q})$ is finitely generated.
Proof:

- Choose coset reps $Q_1, \ldots Q_n$ for $E(\mathbb{Q})/2E(\mathbb{Q})$
- Let $S = \{P \in E(\mathbb{Q}) \mid H(P) \leq \max(H(Q_i))\}$.
- If S does not generate $E(\mathbb{Q})$, choose $R \in E(\mathbb{Q}) - \langle S \rangle$ of minimal height.
- Write $R - Q_i = 2P$. Note $P \notin \langle S \rangle$.
- Use properties of heights to show $H(P) < H(R)$:

$$\begin{aligned} 4H(P) &= H(2P) = H(R - Q_i) \\ &\leq H(R - Q_i) + H(R + Q_i) = 2H(R) + 2H(Q_i) < 4H(R) \end{aligned}$$

Step 2: Proof of finiteness of $E(\mathbb{Q})/2E(\mathbb{Q})$

Consider the special case where the cubic has 3 rational roots:

$$E\colon\ y^2 = (x - e_1)(x - e_2)(x - e_3)\,, \quad e_i \in \mathbb{Q}.$$

- For any $P \in E(\mathbb{Q})$ there are unique square free integers δ_1, δ_2 and $z_i \in \mathbb{Q}$ unique up to sign such that

$$\begin{aligned} x(P) - e_1 &= \delta_1 z_1^2 \qquad\qquad & y = \delta_1\delta_2 z_1 z_2 z_3 \\ x(P) - e_2 &= \delta_2 z_2^2 & \\ x(P) - e_3 &= \delta_1\delta_2 z_3^2 & \end{aligned}$$

- If the e_i are distinct modulo p, then $p \nmid \delta_i$. So there are only finitely many possibilities for δ_1, δ_2.
- The map $\delta : E(\mathbb{Q}) \to \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \times \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ is a homomorphism with kernel $2E(\mathbb{Q})$.

Geometric interpretation

- The equations can be rearranged to give:

$$Q_1(\mathbf{z}) = Q_2(\mathbf{z}) = 0, \quad (x, y) = (f_1(\mathbf{z}), f_2(\mathbf{z}))$$

  defining a genus 1 curve $C_\delta \subset \mathbb{P}^3$ and a map $\pi_\delta : C_\delta \to E$.
- When $\delta = (1, 1)$, $C_\delta \simeq E$ and π_δ is multiplication by 2.
- For varying δ these give a partition:

$$E(\mathbb{Q}) = \coprod_\delta \pi_\delta(C_\delta(\mathbb{Q})) \quad \text{where } \pi_\delta(C_\delta(\mathbb{Q})) = \begin{cases} \emptyset \\ \text{coset of } 2E(\mathbb{Q}) \end{cases}$$

- All but finitely many of the C_δ have $C_\delta(\mathbb{Q}) = \emptyset$ due to a local obstruction.
- Some $C_\delta(\mathbb{Q})$ may be empty even though there is no local obstruction (so the proof is not effective unless we know how to decide if the genus one curves C_δ have rational points).

Rational Points on genus one curves, a summary

Suppose $C/\mathbb{Q}$ is a genus one curve.

Problem 1:

Decide if $C(\mathbb{Q})$ is nonempty.

- Difficult because local obstructions do not suffice.
- One must define new obstructions and study these (Descent, Brauer-Manin)

Problem 2:

If $C(\mathbb{Q})$ is nonempty, the points form a finitely generated abelian group. Determine the structure and find generators.

- Can be reduced to Problem 1 for a finite collection of auxiliary curves.