Elliptic curves and the BSD conjecture

1. Motivation

▷ Geometry : rational parametrization

- Given an affine plane curve $C = f(x,y)/\mathbb{C}$, does it possess a rational parametrization?
- $\exists$? rational functions $x(t)$, $y(t)$ s.t.

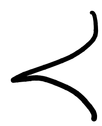
  (1) for almost all $t \in \mathbb{C}$ $f(x(t), y(t)) = 0$

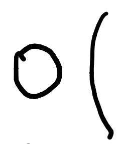
  (2) for almost all $P \in C$ $\exists\, t \in \mathbb{C}$ s.t. $P = (x(t), y(t))$

- **Examples:**

  ① degree 1 : $y = ax+b \Rightarrow (x,y) = (t, at+b)$

  ② degree 2 : $y = x^2 \Rightarrow (x,y) = (t, t^2)$

  ③ degree 3 : $y^2 = x^2(x+1) \Rightarrow (x,y) = (t^2-1, t^3-t)$ 

  $y^2 = x^3 - x \Rightarrow$ impossible 

- **Theorem:** An irreducible affine curve C is rational if and only if it's birationally equivalent to the affine line $\mathbb{A}^1$ $\Leftrightarrow$ $\text{genus}(C) = 0$

- **Take away:** Genus 1 curves are the first example of non-rational curves

▷ Number Theory: Hasse principle

- Given an affine plane curve $C = f(x,y)/\mathbb{Q}$, does it possess a $\mathbb{Q}$-rational point?
- If so, then under the natural embedding of $\mathbb{Q}$, C has a point defined over $\mathbb{R}$ and $\mathbb{Q}_p$ $\forall p$ (global-to-local)
- Easy to check for $\mathbb{R}$; for $\mathbb{Q}_p$ reduces to some finite field by Hensel's Lemma
- Conversely, if C has a point defined over $\mathbb{R}$ and $\mathbb{Q}_p$ $\forall p < \infty$, do they come from a $\mathbb{Q}$-rational point (local-to-global)?
- Hasse principle! True in some cases, e.g. linear & quadratic equations (genus 0)

- **Theorem:** A quadratic form $f(x_1, \dots, x_n) = \sum_{i=1}^{n} a_i x_i^2 / \mathbb{Q}$ represents 0 if and only if it does so over $\mathbb{R}$ and $\mathbb{Q}_p$ $\forall p$

- **Non-example:** $2y^2 = x^4 - 17$ (use Hasse's bound)

- **Takeaway:** Genus 1 curves are the first example of the failure of the Hasse principle

2. Elliptic curves

- **Definition:** An elliptic curve $\mathcal{E}$ over $\mathbb{Q}$ is a smooth projective curve of genus 1 with a $\mathbb{Q}$-rational point $\mho$ known as the origin. More concretely,

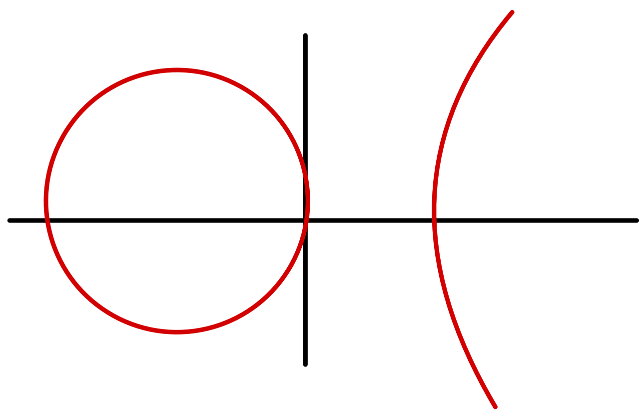
$$\mathcal{E}: y^2 = x^3 + ax + b \qquad a, b \in \mathbb{Q} \qquad D = -16(4a^3 + 27b^2) \neq 0$$

with 1-point-compactification given by $\mho$. In general, Weierstrass equation $\mathcal{E}: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$

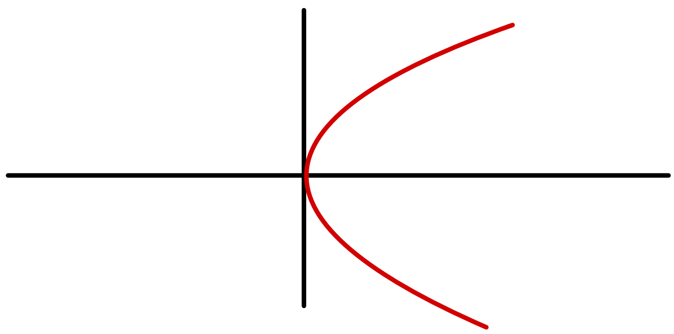
- **Examples:**

① $y^2 = x^3 - x$

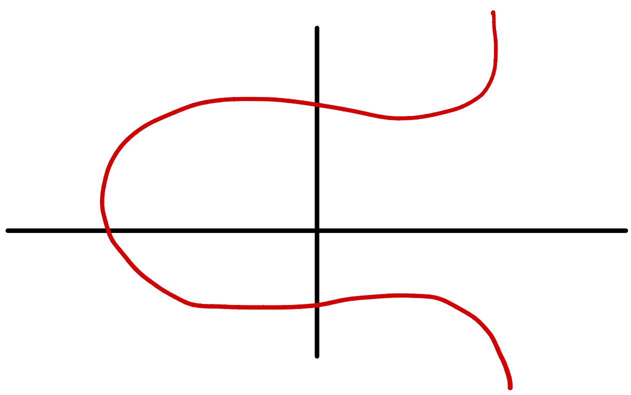
$D > 0$



② $y^2 = x^3 + x$



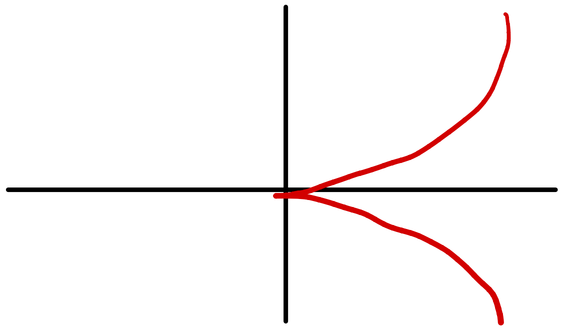
③ $y^2 = x^3 - 3x + 3$



- **Non-examples:**

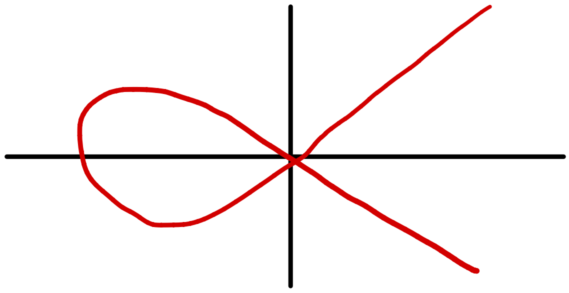
① $y^2 = x^3$

(cuspidal cubic)



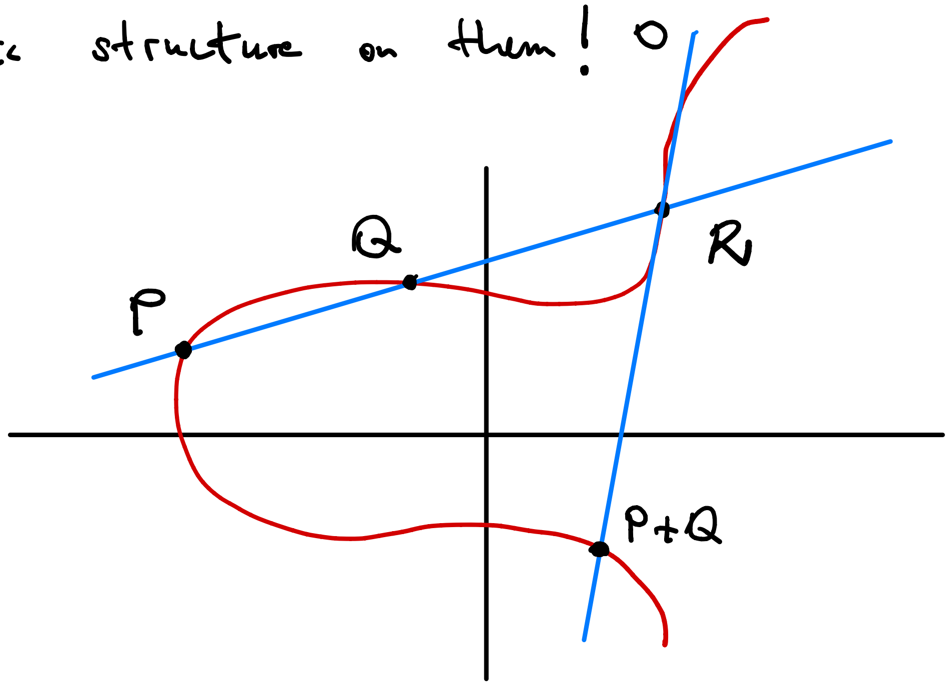
② $y^2 = x^3 + x^2$

(nodal cubic)



- How to study the rational points of $\mathcal{E}$? Impose an algebraic structure on them!

existence, finiteness?



- $\mathcal{E}$ becomes an abelian group!
- $\mathrm{Pic}^0(\mathcal{E}) = \{\text{degree zero divisors on } \mathcal{E}\}/\sim$

$\Rightarrow \mathcal{E} \cong \mathrm{Pic}^0(\mathcal{E})$ under the map $P \to (P) - (\mathcal{O})$

- If $P, Q \in \mathcal{E}(\mathbb{Q})$, then $P + Q \in \mathcal{E}(\mathbb{Q})$ as well, so $\mathcal{E}(\mathbb{Q}) \subset \mathcal{E}$ is a well-defined subgroup (Mordell-Weil)

▷ Rank:

- **Theorem (Mordell '1922):** $\mathcal{E}(\mathbb{Q})$ is a finitely generated abelian group $\Rightarrow \mathcal{E}(\mathbb{Q}) \cong \mathcal{E}(\mathbb{Q})_{tors} \times \mathbb{Z}^r$ where r is called the rank of $\mathcal{E}$
- Proof relies on fundamental results in algebraic number theory:
  1. finiteness of ideal class group
  2. finite generation of units (Dirichlet's unit theorem)
  3. theory of heights
- Drawback is non-effectiveness; cannot determine r! In fact, no known theoretical algorithm to date
- In practice, use 2-descent (mwrank in C++ by J. Cremona)
- If algebraic methods cannot determine r, is there some other way? Yes (conjecturally): analytically via the curve's L-function!

3. L-function

- Every elliptic curve $\mathcal{E}/\mathbb{Q}$ has a (Weierstrass) equation with integer coefficients
- Can be made minimal so that $|\Delta(\mathcal{E})|$ is an integer and as small as possible

- **Example:**

$\mathcal{E}: y^2 = x^3 + 16$ has $\Delta = -2^{12} 3^3$ and isn't minimal.

Substitute $x = 4x'$ and $y = 8y' + 4$ to get

$\mathcal{E}': (y')^2 + y' = (x')^3$ with $\Delta' = -3^3$

- Given a minimal equation for $\mathcal{E}/\mathbb{Z}$, can reduce the coefficients mod p to obtain a curve $/\mathbb{F}_p$
- Define now $a_p := p + 1 - |\tilde{\mathcal{E}}(\mathbb{F}_p)|$
- The resulting curve may have bad reduction, in which case

$$a_p = \begin{cases} 1 & \text{split mult.} \\ -1 & \text{non-split mult.} \end{cases} \Big\} \text{ nodal}$$
$$\qquad \begin{cases} 0 & \text{additive (cuspidal)} \end{cases}$$

- Define

① p good : $L_p(\mathcal{E},s) = (1 - a_p p^{-s} + p^{1-2s})^{-1}$

② p bad :

$$L_p(\mathcal{E},s) = (1 - a_p p^{-s})^{-1} = \begin{cases} (1-p^{-s})^{-1} & \text{split mult.} \\ (1+p^{-s})^{-1} & \text{non-split mult.} \\ 1 & \text{additive} \end{cases}$$

- **Theorem (Hasse's bound):** $|a_p| \leq 2\sqrt{p}$, so

$L(\mathcal{E},s) := \prod_p L_p(\mathcal{E},s)$ converges for $\mathrm{Re}(s) > \frac{3}{2}$

as $L(\mathcal{E},s) \sim \sum n^{\frac{1}{2}-s}$

- **Modularity theorem (Wiles '95):** $\exists$ cuspidal newform $f \in S_2(\Gamma_0(N))$

s.t. $L(\mathcal{E},s) = L(f,s) := \sum_{n>0} a_n n^{-s}$ where

$f = \sum_{n>0} a_n q^n$, so $L(\mathcal{E},s)$ has an analytic

continuation to all of $\mathbb{C}$ (Hecke's integral

representation $L(f,s) = \int_0^\infty f(iy)\, y^{s-1}\, dy$

as Mellin transform) and functional equation $s \leftrightarrow 2-s$

4. BSD conjecture

- Relates algebraic rank of $\mathcal{E}(\mathbb{Q})$ to analytic properties of $L(\mathcal{E}, s)$

- **Conjecture (Birch-Swinnerton-Dyer, 1960s)**

① Rank: $r_{alg}(\mathcal{E}) = \mathrm{ord}_{s=1} L(\mathcal{E}, s) := r_{an}(\mathcal{E})$

② Leading coefficient: for $r = r_{an}(\mathcal{E})$

$$\frac{L^{(r)}(\mathcal{E}, 1)}{r!} = \frac{\Omega_{\mathcal{E}} R_{\mathcal{E}} \prod_p c_p \, |Sha(\mathcal{E})|}{|\mathcal{E}(\mathbb{Q})_{tors}|^2}$$

- $\Omega_{\mathcal{E}} = \displaystyle\int_{\mathcal{E}(\mathbb{R})} \frac{dx}{2y + a_1 x + a_3}$ -> period of $\mathcal{E}$

- $R_{\mathcal{E}} = \det(\langle P_i, P_j \rangle)$ -> regulator of $\mathcal{E}$

- $c_p = [\mathcal{E}(\mathbb{F}_p) : \mathcal{E}_0(\mathbb{F}_p)]$ -> local Tamagawa numbers measuring bad reduction, so $c_p = 1$ for all but finitely many p

- $Sha(\mathcal{E})$ -> group measuring the failure of the Hasse principle (conjecturally finite)

- Tate, 1974: "This remarkable conjecture relates the behavior of a function L at a point where it is not at present known to the order of a group Sha which is not known to be finite!"

- Discovered with computer calculations at Cambridge in the 1960s
- Initial skepticism by Cassels (Birch's PhD advisor), but plenty of numerical evidence has backed it up

5. Current status

- **Theorem (Gross-Zagier, Kolyvagin, 1980s):**

① $r_{an}(E)=0 \Rightarrow r_{alg}(E)=0$

② $r_{an}(E)=1 \Rightarrow r_{alg}(E)=1$

and in these cases both $L^{(r)}(E,1)$ and the finiteness of Sha are known

- Proof uses two ingredients:

① Kolyvagin's Euler system: $r_{an}(E)\leq 1 \Rightarrow r_{alg}(E)\leq r_{an}(E)$

② Gross-Zagier formula: $r_{an}(E)=1 \Rightarrow r_{alg}(E)\geq 1$ by explicit construction of Heegner points on E