An introduction to the Hasse principle

through examples

Álvaro González Hernández

Outline of the talk

1. Motivation
2. p-adic numbers
3. The Hasse principle
4. Elliptic curves
5. Advanced topics

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

$$2y^2 = 1 - 17x^4$$

Hasse ?

Let's study some equations

$$3x + 5y = 1 \qquad x, y \in \mathbb{Q}$$

Let's study some equations

$$3x + 5y = 1 \qquad x, y \in \mathbb{Q}$$

$$(x, y) = \left(t, \tfrac{1-3t}{5}\right) \quad t \in \mathbb{Q}$$

Let's study some equations

$$x^2 + y^2 = 1 \qquad\qquad x, y \in \mathbb{Q}$$

Setting $x = t$ does not work because $y = \sqrt{1 - t^2}$ may not be rational.

Let's study some equations

$$x^2 + y^2 = 1 \qquad x, y \in \mathbb{Q}$$

By using geometric arguments, we can prove that the solutions are either $(x, y) = (-1, 0)$ or $(x, y) = (\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2})$ with $t \in \mathbb{Q}$

Let's study some equations

$$x^2 + y^2 = 0 \qquad x, y \in \mathbb{Q}$$

Let’s study some equations

$$x^2 + y^2 = 0 \qquad x, y \in \mathbb{Q}$$

$$x = 0, \quad y = 0$$

Let's study some equations

$$x^2 - 3y^2 = 2 \qquad x, y \in \mathbb{Q}$$

Let’s study some equations

$$x^2 - 3y^2 = 2 \qquad x, y \in \mathbb{Q}$$

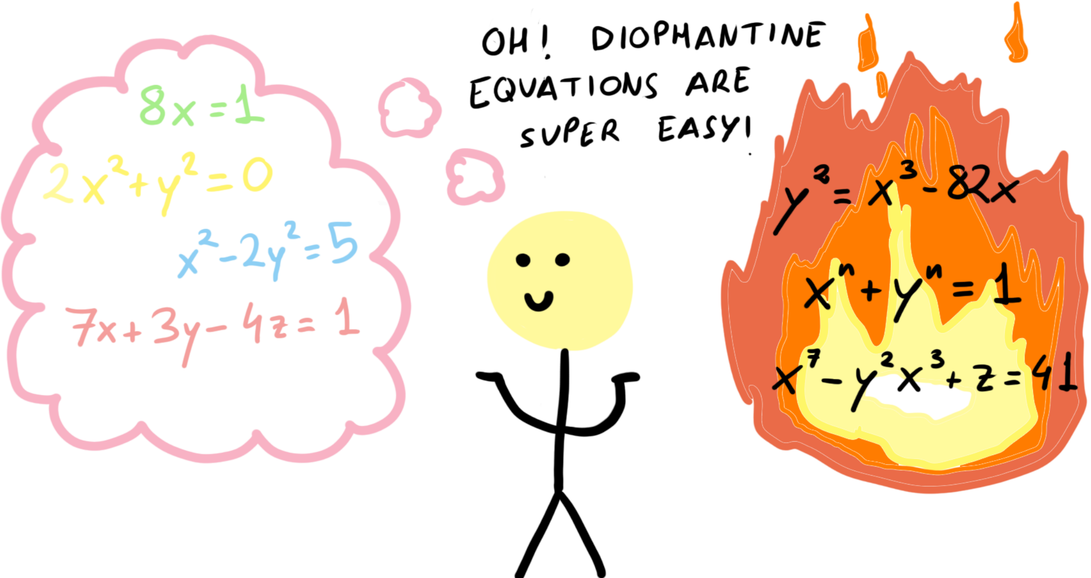
No solutions!

Consider the equivalent equation $X^2 - 3Y^2 = 2Z^2 \qquad X, Y, Z \in \mathbb{Z} \setminus \{0\}$

$X^2 \equiv 2Z^2 \pmod 3$ can only happen if $X \equiv Z \equiv 0 \pmod 3$ because 2 is not a square modulo 3.

This implies that $3|X$, $3|Z$ and $3|Y$. Contradiction!

Let's study some equations



Conclusions of our little study

1. Studying the solutions of Diophantine equations is (generally) **hard**.
2. Finding the **real solutions** of a Diophantine equation can help us determine the existence (or not) of solutions.
3. Considering the homogeneous equations modulo n for appropriate $n \in \mathbb{N}$, we can sometimes determine if an equation does not have integer solutions.

Conclusions of our little study

1. Studying the solutions of Diophantine equations is (generally) **hard**.

2. Finding the **real solutions** of a Diophantine equation can help us determine the existence (or not) of solutions.

3. Considering the equations modulo p^m for an appropriate prime p and $m \in \mathbb{N}$, we can sometimes determine if an equation does not have integer solutions.

Conclusions of our little study

1. Studying the solutions of Diophantine equations is (generally) **hard**.
2. Finding the **real solutions** of a Diophantine equation can help us determine the existence (or not) of solutions.
3. Considering the equations modulo p^m for an appropriate prime p and $m \in \mathbb{N}$, we can sometimes determine if an equation does not have integer solutions.

HOW?

p-adic absolute value

Fix a prime p. Let $x = p^n \frac{a}{b} \in \mathbb{Q}$ non-zero, with $a, b, n \in \mathbb{Z}$ and a, b coprime to p. Then, the ***p*-adic absolute value** of x is defined to be

$$|x|_p = p^{-n}$$

Examples

$$\left| 10 \right|_5 = \frac{1}{5} \qquad \left| \frac{3}{4} \right|_5 = 1 \qquad \left| \frac{1}{125} \right|_5 = 125$$

p-adic numbers

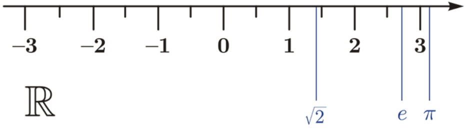
p-adic numbers

The field of ***p*-adic numbers** $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to the absolute value $|\ \ |_p$.

- The completions of $\mathbb{Q}$ with respect to a valuation are known as **local fields** of the ring $\mathbb{Q}$. These are either $\mathbb{R}$ or $\mathbb{Q}_p$ for some p prime.
- The field $\mathbb{Q}$ is known as the **global field** of $\mathbb{R}$ and $\mathbb{Q}_p$.

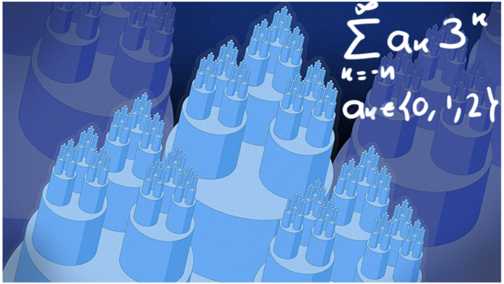
What do local fields look like?

Real numbers



→ Elegant
→ Easy to think of
→ Used by engineers

3-adic numbers

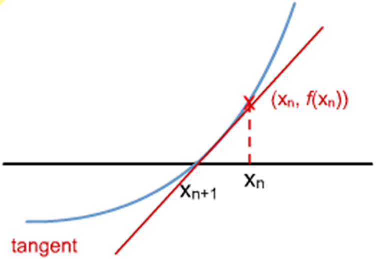


→ Alien looking
→ Mostly used in algebra and number theory

Tools to solving equations

Real numbers

Newton's method



p-adic numbers

Hensel's lemma

polynomial

To solve $x \in \mathbb{Q}_p$ with $f(x) = 0$ we consider the limit of x_n where $x_{n+1} = x_n - \dfrac{f(x_n)}{f'(x_n)}$ for appropriate inicial x_0.

Application of Hensel's lemma

Let $b \in \mathbb{Z}$, $x^2 = b$ has a solution $x \in \mathbb{R}$ iff $b \geq 0$. Let's see what happens in $\mathbb{Q}_p$.

Theorem

The equation $x^2 = b$ has a solution $x \in \mathbb{Q}_2$ if and only if b is of the form $b = 2^{2n} b_0$ with $n \in \mathbb{Z}_{\geq 0}$ and $b_0 \equiv 1 \pmod 8$.

For any odd prime p, the equation $x^2 = b$ has a solution $x \in \mathbb{Q}_p$ if and only if b is of the form $b = p^{2n} b_0$ with $n \in \mathbb{Z}_{\geq 0}$ and b_0 a quadratic residue modulo p (this means $b_0 \equiv a_0^2 \pmod p$ for some a_0).

Example of application of this theorem

$x^2 = 17$ for some $x \in \mathbb{Q}_2$, as $17 \equiv 1 \pmod 8$.
$x^2 = 2$ for some $x \in \mathbb{Q}_{17}$, as $6^2 \equiv 2 \pmod{17}$.

Hasse Principle

No solution in $\mathbb{Q}_p$ for some p or no solution in $\mathbb{R}$ $\Rightarrow$ No solution in $\mathbb{Q}$.

Hasse Principle (The converse statement)

If a system of polynomial equations with rational coefficients has a solution in $\mathbb{R}$ and in $\mathbb{Q}_p$ for every prime p, then it has a solution in $\mathbb{Q}$.

Does this principle always hold?

Hasse Principle

No solution in $\mathbb{Q}_p$ for some p or no solution in $\mathbb{R}$ $\Rightarrow$ No solution in $\mathbb{Q}$.

Hasse Principle (The converse statement)

If a system of polynomial equations with rational coefficients has a solution in $\mathbb{R}$ and in $\mathbb{Q}_p$ for every prime p, then it has a solution in $\mathbb{Q}$.

Does this principle always hold?

No

Counterexample to the Hasse principle

Consider the equation $(x^2-2)(x^2-17)(x^2-34)=0$. It has

- Six real solutions $\{\pm\sqrt{2}, \pm\sqrt{17}, \pm\sqrt{34}\}$.
- At least two 2-adic solutions (as $x^2-17=0$ for some $x \in \mathbb{Q}_2$).
- At least two 17-adic solutions (as $x^2-2=0$ for some $x \in \mathbb{Q}_{17}$).
- At least two p-adic solutions for any other prime p (because if 2 and 17 are not quadratic residues modulo p, then 34 is a quadratic residue and so, at least one of the equations

$$x^2-2=0 \qquad x^2-17=0 \qquad x^2-34=0$$

  must have solutions in $\mathbb{Q}_p$).
- No rational solutions.

Hasse principle for curves

Let $\mathcal{C}$ be a curve (smooth, projective, irreducible variety) over $\mathbb{Q}$.

Theorem

Let $\mathcal{C}$ be a curve over $\mathbb{Q}$ of genus 0. Then, it is $\mathbb{Q}$-birationally equivalent either to a line or to a conic section of the form $aX^2 + bY^2 + cZ^2 = 0$, with $a, b, c \in \mathbb{Q}$.

Theorem (Hasse-Minkowski)

Every curve of genus 0 satisfies the Hasse principle.

Hasse principle for curves

For curves with genus $g > 0$, the Hasse principle does not generally apply.

Challenge

Finding counterexamples to the Hasse principle in curves.

Hasse principle for curves

For curves with genus $g > 0$, the Hasse principle does not generally apply.

Challenge

Finding counterexamples to the Hasse principle in curves.

Lind and Reichart (1940)

$$2y^2 = 1 - 17x^4$$

Selmer (1951)

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

Hasse principle for curves

For curves with genus $g > 0$, the Hasse principle does not generally apply.

Challenge

Finding counterexamples to the Hasse principle in curves.

Lind and Reichart (1940)

$$2y^2 = 1 - 17x^4$$

$$\updownarrow$$

$$y^2 = x^3 + 17x$$

Selmer (1951)

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

$$\updownarrow$$

$$y^2 = x^3 - 2^8 3^5 5^2$$

WARWICK
THE UNIVERSITY OF WARWICK

Elliptic curve

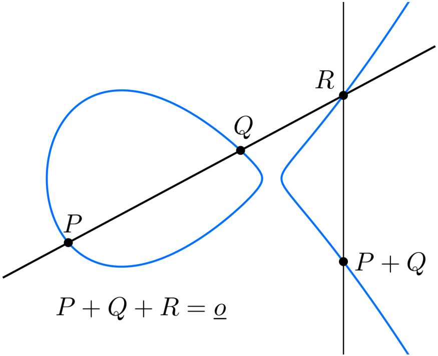
An **elliptic curve** $\mathcal{E}$ is a non-singular curve of genus 1 with a rational point. We denote by $\mathcal{E}(\mathbb{Q})$ its set of rational points.

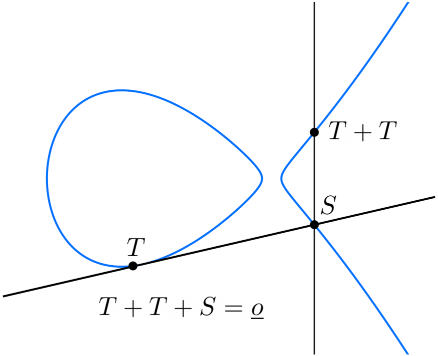
An elliptic curve can always be transformed into a curve that in affine coordinates has equation

$$y^2 = x^3 + Ax + B \qquad \text{with } A, B \in \mathbb{Q}$$

Group Law

We can "sum" points in an elliptic curve and $\mathcal{E}(\mathbb{Q})$ is a group with respect to this operation





Some relevant concepts in elliptic curves

Multiplication-by-m isogeny

$$\begin{aligned}[m]\colon\ \mathcal{E}(\mathbb{Q}) &\longrightarrow \mathcal{E}(\mathbb{Q})\\ P &\longmapsto \underbrace{P+\cdots+P}_{m\text{ terms}}.\end{aligned}$$

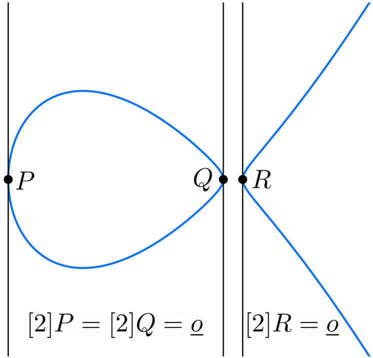
m-torsion subgroup

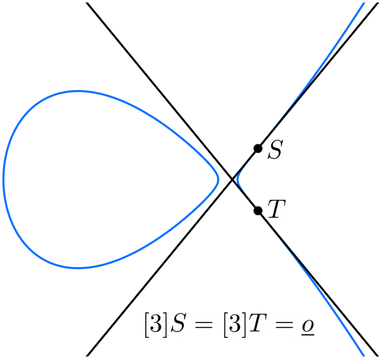
$$\mathcal{E}(\mathbb{Q})[m] = \{P \in \mathcal{E}(\mathbb{Q}) : [m]P = \underline{o}\}.$$

We will denote by $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ the points of finite order in $\mathcal{E}$, i.e.,

$$\mathcal{E}_{\text{tors}}(\mathbb{Q}) = \bigcup_{m=2}^{\infty} \mathcal{E}(\mathbb{Q})[m].$$

Example of torsion points





$\mathcal{E}(\mathbb{Q})$ as a group

Theorem (Mordell-Weil)

Let $\mathcal{E}$ be an elliptic curve. Then, the group $\mathcal{E}(\mathbb{Q})$ is finitely generated and so

$$\mathcal{E}(\mathbb{Q}) \cong \mathcal{E}_{\text{tors}}(\mathbb{Q}) \times \mathbb{Z}^r$$

where $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ is finite, and r is called the **rank** of $\mathcal{E}(\mathbb{Q})$.

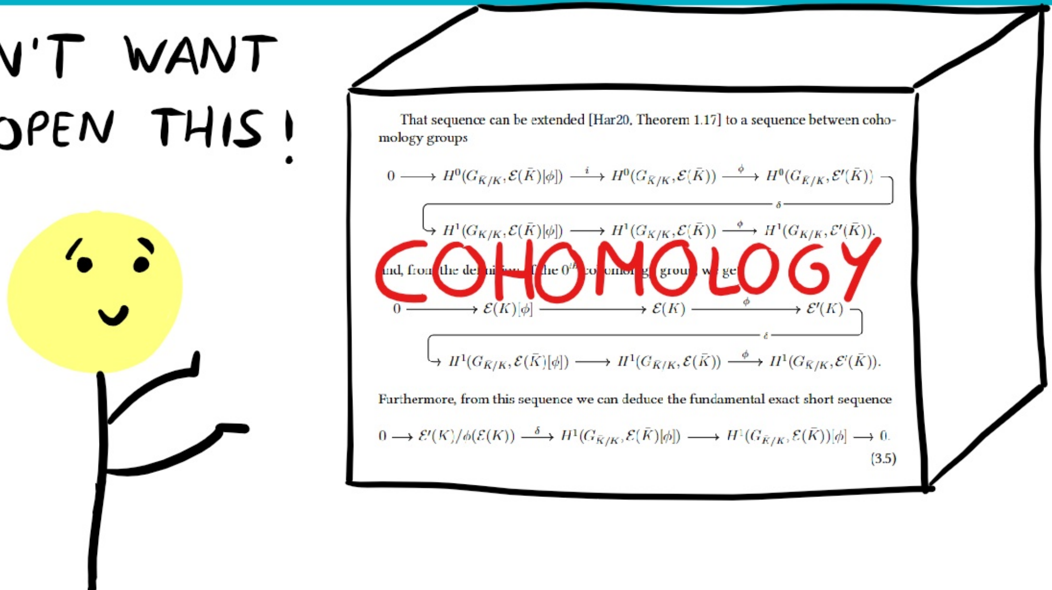
Computing the rank of an elliptic curve is **generally hard** and there are many questions that we don´t know about it. For instance,

Unsolved problem

Is the rank of elliptic curves bounded?

Galois cohomology of an elliptic curve

DON'T WANT TO OPEN THIS!



COHOMOLOGY

That sequence can be extended [Har20, Theorem 1.17] to a sequence between cohomology groups

$$0 \longrightarrow H^0(G_{\bar{K}/K}, \mathcal{E}(\bar{K})[\phi]) \xrightarrow{i} H^0(G_{\bar{K}/K}, \mathcal{E}(\bar{K})) \xrightarrow{\phi} H^0(G_{\bar{K}/K}, \mathcal{E}'(\bar{K}))$$
$$\xrightarrow{\delta} H^1(G_{\bar{K}/K}, \mathcal{E}(\bar{K})[\phi]) \longrightarrow H^1(G_{\bar{K}/K}, \mathcal{E}(\bar{K})) \xrightarrow{\phi} H^1(G_{\bar{K}/K}, \mathcal{E}'(\bar{K})).$$

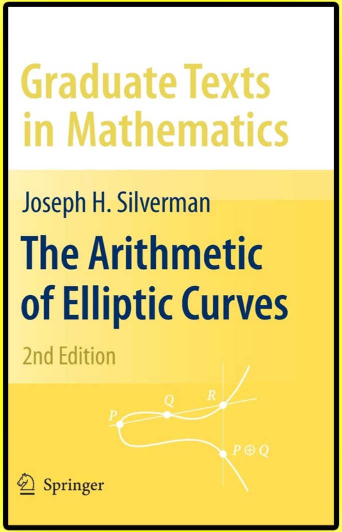
and, from the definition of the 0^{th} cohomology group, we get

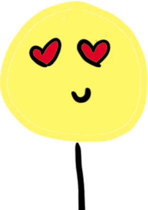
$$0 \longrightarrow \mathcal{E}(K)[\phi] \longrightarrow \mathcal{E}(K) \xrightarrow{\phi} \mathcal{E}'(K)$$
$$\xrightarrow{\delta} H^1(G_{\bar{K}/K}, \mathcal{E}(\bar{K})[\phi]) \longrightarrow H^1(G_{\bar{K}/K}, \mathcal{E}(\bar{K})) \xrightarrow{\phi} H^1(G_{\bar{K}/K}, \mathcal{E}'(\bar{K})).$$

Furthermore, from this sequence we can deduce the fundamental exact short sequence

$$0 \longrightarrow \mathcal{E}'(K)/\phi(\mathcal{E}(K)) \xrightarrow{\delta} H^1(G_{\bar{K}/K}, \mathcal{E}(\bar{K})[\phi]) \longrightarrow H^1(G_{\bar{K}/K}, \mathcal{E}(\bar{K}))[\phi] \longrightarrow 0. \tag{3.5}$$

Galois cohomology





Computing the rank

To find the rank of an elliptic curve, we can study the group $\mathcal{E}(\mathbb{Q})/2\,\mathcal{E}(\mathbb{Q})$, as

$$\mathcal{E}(\mathbb{Q})/2\,\mathcal{E}(\mathbb{Q}) \cong \mathcal{E}(\mathbb{Q})[2] \times (\mathbb{Z}/2\mathbb{Z})^r$$

By the theory of Galois cohomology we get a short exact sequence

$$0 \longrightarrow \mathcal{E}(\mathbb{Q})/2\,\mathcal{E}(\mathbb{Q}) \longrightarrow H^1(\mathcal{E}(\mathbb{Q})[2]) \xrightarrow{\psi} WC(\mathcal{E}(\mathbb{Q}))[2] \longrightarrow 0$$

- $H^1(\mathcal{E}(\mathbb{Q})[2])$ is a finite subgroup of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \times \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$.
- $WC(\mathcal{E}/\mathbb{Q})[2]$ is a group whose elements are **homogeneous spaces.**
- $\ker(\psi) \cong \mathcal{E}(\mathbb{Q})/2\,\mathcal{E}(\mathbb{Q})$ are the elements of $H^1(\mathcal{E}(\mathbb{Q})[2])$ whose images homogeneous spaces **do not have rational points.**

What does this have to do with the Hasse principle?

We can study "**Galois cohomology with respect to local fields**" to get

$$0 \longrightarrow \mathcal{E}(\mathbb{Q})/2\,\mathcal{E}(\mathbb{Q}) \longrightarrow \mathrm{Sel}^{(2)}(\mathcal{E}/\mathbb{Q}) \longrightarrow \text{Ш}(\mathcal{E}/\mathbb{Q})[2] \longrightarrow 0$$

where

- $\mathrm{Sel}^{(2)}(\mathcal{E}/\mathbb{Q})$ is the **2-Selmer group**, which is the subgroup of all elements of $H^1(\mathcal{E}(\mathbb{Q})[2])$ whose images homogeneous spaces **have points in** $\mathbb{R}$ **and in** $\mathbb{Q}_p$ **for every** p.
- $\text{Ш}(\mathcal{E}/\mathbb{Q})$ is the **Tate-Shaferevich** group, which is a group that measures to what extent all possible homogeneous spaces associated to $\mathcal{E}$ satisfy the Hasse principle.

2-Selmer and Tate-Shaferevich groups

$$0 \longrightarrow \mathcal{E}(\mathbb{Q})/2\,\mathcal{E}(\mathbb{Q}) \longrightarrow \mathrm{Sel}^{(2)}(\mathcal{E}/\mathbb{Q}) \longrightarrow Ш(\mathcal{E}/\mathbb{Q})[2] \longrightarrow 0$$

If we are able to prove that $Ш(\mathcal{E}/\mathbb{Q})$ is non-trivial (for instance, by proving that $Ш(\mathcal{E}/\mathbb{Q})[2]$ is non-trivial), then some of the homogeneous spaces of $\mathcal{E}$ are counterexamples of the Hasse principle.

In fact, $2y^2 = 1 - 17x^4$ is a counterexample of the Hasse principle, because it is a homogeneous space associated to the curve $\mathcal{E} : y^2 = x^3 + 17x$, which has $Ш(\mathcal{E}/\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$.

The Tate-Shaferevich group is mysterious

Conjecture

The Tate-Shaferevich group is finite.

If this conjecture is true, then the order of $Ш(\mathcal{E}/\mathbb{Q})$ is a square and so is the order of any of the p-primary components of $Ш(\mathcal{E}/\mathbb{Q})$.

From

$$0 \longrightarrow \mathcal{E}(\mathbb{Q})/2\,\mathcal{E}(\mathbb{Q}) \longrightarrow \mathrm{Sel}^{(2)}(\mathcal{E}/\mathbb{Q}) \longrightarrow Ш(\mathcal{E}/\mathbb{Q})[2] \longrightarrow 0$$

we deduce that

$$\begin{aligned} \mathrm{rank}_{\mathbb{Z}/2\mathbb{Z}}\, Ш(\mathcal{E}/\mathbb{Q})[2] &= \mathrm{rank}_{\mathbb{Z}/2\mathbb{Z}}\, \mathrm{Sel}^{(2)}(\mathcal{E}/\mathbb{Q}) - \mathrm{rank}_{\mathbb{Z}/2\mathbb{Z}}\, \mathcal{E}(\mathbb{Q})/2\,\mathcal{E}(\mathbb{Q}) \\ &= \mathrm{rank}_{\mathbb{Z}/2\mathbb{Z}}\, \mathrm{Sel}^{(2)}(\mathcal{E}/\mathbb{Q}) - \mathrm{rank}_{\mathbb{Z}/2\mathbb{Z}}\, \mathcal{E}(\mathbb{Q})[2] - \mathrm{rank}_{\mathbb{Z}}\, \mathcal{E}(\mathbb{Q}) \end{aligned}$$

Why are we interested in the Hasse principle?

Conjecture (Birch and Swinnerton-Dyer). *The Taylor expansion of $L(C,s)$ at $s=1$ has the form* 1M \$

$$L(C,s) = c(s-1)^r + \textit{higher order terms}$$

with $c \neq 0$ and $r = \operatorname{rank}(C(\mathbb{Q}))$.

In particular this conjecture asserts that $L(C,1)=0 \Leftrightarrow C(\mathbb{Q})$ is infinite.

Remarks. 1. There is a refined version of this conjecture. In this version one has to define Euler factors at primes $p|2\Delta$ to obtain the completed L-series, $L^*(C,s)$. The conjecture then predicts that $L^*(C,s) \sim c^*(s-1)^r$ with

$$c^* = |Ш_C| R_\infty w_\infty \prod_{p|2\Delta} w_p / |C(\mathbb{Q})^{\text{tors}}|^2.$$

Here $|Ш_C|$ is the order of the Tate–Shafarevich group of the elliptic curve C.

Why are we interested in the Hasse principle?

Conjecture (Birch and Swinnerton-Dyer). *The Taylor expansion of $L(C, s)$ at $s = 1$ has the form*

$$L(C, s) = c(s-1)^r + \textit{higher order terms}$$

1M $

with $c \neq 0$ and $r = \operatorname{rank}(C(\mathbb{Q}))$.

In particular this conjecture asserts that $L(C, 1) = 0 \Leftrightarrow C(\mathbb{Q})$ is infinite.

Remarks. 1. There is a refined version of this conjecture. In this version one has to define Euler factors at primes $p|2\Delta$ to obtain the completed L-series, $L^*(C, s)$. The conjecture then predicts that $L^*(C, s) \sim c^*(s-1)^r$ with

$$c^* = |Ш_C| R_\infty w_\infty \prod_{p|2\Delta} w_p / |C(\mathbb{Q})^{\text{tors}}|^2.$$

Here it is!

Here $|Ш_C|$ is the order of the Tate–Shafarevich group of the elliptic curve C.

Thank you!