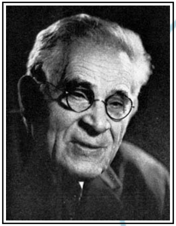
Rational Points on Curves

Caleb McWhorter
Syracuse University

Binghamton University
Arithmetic Seminar Pre-Talk
November 25, 2019

- Can a square and a cube of a rational number differ by 2: $x^2 - x^3 = 2$
- Can a square and a cube of rational numbers differ by 2: $y^2 - x^3 = 2$
- Are there right triangles with all three sides rational, and with rational area: $a^2 + b^2 = c^2$, $\dfrac{ab}{2} = N$. This naturally leads to rational points on $y^2 = x^3 - n^2 x$
- What numbers are the sum of two (or more) cubes: $x_1^3 + x_2^3 + \cdots + x_n^3 = N$



1888–1972

"Mathematicians have been familiar with very few questions for so long a period with so little accomplished in the way of general results, as that of finding the rational [points on elliptic curves]."

– L.J. Mordell, 1922

Question

Let $F(x_1, x_2, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$. Consider the equation $F = 0$.

- When are there rational solutions?
- If there are rational solutions, how many are there?
- Can we find/parametrize all the rational solutions?
- What about integer solutions?

Hilbert's 10th Problem

Ring	Hilbert's 10th
$\mathbb{C}$	✓
$\mathbb{R}$	✓
$\mathbb{F}_q$	✓
p-adic fields	✓
$\mathbb{F}_q((t))$	?
Number Fields	?
$\mathbb{Q}$	?
Global Function Fields	✗
$\mathbb{F}_q(t)$	✗
$\mathbb{C}(t)$	?
$\mathbb{C}(t_1, \ldots, t_n)$	✗
$\mathbb{R}(t)$	✗
$\mathcal{O}_K$	$\approx$?
$\mathbb{Z}$	✗

increasing arithmetic complexity

$n = 1$: $F(x) = 0$

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0$$

$n = 1$: $F(x) = 0$

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0$$

Theorem (Rational Roots Theorem)

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$, where $a_i \in \mathbb{Z}$ and $a_0, a_n \neq 0$. Then the only rational solutions to $f(x) = 0$ have $x = p/q$, where p is an integer factor of a_0 and q is an integer factor of a_n.

$n = 2$: $F(x, y) = 0$

Now $F(x, y) = 0$ defines a curve in the plane, and define

$$d = \deg F(x, y)$$

$n = 2$, $d = 1$: $F(x, y) = 0$

$F(x, y) = ax + by + c \in \mathbb{Q}[x, y]$

$$ax + by + c = 0$$

$n = 2, d = 1$: $F(x, y) = 0$

$F(x, y) = ax + by + c \in \mathbb{Q}[x, y]$

$$ax + by + c = 0$$

- Infinitely many rational points.

$n = 2$, $d = 1$: $F(x, y) = 0$

$F(x, y) = ax + by + c \in \mathbb{Q}[x, y]$

$$ax + by + c = 0$$

- Infinitely many rational points.
- We can parametrize these solutions.

$n = 2, d = 1$: $F(x, y) = 0$

$F(x, y) = ax + by + c \in \mathbb{Q}[x, y]$

$$ax + by + c = 0$$

- Infinitely many rational points.
- We can parametrize these solutions.
- Integer solutions if $\gcd(a, b)$ divides c. If so, infinitely many.

$n = 2$, $d = 2$: $F(x, y) = 0$

$$F(x, y) = ax^2 + bxy + cy^2 + ex + fy + h \in \mathbb{Q}[x, y].$$

$$ax^2 + bxy + cy^2 + ex + fy + h = 0$$

$n = 2, d = 2$: $F(x, y) = 0$

$$F(x, y) = ax^2 + bxy + cy^2 + ex + fy + h \in \mathbb{Q}[x, y].$$

$$ax^2 + bxy + cy^2 + ex + fy + h = 0$$

- These are the conic sections: circles, ellipses, parabolas, hyperbolas, and degenerate cases like a point or pair of lines.

$n = 2, d = 2$: $F(x, y) = 0$

$$F(x, y) = ax^2 + bxy + cy^2 + ex + fy + h \in \mathbb{Q}[x, y].$$

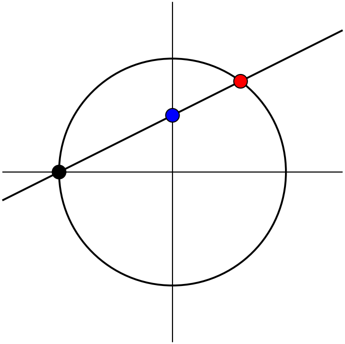
$$ax^2 + bxy + cy^2 + ex + fy + h = 0$$

- These are the conic sections: circles, ellipses, parabolas, hyperbolas, and degenerate cases like a point or pair of lines.
- We want our curves to be smooth, i.e. there is no solution (over $\mathbb{C}^2$) to

$$F(x, y) = \frac{\partial F}{\partial x}(x, y) = \frac{\partial F}{\partial y}(x, y) = 0$$

Finding Rational Points

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



$$C(\mathbb{Q}) = \{(-1,0)\} \cup \left\{ \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right) : t \in \mathbb{Q} \right\}$$

$C(\mathbb{Q}) = \emptyset$

$$x^2 + y^2 + 1 = 0$$

This has no real solutions: $C(\mathbb{R}) = \emptyset$

$C(\mathbb{Q}) = \emptyset$

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

$C(\mathbb{Q}) = \emptyset$

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

- Write $x = a/c$, $y = b/c$, and clear denominators to obtain

$$a^2 + b^2 = 3c^2$$

$C(\mathbb{Q}) = \emptyset$

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

- Write $x = a/c$, $y = b/c$, and clear denominators to obtain

$$a^2 + b^2 = 3c^2$$

- Now $a, b \in \mathbb{Z}$ are not both even, so $a^2 + b^2 \equiv 1 \mod 4$. But $2c^2 \equiv 0, 2 \mod 4$.

Principle (Hasse, Local-Global Principle)

A collection of equations has a solution 'if and only if' it has a solution in $\mathbb{R}$ and $\mathbb{Q}_p$ for all p.

Principle (Hasse, Local-Global Principle)

A collection of equations has a solution 'if and only if' it has a solution in $\mathbb{R}$ and $\mathbb{Q}_p$ for all p.

- Not quite true—Selmer's Example: $3x^3 + 4y^3 + 5z^3 = 0$
- The Hasse Principle shows that the only obstruction to rational points are essentially of one of the two previous forms.

What about higher degree curves?

Theorem (Mordell, 1922, Faltings, 1983)

If C is a curve over $\mathbb{Q}$ of genus $g \geq 2$, then C has at most finitely many rational points.

This leaves the ‘sweet spot’ of cubic equations

$n = 2, d = 3$: $F(x, y) = 0$

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

$n = 2, d = 3$: $F(x, y) = 0$

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

- Make the substitution $y \mapsto y + \dfrac{a_1x + a_3}{2}$.
- Obtain $y^2 = x^3 + a_2'x^2 + a_4'x + a_6'$
- Make the substitution $x \mapsto x + \dfrac{a_2'}{3}$

$n = 2, d = 3$: $F(x, y) = 0$

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

- Make the substitution $y \mapsto y + \dfrac{a_1x + a_3}{2}$.
- Obtain $y^2 = x^3 + a_2'x^2 + a_4'x + a_6'$
- Make the substitution $x \mapsto x + \dfrac{a_2'}{3}$

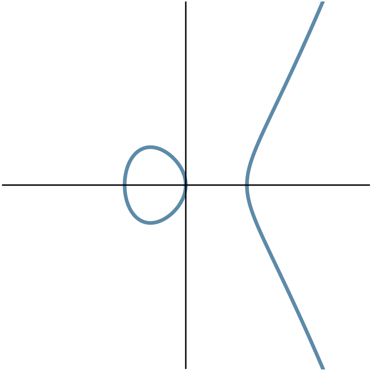
$$E_{A,B} : y^2 = x^3 + Ax + B$$

- Require $\Delta = -16(4A^3 + 27B^2) \neq 0$.
- $C(\mathbb{Q})$ could be empty, finite, or infinite.

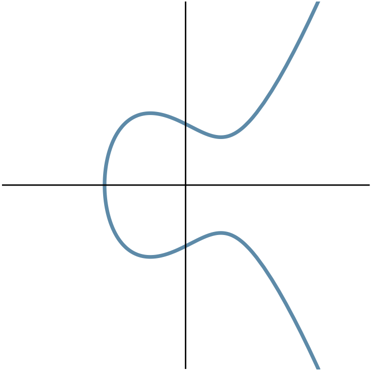
Definition (Elliptic Curve)

An elliptic curve is...

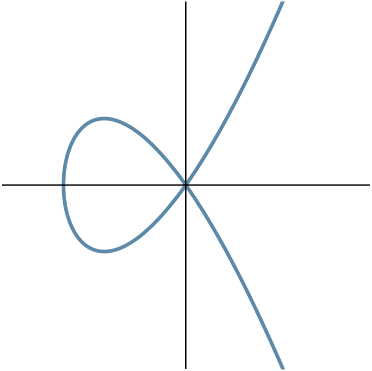
- A nonsingular projective curve of genus 1.
- An abelian variety of dimension 1.
- A nonempty smooth variety, $V(F)$, with $\deg F = 3$.
- A compact Riemann surface of genus 1.
- The set $\{(x, y) : y^2 = x^3 + Ax + B, -16(4A^3 + 27B^2) \neq 0\} \cup \{\infty\}$ with an addition law given by the chord-tangent law.



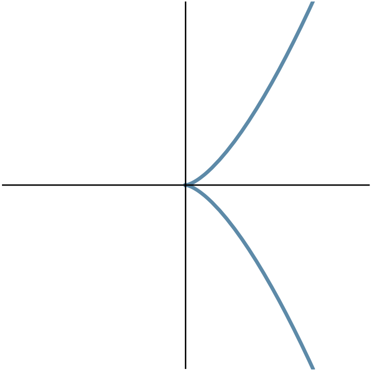
$y^2 = x(x^2+1)$



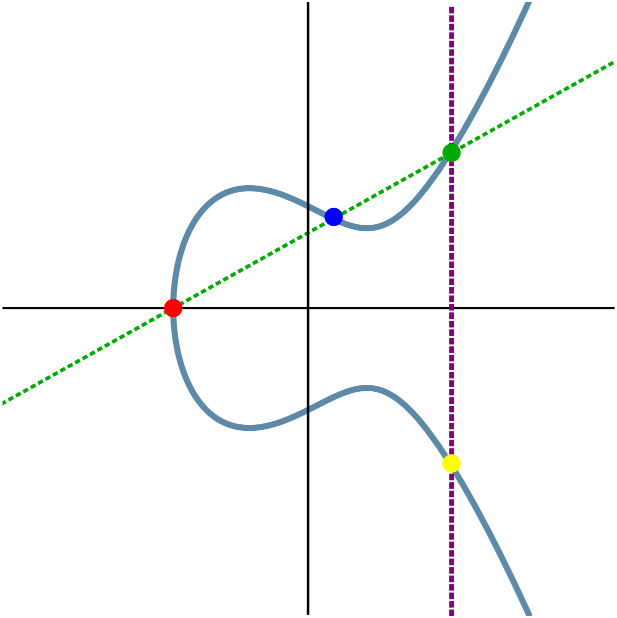
$y^2 = x^3 - x + 1$



$y^2 = x^2(x+2)$



$y^2 = x^3$



What is $E(\mathbb{C})$?

Definition (Weakly Modular Form of Weight k)

Let k be an integer. A meromorphic function $f : \mathcal{H} \to \mathbb{C}$ is weakly modular form of weight k if

$$f(\gamma(\tau)) = (c\tau + d)^k f(\tau) \text{ for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \text{ and } \tau \in \mathcal{H}$$

Definition (Modular Form of Weight k)

Let k be an integer. A function $f : \mathcal{H} \to \mathbb{C}$ is modular form of weight k if

(i) f is holomorphic on $\mathcal{H}$,

(ii) f is weakly modular of weight k,

(iii) f is holomorphic at ∞.

Define the modular form, called the Weierstrass $\wp$-function,

$$\wp(z) = \wp_\Lambda(z) := \frac{1}{z^2} + \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right),$$

and define the Eisenstein series of weight k

$$G_{k,\Lambda} = \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \omega^{-k}$$

$\wp(z)$ satisfies the following:

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6$$

Now define an elliptic curve

$$\begin{aligned} y^2 &= 4x^3 - g_2x - g_3 \\ g_2 &= 60G_4 \\ g_3 &= 140G_6 \end{aligned}$$

Theorem

Let Λ be a lattice, and let E be the elliptic curve $y^2 = 4x^3 - g_2 x - g_3$. Then

$$\begin{aligned} \Phi : \mathbb{C}/\Lambda &\to E(\mathbb{C}) \\ z &\mapsto (\wp(z), \wp'(z)) \\ 0 &\mapsto \infty \end{aligned}$$

is an isomorphism of groups.

To go the other direction, write E as

$$y^2 = 4x^3 - g_2 x - g_3 = 4(x - e_1)(x - e_2)(x - e_3); \quad e_1 < e_2 < e_3$$

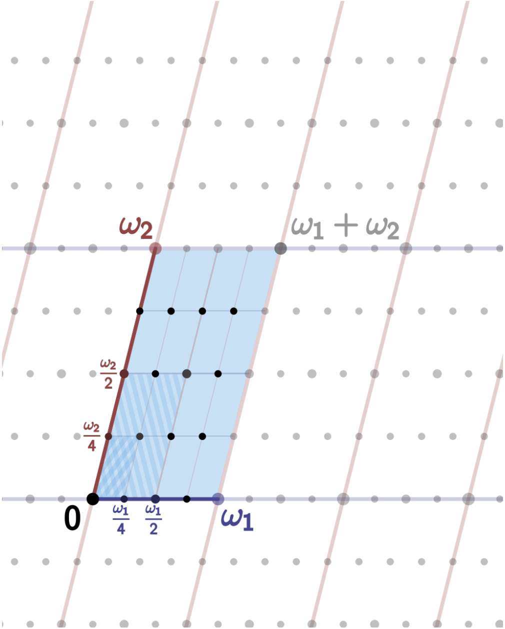
Then define

$$\omega_1 = \frac{2i}{\sqrt{e_3 - e_1} + \sqrt{e_3 - e_2}} \int_1^{1/k} \frac{dt}{\sqrt{(t^2 - 1)(1 - k^2 t^2)}}$$
$$\omega_2 = \frac{2}{\sqrt{e_3 - e_1} + \sqrt{e_3 - e_2}} \int_{-1}^{1} \frac{dt}{\sqrt{(1 - t^2)(1 - k^2 t^2)}}$$

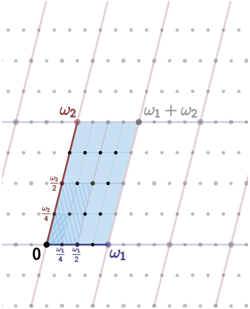
where

$$k = \frac{\sqrt{e_3 - e_1} - \sqrt{e_3 - e_2}}{\sqrt{e_3 - e_1} + \sqrt{e_3 - e_2}}$$

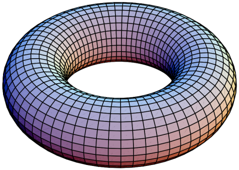
Then $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, where $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$.



ω_2
$\omega_1 + \omega_2$
$\frac{\omega_2}{2}$
$\frac{\omega_2}{4}$
0
$\frac{\omega_1}{4}$
$\frac{\omega_1}{2}$
ω_1



- This shows: $E[n] := \{P \in E\colon nP = \mathcal{O}\} \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$
- $E(\mathbb{C})$ is isomorphic to a torus



What is $E(\mathbb{R})$?

$$E(\mathbb{R}) \cong S^1 \text{ or } E(\mathbb{R}) \cong S^1 \oplus \mathbb{Z}/2\mathbb{Z}$$

The Structure of $E(\mathbb{Q})$ in the next Talk…

Odd ’n Ends

j-INVARIANT

Take an elliptic curve $y^2 = x^3 + Ax + B$. The transformations which preserve this equations are: $x = \mu^2 x$ and $y = \mu^3 y$ for $\mu \in \overline{K}^\times$. We then define the j-invariant

$$j = 1728 \frac{4A^3}{4A^4 + 27B^2}$$

These classify elliptic curves up to isomorphism over $\overline{K}$.

Remark

The j-invariant does not classify elliptic curves over K:

$$y^2 = x^3 - 25x$$
$$y^2 = x^3 - 4x$$

Both have j-invariant 1728 but are not isomorphic over $K = \mathbb{Q}$ (but are over $K = \mathbb{Q}(\sqrt{10})$). So the j-invariant only classifies elliptic curves 'up to twisting'.

Endomorphism Ring

Considering the multiplication by n-map: $P \mapsto nP$

$$\operatorname{End} E \supseteq \mathbb{Z}$$

Generally, $\operatorname{End} E$ is one of the following:

- $\mathbb{Z}$
- an order in an imaginary quadratic field
- an order in a quaternion algebra (not if $\operatorname{char} K = 0$)

If End $E \supsetneq \mathbb{Z}$, we say that E has complex multiplication (CM).

Example

$$y^2 = x^3 + B$$
$$(x, y) \mapsto (\zeta_3 x, -y)$$
$$y^2 = x^3 + Ax$$
$$(x, y) \mapsto (-x, iy)$$

Division Polynomials

Consider an elliptic curve $y^2 = x^3 + Ax + B$ and define

$$
\begin{aligned}
\psi_0 &= 0 \\
\psi_1 &= 1 \\
\psi_2 &= 2y \\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2 \\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \\
&\vdots \\
\psi_{2n+1} &= \psi_{n+2}\psi_n^3 - \psi_{n-2}\psi_{n+1}^3 \\
\psi_{2n} &= \left(\frac{\psi_n}{2y}\right)(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2)
\end{aligned}
$$

The polynomial ψ_n is called the nth division polynomial. The roots of ψ_n give the x-coordinates of the p-torsion points.

Weil Pairing

There is a pairing $e_n : E[n] \times E[n] \to \mathbb{Q}(\zeta_n)$, called the Weil pairing, satisfying

(i) e_n is bilinear
(ii) e_n is non-degenerate
(iii) $e_n(P, P) = 1$
(iv) $e_n(P, Q) = e_n(Q, P)^{-1}$
(v) $e_n(P^\sigma, Q^\sigma) = \sigma e_n(P, Q)$ for all automorphisms of $\overline{K}$ which fix A, B.

Remark

Using the Weil pairing, it is routine to verify that if $E[n] \subseteq K^2$, then $\mathbb{Q}(\zeta_n) \subseteq K$.

Galois Representations

- Let $G_K := \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group of K.
- G_K acts on $E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$
- Fix a basis of $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, then we have a representation

$$\rho_{E,n} : G_K \to \mathrm{Aut}(E[n]) \simeq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}),$$

  the so-called mod n Galois representation.
- One also forms the ℓ-adic Tate module: $T_\ell(E) := \varprojlim_n E[\ell^n]$ and the ℓ-adic representation $\rho_\ell : G_K \to \mathrm{Aut}(T_\ell(E))$.

Theorem (Serre)

Let K be a number field, and let E/K be an elliptic curve without CM. Then for all but finitely many primes ℓ, $\rho_{E,\ell} : G_K \to \mathrm{GL}_2(\mathbb{F}_\ell)$ is surjective.

Hasse Principle: $|p+1-\#E(\mathbb{F}_p)| \leq 2\sqrt{p}$. We define 'error terms' $a_p := p+1-\#E(\mathbb{F}_p)$.

L-FUNCTIONS

Hasse Principle: $|p+1-\#E(\mathbb{F}_p)| \leq 2\sqrt{p}$. We define 'error terms' $a_p := p+1-\#E(\mathbb{F}_p)$.

Then we define the Hasse-Weil L-function of E to be

$$L(E,s) = \prod_{p \nmid \Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

Hasse Principle: $|p+1-\#E(\mathbb{F}_p)| \leq 2\sqrt{p}$. We define 'error terms' $a_p := p+1-\#E(\mathbb{F}_p)$.

Then we define the Hasse-Weil L-function of E to be

$$L(E,s) = \prod_{p \nmid \Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

We can also write

$$L(E,s) = \sum_{n \geq 1} \frac{a_n}{n^s},$$

where a_n are the Fourier coefficients given by

$$a_p = \begin{cases} p+1-N_p, & \text{if } E \text{ has good reduction at } p \\ 1, & \text{if } E \text{ has split multiplicative reduction at } p \\ -1, & \text{if } E \text{ has non-split multiplicative reduction at } p \\ 0, & \text{if } E \text{ has additive reduction at } p \end{cases}$$

Theorem (Wiles, Taylor, Brueil, Conrad, Diamond)

$L(E, s)$ can be analytically continued to $\mathbb{C}$.

Andrew Wiles

Richard Taylor

Christophe Breuil

Brian Conrad

Fred Diamond

In particular, $L(E,s)$ has a Taylor expansion about $s=1$:

$$L(E,s) = c_0 + c_1(s-1) + c_2(s-1)^2 + \cdots$$

In particular, $L(E, s)$ has a Taylor expansion about $s = 1$:

$$L(E, s) = c_0 + c_1(s - 1) + c_2(s - 1)^2 + \cdots$$

Define the analytic rank r_{an} of E to be the order of vanishing of $L(E, s)$ at $s = 1$,

$$L(E, s) = c_{r_{an}}(s - 1)^{r_{an}} + \cdots$$

Conjecture (BSD)

The algebraic and analytic ranks of elliptic curves are equal.

Bryan Birch

(Sir Henry) Peter
Francis Swinnerton-Dyer

Conjecture (BSD)

The algebraic and analytic ranks of elliptic curves are equal.

Bryan Birch

(Sir Henry) Peter
Francis Swinnerton-Dyer

Due to work of Gross, Zagier, Kolyvagin, if $r_{an} \leq 1$, then $r_{\text{anal}} = r_{alg}$. If BSD is true, there is an algorithm to compute the rank of an elliptic curve.

Conjecture (BSD)

The algebraic and analytic ranks of elliptic curves are equal.

Bryan Birch

(Sir Henry) Peter
Francis Swinnerton-Dyer

Due to work of Gross, Zagier, Kolyvagin, if $r_{an} \leq 1$, then $r_{\mathrm{anal}} = r_{alg}$. If BSD is true, there is an algorithm to compute the rank of an elliptic curve.

$$\lim_{s \to 1} \frac{L(E,s)}{(s-1)^{r_E}} = \frac{\Omega_E \; \mathrm{Reg}(E) \, \#\text{Ш}(E/\mathbb{Q}) \, \prod_p c_p}{\#E(\mathbb{Q})_{tors}^2}$$

Questions?