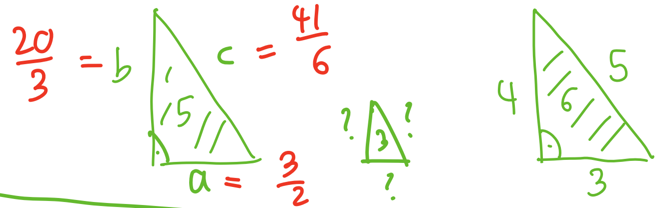
Elliptic curves

Lecture 1

12th April 2024

Can you find $a,b,c \in \mathbb{Q}$

Area $= 6 = \frac{4 \cdot 3}{2}$

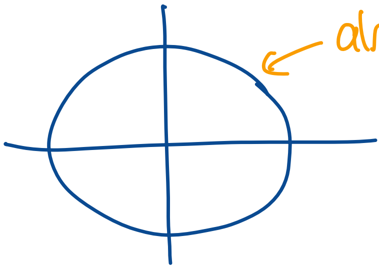


Area $= n$ possible for which n?

?

also a "curve" but it is a conic

Ellipse



$\neq$ Elliptic curve

But: Name comes originally from its connection to computing the arc length of an ellipse. $\rightsquigarrow$ "elliptic integrals".

Q: What is an elliptic curve (over K)?

K: field, often $\underbrace{\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}_p}_{\text{char}(K) = 0}$

later $\mathbb{Z}/p\mathbb{Z}$ $(\text{char}(K) = p)$

Shortest answer:

" abelian variety (over K) of dimension 1 "

group structure

zero set of polynomials

curve

Equivalent answers:

"irreducible non-singular (smooth) projective algebraic curve (over K) of genus 1 furnished with a point O"

This might still not be explicit, but if $\mathrm{char}(K) \neq 2,3$ (as in most cases) we have the following explicit definition:

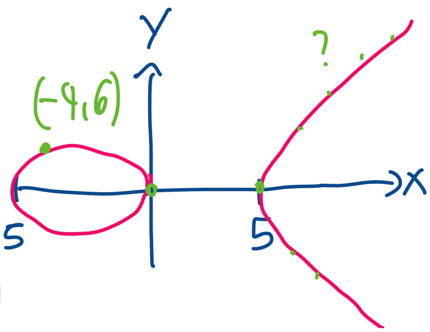
Def 1 An elliptic curve over a field K (with $\mathrm{char}(K) \notin \{2,3\}$) is a plane algebraic curve given by

$$E: y^2 = x^3 + Ax + B$$

(Notation E/K "elliptic curve over K")

with $A, B \in K$ and $4A^3 + 27B^2 \neq 0$.

Example: $E: y^2 = x^3 - 25x$



$E(K)$ — "K-rational pts"

real pt. $E(\mathbb{R})$

rational points $E(\mathbb{Q}) \ni (-4,6)$

Q: why < this definition?
are they interesting?

- Elliptic curves turned out to be useful to answer classical (number theoretical) mathematical questions.

Most famous example: Fermat's last theorem (FLT):

For $n \geq 3$ $a^n + b^n = c^n$ has no integer solutions $a, b, c \in \mathbb{Z}$ with $a \cdot b \cdot c \neq 0$.

Frey & Ribet $\rightsquigarrow$ If there is a solution the the elliptic curve

$$E: y^2 = x(x - a^n)(x + b^n)$$

(after change of variables one can bring this to $y^2 = x^3 + Ax + B$)

is not "modular".

Taniyama – Shimura Conj: Every $E/\mathbb{Q}$ is modular.

Wiles (1994) (+Taylor): This is true! $\Rightarrow$ FLT
"Modularity theorem"

- Elliptic curves also have practical applications in cryptography, factoring integers, etc... (later).

We start by talking about general <u>diophantine equations</u>: (named after Diophantus of Alexandria)

$$C: f(x_1, x_2, \ldots, x_r) = 0$$

$f(x_1, \ldots, x_r) \in \mathbb{Z}[x_1, \ldots, x_r]$, $\deg(f) = n$

Natural questions:

a) Are the rational or integer solutions?

b) If so, can we find them?

c) If we have solutions can we find more?

d) Can we find all?

$\rightsquigarrow$ Determine $C(\mathbb{Z})$, $C(\mathbb{Q})$.

Case $r=1$ variable (any degree)

$$C: f(x) = a_n x^n + \dots + a_1 x + a_0, \quad a_i \in \mathbb{Z}$$

Lemma: If $x = \frac{p}{q} \in \mathbb{Q}$, $f(x) = 0$
$\Rightarrow p \mid a_0, \; q \mid a_n$.

$\rightsquigarrow$ For given $a_0, \dots, a_n$ one just needs to check finitely many x.

Case $r=2$ variables, degree $n=1$

$$C: \; ax + by = c, \quad a, b \neq 0, \; \in \mathbb{Z}$$

- Infinitely many solutions over $\mathbb{Q}$
  (For any $x \in \mathbb{Q}$, $y = \frac{c - ax}{b}$)
- Over $\mathbb{Z}$: Solution over $\mathbb{Z}$ $\Leftrightarrow$ $\gcd(a,b) \mid c$
  (Euklids algorithm / Bézout's lemma)

Case $r=2$ var, degree $n=2$ (Conics)

$C: ax^2+bxy+cy^2+dx+ey+f=0$

(for a):

Over $\mathbb{Q}$: "local-to-global" principle:

Thm (Hasse-Minkowski Theorem)

C has a $\mathbb{Q}$-pt $\iff$ C has points "locally" at all "places":

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

$C(\mathbb{R})\neq\emptyset$ and

$C(\mathbb{Q}_p)\neq\emptyset$ for all p.

(See [L] Appendix C) p-adic numbers

"solutions mod p^n for all n".

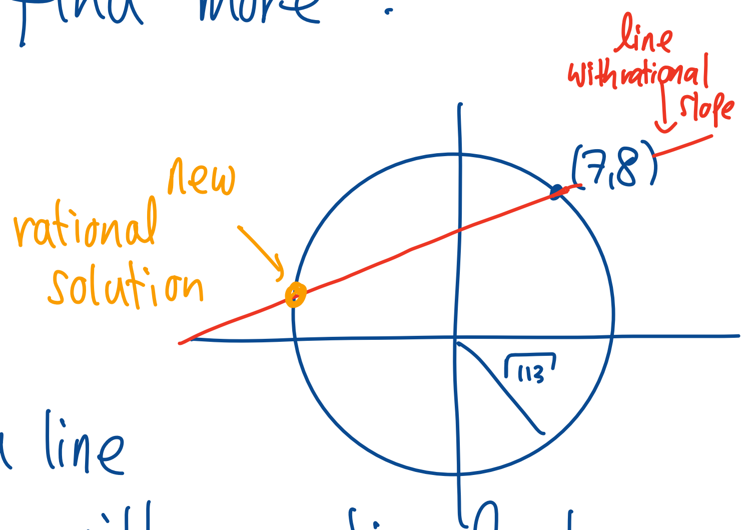
Example: • $C: x^2+y^2+1=0$, $C(\mathbb{R})=C(\mathbb{Q})=\emptyset$

• $C: x^2+y^2-3=0$ has no rational solution since it has no solution mod 4

Here $C(\mathbb{Q}) = \emptyset = C(\mathbb{Q}_4)$
(but $C(\mathbb{R}) \neq \emptyset$)

- $x^2 + y^2 = 113$ has solution $(x,y) = (7,8)$.

Can we find more?



If one starts with one $\mathbb{Q}$-pt and considers a line through this pt with a rational slope. This line intersects with another point on $C(\mathbb{Q})$! $\rightsquigarrow$ This gives all $\mathbb{Q}$-pts.
(Stereographic projection)

(See [ST], Ch. 1.1)

Integral points are more difficult. (cf. Pell's equation $x^2 - Dy^2 = 1$)

Case $r=2$ var, deg f $n=3$ (plane cubic)

$C: ax^3 + bx^2y + cxy^2 + \dots + j = 0$

In $n=2$ case we had either no $\mathbb{Q}$-pt or ∞-many. For $n=3$ we can also just have finitely many $\mathbb{Q}$-pts.

But everything is much harder!

- the local-to-global principle doesn't work: There are cubics with sol's over $\mathbb{R}$, $\mathbb{Q}_p$ but no $\mathbb{Q}$-sol.

  "Selmer's example" $3x^3 + 4y^3 = 5$.

- No algorithm to find all $\mathbb{Q}$-pts (even if we have one)

Elliptic curve: non-singular plane cubic (projective)-curve with at least one $\mathbb{Q}$-pt.

later

$\rightsquigarrow$ can always bring it in the form $y^2 = x^3 + Ax + B$