WHAT IS AN ELLIPTIC CURVE / WHY DO WE CARE?

"AN ELLIPTIC CURVE IS A SMOOTH PROJECTIVE CURVE OF GENUS 1"
↳ WHERE THERE IS A SPECIFIED POINT $\mathcal{O}$.

"ELLIPTIC CURVES" REFERS TO THE STUDY OF CUBIC EQNS, IN PARTICULAR THE STRUCTURE OF THE SET OF ALL SOLNS TO A GIVEN EQN OVER A PARTICULAR FIELD.

⁝ BIG RESULTS ⁝

THM (MORDELL): LET C BE A NONSINGULAR CUBIC CURVE WITH RATIONAL COEFFS. THEN, THE GROUP OF RATIONAL POINTS ON C IS FINITELY-GENERATED. (IT'S ALSO ABELIAN...)

$E(\mathbb{Q})$ = solutions of eqn E over the field $\mathbb{Q}$.

THM (MAZUR) WRITE $E(\mathbb{Q}) = \mathbb{Z}^{(r)} \times \mathrm{Tor}(E(\mathbb{Q}))$

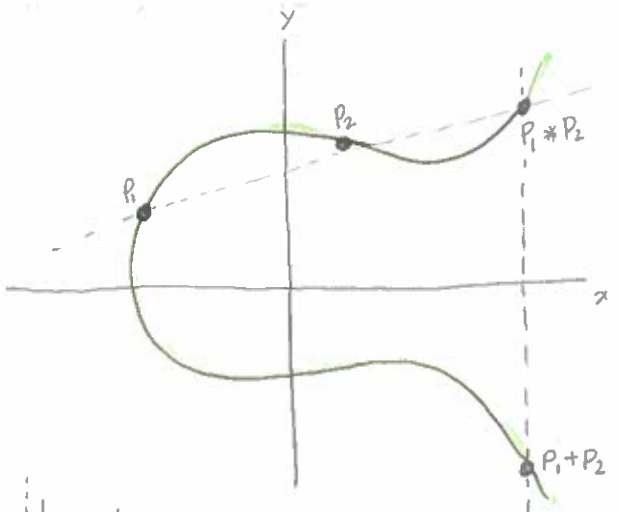
- $\mathbb{Z}^{(r)}$: FREE PART
- $\mathrm{Tor}(E(\mathbb{Q}))$: TORSION PART (FINITE ORDER)

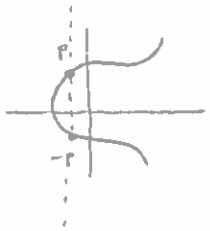
THEN EITHER:

$$\mathrm{Tor}(E(\mathbb{Q})) \cong \mathbb{Z}/m\mathbb{Z} \quad \text{for} \quad m = 1, 2, \ldots, 10, 12, \text{ OR}$$

$$\mathrm{Tor}(E(\mathbb{Q})) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad \text{for} \quad m = 2, 4, 6, 8.$$

[* I SHOULD PREFACE THIS WITH.. I DONT KNOW A LOT ABOUT PROJECTIVE GEOMETRY... *]





WORKING IN PROJECTIVE COORDS...

(NOTE: WE ADJOIN POINTS/LINES @ ∞ SO THAT IT IS ALWAYS TRUE THAT EVERY 2 DISTINCT POINTS DETERMINE A LINE & EVERY TWO DISTINCT LINES INTERSECT AT A DISTINCT POINT)

WE ENDOW AN ELLIPTIC CURVE WITH A POINT AT INFINITY SO THAT ALL LINES INTERSECT THE CURVE AT EXACTLY 3 POINTS (WITH MULTIPLICITY)

$\mathcal{O}$ = PT AT ∞ = 'identity'

WE CAN VERIFY THE FOLLOWING:

- $P + Q = Q + P$
- $P + \mathcal{O} = P$
- $(-P) + P = \mathcal{O}$.

AN ELLIPTIC CURVE IS A SMOOTH PROJECTIVE CURVE OF GENUS 1 → were there is a specified point $\mathcal{O}$.

ITS AN ALGEBRAIC CURVE DEFINED BY $y^2 = x^3 + ax + b$ THAT HAS NO CUSPS / SELF INTERSECTIONS.

I WANT TO UNRAVEL THE DEFN FIRST...

RECALL THE FOLLOWING...

every algebraic extension of k is separable

DEFN. PROJECTIVE n-SPACE OVER A PERFECT FIELD k, DENOTED $\mathbb{P}^n_k$ IS THE SET OF $(n+1)$-TUPLES

$$(x_0, \dots, x_n) \in \mathbb{A}^{n+1}$$

WITH AT LEAST ONE $x_i \neq 0$ MODULO THE EQUIV. REL^n:

$$(x_0, \dots, x_n) \sim (y_0, \dots, y_n)$$

IF $\exists\ \lambda \in \bar{k}^*$ SUCH THAT $x_i = \lambda y_i$ $\forall\ 0 \leq i \leq n$.

WE DENOTE AN EQUIV. CLASS BY $[x_0, \dots, x_n]$

GIVEN A HOMOGENEOUS POLYNOMIAL $f \in \bar{k}[x]$ & SOME $P \in \mathbb{P}^n$.

WE MAY ASK IF $f(P) = 0$?

TO EACH HOMOGENEOUS IDEAL I WE ASSOCIATE A SUBSET OF $\mathbb{P}^n$:

$$V_I = \{ P \in \mathbb{P}^n : f(P) = 0 \ \forall \text{ homogeneous } f \in I \}$$

↳ THIS IS A (PROJECTIVE) ALGEBRAIC SET

Ex. $V: x^2 + y^2 = 3z^2$ DEFINED OVER $\mathbb{Q}$

BUT $V(\mathbb{Q}) = \emptyset$.

Why?

Remember the equivalence relation..

Spose $[x,y,z] \in V(\mathbb{Q})$ with $x, y, z \in \mathbb{Z}$ & $\gcd(x,y,z) = 1$

Then.. $x^2 + y^2 \equiv 0 \pmod 3$

The squares modulo 3 are: 0 & 1..

so we must have $x \equiv y \equiv 0 \pmod 3$ → Further, we have that $3 \mid z$ as well. but then $x \equiv y \equiv z \equiv 0 \pmod 3$ ⇒⇐ $\gcd(x,y,z) = 1$.

→ In general, to show an algebraic set $V/\mathbb{Q}$ has no $\mathbb{Q}$-rational points, it suffices to show that the corresponding homogeneous polynomials have no nonzero solutions modulo p for any one prime p

---

DEFN. A (PROJECTIVE) ALGEBRAIC SET IS CALLED A PROJECTIVE VARIETY IF ITS HOMOGENEOUS IDEAL $I(V)$ IF IT IS PRIME IN $\bar{k}[x]$.

↳ ZERO-LOCUS OF SOME FINITE FAMILY OF HOMOGENEOUS POLYNOMIALS (OF $n+1$ VARIABLES, COEFFS IN FIELD k) THAT GENERATE A PRIME IDEAL.

DEFN. LET V/K A PROJECTIVE VARIETY & CHOOSE $\mathbb{A}^n \subset \mathbb{P}^n$ SUCH THAT $V \cap \mathbb{A}^n \neq \emptyset$. THE DIMENSION OF V IS THE DIMENSION OF $V \cap \mathbb{A}^n$.

DEFN. Let V A PROJ. VARIETY, $P \in V$, & $\mathbb{A}^n \subset \mathbb{P}^n$ WITH $P \in \mathbb{A}^n$. THEN V IS NONSINGULAR (SMOOTH) AT P IF $V \cap \mathbb{A}^n$ IS NONSINGULAR AT P.

PROPOSITION: FOR SMOOTH CURVES, A RATIONAL MAP IS DEFINED AT EVERY POINT.

↳ Let $V_1, V_2 \subset \mathbb{P}^n$ be projective varieties A rational map from V_1 to V_2 is a map of the form:

$$f: V_1 \to V_2 \qquad \phi = [f_1, \ldots, f_n],$$

where the functions $f_0, \ldots, f_n \in \bar{k}(V_1)$ have the property that for every point $P \in V_1$ at which $f_0, \ldots, f_n$ are all defined,

$$\phi(P) = [f_0(P), \ldots, f_n(P)] \in V_2.$$

A rational map

$$\phi = [f_0, \ldots, f_n] : V_1 \to V_2$$ is regular (or defined) at $P \in V_1$

if there is a function $g \in \bar{k}(V_1)$ such that

(i) each gf_i is regular at P

(ii) there is some i for which $(gf_i)(P) \neq 0$

IF such a g exists, then set $\phi(P) = [(gf_0)(P), \ldots, (gf_n)(P)]$.

→ A RATIONAL MAP THAT IS REGULAR AT EVERY POINT IS CALLED A MORPHISM.

DIVISORS

DIVISORS ARE A WAY TO KEEP TRACK OF POLES & ZEROS ...

DEFN. THE **DIVISOR GROUP** OF A CURVE C (DENOTED $\mathrm{Div}(C)$) IS THE FREE ABELIAN GROUP GENERATED BY THE POINTS OF C.

$D \in \mathrm{Div}(C)$ IS A FORMAL SUM

$$D = \sum_{P \in C} n_P (P)$$

$n_P \in \mathbb{Z}$ & $n_P = 0$ FOR ALL BUT FINITELY-MANY $P \in C$.