# Rational and Integral Points on Algebraic Curves

<u>Question</u> - Given a polynomial $f$ in some # of variables, does it have a soln in $\mathbb{Q}$? How many solns?
More generally, in a number field $K$?

- If $f$ has one variable, this is "easy" to compute
- Next case: 2 variables, i.e

$$f(x,y) = 0$$

The solution set(s) to this equation
(for any ring, e.g. $\mathbb{C}$, or $\overline{\mathbb{Q}}$)
form a geometric: an algebraic curve

<u>Slogan</u> The geometry (even topology) of this geometric object determines what the answer to that question looks like.

<u>In particular</u> the <u>genus</u> $g$ of the curve

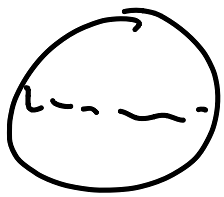
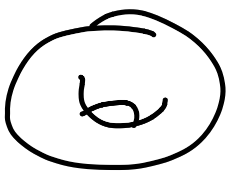
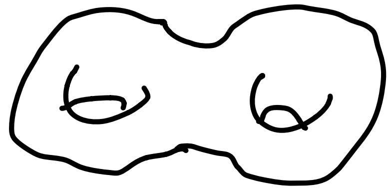
(ell curve means $g = 1$)

<u>Genus</u> comes from theory of compact orientable 2-dim real mflds

# Classification of these

Classified by a non-neg integer $g$.

| $g=0$ | $g=1$ | $g=2$ |
|---|---|---|
| sphere | torus | two-holed torus |

$g>2$

$g$-holed torus

**Notation** $X$ = alg. var defined by $f$

- assume $f$ has integer coeffs
- for any ring $R$, set

$$X(R) = \{(x,y) \in R^2 \mid f(x,y) = 0\}$$

## How does this relate to $f(x,y)$?

- Could consider $X(\mathbb{R})$

  1 eqn 2 vars $\Rightarrow$ 1-dim'l

- Can consider $X(\mathbb{C})$

  complex 1-dim'l $\Rightarrow$ real 2-dim'l and oriented!

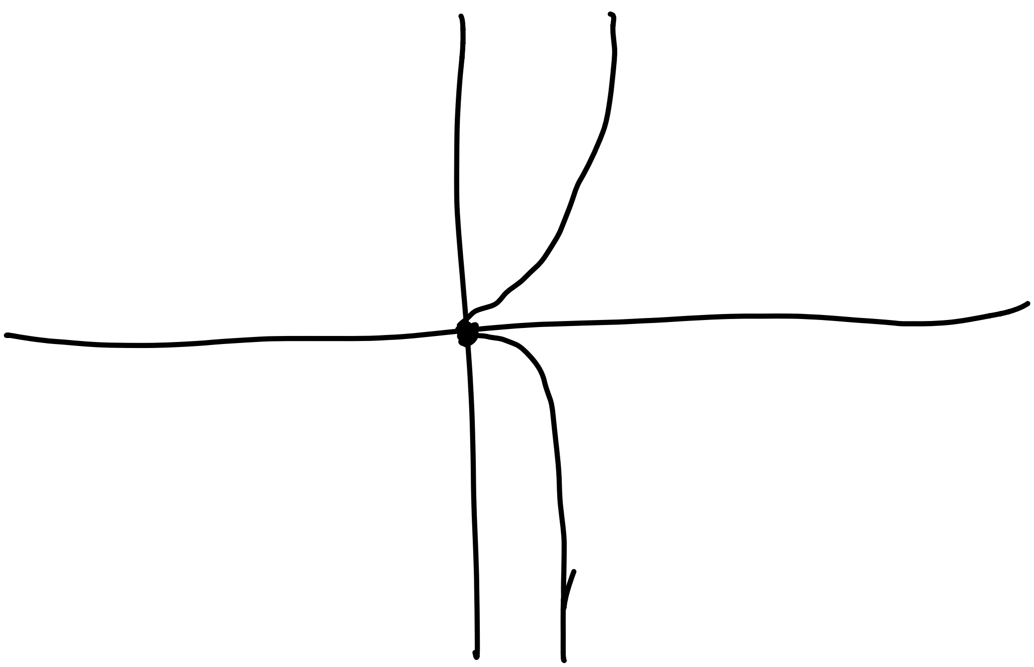
$X(\mathbb{C})$ is "almost" a real 2-dim'l compact orientable mfld

Two caveats

1. compact (will use projective space)
2. manifold (might have singularities)

E.g. $f(x,y) = y^2 - x^3 = 0$

Graph of $X(\mathbb{R})$



singularity at $(0,0)$

How to resolve the singularity?

Two ways

① Parametrization (by $\mathbb{A}^1$)

$\mathbb{A}^1$ to $X$

coordinate $t$ coords $(x, y)$

$$t \overset{F}{\longmapsto} (t^2, t^3)$$

Over $\mathbb{C}$, this is a bijection.

inverse via $t = y/x$

Note $y/x$ is a rational fcn, but not a polynomial

$\Longrightarrow \mathbb{A}^1$ is not isomorphic to $X$ as an algebraic but is birational

I.e. $F$ is an isomorphism

$$\mathbb{A}^1 \setminus \{0\} \longrightarrow X \setminus \{(0,0)\}$$

but not $\mathbb{A}^1 \to X$

<u>General Fact</u> Any curve is birationally the same as a smooth curve. (<u>Note</u> birationally means outside a finite set of points)

In particular, question of finding rat'l points on $X$ is equivalent to find rat'l pts on a smooth version ("model").

## ② Integral Closure

$$X = \mathrm{Spec}\left(\mathbb{Q}[x,y]/(x^3-y^2)\right),$$

$$\mathbb{A}^1 = \mathrm{Spec}\left(\mathbb{Q}[t]\right)$$

$$\mathbb{Q}[x,y]/(x^3-y^2) \hookrightarrow \mathbb{Q}[t]$$

$$x \longmapsto t^2$$

$$y \longmapsto t^3$$

This is an isom on fraction fields
(corresponds to being birational)

$t = y/x \in \mathrm{Frac}\left(\mathbb{Q}[x,y]/(x^3-y^2)\right)$

$\mathbb{Q}[t]$ is the integral closure

of $\mathbb{Q}[x,y]/(x^3-y^2)$ in its

fraction field

<u>In alg geo</u>:

$A'$ is "normalisation"

set of elements
of fraction field satisfying

of $X$.

a monic poly w/ coeff in $\mathbb{Q}[x,y]/(x^2-y^2)$

(can prove general fact using this)

done w/ smoothness.

---

Overall Goal Given $X$, get a smooth, compact (projective) curve $\overline{X}$ that is birational to $X$ and then the genus $g$ is the genus of $\overline{X}(\mathbb{C})$

Make $X$ compact by adding "points at $\infty$ via projective space

<u>Recall</u> let $K$ be a field

$$\mathbb{P}^1(K) = \left\{ (x,y) \in K^2 \;\middle|\; (x,y) \neq (0,0) \right\} \Big/ (x,y) \sim (\lambda x, \lambda y)$$

for $\lambda \in K^{\times}$

Two cases

(A) $y \neq 0$. Then $(x,y) \sim (\frac{x}{y}, 1)$

the set of such $(x,y)$ is set of $\frac{x}{y} \in K$, i.e. $\mathbb{A}^1(K)$

(B) $y = 0$ $(x,y) \sim (1,0)$

"$\infty$" one point in this case

If $k=\mathbb{C}$, $\mathbb{A}^1(\mathbb{C})=\mathbb{C}$

(not compact)

$\mathbb{P}^1(\mathbb{C})=\mathbb{C}\cup\{\infty\}=$

Riemann <u>sphere</u>

$\hookrightarrow \mathbb{P}^1$ is a

curve of genus 0

applies e.g. to any linear $f(x,y)$ (in fact, to any quadratic)

$$\mathbb{P}^2(k) = \left\{ \begin{array}{l} (x,y,z)\in k^3 \mid \\ (x,y,z)\neq 0 \end{array} \right\} \Big/ \begin{array}{l}(x,y,z)\sim(\lambda x,\lambda y,\lambda z) \\ \lambda\in k^{\times}\end{array}$$

<u>Two cases</u>

A $z\neq 0$

then $(x,y,z)\sim\left(\frac{x}{z},\frac{y}{z},1\right)$

corresponds to <u>all</u> pairs

$$\left(\frac{x}{z}, \frac{y}{z}\right) \in K^2 = \mathbb{A}^2(K)$$

B $\quad z = 0.$

Then the set of $(x, y, 0)$ modulo equivalence $\sim$ is $\mathbb{P}^1$ (at "infinity" or at "boundary")

__Idea__ to associate to $X = \{f(x,y) = 0\}$ a projective variety,

consider $f\left(\frac{x}{z}, \frac{y}{z}\right) = 0$

__Notice__ $\frac{x}{z}, \frac{y}{z}$ are scaling-invariant

Problem don't work if $z=0$.

let $d = \deg(f)$

set $F(x,y,z) = z^d f\left(\frac{x}{z}, \frac{y}{z}\right)$

then $F$ is a homogeneous polynomial in 3 variables.

homog $F(\lambda x, \lambda y, \lambda z) = \lambda^d F(x,y,z)$

$\Longrightarrow$ condition $F(x,y,z) = 0$

respects equivalence relation defining $\mathbb{P}^2$

<u>E.g.</u>

$f(x,y) = y^2 - x^3$

$F(x,y,z) = zy^2 - x^3$

$f(x,y) = y^2 - x^3 - x$

$F(x,y,z) = zy^2 - x^3 - z^2 x$

See Poonen

"$p$-adic approach to rational points on curves" (14-page) (section 1)

"computing rational pts on curve"

## Fri Oct 2

**Recall** Given $f(x,y)$ (w/ coeff in $\mathbb{Z}$)

Does $f(x,y) = 0$ have solns in $\mathbb{Q}$? How many?
(same question for $\mathbb{Z}$)

**Recall** $f \rightsquigarrow$ variety $X$

For any ring $R$, $X(R)$ is the

of solutions to $f(x,y)=0$
for $x,y \in R$.

<u>Slogan</u> genus of $f$ determines the "structure" of the question for $X(\mathbb{Q})$.

<u>Assumption</u> $f$ irreducible in $\overline{\mathbb{Q}}[x,y]$.

<u>What is genus?</u>

<u>Fact</u> $X$ is birational

(i.e. isomorphism outside finitely many pts)

to a smooth projective variety

$\tilde{X}$.

understanding $\tilde{X}(\mathbb{Q})$ is equivalent to understanding $X(\mathbb{Q})$

More specifically:

$$\begin{tikzcd} & \tilde{X} \arrow[d, "\leftarrow \text{resolve singularities}"] \\ X \arrow[r, hook] & \overline{X} \end{tikzcd}$$

$X = \{f(x,y)=0\} \subseteq \mathbb{A}^2$ and $\overline{X} = \{z^d f(\frac{x}{z}, \frac{y}{z}) = 0\} \subseteq \mathbb{P}^2$

$d = \deg f$

$\tilde{X}(\mathbb{C})$ is a compact 1-dim $\mathbb{C}$-mfld $\Longrightarrow$ compact orientable 2 dim real mfld

$\Longrightarrow$ has a genus, $g$.

(E.g. $g=0$ sphere, $g=1$ torus, $g=2$ two-holed torus, etc)

How to compute genus?

---

If $f(x,y)$ has has degree $d$,

then $g = \frac{(d-1)(d-2)}{2} -$ terms for singularities in $\bar{X}$

<u>E.g.</u> <u>$d=1$</u> then $\bar{X}=\tilde{X}$ is $\mathbb{P}^1$

and $\mathbb{P}^1(\mathbb{C})=\mathbb{C}\cup\{\infty\}$ Riemann sphere

$g=0$.

<u>$d=2$</u> then $z^2 f\left(\frac{x}{z},\frac{y}{z}\right)$ is a quadratic form in 3 variables

If nondegen $\Longrightarrow$ $\bar{X}$ is smooth

$g=0$.

<u>$d=3$</u> $f(x,y)=y^2-p(x)$

$p(x)=x^3+ax+b$

smooth $\left(\text{hence } g = \frac{(3-1)(3-2)}{2} = 1\right)$

iff $p(x)$ is separable

$\Longleftrightarrow \Delta = 4a^3 + 27b^2 \neq 0$

In this case it defines an elliptic curve.

What is $\Delta = 0$?

Then $g = 0$.

E.g. $y^2 - x^3$. How is it birational to $\mathbb{P}^1_{(\text{w/ coord } t)}$?

$$t \longmapsto (t^2, t^3)$$

$$\frac{y}{x} \longleftarrow\!\shortmid \ (x,y)$$

---

## Rational Points

<u>$d=1$</u> $\bar{X}$ is $\mathbb{P}^1$

$$\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$$

$\Rightarrow$ countably many

In fact, can parametrize them.

<u>$d=2$</u> Either $X(\mathbb{Q})$ is infinite

or $X(\mathbb{Q}) = \emptyset$,

<u>E.g.</u> $f(x,y) = x^2 + y^2 + 1$

$X(\mathbb{R}) = \emptyset$

$\overline{X} = \{x^2 + y^2 + z^2 = 0\}$

$\overline{X}(\mathbb{Q}) = \overline{X}(\mathbb{R}) = \emptyset$.

<u>E.g.</u> $f(x,y) = x^2 + y^2 - 1$

This is a circle! of radius 1

Some elements of $X(\mathbb{Q})$?

$(\pm 1, 0) \quad (0, \pm 1)$

$(\pm 3/5, \pm 4/5) \quad \left(\pm \frac{7}{25}, \pm \frac{24}{25}\right)$

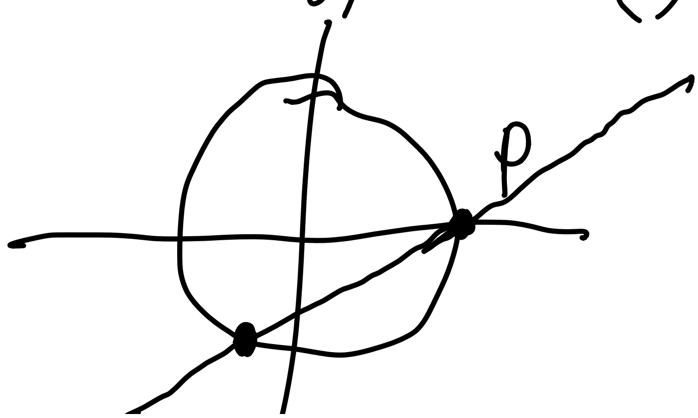
given by Pythagorean triples

__Note__ if $x = \frac{a}{c}, y = \frac{b}{c} \quad a,b,c \in \mathbb{Z}$

then $a^2 + b^2 = c^2 \iff x^2 + y^2 - 1 = 0$

__Idea__: start w/ $P = (1,0)$

$X(\mathbb{R})$ circle



Draw a line through $P$
w/ slope $\lambda$ and intersect w/ $X$

$$y = \lambda(x-1).$$

e.g. $\lambda = \frac{1}{2}$

Geometric intuition: intersect at one other point

<u>Algebraically</u>

$$x^2 + (\lambda(x-1))^2 - 1 = 0$$

$\Longrightarrow$ quadratic eqn in $x$

<u>Know</u> it has a rational root corresp.

to P

$\Longrightarrow$ other root is rational.

$\Longrightarrow$ for any $\lambda \in \mathbb{Q}$, get another element of $X(\mathbb{Q})$.

Conversely if $Q \in X(\mathbb{Q})$ then the line from $P$ to $Q$ has rational slope

$\Longrightarrow$ $Q$ corresponds to same $\lambda$.

Extremal case $Q = P$

then get line tangent to $X$ at $P$

$\Longrightarrow$ vertical line $\Longleftrightarrow$ $\lambda = \infty$

$$X(\mathbb{Q}) \xrightarrow{\sim} \mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$$

$$\begin{array}{ccc} \psi & & \\ Q & \longmapsto & \lambda = \text{slope of line from } P \text{ to } Q \end{array}$$

<u>More generally</u> if $X$ is any smooth variety given by $f$ of deg $2$ (aka "conic") and $P \in X(\mathbb{Q})$

can use the line method to get a bijection btw

$\overline{X}(\mathbb{Q})$ and $\mathbb{P}^1(\mathbb{Q})$

$\Longrightarrow$ If $X(\mathbb{Q})$ is nonempty, then $X(\mathbb{Q})$ is infinite.

<u>Notice</u> $X(\mathbb{R}) = \emptyset$

hence $X(\mathbb{Q}) = \emptyset$

for $f(x,y) = x^2 + y^2 + 1$

I.e. how did we know $X(\mathbb{Q}) = \emptyset$?

b/c $X(\mathbb{R}) = \emptyset$.

Determining if $X(\mathbb{R}) = \emptyset$ is computable

Determining if $\overline{X}(\mathbb{Q}_p) = \emptyset$ also computable

Similarly if $X(\mathbb{Q}_p) = \emptyset$ then $X(\mathbb{Q}) = \emptyset$.

Q If $X(\mathbb{Q}) = \emptyset$, can we always do this?

Ans: Yes! (Local-global principle of Hasse-Minkowski)

$\underline{d=3}$ $\underline{\text{Case 1}}$ $\Delta = 0$

then $X$ has genus $0$

then we can (birationally) parametrize by $\mathbb{P}^1$

— did this explicitly for $f(x,y) = y^2 - x^3$

then $X(\mathbb{Q}) = \{(t^2, t^3) \mid t \in \mathbb{Q}\}$

— more generally, either

$X(\mathbb{Q}) = \emptyset$ or infinite.

$\underline{\text{Case 2}}$ $\Delta \neq 0$. $g = 1$.

e.g. $f(x,y) = y^2 - (x^3 - 5x + 8)$.

Is $X(\mathbb{Q}) = \phi$?

No, $P = (1,2)$.

Choose $\lambda \in \mathbb{P}^1(\mathbb{Q})$

Consider line $L$ given by

$$y = \lambda(x-1) + 2$$

Consider $L \cap X$

given by solving

$$(\lambda(x-1)+2)^2 = x^3-5x+8$$

$\Rightarrow$ get a cubic in $x$.

We have one rational solution corresp. to $P$ or $x=1$.

Problem: $L \cap X$ might have no rat'l pts besides $P$

b/c $\overline{X}(\overline{\mathbb{Q}}) \cap L$, which has 3 pts might $P$ union a 2-element set of pts with quadratic irrational coords.

How to ensure that a cubic polynomial (w/ $\mathbb{Q}$-coeff) has <u>another</u> rat'l root?

<u>Ans</u> design it to already have 2 rat'l roots.

<u>How</u>? <u>Ans</u> start w/ $P, Q \in X(\mathbb{Q})$

take $L$ = unique line from $P$ to $Q$

<u>then</u> $L \cap X$ has 3 rational pts

(possibly w/ multiplicity, possibly at $\infty$ in proj. space)

$\Longrightarrow$ gives a way of taking two elements of $X(\mathbb{Q})$ and getting a third.

Will define a binary operation on $X(\mathbb{Q})$ that makes $X(\mathbb{Q})$ into a group. (w/ operation $+$)

given $P, Q$, take line through $P, Q$, take the

Naive other intersection pt, call it $R$)

Try set $P+Q=R$

Problem then $P=Q+R$

so $Q+R+Q=R$

$\Rightarrow 2Q=0 \Rightarrow$ not interesting.

Ans if $P, Q, R$ lie on a line

set $P+Q+R=0$.

Thank you!

## Wed Oct 7

**Previously** $X = \{f(x,y)=0\}$ an algebraic curve
has a genus $g$ (= top. genus of $\tilde{X}(\mathbb{C})$)

$$g = \frac{(d-1)(d-2)}{2} - \text{terms for singularities} \qquad d = \deg(f)$$

**$g=0$** $X(\mathbb{Q})$ finite

$$\Updownarrow$$

$X(\mathbb{Q})$ empty

$$\Updownarrow \text{ Hasse-Minkowski}$$

$X(\mathbb{Q}_p)$ empty $\forall p$ (incl. $\mathbb{Q}_\infty = \mathbb{R}$)

**$g=1$** elliptic curve

take $f(x,y) = y^2 - (x^3 + ax + b)$

non-singular iff $\Delta = 4a^3 + 27b^2 \neq 0$

$$E \cong \tilde{X} = \{y^2z - (x^3 + axz^2 + bz^3)\}$$
$$\subseteq \mathbb{P}^2$$

Given $P, Q \in E(\mathbb{Q})$

the line $\overline{PQ}$ intersects $E(\mathbb{Q})$

at exactly 1 other point $R$

defines binary operation on $E(\mathbb{Q})$.

<u>Naive</u> defines a group structure

via $P + Q = R$.

<u>Problem</u> $P, Q, R$ collinear is

symmetric in $P, Q, R$

but $P+Q=R$ is not a symmetric relation in a group

(unless $P+P=O$ $\forall P$)

<u>Solution</u> define $+$ so that $P, Q, R$ collinear iff $P+Q+R=O$, use this to define group operation $+$

Notice $P+Q+R=O \iff R=-P-Q$

$$= -(P+Q)$$

Define $P+Q$ as $-R$. But how?

Notice if we have point $O$ corresponding to the identity

then $R + (-R) + O = O$

so $R$, $-R$, and $O$ are collinear

If we have $O$, we can define $-R$ to be 3rd intersection point of $\overline{OR}$ with $E$.

Canonical choice $O = (x,y,z) = (0,1,0)$

$=$ pt at $\infty$ in $\mathbb{P}^2 = (0,\lambda,0)$

$\forall \lambda \in \mathbb{Q}^\times$

When does a line in the plane go through $(0,1,0)$ in the projective plane?

Ans iff the line is vertical

So $R$, $-R$, and $O$ are collinear

iff line through $R$ and $-R$ is vertical

$\iff x(R) = x(-R)$

So then $y(R) = -y(-R)$

Note
$y(R)=0$
$\iff$
$R=-R$
$\iff$
$R+R=O$

$\therefore$ $P+Q$ is given by intersecting $\overline{PQ}$ with $E(\mathbb{Q})$ and then negating y-coord.

**Fact** $E(\mathbb{Q})$ is a group under this operation.

## Another description of the group

$$E(\mathbb{Q}) \xrightarrow{\sim} \mathbb{Z}[E(\mathbb{Q})] \Big/ \left\{ \begin{array}{c} [P]+[Q]+[R] \text{ and } [O] \\ \text{for } PQR \text{ collinear} \end{array} \right\}$$

$$P \longmapsto [P]$$

**Note** if $K$ is any field, $E(K)$ forms a group under the same operation.

In particular $E(\mathbb{C})$ is a group.

Recall $E(\mathbb{C})$ is topologically a torus, which is top. $S^1 \times S^1$
($S^1$ is a circle)

Notice $S^1$ has a group structure via $S^1 = (\{z \in \mathbb{C} \mid |z| = 1\}, \cdot)$

Fact $E(\mathbb{C}) \cong S^1 \times S^1$ as a topological group

---

Theorem (Mordell-Weil)
$E(\mathbb{Q})$ is finitely generated as an abelian group.

(More generally, $E(K)$ for any finite extension $K/\mathbb{Q}$)

Rmk We know $E(\mathbb{Q})$ is countable but that does not imply f.g.

Cor $E(\mathbb{Q}) \underset{\text{as a group}}{\cong} \mathbb{Z}^r \oplus T$

for $r \in \mathbb{Z}_{\geq 0}$

$T$ a finite ab. grp

$r$ is called the rank of $E$.

Notice $E(\mathbb{Q})$ finite $\iff r=0$.

Question Given $a, b \in \mathbb{Q}$ at random, what is $r$?

Conj $\frac{1}{2}$ of time $r=0$

$\frac{1}{2}$ of time $r = 1$

0% of time $r > 1$.
(but only often)

(progress by Manjul Bhargava et al)

<u>Conj</u> $r$ is bounded above.

<u>Record for largest $r$</u> $r = 28$
(Elkies)

There is a conjectural algorithm for finding $r$ given $a, b$.

the Birch and Swinnerton-Dyer

Conjecture (BSD) implies that this halts.

- What about $T$?

<u>Thm</u> (Mazur)

$$|T| \leq 16.$$

---

<u>Proof idea of MW</u>

uses algebraic NT.

given $P \in E(\mathbb{Q})$, consider the

set $\{Q \in E(\mathbb{C}) \mid Q+Q=P\}$.

By $E(\mathbb{C}) = S^1 \times S^1$, we know

this set has 4 elements.

Because "+" operation on $E$ is given by polynomials, all $Q$ in this set are in $E(\overline{\mathbb{Q}})$.

Consider $K_p$ = extension field of $\mathbb{Q}$ generated by coords of the four $Q$ in this set.

[More precisely: consider a torsor under $E[2]$ = 2-torsion; see my DDC postdoc seminar]

Can show certain limits on ramified primes in $K_p$. This limits the set of possible $K_p$.

Can use this to show $E(\mathbb{Q})$

"not too large", and using "heights"
can prove $E(\mathbb{Q})$ is f.g.

---

<u>$g \geq 2$</u>

<u>Fact</u> $X(\mathbb{Q})$ <u>finite</u>

<u>always</u>

- Conjecture in 1920's of Mordell
- Proven in 1983 by Faltings
- True for $X(K)$ for any finite extension $K/\mathbb{Q}$.

## Why this is amazing

It says if we write down any $f(x,y)$ of sufficiently high degree w/o too many singularities/degeneracy then $\{(x,y)\in\mathbb{Q}^2 \mid f(x,y)=0\}$ is automatically finite.

**Grothendieck** $\pi_1(\tilde{X}(\mathbb{C}))$

is non-abelian iff $g \geq 2$

and philosophically this should explain Faltings' Thm.

(c.f. anabelian geometry)

see "Galois Groups and Fundamental Groups" on my page

Open Question

Given $X$, can we find

$X(\mathbb{Q})$?

Believed to be computable.

work in progress based on ideas of $\boxed{\text{Chabauty-Kim}}$

Lawrence-Venkatesh

→ see work of Balakrishnan et al

→ my own ongoing work

(Goal: find a conjectural algorithm)

<u>Now</u> there's no group operation on $X(\bar{\mathbb{Q}})$ for $g \geq 2$.

<u>But</u> we can choose $O \in X(\bar{\mathbb{Q}})$ and form

$$\begin{array}{ccc} X(\bar{\mathbb{Q}}) & \to & \mathbb{Z}[X(\bar{\mathbb{Q}})] \Big/ \left\{ \sum_{i=1}^{k} [P_i] \text{ if } \{P_i\} \text{ is the intersection of } X \text{ with a line in } \mathbb{P}^2 \right\} \\ \cup & & \\ P & \longmapsto & [P] \end{array}$$

and mod out by $[O]$

This is map is injective
but <u>not</u> surjective

There is a $g$-dimension
variety $J$ with an embedding

$$X \hookrightarrow J$$

and a group structure on

$$J(\overline{\mathbb{Q}}) \text{ and } J(\mathbb{Q}) = J(\overline{\mathbb{Q}})^{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}$$

where $J(\overline{\mathbb{Q}}) = \mathbb{Z}[X(\overline{\mathbb{Q}})] / \{\text{relations}\}$

Mordell-Weil also implies

$J(\mathbb{Q})$ is finitely generated.

Most approaches above use

$J(\mathbb{Q})$ and its group structure

to study $X(\mathbb{Q})$.

See articles of Poonen mentioned

in 1st and 2nd lecture
for more details.

<u>See</u>

Poonen – McCallum:
– Method Chabauty – Coleman

<u>Poonen</u>

– Computing Rational Points on
Curves (~15 yrs old)

— p-adic Approach to Rational Points (covers Lawrence-Venkatesh)