Algebraic Number Theory (Math 223b)

0. Overview

0.1. Geometry and arithmetic of curves

Let $C \subset \mathbb{P}^m$ be an irreducible smooth projective curve defined over $\mathbb{Q}$.

What can we say about $C(\mathbb{Q})$?

Question Is $C(\mathbb{Q})$ infinite?

Def The *height* of a point $p = [x_0 : \dots : x_m] \in \mathbb{P}^m(\mathbb{Q})$ with $x_0, \dots, x_m \in \mathbb{Z}$, $\gcd(x_0, \dots, x_m) = 1$ is $H(p) = \max(|x_0|, \dots, |x_m|) \geq 1$.

Question If $C(\mathbb{Q})$ is infinite, how quickly does $\#\{p \in C(\mathbb{Q}) \mid H(p) \leq T\}$ grow as $T \to \infty$?

Example $C = \mathbb{P}^1$ $\qquad$ $g = 0$

$\#C(\mathbb{Q}) = \infty$

$$\#\{p \in C(\mathbb{Q}) \mid H(p) \leq T\} = \underbrace{\#\{(x,y) \in \mathbb{Z}^2 \mid |x|, |y| \leq T,\ \gcd(x,y) = 1\}}_{2} \asymp T^2 \quad \text{as } T \to \infty \qquad (I)$$

$A \asymp B$ means that $\exists\, C, D > 0$: $|A| \geq C \cdot |B|$, $|B| \geq D \cdot |A|$ for sufficiently large T

Example circle $C = \{[x:y:z] \mid x^2+y^2=z^2\} \subseteq \mathbb{P}^2$

There are ∞ many Pythagorean triples (x,y,z) with $\gcd(x,y,z)=1$.

$\Rightarrow \#C(\mathbb{Q}) = \infty$.

$g=0$

Geometric explanation: $C \cong \mathbb{P}^1$ over $\mathbb{Q}$

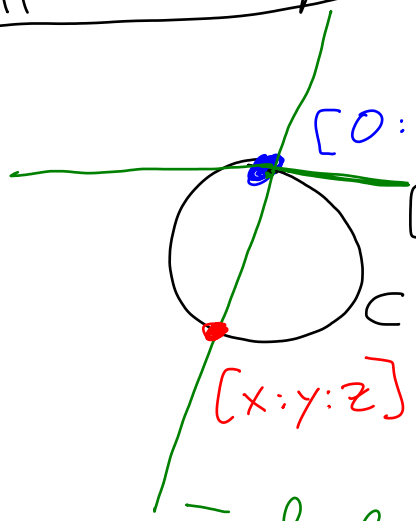
$\Rightarrow C(\mathbb{Q}) \leftrightarrow \mathbb{P}^1(\mathbb{Q})$

Affine ($z=1$) picture

$[x:y:z] \longmapsto [x:y-z]$ (unless $x=y-z=0$)

$= [y+z:-x]$ (unless $y+z=-x=0$)

$[t:u] \longmapsto [2ut : u^2-t^2 : -u^2-t^2]$



$-\text{slope} \dfrac{x}{y-z} = \dfrac{y+z}{-x}$

$\gcd(2ut,\ u^2-t^2,\ -u^2-t^2)$

$\mid \gcd(2u^2, 2t^2) = 2$ if $\gcd(t,u)=1$.

$\max(|2ut|, |u^2-t^2|, |-u^2-t^2|) \asymp \max(|t|,|u|)^2$

$\Rightarrow H([2ut:\dots]) \asymp H([t:u])^2$

$\overset{(I)}{\Rightarrow} \#\{p \in C(\mathbb{Q}) \mid H(p) \le T\} \asymp T$

Example $C = \{x^2 + y^2 = -z^2\} \subseteq \mathbb{P}^2$

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

$g = 0$

Here, $C \cong \mathbb{P}^1$ over $\mathbb{C}$, but $C \not\cong \mathbb{P}^1$ over $\mathbb{Q}$.

(same argument as before)

"Geometry over $\mathbb{C}$" $\neq$ "Geometry over $\mathbb{Q}$".

Example Fermat curve $C = \{X^3 + Y^3 = Z^3\} \subseteq \mathbb{P}^2$

$C(\mathbb{Q}) = \{[0:1:1], [1:0:1], [1:-1:0]\}$. $g = 1$

This was proved using infinite descent:

Consider any other point $p \in C(\mathbb{Q})$ with minimal height $H(p)$. You can use it to construct a point $q \in C(\mathbb{Q})$ with $H(q) < H(p)$. ↯

Example Fermat curve $C = \{x^n + y^n = z^n\} \subseteq \mathbb{P}^2$

$C(\mathbb{Q}) = \{[0:1:1], [1:0:1], [1:-1:0]\}$ for $n \geq 4$

This is Fermat's Last Theorem (Wiles 1995).

$$g = \frac{(n-1)(n-2)}{2} \geq 3$$

Example $C = \{3x^3 + 4y^3 + 5z^3 = 0\}$

$C(\mathbb{Q}) = \emptyset$ although $C(\mathbb{Q}_p) \neq \emptyset$ $\forall p$ and $C(\mathbb{R}) \neq \emptyset$

(Selmer, 1951)

$g = 1$

Example Elliptic curve $C = \{x^3 - 5xz^2 = y^2 z\} \in \mathbb{P}^2$

$\# C(\mathbb{Q}) = \infty$

$\# \{p \in C(\mathbb{Q}) \mid H(p) \leq T\} \asymp (\log T)^{1/2}$

$\Rightarrow$

$g = 1$

Example (Elkies, Klagsbrun) ell.-curve $C = \dots$

$\# C(\mathbb{Q}) = \infty$

$\# \{ \dots \} \asymp (\log T)^{20/2}$.

$g = 1$

What does this have to do with algebraic geometry? A geometric invariant of C is its genus $g \geq 0$.

Thm If $g=0$, then either

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

b) $C \cong \mathbb{P}^1$ over $\mathbb{Q}$

$\#C(\mathbb{R})=\infty$

$\#\{p\in C(\mathbb{Q}) \mid H(p)\le T\} \asymp T^{\alpha}$ for some $\alpha>0$.

Idea of pf as for the circle curve. □

Thm If $g=1$, then either

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

b) $\#\{p\in C(\mathbb{Q}) \mid H(p)\le T\} \asymp (\log T)^{r/2}$

for some $r\in\mathbb{Z}_{\ge 0}$.

(Note: $\#C(\mathbb{Q})<\infty \iff r=0$.)

Idea of pf

- Pick a point $O\in C(\mathbb{Q})$. (abelian)
- Geometrically construct a group operation on $C(\mathbb{Q})$ with identity O. ("Elliptic curve").
- Show that the group $C(\mathbb{Q})$ is finitely generated (Mordell-Weil Theorem).
- $r := \mathrm{rk}(C(\mathbb{Q}))$ $\rightsquigarrow$ $C(\mathbb{Q}) \cong \mathbb{Z}^r \times$ (fin. grp.)
- Show that $\log H \approx$ quadratic form on $C(\mathbb{Q}) \approx \mathbb{Z}^r \times$ (fin. grp.)

□

Thm (Faltings, 1983) Vojta, Bombieri

If $g \geq 2$, then $\#C(\mathbb{Q}) < \infty$.

Idea of pf Assume $C(\mathbb{Q}) \neq \emptyset$. There is no good "geometric" group operation on $C(\mathbb{Q})$.

But we can embed C into a smooth projective g-dimensional variety $J \subseteq \mathbb{P}^s$ (the Jacobian variety of C) with a geometrically defined group operation $+$ on $J(\mathbb{Q})$.

$C(\mathbb{Q}) \subseteq J(\mathbb{Q})$

finitely generated abelian group (Mordell-Weil Theorem)

If $J(\mathbb{Q})$ is finite, we're done!

$J(\mathbb{Q})$ has "few" points:

$$\#\{D \in J(\mathbb{Q}) \mid H(D) \leq T\} \ll (\log T)^{r/2}$$

for some $r \geq 0$.

You wouldn't expect many to satisfy the equations defining the 1-dimensional subvariety C of J. Use heavy machinery/diophantine approximation to prove there are

only finitely many such points. □