Quadratic Forms and the local global principle

Lecture 5: Hasse principle violations

Part 1. Curves ($g \geq 2$)

Part 2. Weil conj. for elliptic curves (genus 1)

Part 3. Lind's Hasse violation

Road map:

Wk 1: Quad forms$/k$

Week 2: Quad forms$/\mathbb{F}_q$ ······ Hensel's ······ Week 3: Quad forms$/\mathbb{Q}_p$

Week 4: Quad forms$/\mathbb{Q}$ —— Hasse-Minkowski $g=0$

success

Hasse principle

fails

TODAY e.g. Selmer curve $g=1$

Let $f(x)$ = any homogeneous deg 2 poly in $X_1, \ldots, X_n$.

$$= \sum_{1 \leq i \leq j \leq n} c_{ij} X_i X_j \leftarrow \text{this is a quad form!}$$

from Wk 1: can extract an assoc symm matrix:

$$(a_{ij}) \qquad a_{ij} = \begin{cases} c_{ii} & \text{if } i=j \\ \frac{1}{2} c_{ij} & \text{if } i<j \\ \frac{1}{2} c_{ji} & \text{if } i>j \end{cases}$$

Thm (Hasse-Minkowski) Any homog deg 2 polynomial satisfies the Hasse principle.

($f=0$ has a soln over $\mathbb{Q}$ $\Leftrightarrow$ $f=0$ has a soln over $\mathbb{Q}_p$ $\forall p \leq \infty$)

Q: deg 3?

A. No :(

Selmer example: $3X^3 + 4Y^3 + 5Z^3 = 0$

has nontriv solns on $\mathbb{Q}_p$ $\forall p \leq \infty$

BUT no nontriv soln over $\mathbb{Q}$.

i.e. $3X^3 + 4Y^3 + 5Z^3 = 0$ violates the Hasse principle

[$3X^3+4Y^3+5Z^3=0$ seems to have "2-dim" worth of soln. "generically"

But: If (X_0, Y_0, Z_0) is a soln to, then

$(\lambda X_0, \lambda Y_0, \lambda Z_0)$ is also a nontriv soln. !

feels similar to (X_0, Y_0, Z_0)

we often quotient by this scaling.

Instead of viewing $3X^3+4Y^3+5Z^3=0$

in $\{(X,Y,Z) \in k^{\oplus 3}\}$

we prefer to view this in

$$\{(X,Y,Z) \in k^{\oplus 3}\} / \text{scaling} = \mathbb{P}^2$$

So now we see $3X^3+4Y^3+5Z^3=0$ as a curve (one dim'l) $g=1$

Quad form of rk 3 e.g. $X^2+Y^2+Z^2=0$ defines a curve $g=0$

Part 1: Curves ($g \geq 2$)

Solutions to $C: y^2 = f(x)$

where $f(x) \in \mathbb{Z}[x]$

and $f(x)$ has no repeated roots over $\bar{\mathbb{Q}}$.

$f(x) = \prod (x - \alpha_i)$ $\alpha_i \in \bar{\mathbb{Q}}$ all distinct

- $\deg C := \deg f$
- $\deg C = 3$ elliptic curve $g=1$
- $\deg C \geq 4$ hyperelliptic curve $g \geq 2$

Q: How do we produce Hasse violations?

Work of Clark–Watson

study Hasse violations in families of "twists"

$$\{ C_d : dy^2 = f(x) \mid d \in \mathbb{Z} \text{ sq free} \}.$$

Thm. (Clark–Watson) Assume the abc conj.
If C has even deg ≥ 6 & f has no roots in $\mathbb{Q}$, then there are inf. many $d \in \mathbb{Z}$ sq. free s.t. C_d violates the Hasse principle.

Part 2. Weil conj. for elliptic curves

X genus 1 curve defined over $\mathbb{F}_q$, smooth.

$X(\mathbb{F}_{q^m}) :=$ set of all solns to the eqn over $\mathbb{F}_{q^m}$.

$\# X(\mathbb{F}_{q^m}) \leftarrow$ study this!

Zeta function for X:

$$Z(X;t) := \exp\left(\sum_{m \geq 1} \frac{1}{m} \# X(\mathbb{F}_{q^m})\, t^m\right)$$

$$= 1 + (\quad) + \frac{1}{2}(\quad)^2 + \frac{1}{6}(\quad)^3 + \cdots$$

Thm. (Deligne)

$$Z(X;t) = \frac{(1-\alpha t)(1-\beta t)}{(1-t)(1-qt)} \qquad (*)$$

where α, β alg integers and $|\alpha| = |\beta| = \sqrt{q}$.

Cor. (Hasse-Weil bound)

$$|q - \# X(\mathbb{F}_q) + 1| \leq 2\sqrt{q}$$

In particular, $X(\mathbb{F}_q) \neq \emptyset$.

Pf. By defn: mod. t^2,

$$Z(X,t) = 1 + \#X(\mathbb{F}_q)t$$

Using (*) & still works mod t^2:

$$1 + \#X(\mathbb{F}_q)t \equiv \frac{(1-\alpha t)(1-\beta t)}{(1-t)(1-qt)}$$

$$\equiv (1-\alpha t)(1-\beta t)(1+t)(1+qt)$$

$$\equiv 1 + (q+1-(\alpha+\beta))t$$

$$\Rightarrow \#X(\mathbb{F}_q) = q+1-(\alpha+\beta)$$

$$\Rightarrow |\alpha+\beta| = |q - \#X(\mathbb{F}_q) + 1|$$

$$\begin{array}{ccc} |\alpha+\beta| & = & |q-\#X(\mathbb{F}_q)+1| \\ \wedge\!| & & \| \\ |\alpha|+|\beta| = 2\sqrt{q} & & |\#X(\mathbb{F}_q) - q - 1| \end{array}$$

$$\Rightarrow -2\sqrt{q} \leq \#X(\mathbb{F}_q) - q - 1 \leq 2\sqrt{q}$$

$$\Rightarrow q+1-2\sqrt{q} \leq \#X(\mathbb{F}_q) \leq q+1+2\sqrt{q}$$

$$\begin{array}{c} q+1-2\sqrt{q} \\ \| \\ (\sqrt{q}-1)^2 \\ \vee \\ 0 \end{array} \qquad \Rightarrow \#X(\mathbb{F}_q) > 0$$

$$\Rightarrow X(\mathbb{F}_q) \neq \emptyset \qquad \square$$

Part 3: Lind - Reichardt curve

$$C: -x^4 + 17y^4 + 2z^2 = 0$$

smooth genus 1 curve $/\mathbb{Q}$

Want: show $C(\mathbb{Q}_p) \neq \emptyset \;\forall\, p \leq \infty$ and $C(\mathbb{Q}) = \emptyset$.

① $C(\mathbb{R}) \neq \emptyset$

② $C(\mathbb{Q}_p) \neq \emptyset \quad \forall\, p \neq 2, 17 \leftarrow$ "good red."

③ $C(\mathbb{Q}_2), C(\mathbb{Q}_{17}) \neq \emptyset$

④ $C(\mathbb{Q}) = \emptyset$

① $(1, 0, \frac{1}{\sqrt{2}}) \in C(\mathbb{R})$

② If $p \neq 2, 17$ then C is smooth over $\mathbb{F}_p$.

$\Rightarrow$ can apply the Hasse-Weil bound to $X = C$

$\Rightarrow C(\mathbb{F}_p) \neq \emptyset$

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

Hensel's lemma

③ $C(\mathbb{Q}_{17})$ If $\sqrt{2} \in \mathbb{Q}_{17}^{\times}$, then $(1, 0, \frac{1}{\sqrt{2}}) \in C(\mathbb{Q}_{17})$

Claim: $\sqrt{2} \in \mathbb{Q}_{17}$.

Pf: Is $\sqrt{2} \in \mathbb{F}_{17}$? Check: $(\mathbb{F}_{17}^{\times})^2 = \{1, 4, 9, 16, 8, 2, \ldots$

so $x^2 - 2 = 0$ has a soln mod 17 $(x = 6)$

Hensel's $\Rightarrow$ $x^2 - 2 = 0$ has a soln in $\mathbb{Z}_{17}$

$\Rightarrow \sqrt{2} \in \mathbb{Q}_{17}$

$C(\mathbb{Q}_2)$

Exercise: $\sqrt[4]{17} \in \mathbb{Q}_2$. $\quad 0 = -x_0^4 + 17y_0^4 + 2z_0^2$

$\Rightarrow (\sqrt[4]{17}, 1, 0) \in C(\mathbb{Q}_2)$

(4) Suppose $(x_0, y_0, z_0) \in C(\mathbb{Q})$.

- can assume $x_0, y_0, z_0 \in \mathbb{Z}$
- Claim: can assume that x_0, y_0, z_0 are all rel prime

Pf: $p \mid x_0, y_0 \Rightarrow p^4 \mid 2z_0^2 \Rightarrow p^2 \mid z_0$

$\Rightarrow \left(\frac{x_0}{p}, \frac{y_0}{p}, \frac{z_0}{p^2}\right) \in \mathbb{Z}^{\oplus 3} \cap C(\mathbb{Q})$.

- Claim: $z_0 \neq 1$

  If it were: $-x_0^4 + 17y_0^4 + 2 = 0$

  reduce mod 17: $x_0^4 = 2 \mod 17$.

  (Check: $(\mathbb{F}_{17}^\times)^4 = \{1, \underline{4, 13, 16}\}$) ※

- Claim: $z_0 \neq 2^N$, $N \in \mathbb{Z}_{\geq 1}$.

  → If it were: $-x_0^4 + 17y_0^4 + 2 \cdot (2^N)^2 = 0$

  mod 17: $x_0^4 = 2^{2N+1}$

  (Check: $2^{2N+1} \mod 17$
  $\in \{\underline{2, 8, 9, 15}\}$)

  ※

- Claim: z_0 is not div by any odd prime!

  Pf: say $p \mid z_0$.

  Then $x_0^4 = 17y_0^4 \mod p^2$ (Note: $p \nmid x_0, y_0$)

  $\Rightarrow 17 \in (\mathbb{F}_p^\times)^2$

  Pset 2 #10 $\Rightarrow p \in (\mathbb{F}_{17}^\times)^2$

Applying this to every odd p dividing z_0:

$$z_0 = 2^N \cdot \underline{(z_0')^2} \mod 17$$

$$\Rightarrow x_0^4 = 2 \cdot \left(2^N \cdot (z_0')^2\right)^2 \mod 17$$

$$\Rightarrow \underline{x_0}^4 = 2^{2N+1} \underline{z_0'}^4 \mod 17$$

$$\Rightarrow 2^{2N+1} \in (\mathbb{F}_{17}^\times)^4 \quad ※$$

So: $z_0 \neq 1$, power of 2, div by an odd pr ※

$\therefore \underline{C(\mathbb{Q}) = \emptyset}$.