

Geometry of Numbers Methods over Number Fields

Joint work w/ M. Bhargava and X. Wang

Fixed number field  $F$ , totally real (though results work for not totally real fields) $E/F$ 

$$E: y^2 = x^3 + Ax + B, \quad A, B \in F.$$

Thm (Mordell-Weil):  $E(F) \cong \mathbb{Z}^r \oplus T$  $r = \text{rank of } E.$ In part, we can assume  $A, B \in \mathcal{O}$ .

$$\{E/F\} \leftrightarrow \{G_m(F) \setminus F^2\} \setminus \{\Delta(A, B) = 0\}$$

 $\{(A, B) \in \mathcal{O}^2 : \alpha^3 | A \text{ and } \alpha^6 | B, \text{ then } \alpha \in \mathcal{O}^\times\}$  is not exactly the set, but it is close to this.

Height:

$$H(E_{A,B}) = \prod_v \max\{|A|_v^3, |B|_v^2\}$$

↑  
v/c in F.

We order the elliptic curves w.r.t this height.

$$N_X(E) = \lim_{X \rightarrow \infty} \frac{\sum_{H(E) \leq X} f(E)}{\sum_{H(E) \leq X} 1}$$

Thm:  $Av(\text{rank}) \leq 1.5$ ,  $Av(\#\text{Sol}_2) = 3$

This talk will concern proving this Theorem.

We have the following exact sequence:

$$0 \rightarrow E(F)/_{2E(F)} \rightarrow \text{Sol}_2(E) \rightarrow H_E(\mathbb{Z}) \rightarrow 0.$$

We have  $2^r \leq \#\text{Sol}_2(E)$ , so it is enough to prove  $Av(\#\text{Sol}_2) = 3$ .

The conjecture is that  $Av(\text{rank}) = 1/2$ , but since one is using the 2-torsion group one cannot get near this bit of the Shaf-Tate group.

$\sigma \in \text{Sol}_2(E) \leftrightarrow$  locally, isotrivial 2-coverings of  $E$ .

$$\begin{array}{ccc} C & & \\ \text{over } G \downarrow & \searrow \text{over } F & \\ E & \xrightarrow{[2]} & E \end{array}$$

$C$  is said to be isotrivially isotrivial  
if  $C(F) \neq \emptyset$ .

$C$  is said to be locally isotrivial  
if  $C(F_v) \neq \emptyset \forall v$ .

Thm (Cassels): If  $C$  is a locally isotrivial 2-covering,  $C$  has

a degree 2 line bundle def. over  $F$ .

$C \rightarrow \mathbb{P}^1 \leftrightarrow$  binary quadratic form.

Binary quartic forms:

$V =$  binary quartic forms

$$V \cong \text{PGL}_2$$

$$v \cdot f(x,y) = \frac{1}{(\det v)^2} f((x,y) \cdot v)$$

invariants

Ring of invariants for this action is freely generated  $I, J$ .

Thm (Cassels, Biles - Skolem - Dyer):

$$\text{Sol}_2(E, A, B) \leftrightarrow \left\{ \text{PGL}_2(F) \setminus V(F)_{A, B} \right\}^{\text{L.S.}}$$

loc. soluble

Thm (Cremers, Fischer, Stall):

$F_p, f \in V(F_p), I(F), J(F) \in \mathcal{O}_p$ . Then

$$\exists v_p \in \text{PGL}_2(F_p) : v_p f \in V(\mathcal{O}_p)$$

$$\text{PGL}_2(\mathcal{O}_p) = \coprod_{i=1}^{c_1} \left( \prod_p \text{PGL}_2(\mathcal{O}_p) \right) \beta_i \text{PGL}_2(F) \quad (\text{Strong approx})$$

$$(v_p) = (\delta_p) \cdot \beta_i \cdot \gamma \quad \gamma \in \text{PGL}_2(F)$$

$$\Rightarrow (\beta_i \cdot \gamma) \cdot f \in V(\mathcal{O}_p)$$

$$\mathcal{Z}_{\text{PGL}_2} = \{ f \in V(F) : f \in \beta_i^{-1} V(\mathcal{O}_p) \}$$

Thm:  $\cup_f f \in V(F), I(F), J(F) \in \mathcal{O} \Rightarrow \exists \gamma \in \text{PGL}_2(F)$  s.t.

$$\gamma \cdot f \in \mathcal{Z}_p \text{ for some } p.$$

$$\Gamma_p = \{ \forall \gamma \in \text{PGL}_2(F) : \gamma \in \beta_i^{-1} \text{PGL}_2(\mathcal{O}_p) \beta_i \}$$

$$\Gamma_p \cong \mathcal{Z}_p$$

Next Goal: Estimate  $\#(\Gamma \backslash \mathbb{H}^n)_{H < X}$ .

$$\mathcal{D}_F \longleftrightarrow V(F_\infty) \quad F_\infty = \prod_{v|\infty} F_v$$

$$\Gamma_F \longleftrightarrow \mathrm{PGL}_2(F_\infty)$$

We want to construct a fundamental domain  $\Gamma_F \backslash V(F_\infty)$ .

$$\mathrm{PGL}_2(F_\infty) \backslash V(F_\infty) \cong \coprod F_\infty^2$$

$$\mathrm{PGL}_2(\mathbb{R}) \backslash V(\mathbb{R}) \cong \coprod \mathbb{R}^2$$

the image

Let  $R$  be  $V$ 's section  $F_\infty^2 \rightarrow V(F_\infty)$ .

$\{X^3y + IXy^3 + Jy^4\}$  is  $R$  when  $F = \mathbb{Q}$ .  $\left( \begin{matrix} I=A \\ J=B \end{matrix} \right.$  in this case.)

$$\Gamma \backslash \mathrm{PGL}_2(F_\infty) \cdot \mathrm{PGL}_2(F_\infty) \backslash V(F_\infty)$$

$\cong$

$$\mathcal{F}$$

It turns out  $\mathcal{F}$  can be put in a Siegel domain.

Siegel domain  $\mathcal{D}$ :

$$\mathcal{D} = N'A'K \subseteq \mathrm{PGL}_2(F_\infty)$$

bounded unipotent set  $\rightarrow$  Maximal compact  $\rightarrow \left\{ \begin{pmatrix} t_1^{-1} & \\ & t_1 \end{pmatrix}, \begin{pmatrix} t_2^{-1} & \\ & t_2 \end{pmatrix}, \dots, \begin{pmatrix} t_n^{-1} & \\ & t_n \end{pmatrix} \right\}$

where each  $t_i \geq c > 0$ .

$$|t_i/t_j| < C' \quad \forall i, j$$

Thm:  $\Gamma \backslash \text{PGL}_2(\mathbb{F}_{\infty}) \cong \coprod_{g_i} g_i \cdot D$ ,  $g_i \in \text{PGL}_2(\mathbb{F})$ .

Thm:  $\mathbb{F} \cdot R$  is an  $n$ -fold cover of a fundamental domain for the action of  $\Gamma$  on  $V(\mathbb{F}_{\infty})$   
 $n = \# \text{Stab}_{\text{PGL}_2(\mathbb{F}_{\infty})}(f)$  for  $f \in R$ .

Now we want to count  $\#(\mathbb{F} \cdot R_{H^{\infty} X} \cap \mathcal{Z}^{\text{irr}})$

Thm:  $\#(\mathbb{F} \cdot R_{H^{\infty} X} \cap \mathcal{Z}^{\text{irr}}) = \text{Vol}(\mathbb{F} \cdot R_{H^{\infty} X}) + O(E)$ .

We now count weighted lattice points.

0 if  $f$  is not loc. soluble

$$m(f) := \frac{1}{\# \text{Conj}_{\text{red}}} \left( \sum \sum \# \frac{1}{\# \text{Aut}_{\mathbb{F}_p}(V_i)} \right)^{-1}$$

$$M(f) = \prod_{\mathfrak{p}} M_{\mathfrak{p}}(f).$$

$\Rightarrow$

$$\sum_{H(E)^{\infty} X} (\# \text{Sol}_2(E) - 1) \sim \sum_{\mathfrak{p}} \#_m(\Gamma_{\mathfrak{p}} \backslash \mathcal{Z}_{\mathfrak{p}}^{\text{irr}})$$

orbits weighted by  $m$ .

$$= \sum_{\mathfrak{p}} \frac{\# \text{inf. orbits}}{\# \text{inf. stab}} \text{Vol}(\mathbb{F}_{\mathfrak{p}} \cdot R_{H^{\infty} X})$$

$$\prod_{\mathfrak{p}} \int_{V(\mathbb{Q}_{\mathfrak{p}})} m_{\mathfrak{p}}(f) df$$

$$= \sum_{\beta} \frac{\# \text{ inf. orbits}}{\# \text{ stab at } \infty} |J| \text{Vol}(F_{\beta}) \text{Vol}(R_{\text{hex}})$$

$$\prod_{\beta} |f|_{\beta} \text{Vol}(PGL_2(\mathcal{O}_{\beta})) \int_{\mathcal{O}_{\beta}^2} \frac{\# \text{ orbits}}{\# \text{ stab}} dA dB$$

$$= \sum_{\beta} \text{Vol}(F_{\beta}) \prod_{\beta} \text{Vol}(PGL_2(\mathcal{O}_{\beta})) \text{Vol}(R_{\text{hex}})$$

$$= 2 \text{Vol}(R_{\text{hex}}).$$