Computing a lower bound for $\hat{h}$ on elliptic curves over $\mathbb{Q}$

John Cremona & Samir Siksek
Nottingham Warwick

A basic problem of ANT is: if $E/\mathbb{Q}$ is an elliptic curve, find basis for $E(\mathbb{Q})$.

Usual method

Step 1 Use descent to find a basis $P_1, \dots, P_r$ for a subgroup $G \leqslant E(\mathbb{Q})$ of finite index.

Step 2 Compute a lower bound $\lambda > 0$ for $\hat{h}$ on $E(\mathbb{Q}) \setminus \{\text{torsion}\}$.

$$\hat{h} > \lambda \implies [E(\mathbb{Q}) : G] \leq \underset{\substack{\uparrow \\ \text{explicit}}}{N}$$

Step 3 (saturation / sieving) (very fast)
Deduce basis for $E(\mathbb{Q})$.

Old approach to Step 2 (old = before 24/7/06)

Suppose $\hat{h}(P) \leq \lambda$.

Write $x(P) = \dfrac{X}{Z^2}$ $\quad X, Z \in \mathbb{Z}$, $Z > 0$ coprime

Then

$$K' \leq \underbrace{\log \max\{|X|, Z^2\}}_{\text{logarithmic height}} - \hat{h}(P) \leq \underset{\substack{\uparrow \\ \text{computable}}}{K}$$

$\therefore$ Search for P satisfying

$$|X| \leq \exp(K + \lambda), \quad Z \leq \exp\left(\frac{K+\lambda}{2}\right).$$

If K is large then impractical. (3)

New approach to step 2 (New = after 24/7/06)
(Search-free method)

Properties of $\hat{h}$

(i) $\hat{h}(P) = 0 \iff P$ is torsion.

(ii) $\hat{h}(nP) = n^2\,\hat{h}(P)$

(iii) Define

$$E_{gr}(\mathbb{Q}) = E(\mathbb{Q}) \cap \prod_{p} E_0(\mathbb{Q}_p)$$

good reduction

inc ∞

For $P \in E_{gr}(\mathbb{Q})$

$$\hat{h}(P) = \lambda_\infty(P) + \log(\mathrm{denom}(x(P)))$$

where

$$\lambda_\infty : E_0(\mathbb{R}) \setminus \{0\} \longrightarrow \mathbb{R}$$

local real height

Strategy Find $\mu > 0$ such that

$\hat{h}(P) > \mu$ for $P \in E_{gr}(\mathbb{Q}) \setminus \{\text{torsion}\}$

$\Longrightarrow$ $\hat{h}(P) > \frac{\mu}{C^2}$ for $P \in E(\mathbb{Q}) \setminus \{\text{torsion}\}$

where $C = \operatorname{lcm} c_p$ (Tamagawa indecies).

Property of λ_∞

Define $\log_+ x = \log \max\{1, x\}$

Then $\lambda_\infty(P) \geq \log_+ |x(P)| - \alpha$

computable ($\alpha \geq 0$)

$\therefore$ For $P \in E_{gr}(\mathbb{Q})$

$\hat{h}(P) \geq \log_+ |x(P)| - \alpha + \log \operatorname{denom} x(P)$

Define

e_q exponent of $E_{ns}(\mathbb{F}_q) \cong E_0(\mathbb{Q}_q)/E_1(\mathbb{Q}_q)$

$$D_n = \sum_{q<\infty,\ e_q \mid n} 2\left(1 + \operatorname{ord}_q\left(\frac{n}{e_q}\right)\right)\log q$$

Lemma $P \in E_{gr}(\mathbb{Q}) \Longrightarrow$

$\log \operatorname{denom}(x(nP)) \geq D_n$

Cor $P \in E_{gr}(\mathbb{Q}) \Longrightarrow$

$\hat{h}(nP) \geq \log_+ |x(nP)| - \alpha + D_n$

Algorithm Suppose $\mu > 0$ & want

to prove $\hat{h}(P) > \mu$ $\forall P \in E_{gr}(\mathbb{Q})$ non-torsion

By contradiction :

Suppose $\exists \; P \in E_{gr}(\mathbb{Q}) \setminus \{\text{torsion}\}$

with $\hat{h}(P) \leq \mu$.

$\therefore \quad \hat{h}(nP) \leq n^2 \mu \quad \forall \, n$

$\therefore \quad \log_+ |x(nP)| \leq n^2\mu + \alpha - D_n$

Let $B_n(\mu) = \exp(n^2\mu + \alpha - D_n)$

$\therefore \quad \max\{1, |x(nP)|\} \leq B_n(\mu)$.

Compute $B_n(\mu)$ for $n = 1, 2, \ldots, k$.

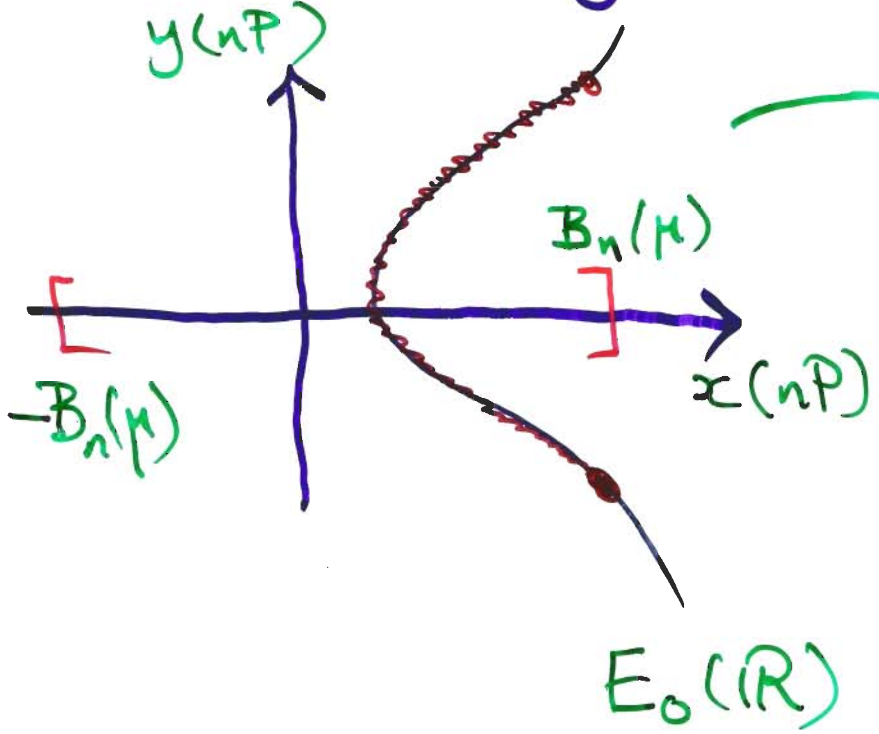
If any $B_n(\mu) < 1$ contradiction.

Otherwise Solve simultaneous system

$$-B_n(\mu) \leq x(nP) \leq B_n(\mu)$$
$$n = 1, 2, \ldots, k$$

How? $\phi : E_0(\mathbb{R}) \longrightarrow \mathbb{R}/\mathbb{Z} = [0, 1)$

elliptic log



$$\xrightarrow{\ \phi\ } \quad \phi(nP) \in [\xi_n, \zeta_n] \subseteq [0,1)$$

$\times \frac{1}{n}$ in $\mathbb{R}/\mathbb{Z}$

$$\phi(P) \in \bigcup_{i=0}^{n-1} \left[\frac{\xi_n + i}{n}, \frac{\zeta_n + i}{n} \right]$$

$$\therefore \ \phi(P) \in \underbrace{\bigcap_{n=1}^{k} \left(\bigcup_{i=0}^{n-1} \left[\frac{\xi_n + i}{n}, \frac{\zeta_n + i}{n} \right] \right)}_{}$$

If empty then contradiction.

Example

$$E: y^2+xy+y = x^3+421152067x + 105484554028056$$

60490d1

Old approach Search region

$$|X| \le \exp(23), \qquad Z \le \exp(11.5)$$

impractical.

New approach Get $\hat{h}(P) \ge 1.9865$

on $E_{gr}(\mathbb{Q})$.

$$\therefore \quad \hat{h}(P) \ge \frac{1.9865}{42^2} = 0.001126$$

on $E(\mathbb{Q})$ $\quad$ ($42 = \operatorname{lcm} c_p$)

2-Descent $\Longrightarrow$ rank $= 1$

+ pt of ∞-te order $\quad Q = \left(\frac{3583035}{169}, \dots\dots\right)$

$$[E(\mathbb{Q}) : \langle Q \rangle] \le \sqrt{\frac{\hat{h}(Q)}{0.001126}} < 78$$

Check $\forall$ $p < 78$ that $Q \notin pE(\mathbb{Q})$

$$\therefore \quad E(\mathbb{Q}) = \langle Q \rangle$$