Henri's Conference

Integral Points on Curves of Higher Genus

Samir Siksek (Warwick)

Joint work with Bugeaud, Mignotte (Strasbourg), Stoll (Bremen), Tengely (Debrecen)

Leiden May '07 Instructional workshop organized by Beukers, Evertse & Tijdeman. Organizers compiled a list of 22 open Diophantine problems:

Problem 1 Solve $y^2 - y = x^5 - x$, $x, y \in \mathbb{Z}$

Problem 2 Solve $\binom{y}{2} = \binom{x}{5}$, $x, y \in \mathbb{Z}$

} genus 2

⋮

$C : y^2 - y = x^5 - x$ $C' : \binom{y}{2} = \binom{x}{5}$

Why existing methods fail?

① **Chabauty** Determines $C(\mathbb{Q})$ if

$$\operatorname{rank}(J_C(\mathbb{Q})) < \operatorname{genus}(C)$$

Inapplicable here:

$$\operatorname{rank}(J_C(\mathbb{Q})) = 3 \qquad \operatorname{rank} J_{C'}(\mathbb{Q}) = 6$$

② **Elliptic Chabauty** Impractical here.

③ **Traditional Approach** to integral points on hyperelliptic curves:

$$a y^2 = f(x) \qquad a \in \mathbb{Z}, \quad f(x) \in \mathbb{Z}[x]$$

monic, separable

$$\Longrightarrow \quad x - \alpha = \kappa \xi^2 \qquad \kappa \in \text{finite set}$$

Conjugate:

$$x - \alpha_1 = \kappa_1 \xi_1^2 = \tau_1^2$$
$$x - \alpha_2 = \kappa_2 \xi_2^2 = \tau_2^2$$
$$x - \alpha_3 = \kappa_3 \xi_3^2 = \tau_3^2$$

by extending field $L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \sqrt{\kappa_1}, \sqrt{\kappa_2}, \sqrt{\kappa_3})$

$$\Rightarrow \tau_i^2 - \tau_j^2 = \alpha_j - \alpha_i$$

$\tau_1 - \tau_2 = \delta_1 \varepsilon_1 \quad \tau_2 - \tau_3 = \delta_2 \varepsilon_3 \quad \tau_3 - \tau_1 = \delta_3 \varepsilon_3$

$\delta_i \in$ finite set $\quad \varepsilon_i$ units.

unit equation $\quad \delta_1\varepsilon_1 + \delta_2\varepsilon_2 + \delta_3\varepsilon_3 = 0$

enormous bounds

Baker's Theory

De Weger If the unit groups can be computed, then LLL can be used to reduce the bounds to something small,

$\Longrightarrow$ can solve $a y^2 = f(x)$

Generic Situation (including C & C')

Unit groups needed cannot be computed.

But still Baker's theory gives bounds.

Baker 1969

$$y^2 = \underbrace{a_0 x^n + \cdots + a_n}_{\in \mathbb{Z}[x], \text{ separable}}$$

$n \geq 3$

$$\Longrightarrow |x| \leq \exp\left(\exp\left(\exp\left[(n^{10n} H)^{n^2}\right]\right)\right)$$

$H = \max |a_i|$

Improved by: Sprindžuk, Bridza, Schmidt, Poulakis, Voutier, Bugeaud, Győry, Bilu

Improving still on these: using for example

(i) Matveev's bounds for linear forms in logarithms

(ii) Landau's estimates for regulators

(iii) Many computations ...

For $C: y^2 - y = x^5 - x$ get

$$|x| \leq \exp\left(10^{565}\right)$$

Arithmetic Geometry

$C: y^2 - y = x^5 - x$

J Jacobian of C

Abel-Jacobi

$$C \xhookrightarrow{\ \jmath\ } J$$
$$P \longmapsto [P - \infty]$$

$$\left.\begin{aligned} J(\mathbb{Q}) &= \mathbb{Z}D_1 \oplus \mathbb{Z}D_2 \oplus \mathbb{Z}D_3 \\ D_1 &= (0,1) - \infty \\ D_2 &= (1,1) - \infty \\ D_3 &= (-1,1) - \infty \end{aligned}\right\} \text{Stoll's magma programs}$$

On J there are two height functions:

h logarithmic height

$\hat{h}$ canonical height (+ve definite qf on $J(\mathbb{Q})$

If $P = (x,y) \in C(\mathbb{Z})$ then

$$h(\jmath P) = \log \max[1, |x|] \leq 10^{565}$$

$$|h(P) - \hat{h}(P)| \leq 2.677$$

Stoll's bound

$$\hat{h}(n_1 D_1 + n_2 D_2 + n_3 D_3) = \underset{\sim}{n}\, \mathcal{H}\, \underset{\sim}{n}^t \geq \lambda \|\underset{\sim}{n}\|^2$$

$\underset{\sim}{n} = (n_1, n_2, n_3)$

$\mathcal{H}$ height pairing matrix

λ smallest eigenvalue of $\mathcal{H}$

$\therefore$ If $P \in C(\mathbb{Z})$, $P = n_1 D_1 + n_2 D_2 + n_3 D_3$

then $\|\underset{\sim}{n}\| \leq 10^{285}$

Need a method for sieving for the $\underset{\sim}{n}$.

Mordell-Weil Sieve

Due to Scharaskin.

Improved by Bruin & Stoll.

Choose prime q of good reduction.

Let M = exponent of $J(\mathbb{F}_q)$.

$$P \longmapsto \sum n_i D_i \longmapsto \underset{\sim}{n}$$

$$\begin{tikzcd}
C(\mathbb{Q}) \arrow[r, hook, "\iota"] \arrow[d] & J(\mathbb{Q}) \arrow[r, "\sim"', "\theta"'] \arrow[d] & \mathbb{Z}^3 \arrow[d] \\
C(\mathbb{F}_q) \arrow[r, hook, "\iota"] & J(\mathbb{F}_q) & (\mathbb{Z}/M\mathbb{Z})^3 \arrow[l, "\phi"']
\end{tikzcd}$$

Suppose $P \in C(\mathbb{Q})$, let $\underset{\sim}{n} = \theta(\iota P)$. Then

$$(\underset{\sim}{n} \bmod M) \in \underbrace{\phi^{-1}(\iota\, C(\mathbb{F}_q))}_{\text{computable}}.$$

Get $\underset{\sim}{n} \equiv \underline{n}_1, \ldots, \underline{n}_k \pmod{M}$

Choose lots of primes q so that the M are smooth and Chinese remainder.

Hopefully $\underset{\sim}{n} \equiv \underbrace{\underline{m}_1, \ldots, \underline{m}_l}_{\text{small}} \bmod \underset{\text{huge}}{B}$

Problem Combinatorial explosion:

Typically $M \approx |J(\mathbb{F}_q)| \approx q^2$

$$|\phi^{-1}(\iota\, C(\mathbb{F}_q))| \approx M^{1.5} \approx q^3$$

New Mordell–Weil Sieve

Construct W_i finite subsets of $J(\mathbb{Q})$

$\mathcal{L}_i$ sublattices of $J(\mathbb{Q})$ of finite index

such that $\mathcal{L}_0 \supsetneq \mathcal{L}_1 \supsetneq \mathcal{L}_2 \supsetneq \cdots\cdots$

and $\iota\, C(\mathbb{Q}) \subseteq W_i + \mathcal{L}_i$.

Start $W_0 = \{0\}$ $\qquad \mathcal{L}_0 = J(\mathbb{Q})$

Inductive Step Let $\mathcal{L}_{i+1} = \ker(\mathcal{L}_i \longrightarrow J(\mathbb{F}_q))$

$$\begin{tikzcd}
C(\mathbb{Q}) \arrow[r, "\iota"] \arrow[d, "\mathrm{red}"'] & W_i + \mathcal{L}_i \arrow[r, equal] \arrow[d, "\mathrm{red}"'] & W_i + (\mathcal{L}_i/\mathcal{L}_{i+1}) + \mathcal{L}_{i+1} \arrow[d] \\
C(\mathbb{F}_q) \arrow[r, "\iota"] & J(\mathbb{F}_q) & W_i + (\mathcal{L}_i/\mathcal{L}_{i+1}) \arrow[l, "\phi"']
\end{tikzcd}$$

Let $W_{i+1} = \phi^{-1}(\iota(C(\mathbb{F}_q)))$.

Choice of q:

(i) ℓ_i/ℓ_{i+1} is small
(ii) $|J(\mathbb{F}_q)|$ is smooth

$\Rightarrow$ hopefully W_{i+1} is small

End Using 922 primes $q \le 10^6$
(37 hours of computation)

$$\Longrightarrow j(C(\mathbb{Q})) \subseteq W + \mathcal{L}$$

$W = j$(17 known rational points)

$$[J(\mathbb{Q}) : \mathcal{L}] \approx 3.32 \times 10^{3240}$$

Shortest vector of $\mathcal{L}$ has length $\approx 1.156 \times 10^{1080}$.

So if $P \in C(\mathbb{Z})$ then

$$j(P) = \underset{\sim}{w} + \underset{\sim}{\ell} \qquad \underset{\sim}{w} \text{ tiny}$$

$$\underset{\sim}{\ell} = \underset{\sim}{0} \quad \text{or} \quad \|\underset{\sim}{\ell}\| \ge 1.156 \times 10^{1080}.$$

But $\|j(P)\| \le 10^{285} \Rightarrow \underset{\sim}{\ell} = \underset{\sim}{0}$

$P \in$ known points.

Theorem The integral points on $C : y^2 - y = x^5 - x$ are

$(-1,0), (-1,1), (0,0), (0,1), (1,0), (1,1),$
$(2,-5), (2,6), (3,-15), (3,16), (30,-4929), (30,4930)$

Observation This method should work for any model of a curve of genus ≥ 2 where the problem of integral points can be reduced to unit equations.

Future Plans

(I) Improve the Mordell–Weil sieve using discrete logarithms

(II) Do $\binom{y}{2} = \binom{x}{5}$

(III) Integral points on genus 2 curves using linear forms of Abelian logs.