# Integral Points on Curves of Higher Genus

Samir Siksek (Warwick)

Joint work with
Bugeaud, Mignotte — Strasbourg
Stoll — Bayreuth
Tengely — Debrecen

Leiden May 2007 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

⋮

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

# 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:

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

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

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

where $\tau_i \in L := \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \sqrt{\kappa_1}, \sqrt{\kappa_2}, \sqrt{\kappa_3})$

$$\Longrightarrow \quad \tau_i^2 - \tau_j^2 = \alpha_j - \alpha_i$$

$$\tau_1 - \tau_2 = \delta_1 \varepsilon_1 \qquad \tau_2 - \tau_3 = \delta_2 \varepsilon_2 \qquad \tau_3 - \tau_1 = \delta_3 \varepsilon_3$$

$\delta_i \in$ finite set $\qquad \varepsilon_i \in$ units

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

$\tau_1 - \tau_2 = \delta_1 \varepsilon_1 \quad \tau_2 - \tau_3 = \delta_2 \varepsilon_2 \quad \tau_3 - \tau_1 = \delta_3 \varepsilon_3$

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

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

Baker's Theory gives (enormous) bounds for unit eqns.

De Weger If unit groups can be computed, then LLL can be used to reduce the bounds to something small $\Rightarrow$ can solve $ay^2 = f(x)$

Generic Situation (including $C$ & $C'$)
Unit groups needed cannot be computed. But still Baker's theory gives bounds.

Baker 1969 $\quad y^2 = \underbrace{a_n x^n + \cdots + a_0}_{\in \mathbb{Z}[x],\ \text{separable}} \quad (n \geq 3)$

$\Rightarrow |x| \leq \exp(\exp(\exp\{(n^{10n} H)^{n^2}\}))$

$H = \max |a_i|$.

Improved by: Sprindžuk, Brindza, Schmidt, Poulakis, Voutier, Bugeaud, Győry, Bilu, ....

We give an <u>algorithm</u> for computing an upper bound for solutions of hyperelliptic equations.

For $\left.\begin{array}{l} C: y^2 - y = x^5 - x \\ C': \binom{y}{2} = \binom{x}{5} \end{array}\right\}$ get

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

Effective bounds exist for superelliptic eqns, Thue-Mahler eqns, .... c.f. Shorey & Tijdeman.

<u>Bilu</u>, <u>Dvornicich & Zannier</u>: Suppose $C/\mathbb{Q}$ curve, $\text{genus}(C) \geq 1$, $f \in \mathbb{Q}(C)$ such that $\overline{\mathbb{Q}}(C)/\overline{\mathbb{Q}}(f)$ is Galois. Then $\{P \in C(\mathbb{Q}) : f(P) \in \mathbb{Z}\}$ is effectively bounded.

~~Arithmetic~~ Geometry $\quad C: y^2 - y = x^5 - x$

$J$ Jacobian of $C$

$$C \xrightarrow{j} J \qquad \text{Abel-Jacobi}$$
$$P \longmapsto [P - \infty]$$

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

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

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

Stoll's bound

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

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

$\mathcal{H}$ height pairing matrix

$\lambda$ 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 $\|\underline{n}\| \leq 10^{285}$

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

# Mordell - Weil Sieve

Due to Scharaskin, Bruin & Elkies

Improved by Bruin & Stoll.

Construct $W_i$ finite subsets of $J(\mathbb{Q})$
$M_i$ +ve integers s.t.

$$M_i \mid M_{i+1} \quad \forall i$$

and $\jmath C(\mathbb{Q}) \subseteq W_i + M_i J(\mathbb{Q})$.

<u>Start</u> $W_0 = \{0\}$ $\quad M_0 = 1$

<u>Inductive Step</u> Let $q$ be a prime of good reduction. Let

$$M_{i+1} = \mathrm{LCM}(M_i, \text{ exponent of } J(\mathbb{F}_p))$$

$$W'_{i+1} = W_i + \frac{M_i J(\mathbb{Q})}{M_{i+1} J(\mathbb{Q})}$$

$$\begin{tikzcd}
C(\mathbb{Q}) \arrow[r, hook, "\jmath"] \arrow[d] & W_i + M_i J(\mathbb{Q}) = W'_{i+1} + M_{i+1} J(\mathbb{Q}) \arrow[d] \arrow[dr] & \\
C(\mathbb{F}_q) \arrow[r, hook, "\jmath"] & J(\mathbb{F}_q) & W'_{i+1} \arrow[l, "\phi"']
\end{tikzcd}$$

Let $W_{i+1} = \{ w \in W'_{i+1} : \phi(w) \in \jmath C(\mathbb{F}_q) \}$.

Clearly $\jmath C(\mathbb{Q}) \subseteq W_{i+1} + M_{i+1} J(\mathbb{Q})$.

<u>In practice</u> $\# W'_{i+1} = \# W_i \times \underbrace{\left(\frac{M_{i+1}}{M_i}\right)^{\operatorname{rk} J(\mathbb{Q})}}_{\text{huge}}$

Combinatorial explosion!

# New Mordell–Weil Sieve

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

$L_i$ sublattices of $J(\mathbb{Q})$ of finite index

such that $L_0 \supsetneq L_1 \supsetneq L_2 \supsetneq \cdots\cdots$

and $\jmath C(\mathbb{Q}) \subseteq W_i + L_i \quad \forall i$

**Start** $W_0 = \{0\} \qquad L_0 = J(\mathbb{Q})$

**Inductive Step** Let $L_{i+1} = \ker\left(L_i \longrightarrow J(\mathbb{F}_q)\right)$

$$W'_{i+1} = W_i + \left(L_i / L_{i+1}\right)$$

$$\begin{tikzcd}
C(\mathbb{Q}) \arrow[r, "\jmath"] \arrow[d] & W_i + L_i = W'_{i+1} + L_{i+1} \arrow[d] \arrow[dr] & \\
C(\mathbb{F}_q) \arrow[r, "\jmath"] & J(\mathbb{F}_q) & W'_{i+1} \arrow[l, "\phi"']
\end{tikzcd}$$

Let $W_{i+1} = \{ w \in W'_{i+1} : \phi(w) \in \jmath\, C(\mathbb{F}_q) \}$.

Clearly $\jmath C(\mathbb{Q}) \subseteq W_{i+1} + L_{i+1}$.

**Note** $\# W'_{i+1} = \# W_i \times \# \left(L_i / L_{i+1}\right)$.

**Choice of $q$:**

(i) $\ell_i / \ell_{i+1}$ is small
(ii) $|J(\mathbb{F}_q)|$ is smooth $\Longrightarrow$ hopefully $|W_{i+1}|$ is small

**End** Using 922 primes $q \leq 10^6$
(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

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

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

**But** $\|j(P)\| \leq 10^{285} \Rightarrow \underset{\sim}{\ell} = \underset{\sim}{0}$
$P \in$ known points.

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

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

**Thm** The only solutions to

$$\binom{y}{2} = \binom{x}{5}$$

are $(x,y) = (15,-77)$, $(7,-6)$, $(6,-3)$, $(5,-1)$, $(0,0)$, $(1,0)$, $(2,0)$, $(3,0)$, $(4,0)$, $(0,1)$, $(1,1)$, $(2,1)$, $(3,1)$, $(4,1)$, $(5,2)$, $(6,4)$, $(7,7)$, $(15,78)$.

Can apply same method for any curve $C$ provided: $g(C) \geq 2$

(i) $C(\mathbb{Z})$ effectively bounded

(ii) Can compute $J(\mathbb{Q})$

(iii) Can compute $\hat{h}$ & bound $h - \hat{h}$