Deciding the existence of rational points on curves

Nils Bruin (SFU)

joint with Michael Stoll (IU Bremen)

Computational Challenges Workshop

Fields Institute, November 3, 2006

Motivation

Hilbert's 10th: Design an automatic procedure that, given a polynomial $f \in \mathbb{Z}[x_1, \ldots, x_n]$, decides if

$$f(x_1, \ldots, x_n) = 0 \text{ has a solution } x_1, \ldots, x_n \in \mathbb{Z}$$

Theorem (Davis, Matyasevitch, Putnam, Robinson): Hilbert's 10th can't be done.

Open questions:

- What if we restrict to a subclass of polynomials?
- What about *rational* solutions rather than *integer* solutions?

Today: (Smooth) Projective curves over $\mathbb{Q}$.

Dilbert's 10th: Small genus 2 curves:

$$C : y^2 = f_6 x^6 + \cdots + f_0 \text{ with } f_i \in \{-3, \ldots, 3\}$$

Method and heuristics

Strategy: Given $C : y^2 = f_6x^6 + f_5x^5 + \cdots + f_0$,

- Search for points on C up to a height bound (say, 10000)
- Look for local obstruction: $C(\mathbb{Q}_p) = \emptyset$ or $C(\mathbb{R}) = \emptyset$.
- **Theorem** (Chevalley, Weil): Given an unramified Galois cover $\pi : D \to C$, there is a finite collection of twists $\{\pi_\delta : D_\delta \to C\}$ such that

$$\bigcup_\delta \pi_\delta(D_\delta(\mathbb{Q})) = C(\mathbb{Q})$$

  Fact: For a given D/C, one can explicitly compute these δ.
  Approach: Try to prove that each D_δ has a local obstruction.

- Determine $\mathrm{Jac}(C)(\mathbb{Q})$ and check if C has a rational degree 1 divisor class (possible in theory if $\text{Ш}(\mathrm{Jac}(C)/\mathbb{Q})$ is finite)
- Try Mordell-Weil Sieving. **GENERALLY APPLICABLE!**

Experimental data

Test curves: $C : y^2 = f_6x^6 + \cdots + f_0$ with $f_i \in \{-3, \ldots, 3\}$.

All isomorphism classes	196 211	100.00 %
Curves with rational points	137 530	70.09 %
Curves without(?) rational points	58 681	29.91 %
ELS curves total	166 808	85.01 %
ELS curves without(?) rational points	29 278	14.92 %

(ELS = Everywhere Locally Solvable)

- The high number of curves with rational points is definitely an artifact of small numbers
- Poonen and Stoll predict that about 85% of all genus 2 curves are ELS.

2-Covers of Hyperelliptic Curves

Curve: Let $f(x) \in \mathbb{Q}[x]$ be square-free and even degree. Consider

$$C : y^2 = f(x).$$

Algebra: For $K \supset \mathbb{Q}$ consider $A_K := K[\theta] = K[X]/f(x)$.

$$\begin{array}{llcll} \mu_K : & C(K) & \longrightarrow & M_K & = A_K^*/K^*A_K^{*2} \\ & (x,y) & \longmapsto & x-\theta & \end{array}$$

$$\begin{tikzcd} C(\mathbb{Q}) \arrow[r, "\mu"] \arrow[d] & M_{\mathbb{Q}} \arrow[d, "r_p"] \\ C(\mathbb{Q}_p) \arrow[r, "\mu_p"] & M_{\mathbb{Q}_p} \end{tikzcd}$$

Definition: $S^{(2)}_{\text{fake}}(C/\mathbb{Q}) = \{\delta \in M_{\mathbb{Q}} : r_p(\delta) \in \mu_p(C(\mathbb{Q}_p))$ for all $p\}$

Geometric interpretation

Definition: $S^{(2)}_{\text{fake}}(C/\mathbb{Q}) = \{\delta \in M_{\mathbb{Q}} : r_p(\delta) \in \mu_p(C(\mathbb{Q}_p))$ for all $p\}$

Interpretation: $\delta \in S^{(2)}_{\text{fake}}(C/\mathbb{Q})$ corresponds to a cover $\pi_\delta : D_\delta \to C$ with $\mathrm{Aut}(D_\delta/C) = \mathrm{Jac}(C)[2]$.

Fake: If $\iota : C \to C$ is $(x,y) \mapsto (x,-y)$, then π_δ and $\iota \circ \pi_\delta$ give same δ:

$$\begin{tikzcd} D_\delta \arrow[rr, dashed, bend left, "?"] \arrow[dr, "\pi_\delta"'] & & D_\delta \arrow[dl, "\iota\circ\pi_\delta"] \\ & C & \end{tikzcd}$$

Criterion:

$$C(\mathbb{Q}) = \bigcup_{\delta \in S^{(2)}_{\text{fake}}(C/\mathbb{Q})} \pi_\delta(D_\delta(\mathbb{Q})) \cup \iota \circ \pi_\delta(D_\delta(\mathbb{Q}))$$

Experimental data

Test curves: $C : y^2 = f_6 x^6 + \cdots + f_0$ with $f_i \in \{-3, \ldots, 3\}$.

All isomorphism classes	196 211	100.00 %
Curves with rational points	137 530	70.09 %
Curves without(?) rational points	58 681	29.91 %
ELS curves total	166 808	85.01 %
ELS curves without(?) rational points	29 278	14.92 %
Curves with ELS 2-covers among these	1 492	0.76 %

(ELS = Everywhere Locally Solvable)

Mordell-Weil Sieving

Embedding: Given $\mathfrak{d} \in \underline{\mathrm{Pic}}^1(C)(\mathbb{Q})$, we have

$$\begin{array}{rccc} i: & C & \hookrightarrow & \mathrm{Jac}(C) \\ & P & \mapsto & [P] - \mathfrak{d} \end{array}$$

Kernel of reduction: $0 \to \Lambda_p \to \mathrm{Jac}(C)(\mathbb{Q}) \to \mathrm{Jac}(C)(\mathbb{F}_p)$

$$\begin{tikzcd} C(\mathbb{Q}) \arrow[r] \arrow[d] & \mathrm{Jac}(C)(\mathbb{Q}) \arrow[d, "\rho_p"] \\ C(\mathbb{F}_p) \arrow[r, "i_p"] & \mathrm{Jac}(C)(\mathbb{F}_p) \end{tikzcd}$$

Cosets: $V_p = (\mathrm{im}(i_p) \cap \mathrm{im}(\rho_p)) + \Lambda_p$.

Intersection: If $\Lambda_p + \Lambda_q \neq \mathrm{Jac}(C)(\mathbb{Q})$ then $V_p \cap V_q$ may be empty even if V_p and V_q are not.

Mordell-Weil Sieving – Heuristics

Idea (Scharaschkin, Flynn, B.,...): Pick a finite set S of (good) primes.

$$\begin{tikzcd} C(\mathbb{Q}) \arrow[r] \arrow[d] & \mathrm{Jac}(C)(\mathbb{Q}) \arrow[d, "\rho_S"] \\ \prod_{p\in S} C(\mathbb{F}_p) \arrow[r, "i_S"] & \prod_{p\in S} \mathrm{Jac}(C)(\mathbb{F}_p) \end{tikzcd}$$

Heuristic (Poonen): $\#\big(\mathrm{im}(\rho_S) \cap \mathrm{im}(i_S)\big)$ is likely very small.

$$\lim_{\#S\to\infty} \frac{\#\big(\prod_{p\in S} C(\mathbb{F}_p)\big) \cdot \#\mathrm{im}(\rho_S)}{\#\big(\prod_{p\in S} \mathrm{Jac}(C)(\mathbb{F}_p)\big)} = 0$$

Sensible choice: For some bound B,

$$S := \left\{ p \le B^2 \text{ prime} \;\middle|\; \begin{array}{l} C \text{ has good reduction at } p \text{ and} \\ \#\mathrm{Jac}(C)(\mathbb{F}_p) \text{ is } B\text{-smooth} \end{array} \right\}$$

Heuristics: Weil bounds

Happy fact: Smooth numbers are plentiful: for $u > 0$,

$$\lim_{B\to\infty} \frac{\#\{n \in [1,\ldots,B] : n \text{ is } B^u\text{-smooth}\}}{B} > 0$$

Weil-Bounds: $\#\mathrm{Jac}(C)(\mathbb{F}_p) = p^{g+o(1)}$ and $\#C(\mathbb{F}_p) = p^{1+o(1)}$.

Assumption: $\#\mathrm{Jac}(C)(\mathbb{F}_p)$ behaves as a typical integer of its size:

$$\lim_{B\to\infty} \#S/B > 0$$

First bound:

$$\prod_{p\in S} \frac{\#C(\mathbb{F}_p)}{\#\mathrm{Jac}(C)(\mathbb{F}_p)} \leq \prod_{p\in S} p^{(1-g+o(1))} < \exp(c(1-g+o(1))B^2)$$

Heuristics: Bounding Mordell-Weil image

Recap:

$$\prod_{p\in S} \frac{\#C(\mathbb{F}_p)}{\#\mathrm{Jac}(C)(\mathbb{F}_p)} < \exp(c(1-g+o(1))B^2)$$

Group Exponent: $\prod_{p\in S} \mathrm{Jac}(C)(\mathbb{F}_p)$ is far from cyclic:

$$\begin{aligned}
\text{exponent}\left(\prod_{p\in S} \mathrm{Jac}(C)(\mathbb{F}_p)\right) &\leq \prod_{\text{primes } p\leq B} B^{2g+o(1)} \\
&\leq B^{\pi(B)(2g+o(1))} \\
&\leq \exp((2g+o(1))B)
\end{aligned}$$

Mordell-Weil rank: If $\mathrm{rkJac}(C)(\mathbb{Q}) = r$ then

$$\#\mathrm{im}(\rho_S) \leq \exp((2g+o(1))B)^r$$

Expected size of $\mathrm{im}(i_S) \cap \mathrm{im}(\rho_S)$**:**

$$\#\mathrm{im}(\rho_S) \cdot \prod_{p\in S} \frac{\#C(\mathbb{F}_p)}{\#\mathrm{Jac}(C)(\mathbb{F}_p)} \leq \exp(r(2g+o(1))B - c(g-1+o(1))B^2)$$

Mordell-Weil Sieving (cont.)

Idea (Scharaschkin, Flynn, B.,...): Pick a finite set S of (good) primes.

$$\begin{tikzcd} C(\mathbb{Q}) \arrow[r] \arrow[d] & \mathrm{Jac}(C)(\mathbb{Q}) \arrow[d, "\rho_S"] \\ \prod_{p\in S} C(\mathbb{F}_p) \arrow[r, "i_S"] & \prod_{p\in S} \mathrm{Jac}(C)(\mathbb{F}_p) \end{tikzcd}$$

Heuristic (Poonen): If S is large enough, then one would expect

$$\mathrm{im}(i_S) \cap \mathrm{im}(\rho_S) = \emptyset.$$

Practice:

- Efficiency demands computing discrete logarithms in $\mathrm{Jac}(C)(\mathbb{F}_p)$.
  (pick S such that the group orders are mainly smooth)
- Combinatorial explosion looms, because $\mathrm{im}(i_S)$ will be huge.
  (work in quotients G/B_iG for $B_1 \mid B_2 \mid B_3 \mid \ldots$)

Determining the Mordell-Weil groups

Mordell-Weil groups:

conj. $Ш(J)$	0	$(\mathbb{Z}/2\mathbb{Z})^2$	$(\mathbb{Z}/4\mathbb{Z})^2$	Total
$\text{rank} J(\mathbb{Q}) = 0$	3		36	39
$\text{rank} J(\mathbb{Q}) = 1$	516	5	5	526
$\text{rank} J(\mathbb{Q}) = 2$	772		1	773
$\text{rank} J(\mathbb{Q}) = 3$	152			152
$\text{rank} J(\mathbb{Q}) = 4$	2			2
all ranks	1445	5	42	1492

- For the second column the ranks are proved using a visualization argument
- For 4 entries in the third colums, we proved the rank using a visualization argument, subject to GRH.
- According to BSD, this whole table is correct.

Experimental data

Test curves: $C : y^2 = f_6 x^6 + \cdots + f_0$ with $f_i \in \{-3, \ldots, 3\}$.

All isomorphism classes	196 211	100.00 %
Curves with rational points	137 530	70.09 %
Curves without(?) rational points	58 681	29.91 %
ELS curves total	166 808	85.01 %
ELS curves without(?) rational points	29 278	14.92 %
Curves with ELS 2-covers among these	1 492	0.76 %
Curves that need GRH or BSD conjecture	42	0.02 %

(ELS = Everywhere Locally Solvable)

Conclusion: For all but 42 curves, we were able to decide their solvability. Subject to standard conjectures, we were able to resolve all.