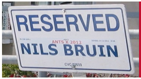
Success and challenges in determining the rational points on curves



SFU

ANTS X,
San Diego, July 13, 2012

Example problems: Find the solutions $x, y \in \mathbb{Q}$ to

$$x^2 + y^2 = 1$$
$$x^2 + y^2 = -1$$
$$x^2 + y^2 = 5$$
$$x^2 + y^2 = 3$$
$$3x^3 + 4y^3 = 5$$
$$x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1 = y^2$$
$$x^6 + x^2 + 1 = y^2$$
$$x^6 + 6x^5 - 15x^4 + 20x^3 + 15x^2 + 30x - 17 = y^2$$
$$(x^3 - x^2 - 2x + 1)y^7 - (x^3 - 2x^2 - x + 1) = 0$$
$$x^4 + y^4 + x^2y + 2xy - y^2 + 1 = 0$$
$$x^2y^2 - xy^3 - x^3 - 2x^2 + y^2 - x + y = 0$$

Note: All of these ask for the *rational points* on curves.

Central Questions

Definition: A curve C over $\mathbb{Q}$ is *nice* if it is:

smooth, *projective*, *absolutely irreducible*.

Typical example: Smooth plane projective curve:

$$C\colon X^4+Y^4+X^2YZ+2XYZ^2-Y^2Z^2+Z^4=0$$

Decision problem: Given a nice curve C over $\mathbb{Q}$,

decide if $C(\mathbb{Q})=\emptyset$.

Determination problem: Given a nice curve C over $\mathbb{Q}$,

find a useful description of $C(\mathbb{Q})$.

For curves of genus >1: List the finite set $C(\mathbb{Q})$.

Outline

1. Outline of a procedure to tackle the decision problem
2. Highlight challenges in executing the procedure
3. Finite Descent as a tool to face these challenges
4. Results for smooth plane quartics

Adelic points:

$$C(\mathbb{Q}) \hookrightarrow C(\mathbb{A}) := C(\mathbb{R}) \times \prod_p C(\mathbb{Q}_p)$$

Global-Local principle:

$$C(\mathbb{Q}) \neq \emptyset \quad \text{implies} \quad C(\mathbb{A}) \neq \emptyset$$

Happy fact: Deciding if $C(\mathbb{A}) = \emptyset$ is decidable.

Local-Global principle fails:

$$C(\mathbb{A}) \neq \emptyset \quad \text{does not imply} \quad C(\mathbb{Q}) \neq \emptyset,$$

Examples:

$$3X^3 + 4Y^3 + 5Z^3 = 0$$

$$X^4 + Y^4 + X^2YZ + 2XYZ^2 - Y^2Z^2 + Z^4 = 0$$

Better information

Alternative approach: Embed curve C in another variety with a sparser set of rational points, e.g., an Abelian variety J.

Theorem (Mordell-Weil): $J(\mathbb{Q})$ is a finitely generated abelian group:

$$J(\mathbb{Q}) \simeq \underbrace{J(\mathbb{Q})_{\mathrm{tors}}}_{\text{finite}} \times \mathbb{Z}^r$$

Principal homogeneous space: $C \subset \underline{\mathrm{Pic}}_C^1$ under $J = \underline{\mathrm{Pic}}_C^0$.

$$\underline{\mathrm{Pic}}_C^1(\mathbb{Q}) \neq \emptyset \quad \text{if and only if} \quad \underline{\mathrm{Pic}}_C^1 \simeq J$$

Challenge: Decide if $\underline{\mathrm{Pic}}_C^1(\mathbb{Q}) = \emptyset$ or find $\mathfrak{d} \in \underline{\mathrm{Pic}}_C^1(\mathbb{Q})$.

If $\underline{\mathrm{Pic}}_C^1(\mathbb{Q}) = \emptyset$ then $C(\mathbb{Q}) = \emptyset$. Otherwise $\iota_{\mathfrak{d}} : C \hookrightarrow J$.

Challenge: Compute $J(\mathbb{Q}) \simeq J(\mathbb{Q})_{\mathrm{tors}} \times \mathbb{Z}^r$, in particular r.

Mordell-Weil group combined with adelic information

Assume:

- We have $\mathfrak{d} \in \underline{\mathrm{Pic}}^1_C(\mathbb{Q})$.
- We have generators for $J(\mathbb{Q})$.

Commutative diagram:

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{\iota} & J(\mathbb{Q}) \\ \downarrow{\tilde{\rho}} & & \downarrow{\tilde{\rho}} \\ C(\mathbb{A}) & \xrightarrow{\iota} & J(\mathbb{A})_{\bullet} \end{array}$$

(Watch the Poonen • which modifies the $J(\mathbb{R})$ factor)

Conjecture: Writing $\overline{C(\mathbb{Q})} \subset C(\mathbb{A})$ for the topological closure,

$$\overline{C(\mathbb{Q})} \stackrel{?}{=} \iota(C(\mathbb{A})) \cap \overline{\tilde{\rho}(J(\mathbb{Q}))}$$

(see [Scharaschkin, B-Elkies (ANTS V), Flynn, B.-Stoll])

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{\iota} & J(\mathbb{Q})/BJ(\mathbb{Q}) \\ \downarrow \rho_S & & \downarrow \rho_S \\ \prod_{p\in S} C(\mathbb{F}_p) & \xrightarrow{\iota_S} & \prod_{p\in S} J(\mathbb{F}_p)/B\cdot \mathrm{im}(\rho_p) \end{array}$$

- Let S be a finite set of primes ; B a positive integer
- Let $\Lambda_p = \ker(\rho_p\colon J(\mathbb{Q}) \to J(\mathbb{F}_p))$ and $\Lambda_S := \bigcap_{p\in S} \Lambda_p$
- $C(\mathbb{Q}) \to V_{S,B} := \mathrm{im}(\iota_S) \cap \mathrm{im}(\rho_S) \subset \dfrac{J(\mathbb{Q})}{\Lambda_S + BJ(\mathbb{Q})}$

Heuristic (Poonen): For appropriate S, B, the set $V_{S,B}$ consists only of cosets containing a point from $C(\mathbb{Q})$.

Decision procedure

INPUT: A nice curve C of genus $g > 0$.
OUTPUT: $P \in C(\mathbb{Q})$ or `Unsolvable` if $C(\mathbb{Q}) = \emptyset$.
Execute in parallel:

0. Try candidates for $P \in C(\mathbb{Q})$ and return P if one is found. Information from $V_{S,B}$ (step 5) helps.

and

1. If $C(\mathbb{A}) = \emptyset$ return `Unsolvable`
2. Determine $\mathfrak{d} \in \underline{\mathrm{Pic}}^1_C(\mathbb{Q})$ or return `Unsolvable` if $\underline{\mathrm{Pic}}^1_C(\mathbb{Q}) = \emptyset$.
3. Determine $J(\mathbb{Q})$.
4. Choose reasonable values for S, B.
5. Mordell-Weil sieving: If $V_{S,B} = \emptyset$ return `Unsolvable`.
6. Increase S, B; go to 5.

How well does this work?

Test case (B.-Stoll): Consider genus 2 curves admitting a model

$$C\colon y^2 = f_6x^6 + f_5x^5 + \cdots + f_0 \text{ with } f_i \in \{-3,\ldots,3\}$$

Success: We were able to decide for all of them!

All curves	196 171	100.00 %
Curves with rational points	137 490	70.09 %
Curves without rational points	58 681	29.91 %
Curves with $C(\mathbb{A}) \neq \emptyset$	166 768	85.01 %
Curves with $C(\mathbb{A}) \neq \emptyset$ and $C(\mathbb{Q}) = \emptyset$	29 278	14.92 %
Curves that need BSD conjecture	42	0.02 %

Disclosure: We only really needed MW-sieving for 1445 of these curves (27786 of these curves have a non-trivial 2-cover obstruction to having rational points)

How to deal with rational points

(see [Chabauty, Coleman, Flynn])

Problem: If $P \in C(\mathbb{Q})$ then $V_{S,B}$ is never empty.

Idea (Chabauty): Construct a p-adic analytic function Φ_p on $C(\mathbb{Q}_p)$ that vanishes on $C(\mathbb{Q})$.

Restriction: Construction only works if $\mathrm{rk} J(\mathbb{Q}) = r < g$.

Sketch of procedure:

1. Use MW-Sieving to find S, B and $P_i \in C(\mathbb{Q})$ such that

$$V_{S,B} = \{P_1, \ldots, P_n\} + \Lambda_S + BJ(\mathbb{Q})$$

2. Find prime p with $BJ(\mathbb{Q}) \subset \Lambda_p$ such that

$$P_i \not\equiv P_j \pmod{p} \text{ for any } i \neq j$$

3. For each P_i, use Φ_p to show that there are no other rational points Q with $Q \equiv P_i \pmod{p}$

No guarantee that either procedure will terminate, i.e.:

- We only have a heuristic that MW-sieving converges to a sharp result.
- We have no guarantee we can always find a p such that Φ_p does not have inconvenient extraneous p-adic zeros.

Bigger problem: we cannot guarantee we can get started:

For decision procedure:

- Decide if $\underline{\mathrm{Pic}}^1_C(\mathbb{Q}) = \emptyset$ or find $\mathfrak{d} \in \underline{\mathrm{Pic}}^1_C(\mathbb{Q})$.
- Determine the r in $J(\mathbb{Q}) \simeq J(\mathbb{Q})_{\mathrm{tors}} \times \mathbb{Z}^r$
- Find generators for $J(\mathbb{Q})$

For determination procedure:

- What to do if $r \geq g$?
  (See [Wetherell, B.; future: Kim, Balakrishnan?])

n-descent

Multiplication-by-n:

$$0 \to J[n] \to J \xrightarrow{n} J \to 0$$

Taking galois cohomology:

$$0 \to \frac{J(\mathbb{Q})}{nJ(\mathbb{Q})} \xrightarrow{\gamma} H^1(\mathbb{Q}, J[n]) \to H^1(\mathbb{Q}, J)$$

Approximate image locally:

$$\begin{array}{ccc} \dfrac{J(\mathbb{Q})}{nJ(\mathbb{Q})} & \xrightarrow{\quad\gamma\quad} & H^1(\mathbb{Q}, J[n]) \\ \downarrow & & \downarrow {\scriptstyle \prod \rho_p} \\ \prod_p \dfrac{J(\mathbb{Q}_p)}{nJ(\mathbb{Q}_p)} & \xrightarrow{\prod \gamma_p} & \prod_p H^1(\mathbb{Q}_p, J[n]) \end{array}$$

$$\mathrm{Sel}^n(J/\mathbb{Q}) := \{\delta \in H^1(\mathbb{Q}, J[n]) : \rho_p(\delta) \in \operatorname{im} \gamma_p \text{ for all } p\}$$

Explicit descent computations: We need to work with

$$\gamma\colon \frac{J(k)}{nJ(k)} \to H^1(k, J[n]) \text{ for } k = \mathbb{Q}, \mathbb{R}, \mathbb{Q}_p$$

- How do we represent $J(k)$?
- How do we represent $H^1(k, J[n])$?
- How do we compute γ?

Representing $J(k)$:
$\mathrm{Pic}^0(C/k) \subset J(k)$; equality if $C(\mathbb{A}) \neq \emptyset$. Use divisors on the curve.

Representing $H^1(k,J[n])$

Problem: We only know how to efficiently represent $H^1(k,M)$ for a very limited class of Galois modules.

Twisted power: Let M be a Galois module and $\Delta = \operatorname{Spec} L = \{\theta_1,\ldots,\theta_m\}$ a Galois set. Define

$$M^\Delta := M\theta_1 \oplus \cdots \oplus M\theta_m$$

Hilbert 90: $H^1(k,\mu_n^\Delta) = L^\times/L^{\times n}$.

Let $J[n] = \operatorname{Spec}(L)$. Consider

$$0 \to J[n] \to (\mu_n)^{J[n]} \to R^\vee \to 0$$

Cohomology: $H^1(k,J[n]) \to L^\times/L^{\times n}$.

(see [Cassels, Schaefer, Poonen-Shaefer, B.-Poonen-Stoll])

Writing $L_p = L \otimes \mathbb{Q}_p$

$$\begin{array}{ccc} \dfrac{J(\mathbb{Q})}{nJ(\mathbb{Q})} & \xrightarrow{\tilde{\gamma}} & \dfrac{L^\times}{L^{\times n}} \\ \downarrow & & \downarrow \\ \dfrac{J(\mathbb{Q}_p)}{nJ(\mathbb{Q}_p)} & \xrightarrow{\tilde{\gamma}_p} & \dfrac{L_p^\times}{L_p^{\times n}} \end{array}$$

- Map $\tilde{\gamma}$ is induced by a function $f \in k(C) \otimes L$.
- Images of $\tilde{\gamma}_p$ are computable.
- For most p, this image lands in “unramified” part
- Image of $\tilde{\gamma}$ is generated by S-units.

$$\mathrm{Sel}^{\tilde{\gamma}}(J) = \{\delta \in L^\times / L^{\times n} : \rho_p(\delta) \in \mathrm{im}\, \tilde{\gamma}_p \text{ for all } p\}$$

Bounding Ranks:

$$\frac{J(\mathbb{Q})}{nJ(\mathbb{Q})} = \frac{J(\mathbb{Q})_{\mathrm{tors}}}{nJ(\mathbb{Q})_{\mathrm{tors}}} \times \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^r$$

So bounding the size of $\operatorname{im}\gamma$ bounds r (hopefully sharply).

Embedding curve in J:

$$[\underline{\mathrm{Pic}}^1_C] \in H^1(\mathbb{Q}, J[2g-2])$$

There exists $\mathfrak{d} \in \underline{\mathrm{Pic}}^1_C(\mathbb{Q})$ if and only if $[\underline{\mathrm{Pic}}^1_C] \in \operatorname{im}\gamma$.

Bonus: Map $\tilde{\gamma}$ can be evaluated immediately on C.

$$\mathrm{Sel}^{\tilde{\gamma}}(C) = \{\delta \in L^\times/L^{\times n} : \rho_p(\delta) \in \tilde{\gamma}_p(C(\mathbb{Q}_p)) \text{ for all } p\}$$

Example: Smooth plane quartics (B.-Poonen-Stoll)

Let C be a smooth plane quartic.

- Set $\Delta = \mathrm{Spec}(L)$ of 28 bitangents
- Even weight vectors $E \subset (\mathbb{Z}/2\mathbb{Z})^\Delta$:

$$\begin{array}{ccccccccc} & & & & \mu_2^\Delta & & & & \\ & & & & \downarrow & & & & \\ 0 & \longrightarrow & J[2] & \longrightarrow & E^\vee & \longrightarrow & R^\vee & \longrightarrow & 0 \end{array}$$

- Cohomology:

$$\begin{array}{ccccccccccc} & & & & & & & & \dfrac{J(k)}{2J(k)} & \xrightarrow{\tilde{\gamma}} & \dfrac{L^\times}{L^{\times 2}k^\times} \\ & & & & & & & & \downarrow \gamma & & \downarrow \\ 0 & \to & J[2](k) & \to & E^\vee(k) & \to & R^\vee(k) & \to & H^1(J[2]) & \to & H^1(E^\vee) \end{array}$$

We need all of computational algebraic number theory ...

$$\begin{array}{ccccccccc} & & & & & & \dfrac{J(k)}{2J(k)} & \xrightarrow{\tilde{\gamma}} & \dfrac{L^\times}{L^{\times 2}k^\times} \\ & & & & & & \Big\downarrow \gamma & & \Big\downarrow \\ 0 \to J[2](k) & \to & E^\vee(k) & \to & R^\vee(k) & \to & H^1(J[2]) & \to & H^1(E^\vee) \end{array}$$

- $\tilde{\gamma}$ consists of evaluation at the “generic” bitangent.
- We need the ring of integers of L and S-units in L.
- $J[2](k)$, $R^\vee(k)$,$E^\vee(k)$ follow from identifying

$$\mathrm{Gal}(L/k) \subset \mathrm{Sp}_6(\mathbb{F}_2).$$

Example results

Theorem: Consider

$$C\colon X^3Y - X^2Y^2 - X^2Z^2 - XY^2Z + XZ^3 + Y^3Z = 0.$$

Then $J(\mathbb{Q}) \simeq \mathbb{Z}/51\mathbb{Z}$ and

$$C(\mathbb{Q}) = \{(1:1:1),(0:1:0),(0:0:1),(1:0:0),(1:1:0),(1:0:1)\}.$$

Theorem: Consider

$$C\colon X^2Y^2 - XY^3 - X^3Z - 2X^2Z^2 + Y^2Z^2 - XZ^3 + YZ^3 = 0.$$

Assuming GRH, we have $J(\mathbb{Q}) \simeq \mathbb{Z}$ and

$$\begin{aligned} C(\mathbb{Q}) = \{&(1:1:0),(-1:0:1),(0:-1:1),(0:1:0),\\ &(1:1:-1),(0:0:1),(1:0:0),(1:4:-3)\}. \end{aligned}$$

Observation: The map $\tilde{\gamma}$ can be evaluated on C directly.

$$\tilde{\gamma}\colon C(\mathbb{Q}) \to \frac{L^\times}{L^{\times 2}\mathbb{Q}^\times}$$

Comparing local images gives another computable obstruction to rational points.

Theorem: Consider

$$C\colon X^4+Y^4+X^2YZ+2XYZ^2-Y^2Z^2+Z^4=0$$

Then $C(\mathbb{A}) \neq \emptyset$ but assuming GRH one can prove that C has no rational points.

Kiran, Everett, Joe, Organizing committee, Program committee

THANK YOU!!

For a wonderful