Computational tools for Arithmetic geometry

Nils Bruin (Simon Fraser University)

Computational arithmetic geometry in Magma

- Arithmetic in $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}_p$ (plus extensions), $\mathbb{F}_p$, Polynomial arithmetic
- Number fields: Arithmetic, Ideals, S-Unit groups, Class groups
- Function fields of curves: Arithmetic, Ideals, Class groups, Divisors, Differentials, Riemann-Roch spaces
- Multivariate polynomial algebra; Groebner Bases
- Affine and projective schemes (wrapper): Rational maps, Patches
- Local solvability testing, Selmer groups of elliptic curves over number fields, Selmer groups of hyperelliptic curves
- Chabauty methods using elliptic curves
- Support for Brauer-Manin type computations on curves

Contributors: Geoff Baily, Gavin Brown, Claus Fieker, Damien Fisher, Florian Hess, David Kohel, Allan Steel, Michael Stoll, Nicole Sutherland,

A first example: Rational points on Klein's Quartic

Consider the projective plane curve:

$$C : x^3y + y^3z + z^3x = 0$$

Automorphism:

$$\begin{array}{rccc} \phi & : & C & \to & C \\ & & (x:y:z) & \mapsto & (y:z:x) \end{array}$$

Question: What are the rational points on C?

Possible answer:

- Determine $D = C/\langle\phi\rangle$
- Determine $D(\mathbb{Q})$
- Pull back: $\phi^{-1}D(\mathbb{Q})$

To compute $\pi : C \to C/\langle\phi\rangle$:

- Pick some generators of $\mathbb{Q}(C)$, e.g. $X := x/z$, $Y := y/z$.
- Compute some ϕ-invariant elements, e.g.

$$f := X + X \circ \phi + X \circ \phi^2 \text{ and } g = Y + Y \circ \phi + Y \circ \phi^2$$

- Compute image D under map

$$\begin{array}{rccc} \pi & : & C & \to & \mathbb{P}^2 \\ & & (x : y : z) & \mapsto & (f : g : 1) \quad =: (u : v : w) \end{array}$$

- Check that the degree of π is indeed 3.

We find the curve (in Weierstrass-form):

$$\mathrm{Im}(\phi) = D : u^3 - 3uvw - 2uw^2 + v^2w + vw^2 + 3w^3 = 0$$

and

$$(u : v : w) = (-x^2y^2 + xy^3 + y^2z^2 - yz^3 : -x^2yz + xy^2z + y^4 - z^4 : y^3z)$$

Finishing the job

- Since D is a curve of genus 1 with a rational point, we get a map

$$\pi : C \to E,$$

  where E is an elliptic curve

- Compute the Torsion Subgroup of $E(\mathbb{Q})$. This is all of $E(\mathbb{Q})$.

- Pull back each of the points along π.

- Determine the rational points in each of these fibers.

Theorem. The rational points on $x^3y + y^3z + z^3x = 0$ are

$$\{(1:0:0), (0:1:0), (0:0:1)\}.$$

Testing Local Solvability

Algorithms available for:

- Complete intersections
- 0-dimensional projective schemes
- Smooth curves represented by (singular) plane curves.
- Hyperelliptic curves.

Efficient case: Hyperelliptic curves (following Merriman-Siksek-Smart)

Observation: Let K be a local field with finite residue field k. Let C be a curve over K, given by a model over $\mathcal{O}_K$. If k has sufficiently many elements, then the reduced curve $\overline{C}$ over k must be *very* bad to have no non-singular points.

Local solvability of hyperelliptic curves (a la Siksek)

Let $\mathcal{O}$ be a discrete valuation ring with maximal ideal $\mathfrak{p} = \pi\mathcal{O}$ and finite residue field $k = \mathcal{O}/\mathfrak{p}$ of odd characteristic.

Consider a curve

$$C : y^2 = f(x) \text{ with } f \in \mathcal{O}[x]$$

Theorem: *If*

$$\deg(f) < \frac{\#k + 1}{\sqrt{\#k}} - 1$$

then one can decide if $C(K)$ is empty in time essentially independent of $\#k$.

Step 1: Write $f(x) = \pi^e f_1(x)$ with $f_1 \not\equiv 0 \pmod{\mathfrak{p}}$.

If $2 \mid e$ then $f(x)$ is a square if and only if $f_1(x)$ is a square.

If $2 \nmid e$ then $f(x)$ can only be a square if $f_1(x) \equiv 0 \pmod{\mathfrak{p}}$. Hence, test solvability of $(y_1)^2 = f_1(x_0 + \pi x_1)$ for lifts x_0 of all roots of $f \pmod{\mathfrak{p}}$
[*recursive step:* branching degree at most $\deg f$].

Local solvability (continued)

Step 2: WLOG $f \equiv gh^2 \pmod{\mathfrak{p}}$, where $g \pmod{\mathfrak{p}}$ is square-free.

If $\deg(g) = 0$ and $g = \square$, then any x_0 with $h(x_0) \not\equiv 0 \pmod{\mathfrak{p}}$ lifts to a point $(x_0, y_0) \in C(K)$.

If $\deg(g) = 0$ and $g \neq \square$, then $f(x)$ can only be a square if $h(x) \equiv 0 \pmod{\mathfrak{p}}$. Hence, test solvability of $(y_1)^2 = f(x_0 + \pi x_1)$ for lifts x_0 of all roots of $h \pmod{\mathfrak{p}}$ [*recursive step:* branching degree at most $\deg h$].

Observation: Any point $(\overline{x}, \overline{y}) \in C(k)$ with $\overline{y} \neq 0$ or $\overline{x}$ a simple root of $f \pmod{\mathfrak{p}}$ is non-singular and hence lifts to a point in $C(K)$.

If $\deg(g) \neq 0$, then select x_0 such that $g(x_0) = \square$ and $f(x_0) \not\equiv 0 \pmod{\mathfrak{p}}$.

The curve $y^2 = g(x)$ has at least $\#k + 1 - (\deg(g) - 1)\sqrt{\#k}$ points over k.
We should avoid at most $\deg(h)$ points:

$$\begin{aligned} \#k + 1 - (\deg(g) - 1)\sqrt{\#k} - \deg(h) &\geq \#k + 1 - (\deg(g) + 2\deg(h) - 1)\sqrt{\#k} \\ &\geq \#k + 1 - (\deg(f) - 1)\sqrt{\#k} > 0 \end{aligned}$$

A problem of Diophantus (Thesis of J.L. Wetherell)

Question: Which rational squares can be written as $x^2 + x^4 + x^8$?

$$C : y^2 = x^6 + x^2 + 1$$

Brute force search:

$$\{\infty^{\pm}, (0, \pm 1), (\pm 1/2, \pm 9/8)\}$$

So we have

$$\left(\frac{9}{16}\right)^2 = \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^4 + \left(\frac{1}{2}\right)^8$$

First try: Is $\mathrm{Jac}_C(\mathbb{Q})$ finite?

Answer: No, $[\infty^+ - \infty^-]$ and $[(0,1) - \infty^-]$ generate a rank 2 subgroup.

Second try: Does C cover a rank 0 elliptic curve?

Answer: $\pi_1 : (x, y) \mapsto (x^2, y)$ and $\pi_2 : (x, y) \mapsto (1/x^2, y/x^3)$ both give maps to elliptic curves, but both are of rank 1.

Using covers

Consider the number field $K = \mathbb{Q}(\alpha)$ with $\alpha^3 + \alpha + 1 = 0$.

$$x^6 + x^2 + 1 = \underbrace{(x^2 - \alpha)}_{Q(x)}\underbrace{(x^4 + \alpha x^2 + \alpha^2 + 1)}_{R(x)}.$$

If $(x, y) \in C(\mathbb{Q})$ then there are $y_1, y_2, \delta \in K$:

$$\begin{aligned} x^2 - \alpha &= \delta y_1^2 \\ x^4 + \alpha x^2 + \alpha^2 + 1 &= \delta y_2^2 \end{aligned}$$

We can take δ to represent an element of K^*/K^{*2} with

$$\nu_{\mathfrak{p}}(\delta) \in 2\mathbb{Z} \text{ for } \mathfrak{p} \nmid 2\mathrm{res}(R, Q).$$

and with $N(\delta) \in \mathbb{Q}^{*2}$.

This leaves $\delta \in \{1, \alpha^2 + 1\}$.

For each $D_\delta : \delta R(X) = y_2^2$ we determine

$$X(D_\delta(K)) \cap \mathbb{P}^1(\mathbb{Q})$$

The case $\delta = \alpha^2 + 1$

Consider the curve

$$D : y_2^2 = (\alpha^2+1)(X^4 + \alpha X^2 + \alpha^2 + 1) \text{ with } X : (X, y_2) \mapsto X$$

We have $(0, \alpha^2 + 1) \in D(K)$ and

$$D \simeq E : y^2 = x^3 + 2\alpha^2 x^2 + (-\alpha^2 + 3\alpha)x$$

The point $(0, 0) \in E$ is two-torsion, so there is a 2-isogeny $\phi : E \to E/\langle (0, 0) \rangle$.

Two-isogeny descent shows that $D(K)$ is finite, consisting of two points:

$$X(D_{\alpha^2+1}(K)) \cap \mathbb{P}^1(\mathbb{Q}) = \{0\}$$

The case $\delta = 1$

Consider the curve

$$D : y_2^2 = X^4 + \alpha X^2 + \alpha^2 + 1$$

We have K-rational points on D with $X = \infty$ and

$$D \simeq E : y^2 = x^3 - 2\alpha^2 x^2 + (-3\alpha^2 - 4)x$$

A 2-isogeny descent gives:

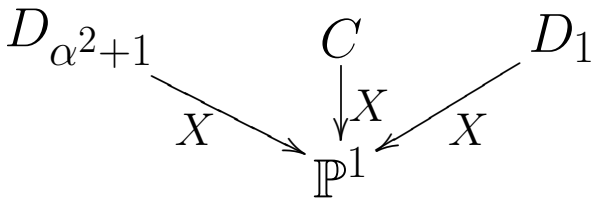
- $\mathrm{rk} E(K) \leq 1$,
- $0, (0,0), (\alpha, 2)$ are distinct in $E(K)/\hat{\phi}(E'(K))$,
- $\langle (0,0), (\alpha, 2) \rangle$ is of finite, odd index in $E(K)$.

Chabauty: Determine $X(\langle (0,0), (\alpha, 2) \rangle \otimes_{\mathbb{Z}} \mathbb{Z}_{11}) \cap \mathbb{P}^1(\mathbb{Q}_{11})$

Result: $\{\pm 1/2, \infty\}$

Summary

Involved curves:



$$\begin{aligned} D_{\alpha^2+1}: \quad y_1^2 &= (\alpha^2+1)(X^4+\alpha X^2+\alpha^2+1) \\ C: \quad y^2 &= X^6+X^2+1 \\ D_1: \quad y_2^2 &= (X^4+\alpha X^2+\alpha^2+1) \end{aligned}$$

Result obtained from covering techniques:

$$X(C(\mathbb{Q})) \subset \left(\mathbb{P}^1(\mathbb{Q}) \cap X(D_{\alpha^2+1}(K))\right) \cup \left(\mathbb{P}^1(\mathbb{Q}) \cap X(D_1(K))\right)$$

Chabauty-like methods:

$$\begin{aligned} X(D_{\alpha^2+1}(K)) \cap \mathbb{P}^1(\mathbb{Q}) &= \{0\} \\ X(D_1(K)) \cap \mathbb{P}^1(\mathbb{Q}) &= \{\pm 1/2, \infty\} \end{aligned}$$

Theorem:

$$C(\mathbb{Q}) = \{\infty^{\pm}, (0, \pm 1), (\pm 1/2, \pm 9/8)\}$$