Numerical p-adic integration and (potential) applications to rational points

Kiran S. Kedlaya
joint work in preparation with Jennifer Balakrishnan (MIT);
partial joint work with Minhyong Kim (University College, London)

Department of Mathematics, Massachusetts Institute of Technology
kedlaya@mit.edu

Rational points: theory and experiment
Zürich, May 28, 2010

These slides are available at http://math.mit.edu/~kedlaya/papers/.

Supported by NSF (CAREER grant DMS-0545904), DARPA (grant HR0011-09-1-0048), MIT (NEC Fund, Cecil and Ida Green professorship).

Contents

Contents

Notation and setup

Throughout this talk, let C be a curve over $\mathbb{Q}$ (i.e., an absolutely irreducible scheme which is smooth proper of relative dimension 1 over $\operatorname{Spec} \mathbb{Q}$) of genus $g \geq 2$. We always mean C to be *explicit*, i.e., it is specified by an explicit model of its function field. Most of our examples will be hyperelliptic curves

$$y^2 = P(x)$$

where $P(x) \in \mathbb{Q}[x]$ is an explicit polynomial with no repeated roots.

We will always assume that C has at least one known rational point O, and that C is embedded into its Jacobian J by the map $P \mapsto (P) - (O)$. (That is, we do not consider the question of whether or not $C(\mathbb{Q}) = \emptyset$.)

Algorithmic determination of rational points: open problems

Recall that $C(\mathbb{Q})$ is finite since we assumed $g \geq 2$.

Problem (Open)

Describe an algorithm that, given a curve C, returns $C(\mathbb{Q})$.

In principle (and often in practice), by searching for points of small height, one can reduce the previous problem to the following.

Problem (Also open)

Describe an algorithm that, given a curve C and an explicit finite set $S \subseteq C(\mathbb{Q})$, returns a proof that $S = C(\mathbb{Q})$ whenever this is true (and may behave arbitrarily otherwise).

Contents

The Chabauty condition

Definition

We say that C satisfies the *Chabauty condition* if $\operatorname{rank} J(\mathbb{Q}) < g$.

Chabauty proved finiteness of $C(\mathbb{Q})$ under the Chabauty condition using p-adic analysis. Coleman gave a beautiful reinterpretation of Chabauty's method by defining a integration pairing

$$\int : \operatorname{Pic}^0 C(K) \times H^0(C_K, \Omega_{C_K/K}) \to K$$

for any field K between $\mathbb{Q}_p$ and a completed algebraic closure.

The method of Chabauty-Coleman describes a certain finite subset of $C(\mathbb{Q}_p)$ containing $C(\mathbb{Q})$. In many cases, one can produce an upper bound on $\#C(\mathbb{Q})$ equal to the size of a set S of known points of $C(\mathbb{Q})$, which proves that $S = C(\mathbb{Q})$.

The Chabauty-Coleman space of differentials

Let p be a prime of good reduction for C. Identify

$$H^0(C_{\mathbb{Q}_p}, \Omega_{C_{\mathbb{Q}_p}/\mathbb{Q}_p}) \cong H^0(J_{\mathbb{Q}_p}, \Omega_{J_{\mathbb{Q}_p}/\mathbb{Q}_p}).$$

Within the right side, let Ω^C be the subspace of forms which pair to zero with every element of $J(\mathbb{Q})$ via Coleman's integration pairing. This space has positive dimension by the Chabauty condition, so

$$S(C,p) = \{P \in C(\mathbb{Q}_p) : \int_O^P \omega = 0 \text{ for all } \omega \in \Omega^C\}$$

(the *Chabauty-Coleman set* of C at p) is finite.

Application to rational points

Note that

$$C(\overline{\mathbb{Q}} \cap \mathbb{Q}_p) \cap J(\mathbb{Q})^{\mathrm{div}} \subseteq S(C, p).$$

For instance, $S(C, p)$ contains $C(\mathbb{Q})$, and any torsion point of J on C.

Following Coleman, one can give upper bounds for $\#S(C, p)$. These occasionally suffice to determine $C(\mathbb{Q})$.

Example (Gordon-Grant, 1993; see also McCallum-Poonen, 2007)

For C the projective model of the affine curve

$$y^2 = x(x-1)(x-2)(x-5)(x-6),$$

we have $\operatorname{rank} J(\mathbb{Q}) = 1 < 2 = g$. Coleman proves $\#S(C, 7) \leq 10$, but

$$\infty, (0,0), (1,0), (2,0), (5,0), (6,0), (3, \pm 6), (10, \pm 120) \in C(\mathbb{Q}).$$

Hence $C(\mathbb{Q}) = S(C, 7)$.

Numerical Coleman integration for hyperelliptic curves

In less favorable cases, it may be helpful to obtain $S(C,p)$ "explicitly", i.e., to obtain good p-adic approximations to the elements of $S(C,p)$. For instance, this may be a useful way to find elements of $C(\overline{\mathbb{Q}} \cap \mathbb{Q}_p) \cap J(\mathbb{Q})^{\mathrm{div}}$ not defined over $\mathbb{Q}$.

This is tricky in general, because the Coleman integral $\int_O^P \omega$ is only a *locally analytic* function of P (analytic on each residue disc). One needs some explicit constants of integration to move between discs.

For hyperelliptic curves $y^2 = P(x)$ with $\deg(P)$ odd, we have an implemented algorithm for this. (The case of $\deg(P)$ even is similar but not implemented.) It is based on the computation of Frobenius matrices in Monsky-Washnitzer cohomology (K, 2001).

Effectiveness of the method: an experiment

If we suspect that $C(\mathbb{Q}) \neq S(C,p)$, we cannot hope to use Chabauty's method to determine $C(\mathbb{Q})$ without some additional information. But no p-adic approximation of a point of $S(C,p)$ would suffice to prove that such a point is *not* defined over $\mathbb{Q}$.

On the other hand, in case

$$C(\overline{\mathbb{Q}} \cap \mathbb{Q}_p) \cap J(\mathbb{Q})^{\mathrm{div}} = S(C,p),$$

then we can identify each point of $S(C,p) - C(\mathbb{Q})$ as a global algebraic point of C.

We have little experimental data about how often we can identify all of $S(C,p)$ in terms of global points. It is now possible to collect such data on a large scale, but we have not yet done so.

Beyond Chabauty?

The Chabauty condition fails in many interesting cases. What can be done in such cases?

The best hope seems to be to perform a descent to pass from C to another curve of higher genus, and hope that the Chabauty condition applies there. For example, Wetherell used this method to treat the curve

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

for which rank $J(\mathbb{Q}) = 2 = g$.

An interesting variant of this has been proposed by Kim.

Contents

Overview of the method

Assuming the finiteness of the Shafarevich-Tate group, the group $J(\mathbb{Q})$ can be identified with the Selmer group

$$H^1_f(G_{\mathbb{Q}}, T_p J) = H^1_f(G_{\mathbb{Q}}, \varprojlim J(\mathbb{Q})[p^n]).$$

We can also think of the coefficient group as the maximal pro-p abelian quotient of the geometric étale fundamental group $\pi_1^{\mathrm{et}}(C_{\overline{\mathbb{Q}}})$.

Kim proposes to replace this quotient with some mildly nonabelian quotients, in which case the Selmer group becomes a pointed *Selmer set*. This set again contains $C(\mathbb{Q})$. Grothendieck's section conjecture suggests that for a large enough quotient, the Selmer set should be "small" (i.e., it should satisfy a nonabelian analogue of the Chabauty condition). In this case, one can again construct a finite set containing $C(\mathbb{Q})$, this time computable using *iterated* Coleman integrals.

A toy example: integral points on elliptic curves

To give a numerical example of the method, Kim constructed the following toy example, in which we consider integral points in genus 1 rather than rational points in genus > 1.

Let E be an elliptic curve over $\mathbb{Q}$ of analytic rank 1 (crucially) and having squarefree discriminant (for simplicity). Let $\mathfrak{E}$ be the minimal regular model over $\mathbb{Z}$.

It is possible to give explicit equations cutting out $\mathfrak{E}(\mathbb{Z})$ within $E(\mathbb{Q})$, e.g., by taking the factor at p of the global p-adic height pairing. These equations appear naturally in the context of Kim's method, from a *rigidified Massey product* in Galois cohomology.

Massey products

Put $X = E - \{e\}$ and let $\mathfrak{X}$ be the complement in $\mathfrak{E}$ of the identity section. Let p be an odd prime of good reduction. One has an Albanese map

$$\mathfrak{X}(\mathbb{Z}_p) \to H^1_f(G_{\mathbb{Q}_p}, U_2)$$

where U_2 is the maximal pro-p two-step nilpotent quotient of the geometric étale fundamental group of X. (Note that we took out a point, so this fundamental group is not abelian!)

The Selmer set on the right may be viewed as a p-adic analytic variety (a *Selmer variety*). Computing coefficients on this variety amounts to computing some double Coleman integrals.

Using the work of Kolyvagin, one constructs an explicit map

$$H^1_f(G_{\mathbb{Q}_p}, U_2) \to H^2(G_{\mathbb{Q}_p}, \mathbb{Q}_p(1)) \cong \mathbb{Q}_p,$$

such that the composition kills the points of $\mathfrak{X}(\mathbb{Z})$.

Explicit equations

One can go through this recipe and recover the explicit equation defining $\mathfrak{X}(\mathbb{Z})$ inside $X(\mathbb{Q})$. Write E in short (not necessarily minimal) Weierstrass form $y^2 = P(x)$, and put $\alpha = dx/y, \beta = x\,dx/y$.

Theorem

Suppose (for simplicity) that there is a nonzero two-torsion point $b \in \mathfrak{X}(\mathbb{Z})$. Then the ratio

$$\frac{\int_b^x \alpha\beta}{\left(\int_b^x \alpha\right)^2}$$

is constant over all $x \in \mathfrak{X}(\mathbb{Z})$ of infinite order.

One has a similar result without the two-torsion point, using a *tangential basepoint* instead (which we have not yet implemented).

Numerical evidence

Let E be Cremona's curve 65A1, with minimal regular model $\mathfrak{E}$ defined by the minimal Weierstrass equation $y^2 + xy = x^3 - x$. We instead compute on the nonminimal model

$$y^2 = x^3 - 1323x + 3942.$$

Let

$$b = (3, 0), \quad P = (39, 108), \quad Q = (-33, -108),$$
$$R = (147, 1728), \quad S = (103, 980), \quad T = (-6, -108)$$

be points on E, which arise from the respective points

$$(0, 0), (1, 0), (-1, 0), (4, 6), (25/9, 85/27), (-1/4, -3/8)$$

on $\mathfrak{E}$. In particular, $b, P, Q, R \in \mathfrak{E}(\mathbb{Z})$ but $S, T \notin \mathfrak{E}(\mathbb{Z})$.

Numerical evidence (continued)

Take the prime $p = 11$ of good reduction. For $x = P, Q, R$, the ratio

$$\frac{\int_b^x \alpha\beta}{\left(\int_b^x \alpha\right)^2}$$

evaluates to

$$3 \cdot 11^{-1} + 6 + 2 \cdot 11 + 10 \cdot 11^2 + 3 \cdot 11^3 + 5 \cdot 11^4 + O(11^5).$$

For $x = S$, it evaluates to

$$3 \cdot 11^{-1} + 10 + 6 \cdot 11 + 9 \cdot 11^2 + 8 \cdot 11^3 + 6 \cdot 11^4 + O(11^5).$$

For $x = T$, it evaluates to

$$6 \cdot 11^{-1} + 1 + 4 \cdot 11 + 4 \cdot 11^2 + 1 \cdot 11^3 + 7 \cdot 11^4 + O(11^5).$$

What next?

We would like to try Kim's method in the context of rational points on hyperelliptic curves of genus at least 2. For this, the p-adic integral computation is ready, but more work is needed on the computation of global Selmer sets.

Advertisement: the computations here are similar to those needed to compute global p-adic canonical heights on hyperelliptic curves. For genus 1, this was implemented by Harvey using a method of Mazur-Stein-Tate. For higher genus, one can instead follow Coleman-Gross, combining p-adic integration with the computation of prime-to-p factors (implemented by S. Müller).