Panoramas & Synthèses
36, 2012, p. 99–117

THE METHOD OF CHABAUTY AND COLEMAN

by

William McCallum & Bjorn Poonen

***Abstract.* —** This is an introduction to the method of Chabauty and Coleman, a p-adic method that attempts to determine the set of rational points on a given curve of genus $g \geq 2$. We present the method, give a few examples of its implementation in practice, and discuss its effectiveness. An appendix treats the case in which the curve has bad reduction.

***Résumé* (? ? ?). —** Cet exposé présente une introduction à la méthode de Chabauty et Coleman, une méthode p-adique qui cherche à expliciter l'ensemble des points rationnels d'une courbe de genre $g \geq 2$. Après avoir exposé la méthode, nous donnons quelques exemples de son utilisation en pratique et puis nous discutons sur son efficacité. Une annexe traite le cas où la courbe a mauvaise réduction.

1. Rational points on curves of genus ≥ 2

We will work over the field $\mathbb{Q}$ of rational numbers, although everything we say admits an appropriate generalization to a number field. Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$. For each finite prime p, let $\mathbb{Q}_p$ be the field of p-adic numbers (see [**Kob84**] for the definition). Curves will be assumed to be smooth, projective, and geometrically integral.

2000 *Mathematics Subject Classification.* — Primary 11G30; Secondary 14G05, 14K20.
***Key words and phrases.* —** Chabauty, p-adic integration, Jacobian.

This article is based partially on lectures given by W. M. at the Arizona Winter School in 1999, and partially on notes from a course given by B. P. as part of the "Explicit methods in number theory" trimester at the Institut Henri Poincaré in Fall 2004; B. P. thanks all the trimester organizers, and especially Karim Belabas, for their support during the trimester. W. M. was supported by NSF grant DMS-9624219, and B. P. was supported by NSF grants DMS-0301280 and DMS-0841321 and the Miller Institute for Basic Research in Science. We thank Matthew Baker, David Brown, Brian Osserman, Michael Stoll, Anthony Várilly-Alvarado, David Zywina, and the referees for comments.

Let X be a curve over $\mathbb{Q}$ of genus $g \geq 2$. We suppose that X is presented as the zero set in some $\mathbb{P}^n$ of an explicit finite set of homogeneous polynomials. We may give instead an equation for a singular (but still geometrically integral) curve in $\mathbb{A}^2$; in this case, it is understood that X is the smooth projective curve birational to this singular curve. Rational points on X can be specified by giving their coordinates. (A little more data may be required if a singular model for X is used.) Let $X(\mathbb{Q})$ be the set of rational points on X.

In 1922 L. Mordell [**Mor22**] conjectured that $X(\mathbb{Q})$ is finite, and in 1983 this was proved by G. Faltings [**Fal83**]. Thus we have the following well-defined problem:

Given X of genus ≥ 2 presented as above, compute $X(\mathbb{Q})$.

An argument of A. N. Parshin (see [**Szp85**]) shows that Faltings' proof can be adapted to give an upper bound on the *cardinality* of $X(\mathbb{Q})$. But Faltings' proof is still ineffective in the sense that it does not provide an algorithm for finding the points in $X(\mathbb{Q})$, even in principle. In fact, it is not known whether *any* algorithm is guaranteed to solve this problem. Even the case $g = 2$ seems hard.

Nevertheless there are a few techniques that can be applied: see [**Poo02**] for a survey. On individual curves these seem to solve the problem often, perhaps even always when used together, though it seems very difficult to prove that they always work. One of the methods used is the method of Chabauty and Coleman.

Remark 1.1. — By [**Ih02**, Theorem 1.0.1], Vojta's conjecture implies that given a family of curves of genus ≥ 2 depending algebraically on parameters $t_1, \ldots, t_n$, the numerators and denominators of the coordinates of all the rational points on a curve in the family are bounded by a polynomial function of the numerators and denominators of the parameter values specifying that curve, where the polynomial depends only on the family. Experimental evidence seems to agree with this prediction [**Sto09**]. In fact, experience suggests a naïve search will quickly yield a list of rational points that is almost certainly complete, at least in the case of curves of low genus ≥ 2 with small integer coefficients (and slightly less naïve algorithms should do the same when the coefficients are a little larger). The difficulty is in *proving* that the list is complete.

Remark 1.2. — In contrast, one expects that for some genus-1 curves, even the simplest rational points can have exponentially large numerators and denominators: see [**Elk94**] for an example of an elliptic curve whose "smallest" non-torsion point has a huge numerator and denominator.

2. The Jacobian

Let J be the Jacobian of X. Thus J is an abelian variety of dimension g over $\mathbb{Q}$. Although J could in principle be presented as a projective variety, for many purposes it seems easier *not* to work with explicit defining equations for J. Instead one can use that there is an $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-equivariant isomorphism between the abelian group $J(\overline{\mathbb{Q}})$ and the group of linear equivalence classes of degree-0 divisors on $X_{\overline{\mathbb{Q}}}$ (the curve defined by the same equation as X, but considered over $\overline{\mathbb{Q}}$). Elements of $J(\mathbb{Q})$ or $J(\overline{\mathbb{Q}})$ can be represented by explicit formal integer combinations of points in $X(\overline{\mathbb{Q}})$.

From now on, we suppose that we know a point $O \in X(\mathbb{Q})$. Then we have an embedding

$$\begin{aligned} \iota\colon X &\hookrightarrow J \\ P &\mapsto [P - O], \end{aligned} \tag{1}$$

where $[D]$ denotes the class of a divisor D. Hence we identify X with a subvariety of J.

Remark 2.1. — As in Remark 1.1, it is usually easy to find a rational point O if it exists. If a rational point cannot be found, we can at least find a divisor D of some degree $d > 0$. Then the morphism

$$\begin{aligned} X &\to J \\ P &\mapsto [dP - D], \end{aligned}$$

is a good substitute for (1), though if $d > 1$ it need not be an embedding.

Now one possible strategy for determining $X(\mathbb{Q})$ is:

1. First compute $J(\mathbb{Q})$.
2. Then determine which points in $J(\mathbb{Q})$ lie on X.

Although $J(\mathbb{Q})$ is not necessarily finite, the Mordell-Weil theorem states that $J(\mathbb{Q})$ is a finitely generated abelian group, so in principle it can be described by giving explicit generators (represented by divisors) and relations. "Computing $J(\mathbb{Q})$" means computing these generators and relations. There exists an algorithm that attempts to compute $J(\mathbb{Q})$, based on descent (a vast generalization of Fermat's method of infinite descent), though it is not known whether it always succeeds. This is not the concern of this article, however: from now on, we assume that $J(\mathbb{Q})$ has been computed.

Remark 2.2. — The method of Chabauty and Coleman can often succeed with less than full knowledge of $J(\mathbb{Q})$. See Remark 6.1, and Examples 1 and 2 in Section 8.

If $J(\mathbb{Q})$ is finite, then in principle it is not hard to determine $X(\mathbb{Q})$: namely, for each element of $J(\mathbb{Q})$, choose a degree-0 divisor D representing it; then the points P with $\iota(P) = [D]$ (actually there will be at most one such P), when viewed as effective degree-1 divisors, are exactly the divisors of the form $D + O + (f)$ for some nonzero rational function f in the space $L(D+O)$ defined as in the statement of the Riemann-Roch theorem. There exist efficient methods for computing the basis of $L(E)$ for any divisor E [**Hes02**].

More generally, if J has a nonzero abelian variety quotient A such that $A(\mathbb{Q})$ is finite, then the composition $\pi\colon X \hookrightarrow J \twoheadrightarrow A$ maps $X(\mathbb{Q})$ to $A(\mathbb{Q})$, so in principle one can determine $X(\mathbb{Q})$ by checking which of the finitely many points in $\pi^{-1}(A(\mathbb{Q}))$ are rational.

But if no such A exists, or equivalently $J(\mathbb{Q})$ is Zariski dense in J, then it is more difficult to determine which of its points lie on X.

3. A real-analytic method that does not work

We can embed $J(\mathbb{Q})$ in the Lie group $J(\mathbb{R})$, which as a compact commutative Lie group is analytically isomorphic to $(\mathbb{R}^g/\mathbb{Z}^g) \times F$ for some finite abelian group F. Let $\overline{J(\mathbb{Q})}$ be the closure of $J(\mathbb{Q})$ in $J(\mathbb{R})$ with its real topology, so $\overline{J(\mathbb{Q})}$ is a Lie subgroup of $J(\mathbb{R})$. We want to find the points in $J(\mathbb{Q})$ that lie on the submanifold $X(\mathbb{R})$ of $J(\mathbb{R})$. In particular, it would be nice if the intersection $X(\mathbb{R}) \cap \overline{J(\mathbb{Q})}$ in $J(\mathbb{R})$ were finite, because then its subset $X(\mathbb{Q})$ would be finite.

But when $J(\mathbb{Q})$ is Zariski dense in J, one conjectures that $\overline{J(\mathbb{Q})}$ is open in $J(\mathbb{R})$, just as the integer multiples of a point $(a_1, \dots, a_g) \in \mathbb{R}^g/\mathbb{Z}^g$ are dense in $\mathbb{R}^g/\mathbb{Z}^g$ whenever $1, a_1, \dots, a_g$ are $\mathbb{Q}$-linearly independent. In this case, $X(\mathbb{R}) \cap \overline{J(\mathbb{Q})}$ will contain a neighborhood of O in $X(\mathbb{R})$, so it will be infinite.

Remark 3.1. — The conjecture just mentioned was made by Mazur (under the additional hypothesis that J is simple) [**Maz92**, Conjecture 5]. It is known to be true when J is simple and $\operatorname{rank} J(\mathbb{Q}) \geq g^2 - g + 1$ [**Wal93**, Theorem 2].

4. Chabauty's idea

C. Chabauty [**Cha41**], inspired by an analogous idea of T. Skolem [**Sko34**] in the context of integer points on subvarieties of tori, had the idea of using $\mathbb{Q}_p$ for a fixed finite prime p instead of $\mathbb{R}$ in the previous section.

4.1. The structure of $J(\mathbb{Q}_p)$. — Before giving Chabauty's theorem, we need some preliminaries on the structure of the p-adic Lie group $J(\mathbb{Q}_p)$. The facts in this section are discussed (in greater generality) in [**Bou98**, III.§7.6].

Let $J_{\mathbb{Q}_p}$ be the variety defined by the same equations as J, but considered over $\mathbb{Q}_p$ instead of $\mathbb{Q}$. Let $H^0(J_{\mathbb{Q}_p}, \Omega^1)$ be the (g-dimensional) $\mathbb{Q}_p$-vector space of regular 1-forms on $J_{\mathbb{Q}_p}$. Suppose $\omega_J \in H^0(J_{\mathbb{Q}_p}, \Omega^1)$. Using the translation-invariance of ω_J, one can show that it has an "antiderivative"

$$\begin{aligned} \eta_J \colon J(\mathbb{Q}_p) &\to \mathbb{Q}_p \\ Q &\mapsto \int_0^Q \omega_J \end{aligned}$$

characterized uniquely by the following two properties:

- It is a homomorphism.
- There is an open subgroup U of $J(\mathbb{Q}_p)$ such that if $Q \in U$, then $\int_0^Q \omega_J$ can be computed by expanding ω_J in power series in local coordinates, finding a formal antiderivative, and evaluating the power series at the local coordinates of Q. Since the coefficients in the power series expansion of ω_J grow at most geometrically, the formal antiderivative converges on a sufficiently small U.

Remark 4.1. — One can take U to be the kernel $J^1(\mathbb{Q}_p)$ of the reduction map $J(\mathbb{Q}_p) \twoheadrightarrow J(\mathbb{F}_p)$. (In the case of good reduction, we may interpret $J(\mathbb{F}_p)$ as the group of $\mathbb{F}_p$-points on the good reduction. In general, $J(\mathbb{F}_p)$ should be interpreted as the group of $\mathbb{F}_p$-points on the special fiber of the Néron model of J. The Néron model is

a smooth group scheme over $\mathbb{Z}_p$ [**BLR90**], and completing it along the zero section yields a smooth formal group over $\mathbb{Z}_p$, whose associated group of points is $J^1(\mathbb{Q}_p)$; then Proposition 14(ii) of [**Bou98**, III.§7.6] implies that the antiderivative above converges as claimed.)

We get a bilinear pairing

$$\begin{aligned} J(\mathbb{Q}_p) \times H^0(J_{\mathbb{Q}_p}, \Omega^1) &\to \mathbb{Q}_p \\ Q \quad , \quad \omega_J \quad &\mapsto \int_0^Q \omega_J. \end{aligned} \tag{2}$$

Let T be the vector space dual of $H^0(J_{\mathbb{Q}_p}, \Omega^1)$. Then we may rewrite (2) as a homomorphism

$$\log\colon J(\mathbb{Q}_p) \to T.$$

The tangent spaces at 0 of the p-adic Lie groups $J(\mathbb{Q}_p)$ and T may both be identified with T; then the derivative of log at 0 is the identity $T \to T$. Thus log is also a local diffeomorphism.

4.2. The p-adic closure of $J(\mathbb{Q})$. — The closure $\overline{J(\mathbb{Q})}$ of $J(\mathbb{Q})$ in $J(\mathbb{Q}_p)$ with its p-adic topology is an analytic subgroup of $J(\mathbb{Q}_p)$. So it has a dimension as a p-adic manifold. Whereas the real closure of $J(\mathbb{Q})$ in $J(\mathbb{R})$ is typically g-dimensional (see Section 3), the p-adic closure of $J(\mathbb{Q})$ is often smaller (and it is this that makes Chabauty's method work over $\mathbb{Q}_p$):

Lemma 4.2. — *Define* $r' := \dim \overline{J(\mathbb{Q})}$ *and* $r := \operatorname{rank} J(\mathbb{Q})$. *Then* $r' \le r$.

Proof. — We have

$$r' = \dim \overline{J(\mathbb{Q})} = \dim \log \left(\overline{J(\mathbb{Q})} \right),$$

since log is a local diffeomorphism. Since log is continuous and $\overline{J(\mathbb{Q})}$ is compact,

$$\log \left(\overline{J(\mathbb{Q})} \right) = \overline{\log J(\mathbb{Q})}.$$

But the closure of any subgroup in $\mathbb{Q}_p^{\oplus g}$ is simply its $\mathbb{Z}_p$-span. Thus

$$r' = \operatorname{rank}_{\mathbb{Z}_p} \left(\mathbb{Z}_p \log J(\mathbb{Q}) \right) \le \operatorname{rank}_{\mathbb{Z}} \log J(\mathbb{Q}) \le \operatorname{rank}_{\mathbb{Z}} J(\mathbb{Q}) = r. \tag{3}$$

□

Remark 4.3. — The second $\le$ in (3) is an equality since log has finite kernel. But the first $\le$ need not be, since $\mathbb{Z}$-independent points in $\log J(\mathbb{Q})$ need not be $\mathbb{Z}_p$-independent. For instance, $r' \le \dim J = g$ always, but it can happen that $r > g$. Thus $r' < r$ is possible.

4.3. Chabauty's theorem. — Now $X(\mathbb{Q}_p)$ is a 1-dimensional submanifold of $J(\mathbb{Q}_p)$. Suppose $r' < g$. The dimensions suggest (but do not immediately prove) that the intersection $X(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ should be (at most) 0-dimensional, and then it will be a discrete subset of a compact space $J(\mathbb{Q}_p)$, so the intersection will be finite, and its subset $X(\mathbb{Q})$ also will be finite. It is this that Chabauty proved.