COMPUTING RATIONAL POINTS ON CURVES

BJORN POONEN

Abstract. We give a brief introduction to the problem of explicit determination of rational points on curves, indicating some recent ideas that have led to progress.

1. Introduction

The solution of diophantine equations (such as $x^{13} + y^{13} = z^{13}$) over the integers often reduces to the problem of determining the *rational* number solutions to a single polynomial equation in two variables. Such an equation describes a curve, and the problem of finding rational number solutions can be interpreted geometrically as finding the rational points on the curve, i.e., the points on the curve with rational coordinates.

Despite centuries of effort, we still do not know if there is a general algorithm that takes the equation of a curve, and outputs a list of its rational points, in the cases where the list is finite[1]. On the other hand, qualitative results such as Faltings' Theorem [Fa1] on the finiteness of the number of rational points on curves of genus at least 2, the wide variety of conjectural effective approaches, and the practical success of recent efforts in determining the rational points on individual curves, have led many to believe that such an algorithm exists.

The reader expecting a thorough introduction or a comprehensive survey of known results may be disappointed by this article. We have selected only a few of the many aspects of the subject that we could have discussed. On the other hand, as we go along, we provide pointers to the literature for the reader wishing to delve more deeply in some particular direction. Finally,

Date: March 23, 2001.

This research was supported by NSF grant DMS-9801104, a Sloan Fellowship, and a Packard Fellowship. This article will appear in the proceedings of the Millennial Conference on Number Theory, May 21–26, 2000, held at the University of Illinois at Urbana-Champaign.

[1]In fact, we do not even know if there is an algorithm that can always decide whether the list *is* finite.

most of what we say for the field $\mathbf{Q}$ of rational numbers can be generalized easily to arbitrary number fields.

2. Hilbert's 10th Problem and undecidability

First[2], let us consider the problem of what can be computed *in theory*, and let us broaden the perspective to millennial proportions by considering not only curves, but also higher dimensional varieties. Also, before asking whether we can compute all rational points, let's ask first whether we can determine whether a variety *has* a rational point. This leads to "Hilbert's 10th Problem over $\mathbf{Q}$"[3]:

> *Is there an algorithm for deciding whether a system of polynomial equations with integer coefficients*
>
> $$f_1(x_1, \dots, x_n) = 0$$
> $$f_2(x_1, \dots, x_n) = 0$$
> $$\vdots$$
> $$f_m(x_1, \dots, x_n) = 0$$
>
> *has a solution with $x_1, x_2, \dots, x_n \in \mathbf{Q}$?*

The system of equations defines a variety[4] over $\mathbf{Q}$, so equivalently we may ask, does there exist an algorithm for deciding whether a variety over $\mathbf{Q}$ has a rational point?

By "algorithm" we mean Turing machine: see [HU] for a definition. The machine is to be fed (for instance) a finite stream of characters containing the TEX code for a system of polynomial equations over $\mathbf{Q}$, and is supposed to output yes or no in a finite amount of time, according to whether there is a rational solution or not. There is no insistence that the running time of the algorithm be bounded by a fixed polynomial in the length of the input stream; in Hilbert's 10th Problem, we are happy as long as the algorithm terminates after some unspecified number of steps on each input.

The answer to Hilbert's 10th Problem over $\mathbf{Q}$ is not known. This can be stated in logical terms as follows: we do not know whether there exists an algorithm for deciding the truth of all sentences such as

$$(\exists x)(\exists y)((2 * x * x + y = 0) \wedge (x + y + 3 = 0))$$

---

[2]This section is not prerequisite for the rest of the article.

[3]The analogous problem with $\mathbf{Q}$ replaced by $\mathbf{Z}$ was Problem 10 in the list of 23 problems that Hilbert presented to the mathematical community in 1900. This question over $\mathbf{Z}$ was settled in the negative [Mati] around 1970.

[4]In this article, varieties will not be assumed to be irreducible or reduced unless so specified.

involving only rational numbers, the symbols $+, *, =, \exists$, logical relations $\wedge$ ("and"), $\vee$ ("or"), and variables x, y, ... bound by existential quantifiers. One can try asking for more, namely, for an algorithm to decide the entire *first order theory* of $(\mathbf{Q}, 0, 1, +, *)$; this would mean an algorithm for deciding the truth of sentences such as the one above, but in which in addition the symbols $\forall$ ("for all") and $\neg$ ("not") are allowed to appear. For this more general problem, it is known that there is no algorithm that solves it [Ro].

To put the situation in perspective, we list the answers for the analogous questions about the existence of algorithms for deciding Hilbert's 10th Problem (existence of solutions to a polynomial system) or for deciding the first order theory, over other commutative rings.[5] Here YES means that there is an algorithm, NO means that no algorithm exists (i.e., Hilbert's 10th Problem of the first order theory is undecidable), and ? means that it is not known whether an algorithm exists.

Ring	Hilbert's 10th Problem	First order theory
$\mathbf{C}$	YES	YES
$\mathbf{R}$	YES	YES
$\mathbf{F}_p$	YES	YES
$\mathbf{Q}_p$	YES	YES
$\mathbf{Q}$	?	NO
$\mathbf{F}_p(t)$	NO	NO
$\mathbf{Z}$	NO	NO

The rings are listed approximately in order of increasing "arithmetic complexity." There is no formal definition of arithmetic complexity, but roughly we can measure the complexity of fields k by the "size" of the absolute Galois group, i.e., the Galois group of the algebraic closure $\overline{k}$ over k. And nonfields can be thought of as more complex than their fields of fractions, for instance because there is "extra structure" coming from the nontriviality of the divisibility relation. Whether or not $\mathbf{F}_p(t)$ is more complex than $\mathbf{Q}$ is debatable, but it is the extra structure coming from the

[5]A technical point: in the cases where the commutative ring R is uncountable ($\mathbf{C}$, $\mathbf{R}$, $\mathbf{Q}_p$), we must be careful with our statement of the problem, because for instance, a classical Turing machine cannot examine the entirety of an infinite precision real number in a finite number of steps, and hence cannot even decide equality of two real numbers if fed the strings of their decimal digits on two infinite input tapes. To circumvent the problem, in the uncountable cases we restrict attention to decidability questions in which the constants appearing in the input polynomial system or first order sentence are *integers*. We still, however, require the machine to decide the existence of solutions or truth of the sentence with the variables ranging over all of R. It makes sense to ask this, since the output is to be simply yes or no.

p-th power map on the former that enabled the proof of undecidability of Hilbert's 10th Problem for it.

For the complex numbers $\mathbf{C}$, the fact that the first order theory (and hence also Hilbert's 10th Problem) is decidable is a consequence of classical elimination theory. The first order theory has elimination of quantifiers: this means that a first order sentence involving $n \geq 1$ quantifiers $(\exists, \forall)$ can be transformed into a sentence with $n-1$ quantifiers, in an algorithmic way, such that the latter sentence is true if and only if the former is. Algebraically, this corresponds to the elimination of a single variable from a system of equations, and geometrically it amounts to the fact that the projection from $\mathbf{C}^n$ to $\mathbf{C}^{n-1}$ of a Boolean combination of algebraic subsets of $\mathbf{C}^n$ can be written as a Boolean combination of algebraic subsets of $\mathbf{C}^{n-1}$. See [Ha, Exercise II.3.19] and the references [CC, Exposé 7] and [Mats, Chapter 2, §6] listed there for a generalization due to Chevalley, which shows that for the same reasons, the first order theory of any algebraically closed field is decidable.

The analogous statement about the decidability of the first order theory of the real numbers $\mathbf{R}$ was proved by Tarski [Ta] using the theory of Sturm sequences. Again there is an elimination of quantifiers, provided that one augments the language by adding a symbol for $\leq$. The proof generalizes to real closed fields: see [Ja].

For the finite field $\mathbf{F}_p$ of p elements, the decidability results are obvious, since a Turing machine can simply loop over all possible values of the variables.

Tarski conjectured that the only fields with a decidable first order theory were the algebraically closed, real closed, and finite fields. This turned out to be false: Ax and Kochen [AK1] proved decidability for the field $\mathbf{Q}_p$ of p-adic numbers, which is the completion of $\mathbf{Q}$ with respect to the p-adic absolute value. (See [Kob] for the definition and basic properties of $\mathbf{Q}_p$.) Then [AK2] gave several other examples of decidable fields. Macintyre [Mac] showed that there is an elimination of quantifiers for $\mathbf{Q}_p$ analogous to that for $\mathbf{R}$.

It is not known whether Hilbert's 10th Problem over the field $\mathbf{Q}$ of rational numbers is decidable or not; see [Maz2] for a survey. On the other hand, Robinson [Ro] proved the undecidability of the first order theory of $\mathbf{Q}$, using the Hasse principle for quadratic forms. For a statement and proof of the latter, see [Ser1, Chapter IV, §3, Theorem 8].

For the field $\mathbf{F}_p(t)$ of rational functions with coefficients in $\mathbf{F}_p$, Pheidas [Ph] proved the undecidability of Hilbert's 10th Problem, at least for $p \neq 2$. The $p = 2$ case was settled shortly thereafter by Videla [Vi]. The simpler problem of proving undecidability of the first order theory was done earlier, by Ershov [Er] and Penzin [Pe] for $p \neq 2$ and $p = 2$, respectively.

Undecidability of Hilbert's 10th Problem itself (over the ring $\mathbf{Z}$ of integers) was proved by Matiyasevich [Mati]. The undecidability of the first order theory followed earlier from the fundamental work of Gödel [Gö]. Hilbert's 10th Problem for the ring of integers $\mathbf{Z}_K$ of a number field K is expected to be undecidable, but has been proved so only for certain K. For an up-to-date account of results in this direction, see [Shl]. For a survey of Hilbert's 10th Problem over commutative rings in general, see [PZ].

3. Rational points on varieties of arbitrary dimension

As discussed in the previous section, we do not know if there is an algorithm to decide in general whether a variety X over $\mathbf{Q}$ has a rational point. In order to pinpoint what is known and what is not, let us subdivide the problem according to the dimension of X. As usual, $X(\mathbf{Q})$ will denote the set of rational points of X, i.e., the set of rational solutions to the system of polynomials defining X.

$\dim X$	$\exists$ algorithm to decide if $X(\mathbf{Q}) \neq \emptyset$?
0	YES
1	not known, but probably YES
≥ 2	?

If $\dim X = 0$, then elimination theory lets us reduce to the case where X is a 0-dimensional subset of the affine line, and hence the problem becomes that of deciding whether a polynomial $f \in \mathbf{Q}[x]$ has a rational root. The latter can be done effectively, even in polynomial time [LLL].

The $\dim X = 1$ case is the main subject of this article. Details follow in later sections.

For varieties of higher dimension, very little has been proved about $X(\mathbf{Q})$. On the other hand, below is a sample of some qualitative conjectures/questions that have been thrown around. All of these are known for $\dim X \leq 1$, and for certain varieties of higher dimension. No counterexamples are known.

3.1. **Bombieri, Lang (independently).** Define the *special set* $S \subset X$ as the Zariski closure of the union of all positive dimensional images of morphisms of abelian varieties to X. Is it true that all but finitely many rational points of X lie in S?

The $\dim X = 1$ case is equivalent to the Mordell conjecture [Mo1], now Faltings' Theorem [Fa1]: it states that a curve of genus at least 2 has at most finitely many rational points. Faltings [Fa2] used diophantine approximation methods of Vojta to prove more generally that the answer is yes whenever X can be embedded in an abelian variety. For more conjectures along these lines, see [La, Chapter I, §3].

3.2. **Colliot-Thélène and Sansuc.** If X is smooth and projective, and X is birational to $\mathbf{P}^d$ over $\overline{\mathbf{Q}}$ (for instance, X could be a smooth cubic surface in $\mathbf{P}^3$), is the Brauer-Manin obstruction to the Hasse principle the only one? Actually, this was posed originally only for surfaces, as question (k1) in [CS] but as Colliot-Thélène has pointed out, the answer could be yes in higher dimensions as well.

The Hasse principle is the statement that $X(\mathbf{Q}) \neq \emptyset$ if and only if $X(\mathbf{Q}_p) \neq \emptyset$ for all primes $p \leq \infty$. (By convention, $\mathbf{Q}_\infty = \mathbf{R}$.) This statement is proven for some varieties X (e.g., all degree 2 hypersurfaces in $\mathbf{P}^n$) and is known to be false for others (e.g., certain genus 1 curves). In 1970, Manin [Man2] discovered a possible obstruction to the Hasse principle coming from elements of the Brauer group of X, and he and others subsequently showed that this obstruction accounted for all violations of the Hasse principle known at the time. Much later, Skorobogatov [Sk] constructed an example of a surface X with no rational points, even though there was no Brauer-Manin obstruction; in other words, one could say that other nontrivial obstructions exist. Nevertheless, it is conceivable, and this is the point of the question of Colliot-Thélène and Sansuc, that for geometrically rational varieties, the nonexistence of a Brauer-Manin obstruction is a necessary and sufficient condition for the existence of rational points.

3.3. **Mazur.** Does the topological closure of $X(\mathbf{Q})$ in $X(\mathbf{R})$ have at most finitely many connected components?

See [Maz1] and [Maz3] for this and related questions. In [CSSD] a counterexample is given to the following stronger version: If X is a smooth integral variety over $\mathbf{Q}$ such that $X(\mathbf{Q})$ is Zariski dense in X, then the topological closure of $X(\mathbf{Q})$ in $X(\mathbf{R})$ is a union of connected components of $X(\mathbf{R})$. The end of the paper [CSSD] also suggests some other variants.

Even if the three questions above were answered tomorrow, we still would not know whether there exists an algorithm for deciding the existence of rational points on varieties.

4. Rational points on curves

For the rest of this article, we consider the problem of determining $X(\mathbf{Q})$ in the case $\dim X = 1$, i.e., the case of curves. We begin with a few reductions, so that in the future we need consider only "nice" curves. Computational algebraic geometry provides algorithms for decomposing X into irreducible components over $\mathbf{Q}$ and over $\overline{\mathbf{Q}}$. Clearly then we can reduce to the case that X is irreducible over $\mathbf{Q}$. If X is irreducible over $\mathbf{Q}$, but not over $\overline{\mathbf{Q}}$, then the action of Galois acts transitively on the $\overline{\mathbf{Q}}$-irreducible components, but rational points are fixed by Galois, so $X(\mathbf{Q})$ is contained

in the intersection of the $\overline{\mathbf{Q}}$-irreducible components; thus in this case we reduce to the 0-dimensional problem, which according to Section 3 is easily solved. Hence from now on, we will assume that X is geometrically integral.

Taking a projective closure and blowing up singularities changes X only by 0-dimensional sets, whose rational points we understand. Therefore, from now on, all our curves will be assumed to be smooth, projective, and geometrically integral. (Alternatively, at the expense of introducing nodes (violating smoothness), we could project X to a curve in $\mathbf{P}^2$ so that X would be described by a single polynomial equation. But in this article we prefer to talk about the smooth curves, except when presenting a curve explicitly, in which case we sometimes give an equation for an affine plane curve birational to the smooth projective curve that we are really interested in.)

The most important geometric invariant of a (smooth, projective, and geometrically integral) curve over $\mathbf{Q}$ is its genus g, which has several equivalent definitions:

(1) $g = \dim_{\mathbf{Q}} \Omega$ where Ω is the vector space of everywhere regular differentials on X. (Here regular means "no poles.") See [Ha, Chapter II, §8, p. 181] or [Si1, Chapter II, §5, p. 39] for more details.
(2) g is the topological genus of the compact Riemann surface $X(\mathbf{C})$.
(3) g is the dimension of the sheaf cohomology group $H^1(X, \mathcal{O}_X)$. See [Ha, Chapter III] for definitions.
(4) $g = \dfrac{(d-1)(d-2)}{2} - (\text{terms for singularities})$
where Y is a (possibly singular) plane curve of degree d birational to X (e.g., the image of X under a sufficiently generic projection to $\mathbf{P}^2$). In this formula one subtracts a computable positive integer for each singularity. The integer depends on the complexity of the singularity: for nodes (ordinary double points), the integer is 1. See [Ha, Chapter V, Example 3.9.2, p. 393] for more details.

(The equivalence of these is certainly not obvious.)

Although the genus is a measure of geometric complexity, it has been discovered over the years that the geometry also influences the rational points. Hence we subdivide the problem of determining $X(\mathbf{Q})$ according to the genus. We summarize the situation in the following table:

genus g	$\exists$ algorithm to determine $X(\mathbf{Q})$?
0	YES
1	YES, if Ш(Jac X) is finite
≥ 2	Not known, but probably YES

4.1. **Genus zero.** In this case, one shows using the Riemann-Roch Theorem [Ha, Chapter IV, §1] that the anticanonical divisor class on X induces an embedding of X as a degree 2 curve in $\mathbf{P}^2$. In other words, X is isomorphic to a conic, the zero locus in $\mathbf{P}^2$ of an absolutely irreducible homogeneous polynomial $f \in \mathbf{Q}[x, y, z]$ of degree 2. By a linear change of variables, we may assume that f has the form $ax^2 + by^2 + cz^2$ for some nonzero $a, b, c \in \mathbf{Z}$. Conversely, nonsingular degree 2 curves in $\mathbf{P}^2$ are curves of genus zero, by the fourth definition of g above. Over an algebraically closed field, we could say further that X is isomorphic to the projective line $\mathbf{P}^1$, but this is not necessarily the case for genus zero curves over $\mathbf{Q}$: for instance, the conic defined by $x^2 + y^2 + z^2 = 0$ in $\mathbf{P}^2$ is not isomorphic to $\mathbf{P}^1$ over $\mathbf{Q}$, because the latter has rational points, whereas the former does not.

As mentioned in Section 3.2, degree 2 curves in $\mathbf{P}^2$ (and more generally degree 2 hypersurfaces in $\mathbf{P}^2$) satisfy the Hasse principle, so we can decide the existence of a rational point by checking the existence of a $\mathbf{Q}_p$-point for each prime $p \leq \infty$. And the latter is in fact a finite problem since one can show a priori that $ax^2 + by^2 + cz^2 = 0$ has $\mathbf{Q}_p$-points for p not dividing $2abc$, and for each of the finitely many remaining p (including ∞) one has an algorithm for deciding the existence of a $\mathbf{Q}_p$-point, as explained in Section 2. For a more explicit criterion, see [Mo2], for instance.

In the case where X does have a rational point P, there is an isomorphism $\mathbf{P}^1 \to X$ defined as follows: thinking of $\mathbf{P}^1$ as the set of lines in $\mathbf{P}^2$ through P, map the line L to the point $Q \in L \cap X$ not equal to P. (If L is the tangent line to X at P, take $Q = P$.) Hence we obtain an explicit parameterization of $X(\mathbf{Q})$.

4.2. **Genus one.** A genus one curve over $\mathbf{Q}$ with a rational point is called an *elliptic curve over* $\mathbf{Q}$. One shows using the Riemann-Roch Theorem that an elliptic curve E over $\mathbf{Q}$ is isomorphic to the projective closure of the affine curve $y^2 = x^3 + Ax + B$ for some $A, B \in \mathbf{Z}$ with $4A^3 + 27B^2 \neq 0$. More importantly, it can be shown that E can be given the structure of an algebraic group [Si1, Chapter 3]. Roughly, this means that there are rational functions that induce a group structure on the set $E(k)$ for any field k containing $\mathbf{Q}$. The Mordell-Weil Theorem[6] states that the set $E(\mathbf{Q})$ of rational points on an elliptic curve form a finitely generated abelian group [Si1, Chapter 8]. The group $E(\mathbf{Q})$ is called the Mordell-Weil group, and its rank is called the Mordell-Weil rank or simply the rank of E. The torsion subgroup of $E(\mathbf{Q})$ is easy to compute. But the equivalent problems

[6]Actually Mordell alone proved this fact. Weil generalized Mordell's result in two directions: elliptic curves were replaced by abelian varieties of arbitrary dimension, and $\mathbf{Q}$ was replaced by an arbitrary number field.

of determining the rank of $E(\mathbf{Q})$ and of determining a list of generators have not yet been solved. There is a proposed method, "descent," for solving these problems, which is a generalization of the infinite descent method used by Fermat. Descent usually works well in practice when A and B are not too large (see [Cr]), but its success in general relies upon the conjecture that the Shafarevich-Tate group $Ш(E)$, a certain abelian group associated to E, is finite, or at least that the p-primary part of $Ш(E)$ is finite for some prime p. Using the modularity of elliptic curves over $\mathbf{Q}$ [BCDT] and the work of Kolyvagin [Kol] supplemented by [BFH] or [MM], we know $\#Ш(E) < \infty$ for infinitely many E, namely, those for which $\operatorname{ord}_{s=1} L_E(s) \leq 1$, where $L_E(s)$ is the L-function of E. (See [Si1, Appendix C, §16] for a definition of $L_E(s)$.)

A general genus one curve X over $\mathbf{Q}$ need not have a rational point. In fact, Lind [Lin] and Reichardt [Rei] independently discovered examples where X does not satisfy the Hasse principle. Explicitly, the smooth projective models of the affine curves $2y^2 = 1-17x^4$ and $3x^3+4y^3 = 5$ (from [Rei] and [Sel], respectively) are curves having $\mathbf{Q}_p$-points for all $p \leq \infty$, but no rational points. To any genus one curve X one can associate an elliptic curve E, namely the *Jacobian* of X. The Jacobian $\operatorname{Jac} X$ of a curve X of genus g is an abelian variety (irreducible projective algebraic group) of dimension g, whose geometric points correspond to elements of $\operatorname{Pic}^0(X_{\overline{\mathbf{Q}}})$, i.e., to divisor classes of degree zero on $X_{\overline{\mathbf{Q}}}$. (Note: $X_{\overline{\mathbf{Q}}}$ denotes the same variety as X except where the defining polynomials are viewed as having coefficients in $\overline{\mathbf{Q}}$, even though the coefficients actually are in the subfield $\mathbf{Q}$. See [Si1, Chapter 2] for a definition of Pic^0, and see [Mi] for details about Jacobians.) In the case where $g = 1$, X is a *principal homogeneous space* [Si1, Chapter 10], or *torsor*, of its Jacobian E. This means that there is an isomorphism $E_{\overline{\mathbf{Q}}} \simeq X_{\overline{\mathbf{Q}}}$ over $\overline{\mathbf{Q}}$, and a morphism of varieties $E \times X \to X$ over $\mathbf{Q}$, which when considered over $\overline{\mathbf{Q}}$ becomes equivalent (after identifying $X_{\overline{\mathbf{Q}}}$ with $E_{\overline{\mathbf{Q}}}$) to the addition morphism $E_{\overline{\mathbf{Q}}} \times E_{\overline{\mathbf{Q}}} \to E_{\overline{\mathbf{Q}}}$. Then $Ш(E)$ is defined as the set of principal homogeneous spaces for E that have $\mathbf{Q}_p$-points for all $p \leq \infty$, up to isomorphism as principal homogeneous spaces of E over $\mathbf{Q}$. It is known that if $Ш(E)$ is finite, then in principle, there is an algorithm for determining whether $X(\mathbf{Q})$ is nonempty: if $X(\mathbf{Q})$ is nonempty, a rational point can be found by search; if $X(\mathbf{Q}_p) = \emptyset$ for some $p \leq \infty$, then $X(\mathbf{Q}) = \emptyset$; if neither holds, then X represents a nonzero element of $Ш(E)$, and this can proved by finding another element Y of $Ш(E)$ such that the Cassels-Tate pairing of X and Y is nonzero in $\mathbf{Q}/\mathbf{Z}$. See [PS] for some definitions of the Cassels-Tate pairing.

4.3. **Genus at least two.** Let X be a curve over $\mathbf{Q}$ of genus at least 2. Mordell [Mo1] conjectured in 1922 that $X(\mathbf{Q})$ is finite, and this was finally proved in 1983 by Faltings [Fa1]. A new proof based on diophantine approximation was found by Vojta [Vo]. Simplifications of Vojta's argument were found by Faltings and by Bombieri, who presented a relatively elementary proof in [Bo].

These proofs let one calculate a bound on the *number* of rational points on X given the equations defining X. But they are ineffective in that they do not provide an upper bound on the numerators and denominators of the coordinates of the rational points, so they cannot be used to determine $X(\mathbf{Q})$ rigorously. They are unable to decide even whether $X(\mathbf{Q})$ is empty.

Ironically, certain other methods (mostly older), which so far have failed to prove the Mordell conjecture in full generality, are the ones that have succeeded in determining $X(\mathbf{Q})$ in many examples. In the next section, we discuss these methods, and the ways in which they have been developed recently into practical algorithms.

5. Methods for curves of genus at least two

We use the following brief names to refer to the various methods that are used to determine $X(\mathbf{Q})$ for a curve X over $\mathbf{Q}$ of genus at least 2:

(1) Local points
(2) Dem'yanenko-Manin
(3) Chabauty
(4) Going-down
(5) Going-up (Chevalley-Weil)

The last two are transitional in the sense that they by themselves do not determine $X(\mathbf{Q})$ directly, but instead reduce the problem of determining $X(\mathbf{Q})$ to the problem of determining the rational points on certain auxiliary varieties. In addition to the methods listed, there is a method based on the modularity of elliptic curves, and another method called "elliptic Chabauty." We will discuss these too, but in fact they can be interpreted as combinations of the methods already listed.

5.1. **Local points.** This method attempts to prove that $X(\mathbf{Q})$ is empty without much work, by showing that $X(\mathbf{Q}_p)$ is empty for some $p \leq \infty$.

For a curve X over $\mathbf{Q}$ of any genus g, it is possible to compute a finite set S of primes such that $X(\mathbf{Q}_p) \neq \emptyset$ for all $p \notin S$. (Because of Hensel's lemma, S can be taken as the set of primes of bad reduction, together with ∞ and the primes p for which the Weil lower bound $p+1-2g\sqrt{p}$ for $X(\mathbf{F}_p)$ is nonpositive.) Then for each $p \in S$, it is possible to check whether $X(\mathbf{Q}_p)$ is empty, since according to Section 2 this problem is decidable for fixed p.

If we find p for which $X(\mathbf{Q}_p)$ is empty, then we know that $X(\mathbf{Q})$ is empty, and we are done. Otherwise we have learned nothing: the Hasse principle, the statement that $X(\mathbf{Q}_p) \neq \emptyset$ for all p implies $X(\mathbf{Q}) \neq \emptyset$, often fails for curves of positive genus.

5.2. **Dem'yanenko-Manin.** This method applies to certain special curves X. If A is an abelian variety, the group structure on A induces a group structure on the set of morphisms $X \to A$ over $\mathbf{Q}$. Let $\mathrm{Mor}(X, A)$ denote the quotient of this group by the subgroup of constant morphisms. If there is an abelian variety A over $\mathbf{Q}$ such that we can prove $\operatorname{rank} \mathrm{Mor}(X, A) > \operatorname{rank} A(\mathbf{Q})$, then the Dem'yanenko-Manin method [De],[Man1] provides an explicit upper bound on the sizes of the numerators and denominators of the coordinates of the rational points on X, so that $X(\mathbf{Q})$ can be computed by a finite search. Note that it is not necessary to know $\operatorname{rank} A(\mathbf{Q})$ exactly. For $\mathbf{Q}$-simple abelian varieties A, the needed inequality is equivalent to the condition that A^m appears in the decomposition of $\operatorname{Jac} X$ into $\mathbf{Q}$-simple abelian varieties up to isogeny, with

$$m > \frac{\operatorname{rank} A(\mathbf{Q})}{\operatorname{rank} \operatorname{End}_{\mathbf{Q}} A},$$

where $\operatorname{End}_{\mathbf{Q}} A$ denotes the ring of endomorphisms of A that are defined over $\mathbf{Q}$. For a fuller exposition of this method, see [Ser2], and for some explicit applications of it, see [Si2], [Ku], and [GR]. Its main disadvantage is that the condition necessary for its application fails for most curves.

5.3. **Chabauty.** This is a method based on p-adic geometry. Suppose that X embeds in an abelian variety A such that $\operatorname{rank} A(\mathbf{Q}) < \dim A$. Suppose also that X generates A in the sense that the differences of points $P - Q$ of $X(\overline{\mathbf{Q}})$ generate the group $A(\overline{\mathbf{Q}})$. For example, A might be $\operatorname{Jac} X$, in which case the condition becomes $\operatorname{rank} A(\mathbf{Q}) < g$, where g is the genus of X. Then the p-adic closure $\overline{A(\mathbf{Q})}$ of $A(\mathbf{Q})$ in $A(\mathbf{Q}_p)$ can be shown to be an "analytic subvariety" of dimension at most $\operatorname{rank} A(\mathbf{Q})$; as a topological group, it is an extension of a finite abelian group by a free $\mathbf{Z}_p$-module of finite rank. The inequality hypothesis guarantees that $\overline{A(\mathbf{Q})}$ has positive codimension in $A(\mathbf{Q}_p)$. Hence by dimension counting, one expects that $X(\mathbf{Q}_p) \cap \overline{A(\mathbf{Q})}$ is at most a zero-dimensional closed subset of the compact group $A(\mathbf{Q}_p)$, hence finite. Chabauty [Ch] proved this finiteness statement. But $X(\mathbf{Q}) \subseteq X(\mathbf{Q}_p) \cap \overline{A(\mathbf{Q})}$, and by computing the intersection to a given p-adic precision, one can bound the number of rational points on $X(\mathbf{Q})$, and obtain p-adic approximations to their possible locations. Coleman [Co] gave an explicit upper bound on the size of this intersection. The intersection can be computed to some p-adic precision either by working with the formal

group of J, or by looking at the p-adic integrals of regular differentials on X. The latter seems to be easier, especially for higher genus curves.

Unfortunately, $X(\mathbf{Q})$ may be strictly smaller than $X(\mathbf{Q}_p) \cap \overline{A(\mathbf{Q})}$, although heuristically this may be rare when $\operatorname{rank} A(\mathbf{Q}) \leq \dim A - 2$: in that case the naive dimension count suggests that the intersection is empty so perhaps, if there are points in the intersection, they are there for a reason! Because of the possibility that $X(\mathbf{Q}) \neq X(\mathbf{Q}_p) \cap \overline{A(\mathbf{Q})}$, the condition $\operatorname{rank} A(\mathbf{Q}) < \dim A$ alone is not sufficient for success. In practice, however, Chabauty's method has proved successful, especially in conjunction with the transitional methods to be discussed below. See for example, [Gr], [McC], [Fl], [Bak], and [LT].

5.4. **Going-down.** If X admits a nonconstant morphism $X \to Y$ over $\mathbf{Q}$ to another variety Y over $\mathbf{Q}$, where $Y(\mathbf{Q})$ is finite and computable, then one can determine $X(\mathbf{Q})$, since it suffices to examine the finitely many points in $X(\overline{\mathbf{Q}})$ mapping to the points in $Y(\mathbf{Q})$: every point in $X(\mathbf{Q})$ must map to some point in $Y(\mathbf{Q})$. In practice, Y is usually an abelian variety with $Y(\mathbf{Q})$ finite, or Y is another curve.

5.5. **Going-up.** If $f : Y \to X$ is an *unramified* morphism of curves over $\mathbf{Q}$, Chevalley and Weil proved that there is a computable finite extension k of $\mathbf{Q}$ such that $f^{-1}(X(\mathbf{Q})) \subseteq Y(k)$. If X has genus at least 2, then Y does too, so $Y(k)$ is known to be finite. Hence one can reduce the problem of computing $X(\mathbf{Q})$ to that of computing $Y(k)$.

One difficulty with this method is that k may be much larger than $\mathbf{Q}$. Fortunately, Coombes and Grant [CG] and Wetherell [We] found variants of the method that instead gave a finite set of unramified covering curves $Y_i \to X$ over $\mathbf{Q}$, $1 \leq i \leq n$, all isomorphic over $\overline{\mathbf{Q}}$, such that $X(\mathbf{Q}) \subseteq \bigcup_{i=1}^{n} f_i(Y_i(\mathbf{Q}))$. Given such a covering collection, one can determine $X(\mathbf{Q})$ if one can determine $Y_i(\mathbf{Q})$ for all i. Specialized to the case where X is an elliptic curve, this becomes the method of descent used to prove the Mordell-Weil Theorem.

Let us give one example of this method, taken from [Brn2]. Suppose that we want to find $X(\mathbf{Q})$, where X is the curve of genus 2 that is the smooth projective model of the affine hyperelliptic curve $y^2 = 6x(x^4 + 12)$. (This is one of the curves that comes up when one studies the integer solutions to the equation $x^8 + y^3 = z^2$.) Suppose we have an affine point $(x_0, y_0) \in X(\mathbf{Q})$ with $x_0, y_0 \neq 0$. If we write $x_0 = X/Z$ in lowest terms with $X, Z \in \mathbf{Z}$, $Z \neq 0$, we obtain $y_0^2 Z^6 = 6XZ(X^4 + 12Z^4)$. Setting $Y = y_0 Z^3$, which must be an integer, since its square equals the right hand side, we obtain $Y^2 = 6XZ(X^4 + 12Z^4)$. If a prime $p \geq 5$ divides both $6XZ$ and $X^4 + 12Z^4$, then it divides either X or Z, and then in order to divide $X^4 + 12Z^4$ it must divide *both* X and Z, contradicting the assumption that

X/Z is in lowest terms. (More generally, one would argue using primes not dividing the resultant of the two homogeneous polynomial factors.) Thus each prime $p \geq 5$ divides at most one of $6XZ$ and $X^4 + 12Z^4$. But their product is a square, so if p divides one of $6XZ$ and $X^4 + 12Z^4$, the exponent of p in that factor is even. Since this holds for all $p \geq 5$, we have $X^4 + 12Z^4 = \delta W^2$ for some $\delta \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$ and $W \in \mathbf{Z}$. Dividing by Z^4, we obtain a rational point (u, v) on the curve $E_\delta : \delta v^2 = u^4 + 12$. We may assume $\delta > 0$ (since otherwise $E_\delta(\mathbf{R}) = \emptyset$) and $2|\delta$ (since otherwise $E_\delta(\mathbf{Q}_2) = \emptyset$). Therefore we need only search for rational points on

$$E_1 : v^2 = u^4 + 12, \quad \text{and} \quad E_3 : 3v^2 = u^4 + 12.$$

These are curves of genus one, and with a little work, using descent, one can show that $E_1(\mathbf{Q})$ and $E_3(\mathbf{Q})$ are finite, each of size 2, counting points on the nonsingular projective models. Checking to see what points on X these give rise to, we find that $X(\mathbf{Q})$ consists of $(0, 0)$ and a point at infinity on the projective model.

Geometrically what has happened here is that for each $\delta \in \mathbf{Q}^*$, the genus 3 curve Y_δ defined by the *system* of equations

$$y^2 = 6x(x^4 + 12), \quad \delta z^2 = x^4 + 12$$

in (x, y, z)-space maps to X via $(x, y, z) \mapsto (x, y)$, and Y_δ is an unramified cover of X. Moreover, the union of the images of $Y_\delta(\mathbf{Q})$ in X equals $X(\mathbf{Q})$. Since the isomorphism class of Y_δ depends only on the image of δ in $\mathbf{Q}^*/\mathbf{Q}^{*2}$, we may assume that $\delta \in \mathbf{Z}$ is nonzero and squarefree. If a prime $p \geq 5$ divides δ, then $Y_\delta(\mathbf{Q}_p) = \emptyset$, so we may discard Y_δ. By also demanding the existence of local points over $\mathbf{R}$ and $\mathbf{Q}_2$, we may discard all but Y_1 and Y_3. (As it turns out, $\mathbf{Q}_3$ gives no further restriction.) Finally, $(x, y, z) \mapsto (x, z)$ gives a nonconstant morphism $Y_\delta \to E_\delta$, so by "going down" it suffices to find $E_1(\mathbf{Q})$ and $E_3(\mathbf{Q})$, if these are finite. We are lucky: both E_1 and E_3 turn out to be elliptic curves of rank zero.

In general, covering collections by geometrically *abelian* covers are described by geometric class field theory. They arise as follows. Suppose that X is embedded in its Jacobian J using a basepoint $P_0 \in X(\mathbf{Q})$. Choose an isogeny $\phi : A \to J$, i.e., a surjective homomorphism between abelian varieties with finite kernel. Choose a representative $R \in J(\mathbf{Q})$ of each element of $J(\mathbf{Q})/\phi(A(\mathbf{Q}))$, let $\phi_R : A \to J$ be the composition ϕ followed by translation-by-R on J, and let Y_R denote the following fiber product:

$$\begin{array}{ccc} Y_R & \longrightarrow & X \\ \downarrow & & \downarrow \\ A & \xrightarrow{\phi_R} & J. \end{array}$$

In other words, Y_R is the inverse image $\phi_R^{-1}(X)$ in A. Then the Y_R form a finite set of unramified covers of X, and the union of the images of $Y_R(\mathbf{Q})$ in X equals $X(\mathbf{Q})$, since $\bigcup_R \phi_R(A(\mathbf{Q})) = J(\mathbf{Q})$.

Note that given X and hence J, there are many pairs (A, ϕ) where $\phi : A \to J$ is an isogeny over $\mathbf{Q}$: if nothing else is available, one can take ϕ as the multiplication-by-m map $[m] : J \to J$ for some $m \geq 2$. Hence going up is always possible. On the other hand, for $\phi = [m]$, the genus of each Y_R equals $m^{2g}(g-1)+1$ by the Riemann-Hurwitz formula [Ha, IV.2.4] so if m is too large, the Y_R may be difficult to work with. In fact, it might be preferable to use an isogeny ϕ of degree lower than $\deg[2] = 2^{2g}$ if one exists.

5.6. **Modularity.** Through the work of Wiles, Taylor, Breuil, Conrad, and Diamond [Wi],[TW],[BCDT], it is now known that every elliptic curve E over $\mathbf{Q}$ is modular, meaning that there exists a nonconstant morphism from the modular curve $X_0(N)$ to E, for some integer $N \geq 1$. See [La, Chapter V] for an introduction to this concept, and see [Shi] and [KM] for more details on modular functions and curves. On the other hand, work of Frey, Serre, and Ribet [Ri1] showed that a nontrivial rational point on $x^p + y^p = 1$ for prime $p > 2$ would give rise to an elliptic curve over $\mathbf{Q}$ that could not be modular. Together, these results proved Fermat's Last Theorem. For an overview of the whole proof, see [DDT] or the book [CSS]. In the past few years, methods based on modularity have been adapted to solve certain other Fermat-like diophantine equations. See [DM] and [Ri2], for instance.

Darmon has pointed out that these proofs can be interpreted as instances of the going-up method. Recall that the geometric class field theory construction at the end of Section 5.5 produces only unramified covers Y that when considered over $\overline{\mathbf{Q}}$ are Galois and abelian over the base curve X. These abelian covers are the easiest unramified covers to work with, but they form only a small subset of *all* the unramified covers. Kummer's partial results on Fermat's Last Theorem can be reinterpreted as a study of the abelian covers of the Fermat curve $X : x^p + y^p = 1$ with Galois group $\mathbf{Z}/p$. The modularity proof of Fermat's Last Theorem is equivalent to a study of certain unramified covers with nonabelian Galois group. More precisely, the map $(x, y) \mapsto x^p$ from $X \to \mathbf{P}^1$ exhibits X as a cover of $\mathbf{P}^1$ ramified above $\{0, 1, \infty\}$, and the latter can be thought of as the modular curve $X(2)$ with its three cusps. The fiber product

$$\begin{array}{ccc} Y & \longrightarrow & X \\ \downarrow & & \downarrow \\ X(2p) & \longrightarrow & X(2). \end{array}$$

is an unramified cover Y of X with Galois group equal to that of $X(2p)$ over $X(2)$, namely the nonabelian group $\mathrm{PSL}_2(\mathbf{F}_p)$. One can then study the rational points on Y and its relevant twists by going down to $X(2p)$ and its twists. Thus one reduces to questions about rational points on modular curves, to which one can apply the work of Mazur.

5.7. **Elliptic Chabauty.** This is not so much a separate method as it is a clever way to combine the going-up and Chabauty methods. It was discovered independently by Bruin [Brn1] and by Flynn and Wetherell [FW1].

Suppose that X is a curve of genus 2 over $\mathbf{Q}$ embedded in its Jacobian J_X using a basepoint $P_0 \in X(\mathbf{Q})$. Consider the curves Y obtained as in Section 5.5 by pulling back X under the multiplication-by-2 isogeny $J_X \to J_X$, or its translates. Then Y is an unramified cover of X, and when considered over $\overline{\mathbf{Q}}$, it is an abelian cover with Galois group $J_X[2](\overline{\mathbf{Q}}) \simeq (\mathbf{Z}/2)^4$. As mentioned in Section 5.5, the Riemann-Hurwitz formula shows that the genus of Y is 17. By Galois theory, there are 15 intermediate covers Z_i of $X_{\overline{\mathbf{Q}}}$ of degree 2, and these have genus 3. Hence each Jacobian J_{Z_i} is isogenous over $\overline{\mathbf{Q}}$ to $J_X \times E_i$ for some elliptic curve E_i, and it follows that J_Y is isogenous to $J_X \times A$ where A is a 15-dimensional abelian variety isomorphic to $\prod_{i=1}^{15} E_i$ over $\overline{\mathbf{Q}}$. More precisely, one can show that one can take A to the Weil restriction of scalars $\mathrm{Res}_{K/\mathbf{Q}} E$ of an elliptic curve E over the 15-dimensional $\mathbf{Q}$-algebra K of global sections of the structure sheaf on $J_X[2] - \{0\}$. (See [BLR, Section 7.6] for the definition of the Weil restriction of scalars.) More concretely, K is the product of the fields of definition of representatives for the Galois orbits of nontrivial 2-torsion points of J; often there is just one orbit and K is a number field of degree 15 over $\mathbf{Q}$. One then can attempt to apply Chabauty to $Y \to A$ for each Y.

Whereas success of the direct Chabauty method required $\operatorname{rank} J_X(\mathbf{Q}) < 2$, elliptic Chabauty requires the (independent?) condition $\operatorname{rank} A(\mathbf{Q}) < \dim A$ for each A that arises. One of the properties of restriction of scalars is that $A(\mathbf{Q}) \simeq E(K)$, and we also know $\dim A = 15$, so the latter condition is equivalent to $\operatorname{rank} E(K) < 15$. Perhaps this is more likely than $\operatorname{rank} J_X(\mathbf{Q}) < 2$. In the worst case, when K is a number field and each nonzero 2-torsion point of E is defined only over a cubic extension of K, we apparently need to compute the 2-part of the class group of a degree 45 number field to complete the descent to compute $\operatorname{rank} E(K)$. But in favorable cases, the number fields are much smaller, and the method is practical.

Elliptic Chabauty has the advantage over the original Chabauty method that one can do all the computations with the group law of E over K, instead of a Jacobian over $\mathbf{Q}$. The former is usually easier from the computational point of view: as Bruin says, "simple geometry over a field with

complicated arithmetic is to be preferred over complicated geometry over a field with simple arithmetic."

6. The Mordell-Weil race

If faced with the problem of determining $X(\mathbf{Q})$ for a specific curve X over $\mathbf{Q}$ of genus $g \geq 2$, it is probably best first to try the method of local points. If this fails, next one can try to see if X admits a nonconstant morphism to a curve Y where Y has genus at least 2, or where Y is a curve of genus 1 for which $Y(\mathbf{Q})$ is finite and can be determined. If not, one can attempt the Dem'yanenko-Manin method, and the method of Chabauty.

If all of these fail, one can go up to a set of unramified covering curves, and then recursively apply the above methods to each of these.

It seems plausible that iteration of going-up and Chabauty alone are sufficient to resolve $X(\mathbf{Q})$ for every curve X of genus $g \geq 2$ over $\mathbf{Q}$! Starting from X, one replaces the problem on X with the problem on a finite set of covering curves Y_R. For each Y_R whose rational points are not resolved by Chabauty, one must replace Y_R by a finite set of its covering curves, and so on. We obtain a tree and hope that all the branches will eventually be terminated by Chabauty. If one applies Chabauty to the Jacobians alone, the issue is whether the genus eventually outpaces the rank of the Jacobian as one goes up along any branch of the tree. If so, Chabauty is likely to succeed in terminating all the branches.

In practice, one can apply Chabauty to morphisms from the curve into *quotients* of its Jacobian at each node of the tree, as in the elliptic Chabauty method of Section 5.7. This is preferable especially if the original X has large rank: if Y covers X, the Jacobian J_Y is isogenous over $\mathbf{Q}$ to $J_X \times A$ for some abelian variety A over $\mathbf{Q}$, so $\operatorname{rank} J_Y(\mathbf{Q}) = \operatorname{rank} J_X(\mathbf{Q}) + \operatorname{rank} A(\mathbf{Q})$, which will still be large, if $\operatorname{rank} J_X(\mathbf{Q})$ was large to begin with. On the other hand, there seems to be no direct correlation between $\operatorname{rank} A(\mathbf{Q})$ and $\operatorname{rank} J_X(\mathbf{Q})$.

Unfortunately, virtually nothing is known about the growth of Mordell-Weil ranks as one ascends an unramified tower of curves, and hence it seems impossible to prove anything about the success of this tree method. All we have now are a few isolated examples in which the method has been successful. For a genus g curve X, is $\operatorname{rank} J_X(\mathbf{Q})$ typically of size around g? Or is it typically $O(1)$ as $g \to \infty$? It seems difficult even to find a heuristic that predicts the answers. Perhaps analytic methods generalizing [Brum] will provide hints.

Even if the truth is that the going-up and Chabauty methods are *not* always enough to determine $X(\mathbf{Q})$, there are several other conjectural approaches towards an effective algorithm. See Section F.4.2 of [HS] for a survey of some of these.

7. Some success stories

7.1. **Diophantus.** About 1700 years ago, Diophantus challenged his readers to find a solution to

$$y^2 = x^8 + x^4 + x^2$$

in positive rational numbers. This is not hard, but these days one wants to know *all* the solutions. Wetherell [We] combined going-up, going-down, and Chabauty to prove that $(1/2, 9/16)$ is the only positive rational solution.

7.2. **Serre.** Over 15 years ago, Serre challenged the mathematical community to find the rational points on $x^4 + y^4 = 17$, a genus 3 curve whose Jacobian is isogenous to $E \times E \times E'$ where E, E' are elliptic curves over $\mathbf{Q}$, each of rank 2. This past year, Flynn and Wetherell [FW2] found suitable unramified covers and applied a version of elliptic Chabauty to them to prove that the only rational points are the obvious eight with

$$\{|x|, |y|\} = \{1, 2\}.$$

7.3. **Generalized Fermat.** Work of Beukers [Beu], and of Darmon and Granville [DG] reduces solving $x^p + y^q = z^r$ in relatively prime integers x, y, z for fixed $p, q, r > 1$ to computing $X(\mathbf{Q})$ for a finite set of curves X over $\mathbf{Q}$. As has already been mentioned, methods based on modularity of elliptic curves solve the equation for many (p, q, r). Some of the small exponent cases, too small for modularity methods to work easily, are worked out in [Brn1], [Brn2], [Brn3], and [Po]. For example, [Brn2] applies elliptic Chabauty and other methods to prove that the only solutions to

$$x^8 + y^3 = z^2$$

in nonzero relatively prime integers are

$$(\pm 1, 2, \pm 3) \quad \text{and} \quad (\pm 43, 96222, \pm 30042907).$$

References

[AK1] J. Ax and S. Kochen, Diophantine problems over local fields. II. A complete set of axioms for p-adic number theory. Amer. J. Math., **87** (1965), 631–648.

[AK2] J. Ax and S. Kochen, Diophantine problems over local fields. III. Decidable fields. Ann. of Math. (2) **83** (1966), 437–456.

[Bak] M. H. Baker, Kamienny's criterion and the method of Coleman and Chabauty. Proc. Amer. Math. Soc. **127** (1999), no. 10, 2851–2856.

[Beu] F. Beukers, The Diophantine equation $Ax^p + By^q = Cz^r$. Duke Math. J. **91** (1998), no. 1, 61–88.

[BCDT] C. Breuil, B. Conrad, F. Diamond and R. Taylor, On the modularity of elliptic curves over $\mathbf{Q}$, preprint 1999.

[Bo] E. Bombieri, The Mordell conjecture revisited. Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **17** (1990), no. 4, 615–640. Errata-corrige: "The Mordell conjecture revisited". Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **18** (1991), no. 3, 473.

[BLR] S. Bosch, W. Lütkebohmert and M. Raynaud, Néron models, Springer, Berlin, 1990.

[Brn1] N. Bruin, Chabauty methods using elliptic curves, preprint, 1999.

[Brn2] N. Bruin, Chabauty methods using covers on curves of genus 2, preprint, 1999.

[Brn3] N. Bruin, The diophantine equations $x^2 \pm y^4 = \pm z^6$ and $x^2 + y^8 = z^3$, Compositio Math. **118** (1999), 305-321.

[Brum] A. Brumer, The average rank of elliptic curves. I. Invent. Math. **109** (1992), no. 3, 445–472.

[BFH] D. Bump, S. Friedberg, J. Hoffstein, Nonvanishing theorems for L-functions of modular forms and their derivatives. Invent. Math. **102** (1990), no. 3, 543–618.

[CC] H. Cartan and C. Chevalley, Géometrie algébrique, Séminaire Cartan-Chevalley, Secrétariat Math., Paris, 1955–1956.

[Ch] C. Chabauty, Sur les points rationnels des courbes algébriques de genre supérieur à l'unité, Comptes Rendus Hebdomadaires des Séances de l'Acad. des Sci., Paris **212** (1941), 882–885.

[CW] C. Chevalley and A. Weil, Un théorème d'arithmétiques sur les courbes algébriques, Comptes Rendus Hebdomadaires des Séances de l'Acad. des Sci., Paris **195** (1930), 570–572.

[Co] R. F. Coleman, Effective Chabauty, Duke Math. J. **52** (1985), 765–780.

[CS] J.-L. Colliot-Thélène et J.-J. Sansuc, La descente sur les variétés rationnelles, in Journées de Géométrie Algébrique d'Angers, Juillet 1979/Algebraic Geometry, Angers, 1979, 223–237, Sijthoff & Noordhoff, Alphen aan den Rijn, 1980.

[CSSD] J.-L. Colliot-Thélène, A. N. Skorobogatov, and P. Swinnerton-Dyer, Double fibres and double covers: paucity of rational points. Acta Arith. **79** (1997), no. 2, 113–135.

[CG] K. R. Coombes, D. R. Grant, On heterogeneous spaces. J. London Math. Soc. (2) **40** (1989), no. 3, 385–397.

[CSS] G. Cornell, J. H. Silverman, and G. Stevens (eds.), Modular forms and Fermat's last theorem. Papers from the Instructional Conference on Number Theory and Arithmetic Geometry held at Boston University, Boston, MA, August 9–18, 1995. Springer-Verlag, New York, 1997.

[Cr] J. E. Cremona, Algorithms for modular elliptic curves. Second edition. Cambridge University Press, Cambridge, 1997.

[DDT] H. Darmon, F. Diamond, and R. Taylor, Fermat's last theorem, 2–140 in: Elliptic curves, modular forms & Fermat's last theorem. Proceedings of the Conference on Elliptic Curves and Modular Forms held at the Chinese University of Hong Kong, Hong Kong, December 18–21, 1993. Edited by John Coates and S. T. Yau. Second edition. International Press, Cambridge, MA, 1997. (Note: the first edition does not contain this paper.)

[DG] H. Darmon and A. Granville, On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$, Bull. London Math. Soc. **27** (1995), no. 6, 513–543.

[DM] H. Darmon and L. Merel, Winding quotients and some variants of Fermat's last theorem. J. Reine Angew. Math. **490** (1997), 81–100.

[De] V. Dem'yanenko, Rational points on a class of algebraic curves, Amer. Math. Soc. Transl. **66** (1968), 246–272.

[Er] Yu. Ershov, Undecidability of certain fields. (Russian) Dokl. Akad. Nauk SSSR **161** (1965), 349–352.

[Fa1] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. (German) Invent. Math. **73** (1983), no. 3, 349–366. English translation: pp. 9–27 in Arithmetic geometry, eds. G. Cornell and J. Silverman, Springer-Verlag, New York-Berlin, 1986.

[Fa2] G. Faltings, The general case of S. Lang's conjecture. Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991), 175–182, Perspect. Math. **15**, Academic Press, San Diego, CA, 1994.

[Fl] E. V. Flynn, A flexible method for applying Chabauty's theorem. Compositio Math. **105** (1997), no. 1, 79–94.

[FW1] E. V. Flynn and J. L. Wetherell, Finding rational points on bielliptic genus 2 curves. Manuscripta Math. **100** (1999), no. 4, 519–533.

[FW2] E. V. Flynn and J. L. Wetherell, Covering collections and a challenge problem of Serre, to appear in Acta Arith.

[Ja] N. Jacobson, Basic Algebra I. Second edition. W. H. Freeman and Company, New York, 1985.

[Gö] K. Gödel, Über formal unentscheidbare Sätze der Principia Mathematica und verwandter System I. Monatshefte für Math. und Physik **38** (1931), 173–198. English translation by Elliot Mendelson: "On formally undecidable propositions of Principia Mathematica and related systems I" in M. Davis, The undecidable, Raven press, 1965.

[Gr] D. Grant, A curve for which Coleman's effective Chabauty bound is sharp, Proc. Amer. Math. Soc. **122** (1994), 317–319.

[GR] G. Grigorov and J. Rizov, Heights on elliptic curves and the equation $x^4 + y^4 = cz^4$, preprint, 1998.

[Ha] R. Hartshorne, Algebraic geometry. Graduate Texts in Mathematics **52**, Springer-Verlag, New York-Heidelberg, 1977.

[HS] M. Hindry and J. H. Silverman, Diophantine geometry. An introduction. Graduate Texts in Mathematics **201**, Springer-Verlag, New York, 2000.

[HU] J. E. Hopcroft and J. D. Ullman, Formal languages and their relation to automata. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. 1969.

[KM] N. M. Katz and B. Mazur, Arithmetic moduli of elliptic curves. Annals of Mathematics Studies **108**. Princeton University Press, Princeton, N.J., 1985.

[Kob] N. Koblitz, p-adic numbers, p-adic analysis, and zeta-functions. Second edition. Graduate Texts in Mathematics, 58. Springer-Verlag, New York-Berlin, 1984.

[Kol] V. Kolyvagin, Finiteness of $E(\mathbf{Q})$ and Ш$(E, \mathbf{Q})$ for a subclass of Weil curves (Russian), Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 3, 522–540, 670–671; translation in Math. USSR-Izv. **32** (1989), no. 3, 523–541.

[Ku] L. Kulesz, Application de la méthode de Dem'janenko-Manin à certaines familles de courbes de genre 2 et 3. J. Number Theory **76** (1999), no. 1, 130–146.

[La] S. Lang, Number theory. III. Diophantine geometry. Encyclopaedia of Mathematical Sciences **60**, Springer-Verlag, Berlin, 1991.

[LLL] A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász, Factoring polynomials with rational coefficients. Math. Ann. **261** (1982), no. 4, 515–534.

[Lin] C.-E. Lind, Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins, Thesis, University of Uppsala, 1940.

[LT] D. Lorenzini and T. J. Tucker, Thue equations and the method of Chabauty-Coleman, preprint, May 2000.

[Mac] A. Macintyre, On definable subsets of p-adic fields. J. Symbolic Logic **41** (1976), no. 3, 605–610.

[Man1] Yu. I. Manin, The p-torsion of elliptic curves is uniformly bounded (Russian), Isv. Akad. Nauk. SSSR Ser. Mat. **33** (1969); English translation in: *Amer. Math. Soc. Transl.*, 433–438.

[Man2] Yu. I. Manin, Le groupe de Brauer-Grothendieck en géométrie diophantienne, in Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 1, 401–411, Gauthier-Villars, Paris, 1971.

[Mati] Yu. Matiyasevich, The Diophantineness of enumerable sets. (Russian) Dokl. Akad. Nauk SSSR **191** (1970), 279–282.

[Mats] H. Matsumura, Commutative algebra. W. A. Benjamin, Inc., New York, 1970.

[Maz1] B. Mazur, The topology of rational points. Experiment. Math. **1** (1992), no. 1, 35–45.

[Maz2] B. Mazur, Questions of decidability and undecidability in number theory. J. Symbolic Logic **59** (1994), no. 2, 353–371.

[Maz3] B. Mazur, Speculations about the topology of rational points: an update. Columbia University Number Theory Seminar (New York, 1992). Astérisque No. 228, (1995), 4, 165–182.

[McC] W. McCallum, On the method of Coleman and Chabauty. Math. Ann. **299** (1994), no. 3, 565–596.

[Mi] J. S. Milne, Jacobian Varieties, in: G. Cornell and J. H. Silverman (eds.), Arithmetic geometry, 167–212, Springer-Verlag, New York, 1986.

[Mo1] L. J. Mordell, On the rational solutions of the indeterminate equations of the third and fourth degrees, Proc. Cambridge Phil. Soc. **21** (1922), 179–192.

[Mo2] L. J. Mordell, On the magnitude of the integer solutions of the equation $ax^2 + by^2 + cz^2 = 0$. J. Number Theory **1** (1969), 1–3.

[MM] M. Ram Murty and V. Kumar Murty, Mean values of derivatives of modular L-series. Ann. of Math. (2) **133** (1991), no. 3, 447–475.

[Pe] Yu. Penzin, Undecidability of fields of rational functions over fields of characteristic 2. (Russian) Algebra i Logika **12** (1973), 205–210, 244.

[Ph] T. Pheidas, Hilbert's tenth problem for fields of rational functions over finite fields. Invent. Math. **103** (1991), no. 1, 1–8.

[PZ] T. Pheidas and K. Zahidi, Undecidability of existential theories of rings and fields: a survey, to appear in the Proceedings of the workshop on Hilbert's 10th Problem, November 2–5, University of Gent, in the Contemporary Mathematics series of the AMS.

[Po] B. Poonen, Some Diophantine equations of the form $x^n + y^n = z^m$. Acta Arith. **86** (1998), no. 3, 193–205.

[PS] B. Poonen and M. Stoll, The Cassels-Tate pairing on polarized abelian varieties, Ann. of Math. (2) **150** (1999), no. 3, 1109–1149.

[Rei] H. Reichardt, Einige im Kleinen überall lösbare, im Grossen unlösbare diophantische Gleichungen, J. Reine Angew. Math. **184** (1942), 12–18.

[Ri1] K. A. Ribet, On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. Invent. Math. **100** (1990), no. 2, 431–476.

[Ri2] K. A. Ribet, On the equation $a^p + 2^\alpha b^p + c^p = 0$. Acta Arith. **79** (1997), no. 1, 7–16.

[Ro] J. Robinson, Definability and decision problems in arithmetic. J. Symbolic Logic **14** (1949), 98–114.

[Sel] E. Selmer, The diophantine equation $ax^3 + by^3 + cz^3 = 0$, Acta Math. **85** (1951), 203–362 and **92** (1954), 191–197.

[Ser1] J.-P. Serre, A course in arithmetic. Translated from the French. Graduate Texts in Mathematics **7**, Springer-Verlag, New York-Heidelberg, 1973.

[Ser2] J.-P. Serre, Lectures on the Mordell-Weil theorem. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt. Aspects of Mathematics, E15. Friedr. Vieweg & Sohn, Braunschweig, 1989.

[Shi] G. Shimura, Introduction to the arithmetic theory of automorphic functions. Reprint of the 1971 original. Publications of the Mathematical Society of Japan **11**. Kanô Memorial Lectures, 1. Princeton University Press, Princeton, NJ, 1994.

[Shl] A. Shlapentokh, Hilbert's Tenth Problem over number fields, a survey, to appear in the Proceedings of the workshop on Hilbert's 10th Problem, November 2–5, University of Gent, in the Contemporary Mathematics series of the AMS.

[Si1] J. H. Silverman, The arithmetic of elliptic curves. Graduate Texts in Mathematics **106**, Springer-Verlag, New York-Berlin, 1986.

[Si2] J. H. Silverman, Rational points on certain families of curves of genus at least 2, Proc. London Math. Soc. (3) **55** (1987), no. 3, 465–481.

[Sk] A. N. Skorobogatov, Beyond the Manin obstruction, Invent. Math. **135** (1999), no. 2, 399–424.

[Ta] A. Tarski, A decision method for elementary algebra and geometry. 2nd ed. University of California Press, Berkeley and Los Angeles, Calif., 1951.

[TW] R. Taylor and A. Wiles, Ring-theoretic properties of certain Hecke algebras. Ann. of Math. (2) **141** (1995), no. 3, 553–572.

[Vi] C. Videla, Hilbert's tenth problem for rational function fields in characteristic 2. Proc. Amer. Math. Soc. **120** (1994), no. 1, 249–253.

[Vo] P. Vojta, Siegel's theorem in the compact case. Ann. of Math. (2) **133** (1991), no. 3, 509–548.

[We] J. L. Wetherell, Bounding the number of rational points on certain curves of high rank, Thesis, University of California at Berkeley, 1997.

[Wi] A. Wiles, Modular elliptic curves and Fermat's last theorem. Ann. of Math. (2) **141** (1995), no. 3, 443–551.

Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA

E-mail address: poonen@math.berkeley.edu