THE OPEN BOOK SERIES 1

ANTS X
Proceedings of the Tenth Algorithmic Number Theory Symposium

Success and challenges in determining the rational points on curves

Nils Bruin

msp

THE OPEN BOOK SERIES 1 (2013)
Tenth Algorithmic Number Theory Symposium
dx.doi.org/10.2140/obs.2013.1.187

Success and challenges in determining the rational points on curves

Nils Bruin

We give an overview of current computational methods for determining the rational points on algebraic curves. We discuss how two methods, based on embedding a curve in an abelian variety, provide a practical method for deciding whether the curve has rational points and, if some additional technical condition is met, for the determination of these points.

While we cannot prove the methods are always successful, we do have a heuristic that makes us expect so. This means that the main problem becomes the determination of rational points on abelian varieties, in particular the determination of the free rank of the finitely generated group they form. We discuss some methods that provide bounds on this rank.

Finally, we report on some recent progress on applying these methods to non-hyperelliptic curves of genus 3.

1. Introduction

This article is an extended abstract from an invited lecture delivered on July 13, 2012, as part of the Tenth Algorithmic Number Theory Symposium (ANTS X), at the University of California, San Diego. It discusses current computational methods for determining the rational points on algebraic curves. Two methods, *Mordell-Weil sieving* (see Section 4) and *Chabauty's method* (see Section 5) together provide a procedure that often decides whether a curve has any rational points and, if so, determines them. While we cannot prove that these methods will always succeed, we do have some heuristics that indicate that this is quite likely.

Both methods rely on embedding a curve in an abelian variety J and on having a rather detailed description of the rational points on J. There is presently no proven

MSC2010: primary 11G30; secondary 11G10, 14G25, 14H45.

Keywords: Selmer group, descent, Mordell-Weil sieving, rational points, curves, Chabauty, coverings.

algorithm for determining the rational points on an abelian variety, but here too we have methods that frequently work in practice. In fact, if Tate-Shafarevich groups are finite, as they are conjectured to be, then it would theoretically be possible to compute the rational points on an abelian variety.

The main point of this article is that the computational bottleneck for determining rational points on curves presently lies in the determination of rational points on abelian varieties. Our main tool is the computation of Selmer sets via finite descent.

After reviewing the Mordell-Weil sieve and Chabauty's method in Sections 4 and 5, we give a brief description in Section 7 of recent joint work [14] with Bjorn Poonen and Michael Stoll to provide a description of descent computations which, to our knowledge, encompasses all previous methods for doing such computations for curves.

We note in Section 8 that descent methods also help in deciding whether a curve C can be embedded in its Jacobian, a requirement for the curve to have rational points and for the application of the Mordell-Weil sieve and Chabauty's method. A good description of Selmer groups also helps in constructing *covering collections*, which can be used to transform problems where Chabauty's method does not apply into problems where it may.

The most difficult ingredient in descent computations usually is the determination of unit groups and ideal class groups of number fields. Especially for number fields of larger degrees, this can be extremely challenging. In Section 7 we describe some ways one can reduce the maximal degree to be considered: from 63 to 28 in the case of smooth plane quartic curves. This has allowed us to perform the required calculations for some genus-3 curves. To our knowledge, these are the first examples of curves with simple Jacobians and trivial automorphism groups to which the methods have been successfully applied. Previous applications made essential use of decompositions of the Jacobian or of the automorphisms to get descriptions more favorable to computation.

Since in general curves have trivial automorphism groups, we believe these examples present evidence that these methods are indeed quite generally applicable, although the computational challenges can be daunting.

We cannot hope to give an exhaustive account of the subject here. Instead, we intend to provide the reader with a bit of insight into how the different methods interact and what the fundamental ideas and problems are. We have also included ample literature references for further reading.

2. Statement of the problems

Consider the equation

$$x^4 + y^4 + x^2y + 2xy - y^2 + 1 = 0. \tag{1}$$

Can you determine the solutions $x, y \in \mathbb{Q}$ to this equation? Can you determine whether this equation has any rational solutions at all? These are questions about *rational points on curves*, and such questions are about as old as mathematics itself. (See Proposition 9.3 for results on this particular equation.)

We concern ourselves with curves C defined over $\mathbb{Q}$, and we want to study the set of rational points $C(\mathbb{Q})$. Every curve has a projective closure, which has at most finitely many additional rational points. Furthermore, every curve admits a morphism from a nonsingular curve that is an isomorphism outside the finitely many singularities, which are easily determined and tested for rationality. We can therefore restrict our attention to nonsingular, absolutely irreducible, projective curves.

The reader does not lose much, and may gain a more concrete conception, by thinking of C as a smooth plane curve such as the projective closure of the curve defined by Equation (1). Although much of what we discuss holds with suitable modifications over arbitrary number fields, we will limit ourselves to $\mathbb{Q}$ for the sake of concreteness and ease of notation.

A common theme in arithmetic geometry is that *geometry* determines *arithmetic*: The geometric classification of curves C has deep ramifications for the structure of $C(\mathbb{Q})$. There are:

- *Curves of genus* 0. These are always isomorphic to plane conics. Either such a curve C has no rational points at all, or C admits a parametrization $\phi\colon \mathbb{P}^1 \to C$, providing an explicit bijection between $\mathbb{P}^1(\mathbb{Q})$ and $C(\mathbb{Q})$.
- *Curves of genus* 1. If C has any rational points, then C is isomorphic to an elliptic curve. In that case, Mordell's Theorem [46] implies that $C(\mathbb{Q})$ can be described as a finitely generated abelian group.
- *Curves of general type* (genus at least 2). Faltings's Theorem [28] states that $C(\mathbb{Q})$ is a finite set.

We concentrate on two explicit questions.

Decision Problem. Given a curve C over $\mathbb{Q}$, decide if $C(\mathbb{Q}) = \varnothing$.

Determination Problem. Given a curve C over $\mathbb{Q}$, give an explicit description of $C(\mathbb{Q})$.

We assume that the curve is given to us in a sufficiently explicit way, for instance by explicit equations like Equation (1). For genus-0 curves, both questions have a reasonably satisfactory solution [44, pp. 512–513] (and see [58] for a modern algorithmic perspective). For genus-1 curves, a satisfactory answer to the determination problem is usually considered to be an explicit listing of a finite set of generators of $C(\mathbb{Q})$ equipped with its group structure. We are primarily interested in curves of general type. For those curves the set $C(\mathbb{Q})$ is finite, so an explicit listing of the set would provide a satisfactory solution to the determination problem.

As we discuss in Section 4, the most important step is to realize C as a subvariety of an abelian variety J. If we take J to be the *Jacobian* of C then a rational point on C gives rise to such an embedding. If we can prove no such embedding exists, then we can conclude that $C(\mathbb{Q})$ is empty.

Challenge A. Given a curve C over $\mathbb{Q}$ of positive genus, determine an embedding of C into its Jacobian or prove no such embedding exists.

The main advantage of considering C as a subvariety of an abelian variety J, rather than of a rational space such as $\mathbb{P}^2$, is that the set of rational points of J is much sparser: The Mordell-Weil Theorem [63] states that $J(\mathbb{Q})$ is a finitely generated group. We can use knowledge about $J(\mathbb{Q})$ to obtain information about $C(\mathbb{Q})$. This leads to our second challenge.

Challenge B. Given a curve C of positive genus, determine $J(\mathbb{Q})$, where J is the Jacobian of C.

Note that if C is of genus 1, then an embedding as in Challenge A establishes an isomorphism between C and J, so Challenge B provides a solution to the determination problem. In the remainder of this text we take C to be a curve of general type.

A major component in determining $J(\mathbb{Q})$ is determining the rank of its free part. A conjectural link suggested by Birch and Swinnerton-Dyer [4] for elliptic curves connects this rank to the vanishing of an L-function at a special point. For elliptic curves over $\mathbb{Q}$ with an L-function that vanishes to order at most 1, this is now proved [38; 43], but for more general abelian varieties even the existence of the function at the point is not generally established.

The only general unconditional approach uses *descent* to provide a hopefully sharp upper bound on the rank. The ideas are most easily explained in the language of Galois cohomology (see Section 6).

Once a bound on the rank is determined, one can try to prove that the bound is sharp by exhibiting sufficiently many independent points on J. Finding them is only a computational problem. Since these points can be drawn from an obviously enumerable set of candidates, generators will eventually be found. Finding generators *efficiently* is a serious computational problem, but we will ignore it here.

The traditional way of showing that a set generates all of $J(\mathbb{Q})$ is by computing *canonical heights*. However, a good algorithm for computing canonical heights efficiently is only available for curves of genus up to 2; see [31; 35; 60; 61]. For our purposes, one only needs a subgroup of $J(\mathbb{Q})$, of finite index prime to some predetermined number B. Proving that a set generates such a group is usually much easier to establish; see Remark 4.6.

Since (sharply) bounding the rank of $J(\mathbb{Q})$ is a crucial step for the methods in Sections 4 and 5, we describe in Section 7 a way to actually compute or approximate the rather abstract objects introduced in Section 6. While one can concentrate on the geometry of J (see [3; 37]), this becomes unwieldy for more complicated J. Another approach emphasizes that J represents the group $\operatorname{Pic}^0(C)$ of degree-0 divisor classes on C and tries to express as much of the data as possible in terms of objects directly related to the curve [18; 21; 23; 48; 49; 53; 54; 56]. We closely follow the exposition in [14].

In Section 8 we describe how the constructions in Section 7 can also be used to attack some related problems, and in Section 9 we give some examples, taken from [14], of successful applications of these methods to smooth plane quartic curves. To our knowledge, these are the first examples fully carried out for curves with trivial automorphism groups. Previous applications all made essential use of nontrivial automorphisms to simplify computations. The fact that these procedures are also shown to be practical when no such automorphisms are available is a hopeful sign that they are applicable in generality.

3. Local considerations

Let C be a curve over $\mathbb{Q}$ and let $K \supseteq \mathbb{Q}$ be a field extension. Then $C(\mathbb{Q}) \subseteq C(K)$. Hence, if C has a $\mathbb{Q}$-rational point then $C(\mathbb{R}) \neq \varnothing$ and $C(\mathbb{Q}_p) \neq \varnothing$ for all primes p.

We introduce some notation to express this observation more concisely. We call $\mathbb{R}$ the completion of $\mathbb{Q}$ at the *infinite* prime and write $\mathbb{R} = \mathbb{Q}_\infty$. We write

$$\Omega_{\mathbb{Q}} = \{p \in \mathbb{Z}_{>1} : p \text{ is prime}\} \cup \{\infty\}.$$

The consideration of all completions of $\mathbb{Q}$ at once leads to the ring $\mathbb{A}$ of *adèles*. We will only use it here as a concise piece of opaque notation and define for a projective curve C the set

$$C(\mathbb{A}) := \prod_{v \in \Omega_{\mathbb{Q}}} C(\mathbb{Q}_v).$$

The observation above now translates to

$$C(\mathbb{Q}) \neq \varnothing \quad \text{implies} \quad C(\mathbb{A}) \neq \varnothing. \tag{2}$$

Fact 3.1. *One can decide algorithmically whether $C(\mathbb{A}) = \varnothing$.*

Determining whether $C(\mathbb{R}) = \varnothing$ is a straightforward application of calculus and the intermediate value theorem. Determining whether $C(\mathbb{Q}_p) = \varnothing$ is also computable thanks to Hensel's lifting criterion (see [10] for a collection of algorithms). Furthermore, for all but a finite and explicitly computable set of primes p we can immediately conclude that $C(\mathbb{Q}_p)$ is nonempty.

The implication (2) is mainly useful for its contrapositive: if we can show that $C(\mathbb{A})$ is empty (that is, that $C(\mathbb{Q}_v)$ is empty for some v) then we can conclude that $C(\mathbb{Q})$ is empty. The converse of implication (2), known as the *local-global* principle, is known to hold for genus-0 curves. Hence, if C is a genus-0 curve and $C(\mathbb{A}) \neq \varnothing$ then C has a rational point.

However, for curves of positive genus the local-global principle is known to fail. For instance, for curves of genus 2 over $\mathbb{Q}$, one can prove that the subset of curves C with $C(\mathbb{A}) \neq \varnothing$ has asymptotic density about 0.85, measured with respect to an appropriate height [50]. However, one would expect the set of curves with a rational point to have asymptotic density 0 — see for instance [52, Conjecture 2.2(i)] for a formal statement of this folklore conjecture in the case of plane curves — so many curves with points everywhere locally should have no rational points at all.

4. The Mordell-Weil sieve

Let C be a smooth projective curve of genus $g \geq 2$. In this section we discuss a method that allows us to obtain significant information on $C(\mathbb{Q})$ by considering an embedding of C into an abelian variety J (usually its Jacobian) for which we can determine $J(\mathbb{Q})$. We write $\iota\colon C \to J$ for the embedding.

The rational points on an abelian variety are sufficiently sparse that the topological closure $\overline{J(\mathbb{Q})} \subset J(\mathbb{A})$ is significantly smaller than $J(\mathbb{A})$. We observe that

$$C(\mathbb{Q}) \subset C(\mathbb{A}) \cap \overline{J(\mathbb{Q})}.$$

The latter set is amenable to computation, or at least to approximation. As it turns out, the small step of taking into consideration a little bit of extra global data, in the form of $\overline{J(\mathbb{Q})}$, provides considerable extra information.

In [57], Scharaschkin presents the method and shows, subject to the standard conjecture that $Ш(J/\mathbb{Q})$ is finite, that the obstruction to the existence of rational points on C that this method exhibits can be interpreted in terms of the *Brauer-Manin obstruction* [59]. See [12; 33; 49] for applications and [15] for a larger scale experiment. Details are provided in [17], including an optimal strategy for avoiding a combinatorial explosion to which this method is prone. See also [20] for an application of to determining integral points on curves.

Let p be a prime of good reduction of the embedding $\iota\colon C \to J$, meaning that there are smooth proper models $\mathscr{C}$ and $\mathscr{J}$ over $\mathbb{Z}_p$ of C and J, respectively, and a morphism $\iota'\colon \mathscr{C} \to \mathscr{J}$ that restricts to ι on the generic fiber. (The conditions on the type of reduction can be significantly relaxed.) We write $C(\mathbb{F}_p) = \mathscr{C}(\mathbb{F}_p)$ and $J(\mathbb{F}_p) = \mathscr{J}(\mathbb{F}_p)$. We use that $J(\mathbb{Q}_p) = \mathscr{J}(\mathbb{Z}_p)$ and write $\rho_p\colon J(\mathbb{Q}) \to J(\mathbb{F}_p)$ for the induced reduction map. Via the same principle we obtain a reduction map

$C(\mathbb{Q}) \to C(\mathbb{F}_p)$. Furthermore, we write $\iota_p\colon C(\mathbb{F}_p) \to J(\mathbb{F}_p)$ for the map that ι' induces on the rational points of the reductions.

Let us fix a finite set S of primes of good reduction of J and a positive integer B. We consider the commutative diagram

$$\begin{tikzcd}
C(\mathbb{Q}) \arrow[r, "\iota"] \arrow[d] & \dfrac{J(\mathbb{Q})}{BJ(\mathbb{Q})} \arrow[d, "\rho_S"] \\
\prod_{p \in S} C(\mathbb{F}_p) \arrow[r, "\iota_S"'] & \prod_{p \in S} \dfrac{J(\mathbb{F}_p)}{B \operatorname{im} \rho_p},
\end{tikzcd}$$

where ρ_S and ι_S are the obvious maps induced by $\{\rho_p : p \in S\}$ and $\{\iota_p : p \in S\}$ respectively.

Each of the four sets in this diagram is finite, so determining

$$V_{S,B} = \operatorname{im} \rho_S \cap \operatorname{im} \iota_S$$

is a matter of combinatorics. For sufficiently large B and S, the map $\rho_S \circ \iota$ will be an injection, so in that case the size of $V_{S,B}$ provides an upper bound on the size of $C(\mathbb{Q})$. In any case, if $V_{S,B}$ is empty, then C has no rational points.

If the domains of ρ_S and ι_S are sufficiently small relative to their codomain, one would expect the intersection of their images to be rather small. One can formulate a reasonable heuristic argument that supports this.

Heuristic 4.1 (Poonen [47]). Subject to plausible assumptions that $\operatorname{im} \iota_S$ and $\operatorname{im} \rho_S$ behave in a way that can be suitably modeled by a random process, one expects that for suitably chosen B and S, the set $V_{S,B}$ consists only of images of $C(\mathbb{Q})$.

While ρ_S and ι_S are maps between finite sets, both B, S have to be quite large in practice for Heuristic 4.1 to apply. So, while $V_{S,B}$ is likely a very small set, it tends to be an intersection of two rather large sets. For practical computations, one has to take some care in constructing the set via appropriate steps. See [17] for some strategies for doing so.

We are left with finding an appropriate embedding $\iota\colon C \to J$ into an abelian variety. A canonical choice for J is the *Jacobian* of C. It is a g-dimensional abelian variety representing the degree-0 divisor classes on C; that is, $J(\overline{\mathbb{Q}}) = \operatorname{Pic}^0(C/\overline{\mathbb{Q}})$. This equality is Galois-equivariant, so $J(\mathbb{Q})$ consists of the Galois-invariant divisor classes $\operatorname{Pic}^0(C/\overline{\mathbb{Q}})^{\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}$. The latter can be strictly larger than $\operatorname{Pic}^0(C/\mathbb{Q})$, the set of linear equivalence classes that contain divisors that are defined over $\mathbb{Q}$. However, for the problem at hand, this is not an issue (see [7], for instance, for some related theory).

Lemma 4.2 (Standard result). *Let C be a curve over a field k, where k is either a finite field or a number field such that $C(k_v)$ is nonempty for all places v of k. Then every Galois-invariant divisor class on C contains a divisor defined over k.*

For our applications, if $C(\mathbb{Q}_v) = \varnothing$ for any place $v \in \Omega_{\mathbb{Q}}$, the results in Section 3 already imply that $C(\mathbb{Q}) = \varnothing$, so we only need to work with $J(\mathbb{Q})$ when we can represent its points by divisors over $\mathbb{Q}$. This allows us to avoid constructing a projective model for J as a variety.

A point on a curve C gives rise to a degree-1 divisor class. Since on a curve of positive genus no two such divisors are linearly equivalent, we obtain an injection $C(\mathbb{Q}) \to \operatorname{Pic}^1(C/\mathbb{Q})$. Similarly to how J is a variety that represents Pic^0, there is also a variety $\underline{\operatorname{Pic}}^1(C)$, that represents Pic^1. Indeed, there is a natural morphism $C \to \underline{\operatorname{Pic}}^1(C)$. There is a natural action of J on $\underline{\operatorname{Pic}}^1(C)$, corresponding to addition of divisor classes, that equips $\underline{\operatorname{Pic}}^1(C)$ with the structure of a $\mathbb{Q}$-torsor under J. A rational point on $\underline{\operatorname{Pic}}^1(C)$ induces an isomorphism between J and $\underline{\operatorname{Pic}}^1(C)$. If there is no such point, then C has no degree 1 divisors and hence certainly no rational points. Therefore, a reformulation of Challenge A is:

Challenge A′. Given a curve C over $\mathbb{Q}$ of positive genus, determine a divisor class $\mathfrak{d} \in \operatorname{Pic}^1(C/\mathbb{Q})$ or prove no such divisor class exists.

If $\mathfrak{d}$ exists then the map $\iota\colon C \to J$ it induces corresponds to

$$\begin{aligned} C(\mathbb{Q}) &\longrightarrow \operatorname{Pic}^0(C/\mathbb{Q}) \\ P &\longmapsto [P] - \mathfrak{d}. \end{aligned}$$

For an appropriate reduction $\mathfrak{d}_p$ modulo p, we get the corresponding map

$$C(\mathbb{F}_p) \to \operatorname{Pic}^0(C/\mathbb{F}_p)$$

given by $P \mapsto [P] - \mathfrak{d}_p$. This suggests the procedure below for solving the decision problem. First note that a choice of smooth projective model for C also provides us with an explicitly enumerable set containing $C(\mathbb{Q})$ — namely, $\mathbb{P}^n(\mathbb{Q})$ — so if C has a rational point we can find it in finite time by enumeration (but see Remark 4.5 for drastic improvements).

Remark 4.3. We use the term *algorithm* in the strict sense: a Turing machine or an equivalent computing device that is guaranteed to produce a correct answer in finite time when given correct input. We use the word *procedure* for a less formal concept than an algorithm. We allow a procedure to include steps that are not guaranteed to succeed, and we do not require that a procedure will stop for all valid input. We do require the guarantee that *if* a procedure finishes then its output is correct.

Procedure 4.4 (Decision procedure).

Input: A curve C over $\mathbb{Q}$ (or more generally, a number field).

Output: A rational point on C or a proof that there is none.

First parallel thread:

0. Enumerate candidates for $C(\mathbb{Q})$. If a point is found, we have shown that $C(\mathbb{Q})$ is not empty.

Second parallel thread:

1. Test if $C(\mathbb{A}) = \varnothing$. If that is the case then $C(\mathbb{Q})$ is empty too. See Fact 3.1.
2. (Challenge A′) Find $\mathfrak{d} \in \operatorname{Pic}^1(C/\mathbb{Q})$ or prove it doesn't exist. We either obtain an embedding $\iota\colon C \to J$ or we prove that $C(\mathbb{Q})$ is empty.
3. (Challenge B) Find a finite set of generators for $J(\mathbb{Q})$.
4. Choose appropriate S and B.
5. Compute $V_{S,B}$. This involves computing $J(\mathbb{F}_p)$, using for instance [39; 42].
6. If $V_{S,B} = \varnothing$ then $C(\mathbb{Q})$ is empty. Otherwise, increase S and B and go to step 5.

Remark 4.5. Once we have determined generators for $J(\mathbb{Q})$, we can enumerate candidates for $C(\mathbb{Q})$ much more efficiently by enumerating $J(\mathbb{Q})$. Furthermore, the set $V_{S,B}$ provides us with a list of cosets modulo $BJ(\mathbb{Q})$ that may contain elements of $C(\mathbb{Q})$, further reducing the number of candidates to consider. This makes it feasible to search up to height bounds that are doubly exponential in time. See [20] for an application to finding *integral* points on curves.

We do not have a proof that this procedure will always terminate, but Heuristic 4.1 suggests it should. Indeed, in [15] we describe an experiment where we test how well the decision procedure works in practice. We consider genus-2 curves admitting models of the form

$$y^2 = f_6x^6 + f_5x^5 + \cdots + f_0 \quad \text{with} \quad f_0, \ldots, f_6 \in \{-3, -2, \ldots, 3\}.$$

For nearly all the roughly 200,000 isomorphism classes represented, we were able to solve the decision problem. For 42 curves we were unable to unconditionally complete step 2. For those we obtained a presumably accurate bound on the rank of $J(\mathbb{Q})$ by assuming the Birch and Swinnerton-Dyer conjecture. The Mordell-Weil sieving itself never posed an insurmountable problem.

The main practical problem with the procedure above is that if either of steps 2 or 3 fails, we have no way of continuing. We can weaken the requirement for step 3 slightly.

Remark 4.6. We only need a set of elements in $J(\mathbb{Q})$ that generate $J(\mathbb{Q})/BJ(\mathbb{Q})$, so a subgroup of finite index prime to B in $J(\mathbb{Q})$ would already be enough. If one knows the rank of $J(\mathbb{Q})$ then one can usually quickly deduce that a given set generates such a group by considering its image under

$$J(\mathbb{Q}) \longrightarrow \textstyle\prod_{p\in S} J(\mathbb{F}_p).$$

for some suitable set of primes S. For instance, let q be a prime dividing B. If we know that $J(\mathbb{Q})/qJ(\mathbb{Q}) \simeq (\mathbb{Z}/q\mathbb{Z})^t$ and the codomain has a direct factor of the form $\prod_{i=1}^{t}(\mathbb{Z}/q^{e_i}\mathbb{Z})$, with $e_1,\dots,e_t \geq 1$, onto which the group generated by our given set surjects, then the set generates a subgroup of finite index prime to q.

5. Isolating rational points: Chabauty's method

While Mordell-Weil sieving can provide a proof that $C(\mathbb{Q})$ is empty, it will not prove that $C(\mathbb{Q})$ is finite, let alone determine $C(\mathbb{Q})$, if there is a rational point on C. Yet for large enough B and S the map $C(\mathbb{Q}) \to V_{S,B}$ is injective, and Heuristic 4.1 predicts that for suitable values of B and S it is surjective as well. Thus, given a rational point $P \in C(\mathbb{Q})$, we mainly need a way to prove the equality

$$\iota C(\mathbb{Q}) \cap (\iota(P) + BJ(\mathbb{Q})) = \{\iota(P)\}. \tag{3}$$

Inspired by Skolem's ideas for subvarieties of multiplicative groups, Chabauty [24] observed that one can construct a nonzero p-adic analytic function

$$\Theta_p\colon J(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p$$

that vanishes on $J(\mathbb{Q})$, provided that the rank r of $J(\mathbb{Q})$ is strictly smaller than the dimension g of J. (Actually, he observed that one can construct such functions locally, and gets the desired result by doing so on a finite open covering of the rational points.) The fact that analytic functions have isolated zeros allows one to conclude that C has only finitely many rational points and, with a bit of extra work, to establish statements like equality (3). See [26] for one of the first modern treatments of the method and [23], [32], and [34] for a flexible way of applying it.

In order to avoid some technical complications, we take a prime p at which C has good reduction. We write $J^{(1)}(\mathbb{Q}_p)$ for the kernel of the reduction homomorphism $J(\mathbb{Q}_p) \to J(\mathbb{F}_p)$ and we write $\Lambda_p = J(\mathbb{Q}) \cap J^{(1)}(\mathbb{Q}_p)$ for the part of the Mordell-Weil group that lies in the kernel of reduction.

The function Θ_p in question arises from the p-adic integration of a regular differential ω. We consider regular differentials obtained by lifting a regular differential $\overline{\omega}$ on C over $\mathbb{F}_p$, so our differentials have *good reduction* at p as well. We sketch the details here.

Let $P \in C(\mathbb{Q}_p)$. We choose a uniformizer $\bar{t} \in \mathbb{F}_p(C)$ at the reduction $\overline{P} \in C(\mathbb{F}_p)$ of P and lift it to a uniformizer $t \in \mathbb{Q}_p(C)$ at P. Let ω be a regular differential on C with good reduction as described above. We have $\omega = h\,dt$ for some function $h \in \mathbb{Q}_p(C)$ regular at P. Localization at P provides a homomorphism $\mathbb{Q}_p(C) \to \mathbb{Q}_p((t))$. Regularity and good reduction imply that when we identify h with its image, we have $h(t) \in \mathbb{Z}_p[[t]]$. We can compute a formal power series

$$\int_{t=0}^{z} h(t)dt \in \mathbb{Q}_p[[z]],$$

and it is straightforward to check that its radius of convergence is at least 1. Let $\overline{\mathbb{Q}}_p$ be an algebraic closure of $\mathbb{Q}_p$, and extend the p-adic absolute value in the natural way to $\overline{\mathbb{Q}}_p$. For any point $Q \in C(\overline{\mathbb{Q}}_p)$ that reduces to $\overline{P} \in C(\mathbb{F}_p)$, we have $|t(Q)|_p < 1$. Hence we can define the integral of ω from P to Q by the formula

$$\int_P^Q \omega = \int_0^{t(Q)} h(t)dt,$$

which is easily checked to not depend on the choice of t. Note that every divisor class in $J^{(1)}(\mathbb{Q}_p)$ admits a representative of the form

$$[Q_1 + \cdots + Q_g - gP],$$

where each $Q_i \in C(\overline{\mathbb{Q}}_p)$ reduces to $\overline{P} \in C(\overline{\mathbb{F}}_p)$. We define the integral of ω over this divisor class by

$$\int_{[Q_1+\cdots+Q_g-gP]} \omega = \sum_{i=1}^{g} \int_P^{Q_i} \omega.$$

One can check that the regularity of ω implies that this provides a well-defined group homomorphism $J^1(\mathbb{Q}_p) \to \mathbb{Q}_p$.

Let $\overline{\omega}_1, \ldots, \overline{\omega}_g$ be a basis of the space of regular differentials of the reduction of C at p and let $\omega_1, \ldots, \omega_g$ be a lift of that basis. We have a $\mathbb{Z}_p$-bilinear pairing

$$J^{(1)}(\mathbb{Q}_p) \times (\mathbb{Z}_p)^g \to \mathbb{Q}_p$$

taking $\big(D, (\lambda_1, \ldots, \lambda_g)\big)$ to

$$\int_D \lambda_1\omega_1 + \cdots + \lambda_g\omega_g.$$

We see that if the $\mathbb{Z}$-rank r of $J(\mathbb{Q})$ is strictly less than g, then the $\mathbb{Z}_p$-submodule generated by $\Lambda_p \subset J^{(1)}(\mathbb{Q}_p)$ has $\mathbb{Z}_p$-rank at most $r < g$, so there is a nonzero differential ω_p such that

$$\int_D \omega_p = 0 \quad \text{for all } D \in \Lambda_p = J(\mathbb{Q}) \cap J^{(1)}(\mathbb{Q}_p).$$

In particular, for a rational point $P \in C(\mathbb{Q})$, we can define

$$\Theta_{p,P}(Q) = \int_P^Q \omega_p \quad \text{for } Q \in C(\mathbb{Q}_p) \text{ that reduce to } \overline{P} \in C(\mathbb{F}_p).$$

It follows that $\Theta_{p,P}(Q)=0$ for every $Q\in C(\mathbb{Q})$ with the same reduction as P modulo p. The following is straightforward to prove by applying Hensel's lemma to the appropriate power series expansion.

Proposition 5.1 [26, proof of Theorem 4]. *If $P\in C(\mathbb{Q})$ and the reduction $\overline{\omega}_p$ is nonzero at $\rho_p(P)\in C(\mathbb{F}_p)$, then we have*

$$\iota C(\mathbb{Q})\cap(\iota(P)+\Lambda_p)=\{\iota(P)\}.$$

We obtain the following procedure (see Remark 4.3 for the technical meaning of this word).

Procedure 5.2 (Determination procedure).

Input: A curve C of genus $g>1$ with $J(\mathbb{Q})$ of free rank $r<g$.

Output: The elements of $C(\mathbb{Q})$.

1. Choose S and B, and search for points $\{P_1,\dots,P_k\}\subset C(\mathbb{Q})$ such that
$$\{P_1,\dots,P_k\}+BJ(\mathbb{Q})=V_{S,B}+BJ(\mathbb{Q}).$$
2. For each point P_i, find a prime p such that $BJ(\mathbb{Q})\subset\Lambda_p$ and $\overline{\omega}_p(\overline{P})\neq 0\in\mathbb{F}_p$. If this succeeds, you have proved that
$$C(\mathbb{Q})=\{P_1,\dots,P_k\}.$$
3. If step 2 fails, go to step 1 and choose larger S and B.

Remark 5.3. The linearity of the integration pairing in the first component implies that for any $D\in J^{(1)}(\mathbb{Q}_p)$ and $m\in\mathbb{Z}$ we have that

$$\int_{mD}\omega=m\int_D\omega.$$

Since $J^{(1)}(\mathbb{Q}_p)\subset J(\mathbb{Q}_p)$ is of finite index, say index m, we have for any $D\in J(\mathbb{Q}_p)$ that $mD\in J^{(1)}(\mathbb{Q}_p)$, so we can use this identity to extend the integration pairing to all of $J(\mathbb{Q}_p)$. This provides a rigid analytic continuation of $\Theta_{p,P}$ to all of $C(\mathbb{Q}_p)$ that vanishes at $C(\mathbb{Q})$ — see also [2].

We cannot prove that step 1 of the determination procedure will succeed, but Heuristic 4.1 suggests it should. We cannot prove that step 2 will succeed eventually either, but given that $\overline{\omega}_p(\rho_p(P))=0$ requires the vanishing of a power series coefficient in $\mathbb{F}_p$, we expect that this happens only one in p cases on average. Indeed, in practice finding an appropriate p in step 2 never seems to be a problem.

Combining Mordell-Weil sieving with Chabauty's method yields the significant benefit that larger residue characteristics pose no problem. Results typical for Chabauty's method by itself bound $\#C(\mathbb{Q})$ in terms of $\#C(\mathbb{F}_p)$, and these bounds are rarely sharp (see [26] and [62]).

A more significant restriction is that the procedure is not guaranteed to apply at all if $r \geq g$. One remedy is to use *covers*. One determines a finite set of covers $\phi_i \colon D_i \to C$ with $i = 1, \dots, m$ and where the D_i are curves of genus larger than g, such that

$$C(\mathbb{Q}) = \bigcup_{i=1}^{m} \phi_i(D_i(\mathbb{Q})),$$

in the hope that the determination procedure does apply to each of $D_1, \dots, D_r$. In Section 8C we see how the ideas from Section 6, in particular Proposition 6.3, can be used to construct such covering sets.

6. Theory of finite descent

Let us first consider Challenge B, finding (a finite index subgroup of) the group $J(\mathbb{Q})$. The first observation is that $J^{(1)}(\mathbb{Q}_p)$ is torsion-free for $p > 2$ (see [41]), so the reduction map $J(\mathbb{Q}) \to J(\mathbb{F}_p)$ is injective on the torsion subgroup $J(\mathbb{Q})_{\text{tors}}$. As a consequence, by computing $J(\mathbb{F}_p)$ for a small number of primes p, which we have to do for Mordell-Weil sieving anyway, we easily obtain a bound on the size of $J(\mathbb{Q})_{\text{tors}}$. This bound is often sharp, so simply exhibiting enough torsion points usually suffices for determining $J(\mathbb{Q})_{\text{tors}}$.

More generally, the kernel of the multiplication-by-n morphism $J \to J$, denoted by $J[n]$, is 0-dimensional. Determining an approximation of it points over, say, $\mathbb{C}$, is straightforward. One can then recognize which of these torsion points are defined over $\mathbb{Q}$. Once $J(\mathbb{Q})_{\text{tors}}$ is obtained, we are left with determining the free part. The structure theorem for finitely generated abelian groups gives us that

$$J(\mathbb{Q}) \simeq J(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r \quad \text{and} \quad \frac{J(\mathbb{Q})}{nJ(\mathbb{Q})} \simeq \frac{J(\mathbb{Q})_{\text{tors}}}{nJ(\mathbb{Q})_{\text{tors}}} \times (\mathbb{Z}/n\mathbb{Z})^r.$$

That means that if we can compute the size of $J(\mathbb{Q})/nJ(\mathbb{Q})$, we can compute r.

Since the multiplication-by-n morphism $J \xrightarrow{n} J$ is surjective over algebraically closed fields, we have a short exact sequence of Galois modules

$$0 \longrightarrow J[n](\overline{\mathbb{Q}}) \longrightarrow J(\overline{\mathbb{Q}}) \xrightarrow{n} J(\overline{\mathbb{Q}}) \longrightarrow 0. \tag{4}$$

The abstract language of Galois cohomology allows us to derive a description of the set $J(\mathbb{Q})/nJ(\mathbb{Q})$ that facilitates a clean proof of the weak Mordell-Weil theorem. It also provides a road map for computing bounds on r. In this section we make a detour into this abstract world. In the next section we investigate how to compute some of the objects introduced here.

For a Galois module $M(\overline{\mathbb{Q}})$ we write $H^i(\mathbb{Q}, M) = H^i(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), M(\overline{\mathbb{Q}}))$. Taking cohomology of the short exact sequence (4), we obtain the exact sequence

$$0 \longrightarrow \frac{J(\mathbb{Q})}{nJ(\mathbb{Q})} \xrightarrow{\gamma} H^1(\mathbb{Q}, J[n]) \longrightarrow H^1(\mathbb{Q}, J). \tag{5}$$

Thus, if we can bound the size of the image of the connecting homomorphism γ then a corresponding bound on r follows.

Indeed, we can consider the same sequence over localizations $\mathbb{Q}_v$ of $\mathbb{Q}$, and by identifying each $\mathrm{Gal}(\overline{\mathbb{Q}}_v/\mathbb{Q}_v)$ with a decomposition subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ we obtain the following commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & \dfrac{J(\mathbb{Q})}{nJ(\mathbb{Q})} \arrow[r, "\gamma"] \arrow[d] & H^1(\mathbb{Q}, J[n]) \arrow[d, "\mathrm{res}_v"] \\
0 \arrow[r] & \dfrac{J(\mathbb{Q}_v)}{nJ(\mathbb{Q}_v)} \arrow[r, "\gamma_v"] & H^1(\mathbb{Q}_v, J[n]).
\end{tikzcd}$$

Since rational points are also $\mathbb{Q}_v$-rational, it follows that $\mathrm{im}\,\gamma$ lies in the *n-Selmer group* of J, defined by

$$\mathrm{Sel}^n(J/\mathbb{Q}) = \left\{\delta \in H^1(\mathbb{Q}, J[n]) : \mathrm{res}_v(\delta) \in \mathrm{im}\,\gamma_v \text{ for all } v \in \Omega_{\mathbb{Q}}\right\}.$$

Part of the proof that $J(\mathbb{Q})$ is finitely generated is establishing that $\mathrm{Sel}^n(J/\mathbb{Q})$ is finite, which is known as the *weak Mordell-Weil theorem*. This fact follows from another interpretation of the set $H^1(\mathbb{Q}, J[n])$, which also has computational significance. Some technical language is required to properly formulate this interpretation.

Let k be a field with separable closure $\bar{k}$, let M be a finite group with a $\mathrm{Gal}(\bar{k}/k)$-action and let X and Y be k-varieties. By limiting ourselves here to a *finite* group M, we guarantee that M can be represented by an affine group scheme; this helps in proving Proposition 6.1 below and simplifies the definition of an X-torsor under M. Dropping the assumption that M be finite invalidates the statement in general (see [5, §6.7]), but the statement does hold under various alternative conditions.

An *X-torsor under a finite M* is an unramified morphism $\phi\colon Y \to X$ of degree $\#M$ between k-varieties, together with an isomorphism $M \to \mathrm{Aut}_{\bar{k}}(Y/X)$ of groups with $\mathrm{Gal}(\bar{k}/k)$-action; see [45, § III.4].

Let $\phi\colon Y \to X$ and $\phi'\colon Y' \to X$ be X-torsors under a finite M. An *isomorphism* of X-torsors is an isomorphism of k-varieties $\sigma\colon Y \to Y'$ such that $\phi = \phi' \circ \sigma$

and such that the induced isomorphism $\mathrm{Aut}_{\overline{k}}(Y/X) \to \mathrm{Aut}_{\overline{k}}(Y'/X)$ is compatible with the isomorphisms $M \to \mathrm{Aut}_{\overline{k}}(Y/X)$ and $M \to \mathrm{Aut}_{\overline{k}}(Y'/X)$.

Let $X_{\overline{k}}$ be the base change of X to $\overline{k}$. Via base change, we can obtain from any X-torsor under M an $X_{\overline{k}}$-torsor under $M_{\overline{k}}$. We say that two torsors are *twists* of one another if they becomes isomorphic to one another upon base change to $\overline{k}$.

If M is not abelian there is still an object denoted $H^1(k, M)$, but it is no longer a group — it is merely a set with a distinguished element, called the *trivial class*. From Theorem III.4.3(a) (p. 121) and Proposition III.4.6 (p. 123) of [45] we obtain the following result.

Proposition 6.1 (Twisting principle). *Let $\phi\colon Y \to X$ be an X-torsor under a finite M. There is a bijection between $H^1(k, M)$ and the set of isomorphism classes of twists of $\phi\colon Y \to X$, and a natural map $\gamma\colon X(k) \to H^1(k, M)$, such that*

(1) *the bijection sends the trivial class of $H^1(k, M)$ to the class of ϕ, and*

(2) *for every $x \in X(k)$, if $\gamma(x)$ corresponds to a twist $\phi_x\colon Y_x \to X$, then x has a k-rational preimage on Y_x.*

In fact, if a twist $\phi'\colon Y' \to X$ has a point $y \in Y'(k)$ then Y' is isomorphic to Y_x, where $x = \phi'(y)$. It follows that the image of γ consists exactly of those twists for which $Y'(k)$ is nonempty. We can approximate the image by considering those that have adelic points.

Definition 6.2. Let $\phi\colon Y \to X$ be an M-cover over $\mathbb{Q}$. We define the *Selmer set* to be

$$\begin{aligned}\mathrm{Sel}(\mathbb{Q}, Y \xrightarrow{\phi} X) &= \bigl\{[\phi'\colon Y' \to X] \in H^1(\mathbb{Q}, M) : Y'(\mathbb{A}) \neq \varnothing\bigr\}\\ &= \bigl\{\delta \in H^1(\mathbb{Q}, M) : \mathrm{res}_v(\delta) \in \mathrm{im}\,\gamma_v \text{ for all } v \in \Omega_{\mathbb{Q}}\bigr\}.\end{aligned}$$

Note that the multiplication-by-n morphism in the exact sequence (4) yields a J-torsor $J \to J$ under the group $M = J[n](\overline{\mathbb{Q}})$. Indeed, this map γ and the connecting homomorphism in Equation (5) agree, as do the concepts of Selmer set and group.

Of particular importance for us is the case where k is a number field. For ease of notation, we restrict to the case $k = \mathbb{Q}$. Let $\mathbb{Q}_v^{\mathrm{unr}}$ be the maximal unramified extension of $\mathbb{Q}_v$ in $\overline{\mathbb{Q}}_v$. We say a class is *unramified* if it becomes trivial under the restriction $H^1(\mathbb{Q}_v, M) \to H^1(\mathbb{Q}_v^{\mathrm{unr}}, M)$. A class in $H^1(\mathbb{Q}, M)$ is *unramified at v* if res_v maps it to an unramified class. For a finite set $S \subset \Omega_{\mathbb{Q}}$ we write $H^1(\mathbb{Q}, M; S)$ for the subgroup of classes unramified at all places outside of S. We find that $H^1(\mathbb{Q}, M; S)$ is finite; this is analogous to Hermite's result that there are only finitely many number fields of bounded degree unramified outside a finite set of primes.

Proposition 6.3 (Chevalley-Weil [25]). *Let X and Y be smooth projective varieties over $\mathbb{Q}$, let M be a finite* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*-group, and let $\phi\colon Y \to X$ be an X-torsor under M. Let $S \subset \Omega_{\mathbb{Q}}$ contain the archimedean places, the places of bad reduction of ϕ, and the places of residue characteristic dividing $|M|$. Then*

$$\gamma(X(\mathbb{Q})) \subset \mathrm{Sel}(\mathbb{Q}, Y \xrightarrow{\phi} X) \subset H^1(\mathbb{Q}, M; S).$$

In particular, $\gamma(X(\mathbb{Q}))$ is finite.

The version in [25] states that $\phi^{-1}(X(\mathbb{Q}))$ lies in $Y(L)$ for some fixed number field L, the compositum of degree-$|M|$ extensions unramified outside S of the splitting field of M. This formulation is not very conducive to computation. A more promising approach is to try to find reasonable computational descriptions of $H^1(k, M)$ and γ for $k = \mathbb{Q}$ and $k = \mathbb{Q}_v$. General theory gives us that the map γ_v for $k = \mathbb{Q}_v$ is continuous and therefore locally constant. If we can determine the neighborhood on which γ_v is constant, we can determine $\operatorname{im} \gamma_v$ and thus compute $\mathrm{Sel}(\mathbb{Q}, Y \xrightarrow{\phi} X)$.

7. Computing Selmer groups

In this section we describe a method for computing (or at least approximating) Selmer groups that goes back to Cassels (see [21] for a survey), and that has been developed and used by many others [23; 48; 53; 54; 56]. The presentation here closely follows that in [14].

We continue our philosophy that points on J are most conveniently represented by divisors on C. We would like to describe $J[n]$ as a Galois module. We do so by presenting a finite Galois-stable set of generators $\Delta = \{\theta_1, \dots, \theta_d\}$. Since this is a finite $\mathrm{Gal}(\bar{k}/k)$-set, it can be viewed as the $\bar{k}$-points of an affine 0-dimensional variety over k, which we also denote by Δ. Its coordinate ring is some finite k-algebra L. Note that L is a field only when $\mathrm{Gal}(\bar{k}/k)$ acts transitively on Δ. In general, L is a direct sum of fields, corresponding to the Galois orbits of Δ.

A certificate that $\theta \in \Delta$ is n-torsion as a divisor class on C can be given as a function f_θ whose divisor is linearly equivalent to $n\theta$. If we take these functions Galois-covariantly, we can combine them into a function $f \in k(C) \otimes_k L$.

We construct an n-torsion Galois module directly from Δ by taking the *twisted power*

$$\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\Delta} := \bigoplus_{i=1}^{d} \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right) \theta_i,$$

which as a group is simply $(\mathbb{Z}/n\mathbb{Z})^d$, but has its Galois action twisted so that the coordinates are permuted according to the action on Δ. The fact that Δ *generates*

$J[n]$ is expressed in the surjectivity of the third arrow in the short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & R \arrow[r] & \left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\Delta} \arrow[r] & J[n] \arrow[r] & 0, \end{tikzcd}$$

where the map to $J[n]$ consists of evaluating the formal linear combinations and R is defined to be the kernel of that map. If we are able to choose a Galois-stable *basis* for $J[n]$ then R is trivial and we obtain an isomorphism to $J[n]$. In general, we have to choose Δ larger than that. In fact, the Galois group may act transitively on the nonzero elements of $J[n]$, in which case $\Delta = J[n] \setminus \{0\}$ is the only choice.

If M is a finite Galois module, we let $M^\vee$ denote the Cartier dual $\operatorname{Hom}(M, \bar{k}^\times)$ of M. We note that

$$((\mathbb{Z}/n\mathbb{Z})^\Delta)^\vee = ((\mathbb{Z}/n\mathbb{Z})^\vee)^\Delta = \mu_n^\Delta,$$

and, thanks to the Weil pairing, that $J[n]^\vee = J[n]$. We obtain

$$\begin{tikzcd} 0 \arrow[r] & J[n] \arrow[r] & \mu_n^\Delta \arrow[r] & R^\vee \arrow[r] & 0. \end{tikzcd}$$

Taking Galois cohomology yields a map from $H^1(k, J[n])$ to $H^1(k, \mu_n^\Delta)$. From Kummer theory we know that $H^1(k, \mu_n) = k^\times/k^{\times n}$, and with a little extra work we find that $H^1(k, \mu_n^\Delta) = L^\times/L^{\times n}$. Hence we obtain the following commutative diagram with exact rows:

$$\begin{tikzcd} & & & & \dfrac{J(k)}{nJ(k)} \arrow[r, "\tilde{\gamma}"] \arrow[d, "\gamma"'] & \dfrac{L^\times}{L^{\times n}} \arrow[d, equal] \\ 0 \arrow[r] & J[n](k) \arrow[r] & (\mu_n^\Delta)(k) \arrow[r] & R^\vee(k) \arrow[r] & H^1(k, J[n]) \arrow[r] & H^1(k, \mu_n^\Delta) \end{tikzcd}$$

Note that we represent elements of $J(k)/nJ(k)$ by divisors on C. Our function f provides a partial map

$$\begin{tikzcd} \operatorname{Div}(C/k) \arrow[r, dashed] & L^\times \\ \displaystyle\sum_{P \in C(\bar{k})} n_P P \arrow[r, mapsto] & \displaystyle\prod_{P \in C(\bar{k})} f(P)^{n_P} \end{tikzcd}$$

defined for divisors supported away from poles and zeros of f. The main work, for which we refer the reader to [14], is to prove that this map induces the map $\tilde{\gamma}$ above.

For $k = \mathbb{Q}$ and $S \subset \Omega_{\mathbb{Q}}$ a finite set containing the infinite place and the primes dividing n, we also need to describe the subgroup $H^1(\mathbb{Q}, \mu_n^\Delta; S)$. To that end, we denote by $\mathcal{O}_{L,S}$ the ring of the elements of L that are integral over $\mathbb{Z}_S$. This ring decomposes into a direct product of Dedekind domains, namely the rings of S-integers of the number fields constituting L. If $\mathbb{O}_{L,S}$ is a principal ideal ring, which can be ensured by enlarging S if necessary, then

$$H^1(\mathbb{Q}, \mu_n^\Delta; S) = \frac{\mathbb{O}_{L,S}^\times}{\mathbb{O}_{L,S}^{\times n}}.$$

Computing an explicit representation amounts to determining class groups and unit groups in number fields.

Our explicit description of the map $\tilde{\gamma}$ also makes it possible to determine neighborhoods on which the local version $\tilde{\gamma}_v$ is constant. The arguments used are similar to those that show that elements $u, v \in \mathbb{Q}_2^\times$ represent the same class in $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ when $2^\epsilon(u-v) \in 1 + 8\mathbb{Z}_2$ for some $\epsilon \in \mathbb{Z}$.

For appropriate sets $S, T \subset \Omega_{\mathbb{Q}}$ we define

$$\begin{aligned}\mathrm{Sel}^{\tilde{\gamma}}(\mathbb{Q}, J) &:= \{\delta \in H^1(\mathbb{Q}, \mu_n^\Delta) : \mathrm{res}_v(\delta) \in \mathrm{im}\,\tilde{\gamma}_v\} \\ &\subseteq \{\delta \in \mathbb{O}_{L,S}^\times/\mathbb{O}_{L,S}^{\times n} : \mathrm{res}_v(\delta) \in \mathrm{im}\,\tilde{\gamma}_v \text{ for all } v \in T\},\end{aligned}$$

where, for a large enough finite set $T \subset \Omega_{\mathbb{Q}}$, the inclusion stabilizes to an equality.

We have a map $\mathrm{Sel}^n(J/\mathbb{Q}) \to \mathrm{Sel}^{\tilde{\gamma}}(\mathbb{Q}, J)$ but this need be neither surjective nor injective. We do know that the kernel is contained in the group K defined by the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & J[n](k) \arrow[r] & \mu_n^\Delta(k) \arrow[r] & R^\vee(k) \arrow[r] & K \arrow[r] & 0, \end{tikzcd}$$

and in practice K is frequently trivial. In any case, we can use $\mathrm{Sel}^{\tilde{\gamma}}(\mathbb{Q}, J)$ to obtain an upper bound on the rank of $J(\mathbb{Q})$. It may be larger than the one that can be derived from the actual Selmer group, but it has the advantage that it is more easily computed. There are also auxiliary computations one can do to obtain more detailed information on the difference; see [14, Appendix A].

Requiring a set Δ as above is often too demanding. Indeed, in general one does not expect a more favorable choice than $\Delta = J[n] \setminus \{0\}$ to be available. In that case, L is usually a number field of degree $n^{2g} - 1$, where g is the genus of C. So even in the case $g = 3$ and $n = 2$ one expects to have to compute with a number field of degree 63.

At the expense of getting even further removed from a description of $H^1(\mathbb{Q}, J[n])$, one can use a smaller set Δ. We restrict to the case $n = 2$. We take Δ to be a set so that the *differences* of elements of Δ generate $J[2]$. We consider the submodule E of even weight vectors,

$$\begin{tikzcd} 0 \arrow[r] & E \arrow[r] & (\mathbb{Z}/2\mathbb{Z})^\Delta \arrow[r, "\mathrm{sum}"] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & 0, \end{tikzcd}$$

and we obtain a short exact sequence

$$0 \longrightarrow R \longrightarrow E \longrightarrow J[n] \longrightarrow 0.$$

Taking cohomology of the dual sequence gives

$$H^1(k, \mu_2) \longrightarrow H^1(k, \mu_2^\Delta) \longrightarrow H^1(k, E^\vee),$$

which leads to

$$\frac{L^\times}{L^{\times 2} k^\times} \subset H^1(k, E^\vee).$$

Provided that $\operatorname{Pic}^0(C/k) = J(k)$, which holds for us by Lemma 4.2, we can show that the part of $H^1(k, E^\vee)$ relevant to us lies in the subgroup we can describe, and we obtain a map

$$\tilde{\gamma}\colon \frac{J(k)}{nJ(k)} \longrightarrow \frac{L^\times}{L^{\times 2} k^\times}$$

which we can use in essentially the same way as above. One can choose Δ to be the set of classes of *odd theta characteristics*, which has size $2^{g-1}(2^g - 1)$, less than half of what we needed before. For $g = 3$ this results in an algebra L of degree 28.

8. Application of descent to other problems

8A. ***Descent on the curve.*** If we embed the curve C in its Jacobian then we can restrict the maps γ and $\tilde{\gamma}$ to C. In that case we can construct a C-torsor under $J[n]$ by pulling C back along the multiplication-by-n map $J \to J$. The result is an unramified cover $\phi\colon D \to C$ of degree n^{2g}.

We can compute approximations of $\operatorname{Sel}(\mathbb{Q}, D \xrightarrow{\phi} C)$ using the same approach as in Section 7. If that approximation turns out to be empty, then C has no rational points. This can happen even if $C(\mathbb{A})$ is nonempty. When it works, this method is easier to apply than Mordell-Weil sieving, because the data we need is required for determining $J(\mathbb{Q})$ anyway, and we do not have to actually find generators for $J(\mathbb{Q})$.

Given that the map $\tilde{\gamma}$ is computed by evaluating a function on representative divisors, we can evaluate $\tilde{\gamma}$ directly on C, without choosing an embedding in J, and even if such an embedding does not exist. See [16] for a more thorough analysis of this method for hyperelliptic curves.

8B. ***Finding an embedding in J.*** A curve C has a degree-n point for some n. For instance, on a curve of genus $g \geq 2$, the canonical divisor class always contains a rational effective divisor, so one can take $n \leq 2g - 2$. It follows that $\underline{\operatorname{Pic}}^n(C) \simeq J$ and hence that multiplication-by-n yields a cover $\underline{\operatorname{Pic}}^1 \to J$. Note that over $\overline{\mathbb{Q}}$ we have $J \simeq \underline{\operatorname{Pic}}^1(C)$ in a way that is compatible with the multiplication-by-n map, so this cover expresses $\underline{\operatorname{Pic}}^1$ as a J-torsor under $J[n]$. By Proposition 6.1, this torsor corresponds to some class in $H^1(\mathbb{Q}, J[n])$. In fact, if $C(\mathbb{A}) \neq \varnothing$, we have $[\underline{\mathrm{Pic}}^1(C)] \in \mathrm{Sel}^n(J/\mathbb{Q})$. If we have succeeded in determining $J(\mathbb{Q})$, we can check if $[\underline{\mathrm{Pic}}^1(C)]$ lies in the image of $J(\mathbb{Q})$. If it does, then we have an explicit rational point that we can lift to $\underline{\mathrm{Pic}}^1(C)$. If it does not then we have proved that $\underline{\mathrm{Pic}}^1(C)$ does not have a rational point, and therefore neither does C.

We can also adapt the ideas from Section 8A to do further descent computations on $\underline{\mathrm{Pic}}^1$, although doing a descent directly on C yields stronger information for our purposes — see [27].

8C. ***Covering collections.*** Proposition 6.3 also provides useful information when Chabauty's method (Section 5) does not apply because $J(\mathbb{Q})$ is of too high rank. As we saw in Section 8A, we can use the embedding $C \to J$ to obtain unramified Galois covers $D \xrightarrow{\phi} C$. As Proposition 6.3 shows, one has

$$C(\mathbb{Q}) = \bigcup_{[D' \overset{\phi'}{\to} C] \in \mathrm{Sel}(\mathbb{Q}, D \overset{\phi}{\to} C)} \phi'(D'(\mathbb{Q})).$$

Note that D (and hence any of the D') is of higher genus than C, so Chabauty's method might apply to D' even if it does not to C; see also [64]. *A priori* it may seem computationally unattractive to compute with a curve of much higher genus. However, by construction, the curve D is far from general; for example, it has many automorphisms. That usually means that its Jacobian can be decomposed into factors of lower dimension. For instance, if C is a hyperelliptic curve and D is a C-torsor under $J[2]$, the Jacobian of D has many elliptic isogeny factors, although not necessarily over $\mathbb{Q}$. This means that many of the computations that would normally take place on the Jacobian of D can now be done on elliptic curves. This greatly simplifies computations and has led to a variant of Chabauty's method commonly referred to as *elliptic curve Chabauty*. See [36] for a special case and [8], [9] for the general case, as well as an application that amounts to a Chabauty computation on a 12-dimensional abelian variety. See also [16] on how to use descent computation to determine which twists to consider and [13] for an iterated application of these ideas. See [11] for an application to a curve of genus 3 admitting a double cover; this example involves Mordell-Weil sieving and a Chabauty computation on a genus-5 curve embedded in an abelian surface presented as the Jacobian of an otherwise unrelated curve of genus 2.

9. Smooth plane quartics

As an example, let us see how the ideas in the previous sections apply to smooth plane quartics — that is, nonhyperelliptic genus-3 curves. In a way, this is the simplest collection of truly *general* curves, in the sense that genus-2 curves are always hyperelliptic and hence necessarily have a nontrivial automorphism. The examples come from [14], to which the reader is referred for further details and references.

Let $C \subset \mathbb{P}^2$ be a smooth plane quartic curve over $\mathbb{Q}$. We apply the procedure described in Section 7 for $n = 2$. The set Δ has a particularly explicit description. A smooth plane quartic has 28 *bitangents*. If l and m are degree-1 forms on C that describe bitangents, then l/m obviously induces a function on the curve whose divisor is twice another divisor. That divisor therefore represents a 2-torsion class. It is a matter of combinatorics to compute that every nonzero 2-torsion point can be described this way (in fact, in 6 different ways). Let $\Delta \subset (\mathbb{P}^2)^*$ be the 0-dimensional, degree-28 locus in the dual space corresponding to these 28 bitangents, and let L be the affine coordinate ring of Δ, so that L is a finite algebra over $\mathbb{Q}$ of degree 28.

The Galois group of (a splitting field of) L is a subgroup of $\mathrm{Sp}_6(\mathbb{F}_2)$, which is also the generic Galois group of $J[2]$. For this full group, the module $(\mathbb{Z}/2\mathbb{Z})^\Delta$ has unique submodules E and R of dimensions 27 and 21 respectively, giving us a unique sequence of $\mathrm{Sp}_6(\mathbb{F}_2)$-modules

$$0 \longrightarrow R \longrightarrow E \longrightarrow J[2] \longrightarrow 0.$$

If we identify the conjugacy class in $\mathrm{Sp}_6(\mathbb{F}_2)$ of the group through which $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on L, then we can determine the action on the sequence via restriction. This means we can determine the sequence

$$0 \longrightarrow J[2](\mathbb{Q}) \longrightarrow E^\vee(\mathbb{Q}) \longrightarrow R^\vee(\mathbb{Q})$$

by identifying the Galois group of L as a subgroup of $\mathrm{Sp}_6(\mathbb{F}_2)$. Determining Galois groups is one of the classic problems in computational algebraic number theory.

For each $\theta \in \Delta$ we obtain a linear form $l_\theta \in L[x, y, z]$, where x, y, z are the coordinates on $\mathbb{P}^2$. Evaluating $\tilde{\gamma}$ at a point on C amounts to evaluating l_θ at that point.

In order to compute $\mathrm{Sel}^{\tilde{\gamma}}(\mathbb{Q}, J)$, we need to compute the ideal class group and unit group of L, for which we need an integral basis as well. The computation of class groups, unit groups, and integral bases are three further classical problems in computational algebraic number theory.

We give some examples.

Proposition 9.1. *If C is the curve*

$$x^3y - x^2y^2 - x^2z^2 - xy^2z + xz^3 + y^3z = 0$$

in $\mathbb{P}^2_{\mathbb{Q}}$, then $J(\mathbb{Q}) = \langle[(0:1:0) - (0:0:1)]\rangle \simeq \mathbb{Z}/51\mathbb{Z}$ and

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

For this example the Galois group of L is a member of the unique index-36 conjugacy class of $\mathrm{Sp}_6(\mathbb{F}_2)$. For that group we find that $R^\vee(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$ and that $E^\vee(\mathbb{Q}) = 0$. *A priori* this leaves room for a nontrivial kernel in

$$\mathrm{Sel}^2(\mathbb{Q}, J) \to \mathrm{Sel}^{\tilde{\gamma}}(\mathbb{Q}, J).$$

However, we find that $R^\vee(\mathbb{Q}_2) = R^\vee(\mathbb{Q})$ and $E^\vee(\mathbb{Q}_2) = E^\vee(\mathbb{Q})$ and that the image of $R^\vee(\mathbb{Q}_2)$ does not lie in the image of γ_2. This means that the map is an injection anyway and, since $\mathrm{Sel}^{\tilde{\gamma}}(\mathbb{Q}, J) = 0$, that $J(\mathbb{Q})$ is finite and of odd order. Further investigation shows that there is 51-torsion. Finding the rational points of C from the finite set $J(\mathbb{Q})$ is trivial.

Proposition 9.2. *Let C be the curve*

$$x^2y^2 - xy^3 - x^3z - 2x^2z^2 + y^2z^2 - xz^3 + yz^3 = 0$$

in $\mathbb{P}^2_{\mathbb{Q}}$. If the generalized Riemann hypothesis holds, then $J(\mathbb{Q}) \simeq \mathbb{Z}$ and

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

For this curve, the Galois group of L is all of $\mathrm{Sp}_6(\mathbb{F}_2)$. Then $R^\vee(\mathbb{Q}) = 0$, so

$$\mathrm{Sel}^2(\mathbb{Q}, J) \subseteq \mathrm{Sel}^{\tilde{\gamma}}(\mathbb{Q}, J).$$

Further computation shows that the latter has size 2, so $J(\mathbb{Q})$ has rank at most 1. Furthermore, we have $J(\mathbb{F}_3) \simeq \mathbb{Z}/85\mathbb{Z}$ and $J(\mathbb{F}_7) \simeq \mathbb{Z}/336\mathbb{Z}$. These group orders are coprime, so $J(\mathbb{Q})$ is torsion free. It is straightforward to exhibit a nontrivial point in $J(\mathbb{Q})$, so it follows the rank is 1. A straightforward application of Chabauty's method yields the rest of the statement.

We invoke the generalized Riemann hypothesis to verify the class group information. The Minkowski bound of L (which is a field in this case) is 1,008,340,641, so a dedicated enthusiast could probably confirm the class group information unconditionally.

Proposition 9.3. *Let C be the curve in $\mathbb{P}^2_{\mathbb{Q}}$ defined by*

$$x^4 + y^4 + x^2yz + 2xyz^2 - y^2z^2 + z^4 = 0.$$

Then $C(\mathbb{R}) \neq \varnothing$ and $C(\mathbb{Q}_p) \neq \varnothing$ for all p, but if the generalized Riemann hypothesis holds, then $C(\mathbb{Q}) = \varnothing$.

For this curve we verify that its $\tilde{\gamma}$-Selmer set is empty. The Minkowski bound for L exceeds 10^{22} so unconditional verification is out of the question.

Acknowledgments

I would like to thank the ANTS X Program Committee, and in particular Everett Howe and Kiran Kedlaya, for their hard work in organizing an excellent symposium. I would also like to thank an anonymous referee for comments on an earlier draft of this article. It helped clarify the exposition greatly.

This research was supported by NSERC.

References

[1] Scott D. Ahlgren, George E. Andrews, and Ken Ono (eds.), *Topics in number theory: Proceedings of the conference held at the Pennsylvania State University, University Park, PA, July 31–August 3, 1997*, Mathematics and its Applications, no. 467, Dordrecht, Kluwer Academic Publishers, 1999. MR 99m:11004

[2] Jennifer S. Balakrishnan, *Iterated Coleman integration for hyperelliptic curves*, in Howe and Kedlaya [40], 2013, pp. 41–61.

[3] B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves, I*, J. Reine Angew. Math. **212** (1963), 7–25. MR 26 #3669

[4] ———, *Notes on elliptic curves, II*, J. Reine Angew. Math. **218** (1965), 79–108. MR 31 #3419

[5] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), no. 21, Springer, Berlin, 1990. MR 91i:14034

[6] Wieb Bosma and John Cannon (eds.), *Discovering mathematics with Magma: Reducing the abstract to the concrete*, Algorithms and Computation in Mathematics, no. 19, Springer, Berlin, 2006. MR 2007h:00016

[7] N. Bruin and E. V. Flynn, *Rational divisors in rational divisor classes*, in Buell [19], 2004, pp. 132–139. MR 2005m:11117

[8] N. R. Bruin, *Chabauty methods and covering techniques applied to generalized Fermat equations*, CWI Tract, no. 133, Stichting Mathematisch Centrum Centrum voor Wiskunde en Informatica, Amsterdam, 2002. http://persistent-identifier.org/?identifier=urn:nbn:nl:ui:18-13154 MR 2003i:11042

[9] Nils Bruin, *Chabauty methods using elliptic curves*, J. Reine Angew. Math. **562** (2003), 27–49. MR 2004j:11051

[10] ———, *Some ternary Diophantine equations of signature $(n, n, 2)$*, in Bosma and Cannon [6], 2006, pp. 63–91. MR 2007m:11047

[11] ———, *The arithmetic of Prym varieties in genus* 3, Compos. Math. **144** (2008), no. 2, 317–338. MR 2009f:11074

[12] Nils Bruin and Noam D. Elkies, *Trinomials $ax^7 + bx + c$ and $ax^8 + bx + c$ with Galois groups of order* 168 *and* $8 \cdot 168$, in Fieker and Kohel [30], 2002, pp. 172–188. MR 2005d:11094

[13] Nils Bruin and E. Victor Flynn, *Towers of* 2*-covers of hyperelliptic curves*, Trans. Amer. Math. Soc. **357** (2005), no. 11, 4329–4347. MR 2006k:11118

[14] Nils Bruin, Bjorn Poonen, and Michael Stoll, *Generalized explicit descent and its application to curves of genus* 3, 2012. arXiv 1205.4456 [math.NT]

[15] Nils Bruin and Michael Stoll, *Deciding existence of rational points on curves: an experiment*, Experiment. Math. **17** (2008), no. 2, 181–189. MR 2009d:11100

[16] ———, *Two-cover descent on hyperelliptic curves*, Math. Comp. **78** (2009), no. 268, 2347–2370. MR 2010e:11059

[17] ———, *The Mordell-Weil sieve: Proving non-existence of rational points on curves*, LMS J. Comput. Math. **13** (2010), 272–306. MR 2011j:11118

[18] Armand Brumer and Kenneth Kramer, *The rank of elliptic curves*, Duke Math. J. **44** (1977), no. 4, 715–743. MR 56 #15658

[19] Duncan Buell (ed.), *Algorithmic number theory: Proceedings of the 6th International Symposium (ANTS-VI) held at the University of Vermont, Burlington, VT, June 13–18, 2004*, Lecture Notes in Computer Science, no. 3076, Berlin, Springer, 2004. MR 2005m:11002

[20] Yann Bugeaud, Maurice Mignotte, Samir Siksek, Michael Stoll, and Szabolcs Tengely, *Integral points on hyperelliptic curves*, Algebra Number Theory **2** (2008), no. 8, 859–885. MR 2010b:11066

[21] J. W. S. Cassels, *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. **41** (1966), 193–291. MR 33 #7299

[22] ———, *Corrigenda: "Survey article: Diophantine equations with special reference to elliptic curves"*, J. London Math. Soc. **42** (1967), 183. MR 34 #2523

[23] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus 2*, London Mathematical Society Lecture Note Series, no. 230, Cambridge University Press, 1996. MR 97i:11071

[24] Claude Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, C. R. Acad. Sci. Paris **212** (1941), 882–885. MR 3,14d

[25] Claude Chevalley and André Weil, *Un théorème d'arithmétique sur les courbes algébriques*, C. R. Acad. Sci. Paris **195** (1932), 570–572.

[26] Robert F. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765–770. MR 87f:11043

[27] Brendan Creutz, *Explicit descent in the Picard group of a cyclic cover of the projective line*, in Howe and Kedlaya [40], 2013, pp. 295–315.

[28] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366. MR 85g:11026a

[29] ———, *Erratum: "Endlichkeitssätze für abelsche Varietäten über Zahlkörpern"*, Invent. Math. **75** (1984), no. 3, 381. MR 85g:11026b

[30] Claus Fieker and David R. Kohel (eds.), *Algorithmic number theory: Proceedings of the 5th International Symposium (ANTS-V) held at the University of Sydney, July 7–12, 2002*, Lecture Notes in Computer Science, no. 2369, Berlin, Springer, 2002. MR 2004j:11002

[31] E. V. Flynn, *An explicit theory of heights*, Trans. Amer. Math. Soc. **347** (1995), no. 8, 3003–3015. MR 95j:11052

[32] ———, *A flexible method for applying Chabauty's theorem*, Compositio Math. **105** (1997), no. 1, 79–94. MR 97m:11083

[33] ———, *The Hasse principle and the Brauer-Manin obstruction for curves*, Manuscripta Math. **115** (2004), no. 4, 437–466. MR 2005j:11047

[34] E. V. Flynn, Bjorn Poonen, and Edward F. Schaefer, *Cycles of quadratic polynomials and rational points on a genus-2 curve*, Duke Math. J. **90** (1997), no. 3, 435–463. MR 98j:11048

[35] E. V. Flynn and N. P. Smart, *Canonical heights on the Jacobians of curves of genus 2 and the infinite descent*, Acta Arith. **79** (1997), no. 4, 333–352. MR 98f:11066

[36] E. Victor Flynn and Joseph L. Wetherell, *Finding rational points on bielliptic genus 2 curves*, Manuscripta Math. **100** (1999), no. 4, 519–533. MR 2001g:11098

[37] Daniel M. Gordon and David Grant, *Computing the Mordell-Weil rank of Jacobians of curves of genus two*, Trans. Amer. Math. Soc. **337** (1993), no. 2, 807–824. MR 93h:11057

[38] Benedict H. Gross and Don B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320. MR 87j:11057

[39] F. Hess, *Computing Riemann-Roch spaces in algebraic function fields and related topics*, J. Symbolic Comput. **33** (2002), no. 4, 425–445. MR 2003j:14032

[40] Everett W. Howe and Kiran S. Kedlaya (eds.), *Algorithmic number theory: Proceedings of the 10th Biennial International Symposium (ANTS-X) held in San Diego, July 9–13, 2012*, The Open Book Series, no. 1, Berkeley, Mathematical Sciences Publishers, 2013, THIS VOLUME.

[41] Nicholas M. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. **62** (1981), no. 3, 481–502. MR 82d:14025

[42] Kamal Khuri-Makdisi, *Asymptotically fast group operations on Jacobians of general curves*, Math. Comp. **76** (2007), no. 260, 2213–2239. MR 2009a:14072

[43] V. A. Kolyvagin, *Finiteness of $E(\mathbf{Q})$ and $SH(E,\mathbf{Q})$ for a subclass of Weil curves*, Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 3, 522–540, 670–671. MR 89m:11056

[44] Adrien-Marie le Gendre, *Recherches d'analyse indéterminée*, Histoire de l'Académie royale des sciences **1785** (1788), 465–559. http://gallica.bnf.fr/ark:/12148/bpt6k35847/f649

[45] James S. Milne, *Étale cohomology*, Princeton Mathematical Series, no. 33, Princeton University Press, 1980. MR 81j:14002

[46] L. J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees*, Cambr. Phil. Soc. Proc. **21** (1922), 179–192. JFM 48.1156.03

[47] Bjorn Poonen, *Heuristics for the Brauer-Manin obstruction for curves*, Experiment. Math. **15** (2006), no. 4, 415–420. MR 2008d:11062

[48] Bjorn Poonen and Edward F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math. **488** (1997), 141–188. MR 98k:11087

[49] Bjorn Poonen, Edward F. Schaefer, and Michael Stoll, *Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$*, Duke Math. J. **137** (2007), no. 1, 103–158. MR 2008i:11085

[50] Bjorn Poonen and Michael Stoll, *A local-global principle for densities*, in Ahlgren et al. [1], 1999, pp. 241–244. MR 2000e:11082

[51] Bjorn Poonen and Yuri Tschinkel (eds.), *Arithmetic of higher-dimensional algebraic varieties: Proceedings of the Workshop on Rational and Integral Points of Higher-Dimensional Varieties held in Palo Alto, CA, December 11–20, 2002*, Progress in Mathematics, no. 226, Boston, Birkhäuser, 2004. MR 2004h:11001

[52] Bjorn Poonen and José Felipe Voloch, *Random Diophantine equations*, in Poonen and Tschinkel [51], 2004, pp. 175–184. MR 2005g:11055

[53] Edward F. Schaefer, *2-descent on the Jacobians of hyperelliptic curves*, J. Number Theory **51** (1995), no. 2, 219–232. MR 96c:11066

[54] ———, *Computing a Selmer group of a Jacobian using functions on the curve*, Math. Ann. **310** (1998), no. 3, 447–471. MR 99h:11063

[55] ———, *Erratum: "Computing a Selmer group of a Jacobian using functions on the curve" [Math. Ann. 310 (1998), no. 3, 447–471]*, Math. Ann. **339** (2007), no. 1, 1. MR 2008f:11063

[56] Edward F. Schaefer and Michael Stoll, *How to do a p-descent on an elliptic curve*, Trans. Amer. Math. Soc. **356** (2004), no. 3, 1209–1231. MR 2004g:11045

[57] Victor Scharaschkin, *Local-global problems and the Brauer-Manin obstruction*, Ph.D. thesis, University of Michigan, Ann Arbor, MI, 1999, p. 59. http://search.proquest.com/docview/304517948 MR 2700328

[58] Denis Simon, *Solving quadratic equations using reduced unimodular quadratic forms*, Math. Comp. **74** (2005), no. 251, 1531–1543. MR 2005k:11246

[59] Alexei Skorobogatov, *Torsors and rational points*, Cambridge Tracts in Mathematics, no. 144, Cambridge University Press, 2001. MR 2002d:14032

[60] Michael Stoll, *On the height constant for curves of genus two*, Acta Arith. **90** (1999), no. 2, 183–201. MR 2000h:11069

[61] ———, *On the height constant for curves of genus two, II*, Acta Arith. **104** (2002), no. 2, 165–182. MR 2003f:11093

[62] ———, *Independence of rational points on twists of a given curve*, Compos. Math. **142** (2006), no. 5, 1201–1214. MR 2007m:14025

[63] André Weil, *L'arithmétique sur les courbes algébriques*, Acta Math. **52** (1929), no. 1, 281–315. MR 1555278

[64] Joseph Loebach Wetherell, *Bounding the number of rational points on certain curves of high rank*, Ph.D. thesis, University of California, Berkeley, Ann Arbor, MI, 1997, p. 61. http://search.proquest.com/docview/304343505 MR 2696280

NILS BRUIN: nbruin@sfu.ca
Department of Mathematics, Simon Fraser University, Burnaby, BC V5A 1S6, Canada

VOLUME EDITORS

Everett W. Howe
Center for Communications Research
4320 Westerra Court
San Diego, CA 92121-1969
United States

Kiran S. Kedlaya
Department of Mathematics
University of California, San Diego
9500 Gilman Drive #0112
La Jolla, CA 92093-0112

Front cover artwork based on a detail of
Chicano Legacy 40 Años ©2010 Mario Torero.

Electronic copies can be obtained free of charge from http://msp.org/obs/1 and printed copies can be ordered from MSP (contact@msp.org).

The Open Book Series is a trademark of Mathematical Sciences Publishers.

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-00-2 (print), 978-1-935107-01-9 (electronic)

First published 2013.

msp

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org http://msp.org

THE OPEN BOOK SERIES 1

Tenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the tenth ANTS meeting, held July 9–13, 2012, at the University of California, San Diego. It includes revised and edited versions of the 25 refereed papers presented at the conference, together with extended abstracts of two of the five invited talks.

TABLE OF CONTENTS