Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Michael STOLL

Rational points on curves

Tome 23, n° 1 (2011), p. 257-277.

<http://jtnb.cedram.org/item?id=JTNB_2011__23_1_257_0>

Journal de Théorie des Nombres de Bordeaux **23** (2011), 257-277

Rational points on curves

par Michael STOLL

Résumé. Ceci est la version longue de l'exposé invité que j'ai donné aux Journées Arithmétiques de St. Étienne en juillet 2009.

Nous discutons l'état de l'art pour le problème de trouver l'ensemble des points rationnels sur $\mathbb{Q}$ d'une courbe C (projective lisse) géométriquement intègre. Nous nous concentrons sur les aspects pratiques de ce problème dans le cas où le genre de C est au moins 2, et par conséquent l'ensemble des points rationnels est fini.

Abstract. This is an extended version of an invited lecture I gave at the Journées Arithmétiques in St. Étienne in July 2009.

We discuss the state of the art regarding the problem of finding the set of rational points on a (smooth projective) geometrically integral curve C over $\mathbb{Q}$. The focus is on practical aspects of this problem in the case that the genus of C is at least 2, and therefore the set of rational points is finite.

1. Introduction

As a preliminary remark, let me point out that the following report is somewhat biased, in that it clearly reflects my own predilections. I have tried to mention other approaches at least briefly and give some pointers to the literature, but the main focus of this paper is on methods I have been involved in myself.

1.1. The problem. Let C be a geometrically integral algebraic curve defined over $\mathbb{Q}$. We stick to $\mathbb{Q}$ here for simplicity. In principle, we can replace $\mathbb{Q}$ by an arbitrary number field. In practice, however, many of the necessary algorithms are only implemented for $\mathbb{Q}$, and even when they are available for more general number fields, the computations are usually much more involved. We consider the following problem.

Problem 1. Determine $C(\mathbb{Q})$, the set of *rational points* on C.

We observe that a curve and its smooth projective model only differ in a computable finite set of points (coming from points at infinity and from singularities). Therefore we lose nothing if we assume that C is *smooth and projective.*

Classification math.. 11D41, 11G30, 14G05, 14G25.

1.2. The structure of $C(\mathbb{Q})$. Before we consider curves of 'higher genus' more specifically, let us recall what is known about the structure of the set $C(\mathbb{Q})$ in general. There is a trichotomy, depending on the *genus* g of C, which is the most important geometric (or even topological, if we think of C as a Riemann surface) invariant of the curve. This exemplifies the belief that "Geometry determines arithmetic" — the structure of the set of rational points on a variety should only depend on its geometry.

We have the following three cases.

- $g = 0$:
  In this case, we either have $C(\mathbb{Q}) = \emptyset$ (this is always possible), or else if there is a point $P_0 \in C(\mathbb{Q})$, then C is isomorphic over $\mathbb{Q}$ to the projective line $\mathbb{P}^1$. Any such isomorphism will give us a parameterization of $C(\mathbb{Q})$ in terms of rational functions in one variable. Probably the best-known example is the unit circle $x^2 + y^2 = 1$, whose points can be rationally parameterized in the following way.

  $$t \longmapsto \Big(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\Big)$$

  As t runs through $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$, its image runs through all the rational points on the unit circle. So such a parameterization gives us a finite description of the set $C(\mathbb{Q})$.

- $g = 1$:
  We either have $C(\mathbb{Q}) = \emptyset$, or else if there is a point $P_0 \in C(\mathbb{Q})$, then (C, P_0) is an *elliptic curve*. So C has a geometrically defined structure as an abelian group with P_0 as its origin. This implies that $C(\mathbb{Q})$ is also an abelian group with origin P_0. Mordell [35] has shown that $C(\mathbb{Q})$ is *finitely generated*. (Weil [56] has extended this to elliptic curves and, more generally, Jacobian varieties over arbitrary number fields.) In particular, we can describe $C(\mathbb{Q})$ by listing generators of this group.

- $g \geq 2$:
  This is the case of 'higher genus'. Mordell [35] has conjectured, and Faltings [21] has proved that the set $C(\mathbb{Q})$ is always *finite*. In particular, we can describe $C(\mathbb{Q})$ by simply listing the finitely many points.

We see that in each case, there is a finite description of $C(\mathbb{Q})$. The precise version of Problem 1 above therefore asks for an algorithm that provides this description.

Before we consider the higher genus case in detail, let us give a short discussion of the other two cases.

1.3. Genus zero. If C is a smooth projective geometrically integral curve of genus 0 (over any field k), then C is isomorphic to a smooth *conic*. If we can compute in k, then we can find an explicit such isomorphism. This can be done by computing a basis of the Riemann-Roch space of an anticanonical divisor; the map to $\mathbb{P}^2$ given by this basis provides the desired isomorphism.

Now let $k = \mathbb{Q}$ again. Like all quadrics, conics C satisfy the *Hasse Principle*: If $C(\mathbb{Q}) = \emptyset$, then $C(\mathbb{R}) = \emptyset$ or $C(\mathbb{Q}_p) = \emptyset$ for some prime p, where $\mathbb{Q}_p$ is the field of p-adic numbers. For future reference, we make the following definition.

Definition 2. The curve C has points *everywhere locally*, if $C(\mathbb{R}) \neq \emptyset$ and $C(\mathbb{Q}_p) \neq \emptyset$ for all primes p.

The Hasse Principle then states that a curve that has points everywhere locally must also have rational points.

Let us assume that C is given by a ternary quadratic form with integral coefficients. Then $C(\mathbb{Q}_p) \neq \emptyset$ whenever p does not divide the discriminant of the quadratic form (we use the fact that smooth conics over finite fields always have rational points, plus Hensel's Lemma to lift to a p-adic point). So there are only finitely many primes to check in addition to $C(\mathbb{R})$. (One should note, however, that in general one has to *factor* the discriminant, which can be difficult.) For each given prime, Hensel's Lemma gives us an upper bound for the p-adic precision needed. So the check whether C has points everywhere locally reduces to a finite computation. Therefore we can *decide* if $C(\mathbb{Q})$ is empty or not. This is still true for a number field in place of $\mathbb{Q}$.

If $C(\mathbb{Q}) \neq \emptyset$ and we know the 'bad' primes (those dividing the discriminant), then there is an efficient procedure that exhibits a point $P_0 \in C(\mathbb{Q})$, see for example [45]. This can be seen as a 'minimization' process that finds a $\mathbb{Q}$-isomorphic curve with good reduction at all primes, followed by a 'reduction' process based on lattice basis reduction [31] that brings the curve into the standard form $y^2 = xz$, which has some obvious points. This last (reduction) part of the procedure has, to my knowledge, not yet been generalized to arbitrary number fields in a satisfactory way.

Given $P_0 \in C(\mathbb{Q})$, we can easily compute an isomorphism $\phi : C \to \mathbb{P}^1$ by projecting away from P_0. The inverse of ϕ then provides us with the desired parameterization of $C(\mathbb{Q})$.

1.4. Genus one. For curves of positive genus, the Hasse Principle no longer holds in general. So there is no easy way to check if the curve has rational points or not. If we cannot find a rational point, but C has points everywhere locally, then we can try to use a *descent* computation. For $n \geq 2$, *n-descent* consists in computing a finite number of n-coverings of C such that each of these n-coverings has points everywhere locally and every rational point on C is the image of a rational point on one of the n-coverings. An *n-covering* is a morphism $\pi : D \to C$ of curves over $\mathbb{Q}$ that over $\bar{\mathbb{Q}}$ is isomorphic to the multiplication-by-n map $E \to E$, where E is $C/\bar{\mathbb{Q}}$ considered as an elliptic curve. In principle, this computation is possible for every C and every n over every number field. In practice however, this is feasible only in a few cases.

- $y^2 =$ quartic in x and $n = 2$ [11, 34];
- intersections of two quadrics in $\mathbb{P}^3$ and $n = 2$ [46];
- plane cubics and $n = 3$ [18].

If the finite set of relevant n-coverings turns out to be empty, this proves that $C(\mathbb{Q}) = \emptyset$. If we assume that Shafarevich-Tate groups of elliptic curves do not contain nontrivial infinitely divisible elements (this assumption is weaker than the standard conjecture that Ш$(E/\mathbb{Q})$ is finite), then it follows that if $C(\mathbb{Q}) = \emptyset$, then there must be an n such that there are no n-coverings of C with points everywhere locally. This means that we can, at least in principle, verify that C does not have rational points.

On the other hand, if C does have rational points, then their preimages on suitable n-coverings tend to be 'smaller' and can therefore be found more easily by a search. So n-descent on C serves two purposes: it allows us to show that no rational points exist, but it can also help us find a rational point.

It should be noted that if a curve of genus 1 has infinitely many rational points, the smallest point can be exponentially large in terms of the coefficients of the defining equations. (This comes from the corresponding property of generators of the group of rational points on an elliptic curve.) This phenomenon is what can make life rather hard when we try to find the rational points on a curve of genus 1.

1.5. Elliptic curves. We now assume that we have found a rational point P_0 on our curve C of genus 1. Then, as mentioned above, (C, P_0) is an *elliptic curve*, which we will denote E. By Mordell's Theorem we know that $E(\mathbb{Q})$ is a finitely generated abelian group; our task is now to find explicit *generators* of this group. By the structure theorem for finitely generated abelian groups, we have

$$E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r\,,$$

where $E(\mathbb{Q})_{\text{tors}}$ is the finite subgroup of $E(\mathbb{Q})$ consisting of all elements of finite order. This finite subgroup is easy to find. The hard part is to determine the *rank* $r = \operatorname{rank} E(\mathbb{Q})$.

We can use n-descent again. When we apply it to an elliptic curve, the set of n-coverings with points everywhere locally has a natural group structure;

this group is the *n-Selmer group of E*. Its order gives an upper bound for the size of $E(\mathbb{Q})/nE(\mathbb{Q})$, from which we can deduce an upper bound for r. As before, this computation is always possible in principle (see [50]). In practice, n-descent on an elliptic curve over $\mathbb{Q}$ is currently feasible for $n = 2, 3, 4, 8$ and 9. See [16, 17] for a detailed description. In some cases, we can use what is known about the conjecture of Birch and Swinnerton-Dyer. If the conductor of E is not too large, we can compute the values of the L-series of E and its derivatives at $s = 1$ to sufficient precision. If $L(E, 1) \neq 0$, then $r = 0$, and if $L'(E, 1) \neq 0$, then $r = 1$ [30].

A search for independent points in $E(\mathbb{Q})$ gives a lower bound on r. However, generators may be very large. In the same way as for general curves of genus 1, descent can help us to find them. When $r = 1$, *Heegner points* can be used if the conductor of E is sufficiently small.

Example 3. (See [17].) The group $E(\mathbb{Q})$, where

$$E : y^2 = x^3 + 7823\,,$$

is infinite cyclic and generated by the point

$$P = \Bigl(\frac{2263582143321421502100209233517777}{119816734100955612^2},$$

$$\frac{186398152584623305624837551485596770028144776655756}{11981673410095561^3}\Bigr)\,.$$

This point was found by a 4-descent on E. The Heegner point method is not feasible here, because the conductor of E is $2^4 \cdot 3^3 \cdot 7823^2$, which is a bit too large.

A discussion of how one can try to find the set of rational points on an elliptic curve, or more generally, on a genus 1 curve, would provide enough material for at least one book. But this is a different story and will be told at another occasion.

2. Checking existence of rational points

We now turn to curves of higher genus, meaning $g \geq 2$. The first question we would like to answer is whether there are any rational points on the curve C or not.

2.1. Finding points. If $C(\mathbb{Q})$ is nonempty, we can usually find a rational point by search. This is because (in contrast to the case of genus 1) we expect the rational points to be fairly *small*. The following is a consequence of Vojta's Conjecture; see Su-Ion Ih's thesis [29].

Conjecture 4. *If $\mathcal{C} \to B$ is a family of higher-genus curves, then there are constants γ and κ such that*

$$H_{\mathcal{C}}(P) \leq \gamma H_B(b)^{\kappa} \qquad \textit{for all } P \in \mathcal{C}_b(\mathbb{Q})$$

if the the fiber $\mathcal{C}_b$ is smooth.

Here H_B denotes a (non-logarithmic) height on the base B, and $H_{\mathcal{C}}$ is a suitable height function on $\mathcal{C}$.

If C is hyperelliptic, one can use the `ratpoints` program [55] for the point search.

Examples 5. Consider a curve

$$C : y^2 = f_6x^6 + \cdots + f_1x + f_0$$

of genus 2, with $f_j \in \mathbb{Z}$. Then the conjecture says that there are γ and κ such that the x-coordinate p/q of any point $P \in C(\mathbb{Q})$ satisfies

$$|p|, |q| \leq \gamma \max\{|f_0|, |f_1|, \ldots, |f_6|\}^\kappa .$$

In [7], we consider curves of genus 2 as above such that the coefficients f_j are integers with $|f_j| \leq 3$. We will call these curves *small genus 2 curves* in this paper. If such a curve has rational points, then there is one whose x-coordinate is p/q with $|p|, |q| \leq 1519$. In fact, for all but two such curves (up to isomorphism), we even have $|p|, |q| < 80$. On the other hand, the largest point known on one of these curves (which is very likely the largest point there is) has height 209 040, which indicates that γ and/or κ cannot be too small.

So usually we can assume that we know all the points in $C(\mathbb{Q})$. In particular, if we are unable to find a rational point on C, it is reasonable to suspect that there are indeed no rational points. The problem now is to *prove* this fact in some way.

2.2. Local points. One approach that we can try is to check if C has points everywhere locally. As before, this can be done by a finite computation, which is efficient modulo the determination of the 'bad' primes. This usually comes down to factoring some kind of discriminant. In addition to the bad primes, one also has to look at small primes. The reason is that smooth curves of genus g may fail to have $\mathbb{F}_p$-points when p is small relative to g. (By the Weil bounds, we have $\#C(\mathbb{F}_p) \geq p + 1 - 2g\sqrt{p}$, so there will be $\mathbb{F}_p$-points whenever $p + 1 > 2g\sqrt{p}$.)

Example 6. (Poonen-Stoll [39]) About 84–85% of all curves of genus 2 have points everywhere locally. This percentage is a *density*: we consider all genus 2 curves of the form $y^2 = f(x)$ with $f = f_6x^6 + \cdots + f_1x + f_0 \in \mathbb{Z}[x]$ such that $\max\{|f_j|\} \leq N$, and determine the proportion α_N of curves with points everywhere locally. Then $\lim_{N\to\infty} \alpha_N$ exists and has approximately the value given above. Convergence seems to be rather fast, compare the data given at the end of [8].

The counterpart to this result is the following conjecture.

Conjecture 7. *0% of all curves of genus 2 have rational points.*

In fact, heuristic considerations suggest the following. Let β_N be the proportion of curves of size up to N that possess rational points (similarly to α_N above). Then $\beta_N \ll N^{-1/2}$. See [54] for details and some experimental data.

This indicates that checking for points everywhere locally will usually not suffice to prove that $C(\mathbb{Q}) = \emptyset$: the Hasse Principle is quite likely to fail.

Example 8. (Bruin-Stoll [7]) Among the 196 171 isomorphism classes of small genus 2 curves, there are 29 278 that are counterexamples to the Hasse Principle.

2.3. Descent again. So we need another method of attack. One possibility is again *descent*. We find a covering $\pi : D \to C$ (more precisely, an unramified covering of smooth projective geometrically integral curves that over $\bar{\mathbb{Q}}$ is a Galois covering). As before in the genus 1 case, this covering has finitely many *twists* $\pi_\xi : D_\xi \to C$ such that D_ξ has points everywhere locally.

Example 9. Consider a hyperelliptic curve

$$C : y^2 = g(x)h(x)$$

with $\deg g$, $\deg h$ not both odd. Then

$$D : \quad u^2 = g(x)\,, \quad v^2 = h(x)$$

is an unramified $\mathbb{Z}/2\mathbb{Z}$-covering of C with covering map $\pi : D \to C$ given by $(x, u, v) \mapsto (x, uv)$. Its twists are

$$D_d : \quad du^2 = g(x)\,, \quad dv^2 = h(x)\,, \qquad d \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2\,.$$

Every rational point on C lifts to one of the twists, since $g(x)$ must have some square class d. If g and h have integral coefficients and p is a prime divisor of d (we assume d to be a squarefree integer), then D_d does not have p-adic points unless g and h have a common root mod p. This is the case only when p divides the resultant of g and h. So we see that only finitely many of the twists D_d can have points everywhere locally.

The idea of descent goes back to Fermat ('descente infinie'). The statement that only finitely many twists are relevant is a variant of a result due to Chevalley and Weil [14], see Theorem 11 below.

Here is a concrete example.

Example 10. Consider the genus 2 curve

$$C : y^2 = -(x^2 + x - 1)(x^4 + x^3 + x^2 + x + 2) =: f(x)\,.$$

C has points everywhere locally. This can be seen by observing that

$$f(0) = 2\,, \quad f(1) = -6\,, \quad f(-2) = -3 \cdot 2^2\,,$$
$$f(18) \in (\mathbb{Q}_2^\times)^2 \quad \text{and} \quad f(4) \in (\mathbb{Q}_3^\times)^2.$$

The first three values show that $C(\mathbb{R}) \neq \emptyset$ and that $C(\mathbb{Q}_p) \neq \emptyset$ for all $p \neq 2, 3$; the last two fill the remaining gaps.

The relevant twists of the obvious $\mathbb{Z}/2\mathbb{Z}$-covering are among

$$d\,u^2 = -x^2 - x + 1\,, \qquad d\,v^2 = x^4 + x^3 + x^2 + x + 2$$

where d is one of 1, -1, 19 or -19, since the resultant of the two factors is 19. If $d < 0$, the second equation has no solution in $\mathbb{R}$; if $d = 1$ or 19, the pair of equations has no solution over $\mathbb{F}_3$. This is because the first equation implies that $x \bmod 3$ is one of 0 or -1, whereas the second equation implies that $x \bmod 3$ is one of 1 or ∞.

So there are no twists with points everywhere locally, and therefore $C(\mathbb{Q}) = \emptyset$.

The general result is as follows.

Theorem 11 (Descent Theorem). *Let $\pi : D \to C$ be an unramified covering that is geometrically Galois. Its twists $\pi_\xi : D_\xi \to C$ are parameterized by $\xi \in H^1(\mathbb{Q}, G)$ (a Galois cohomology set), where G is the Galois group of the covering. We then have the following:*

- $C(\mathbb{Q}) = \displaystyle\bigcup_{\xi \in H^1(\mathbb{Q},G)} \pi_\xi\left(D_\xi(\mathbb{Q})\right).$
- $\operatorname{Sel}^\pi(C) := \{\xi \in H^1(\mathbb{Q}, G) : D_\xi$ *has points everywhere locally*$\}$ *is finite (and computable).*

Definition 12. In the situation of the Descent Theorem, we call $\operatorname{Sel}^\pi(C)$ the *Selmer set* of C with respect to π.

Corollary 13. *If we find* $\operatorname{Sel}^\pi(C) = \emptyset$*, then* $C(\mathbb{Q}) = \emptyset$ *as well.*

This follows from the two statements in the theorem, since $D_\xi(\mathbb{Q})$ is empty unless D_ξ has points everywhere locally.

2.4. Abelian coverings. In principle, we can use this approach with any covering of C in the above sense. However, in practice it is easier to restrict to a special kind of coverings.

Definition 14. A covering $\pi : D \to C$ as above is *abelian* if its Galois group G is abelian.

The reason why abelian coverings are especially useful comes from the following fact (which is a result of 'Geometric Class Field Theory'; see [42] for details). We let J denote the *Jacobian variety* of C. We assume for simplicity that there is an embedding $\iota : C \to J$. (This means that there is a divisor class of degree 1 on C that is defined over $\mathbb{Q}$, i.e., stable under the action of the absolute Galois group of $\mathbb{Q}$. If we can show that there is no such divisor class, then it follows that C does not have rational points, since a rational point would provide us with a suitable divisor class.)

Then all abelian coverings of C are obtained from *n-coverings* of J:

(2.1)
$$\begin{tikzcd}
D \arrow[r] \arrow[d, "\pi"'] & X \arrow[r, dashed, "\cong/\bar{\mathbb{Q}}"] \arrow[d] & J \arrow[dl, "\cdot n"] \\
C \arrow[r, "\iota"] & J &
\end{tikzcd}$$

Here $X \to J$ is an n-covering of J, meaning that there is an isomorphism of X with J over $\bar{\mathbb{Q}}$ that makes the triangle in the diagram commute, and $\pi : D \to C$ is the pull-back of $X \to J$ under ι.

We call such a covering $D \to C$ an *n-covering* of C; the set of all n-coverings with points everywhere locally is denoted $\mathrm{Sel}^{(n)}(C)$ and called the *n-Selmer set* of C. Every abelian covering of C can be extended to an n-covering for some n. Therefore the Jacobian gives us a handle on all the abelian coverings of C. The process of computing the set $\mathrm{Sel}^{(n)}(C)$ is called an *n-descent on C*.

2.5. Computing *n*-Selmer sets in practice. In practice, computing $\mathrm{Sel}^{(n)}(C)$ is usually quite hard, even though it is possible in principle. The most difficult obstacle is that the computation requires arithmetic information like ideal class groups and unit groups for number fields that can be rather large. About the only fairly general situation where the fields involved are manageable is the computation of the 2-Selmer group of a *hyperelliptic curve* $C : y^2 = f(x)$. In this case, the relevant number fields are those generated by a root of each irreducible factor of f. This is a generalization of the $y^2 = g(x)h(x)$ example above, where all possible factorizations are considered simultaneously. The paper [8] describes the procedure in detail.

Example 15. (See [7, 8]) Among the small genus 2 curves, there are only 1492 curves C without rational points and such that $\mathrm{Sel}^{(2)}(C) \neq \emptyset$. So 2-descent is a rather efficient tool in this case. Figure 1 at the end of [8] shows that this is still mostly true also for larger coefficients.

2.6. A conjecture. In the example above, we have seen that 2-descent shows that most of the small curves without rational points really do not have rational points. This makes it plausible that perhaps we can deal with the remaining curves by an n-descent with a suitable $n > 2$. Unfortunately, the direct computation of the relevant Selmer sets is infeasible. Still, we can formulate the following conjecture. In [52], we argue that there are good reasons for it to hold.

Conjecture 16. *If* $C(\mathbb{Q}) = \emptyset$*, then* $\operatorname{Sel}^{(n)}(C) = \emptyset$ *for some* $n \geq 1$*.*

The case $n = 1$ is equivalent to checking for points everywhere locally on C, since $\mathrm{id}_C : C \to C$ is the only 1-covering of C.

Remarks 17.

(1) In principle, $\operatorname{Sel}^{(n)}(C)$ is *computable* for every n. The conjecture therefore implies that "$C(\mathbb{Q}) = \emptyset$?" is *decidable.* (Search for points by day, compute $\operatorname{Sel}^{(n)}(C)$ by night.)

(2) The conjecture implies that the *Brauer-Manin obstruction* is the *only* obstruction against rational points on curves. (In fact, the conjecture is equivalent to this statement.) See [52] for details.

3. The Mordell-Weil sieve

3.1. The idea. We now assume that we know explicit generators of the Mordell-Weil group $J(\mathbb{Q})$, where J is, as before, the Jacobian variety of the curve C. By [56], $J(\mathbb{Q})$ is a finitely generated abelian group. It is clear that in the diagram (2.1) we only need to consider those n-coverings X of J that actually have rational points. These n-coverings are of the form

$$J \ni P \longmapsto nP + Q \in J \qquad \text{with } Q \in J(\mathbb{Q});$$

the shift Q is only determined modulo $nJ(\mathbb{Q})$.

The set we are interested in is therefore

$$\{Q + nJ(\mathbb{Q}) : (Q + nJ(\mathbb{Q})) \cap \iota(C) \neq \emptyset\} \subset J(\mathbb{Q})/nJ(\mathbb{Q})\,.$$

By the above, it contains the subset of the n-Selmer set of C that consists of n-coverings of C with rational points. We approximate the condition by testing it modulo p for a set of primes p.

Let S be a finite set of primes of good reduction for C. Consider the following diagram.

(3.1)
$$\begin{tikzcd}
C(\mathbb{Q}) \arrow[r, "\iota"] \arrow[d] & J(\mathbb{Q}) \arrow[r] \arrow[d] & J(\mathbb{Q})/nJ(\mathbb{Q}) \arrow[d, "\beta"] \\
\prod_{p\in S} C(\mathbb{F}_p) \arrow[r, "\iota"] \arrow[rr, bend right, "\alpha"'] & \prod_{p\in S} J(\mathbb{F}_p) \arrow[r] & \prod_{p\in S} J(\mathbb{F}_p)/nJ(\mathbb{F}_p)
\end{tikzcd}$$

We *can compute* the maps α and β, since they only involve finite objects. If their images do not intersect, then it follows that $C(\mathbb{Q}) = \emptyset$. This method is known as the 'Mordell-Weil Sieve'. It was first used by Scharaschkin in his thesis [41]. Flynn [24] used it on a number of genus 2 curves. In [7], it is applied to the remaining undecided small genus 2 curves.

Example 18. If C is a small genus 2 curve without rational points, then either C fails to have points everywhere locally, or $\operatorname{Sel}^{(2)}(C) = \emptyset$, or the Birch and Swinnerton-Dyer Conjecture for J implies that C has no embedding into J (this is needed for 42 curves), or else the Mordell-Weil Sieve with suitable parameters S and n proves that $C(\mathbb{Q})$ is empty.

In order to obtain this result, one needs a carefully optimized implementation of the Mordell-Weil sieve. See [9] for details. The parameter the complexity depends on most sensitively is the rank r of $J(\mathbb{Q})$. If $r \leq 3$, our implementation works quite well; it should be mentioned that it uses not only information mod p for good primes p, but also information modulo powers of (small) primes, even when they are primes of bad reduction. There are not yet enough worked examples where the rank is larger than 3, so it is hard to say anything precise about the performance of the algorithm in this case. At least there are isolated examples that show that it can still work when r is as large as 6.

Poonen [36] shows that under reasonable assumptions, the following should be true.

Conjecture 19 (Poonen Heuristic). *If $C(\mathbb{Q}) = \emptyset$, then the maps α and β in Diagram* (3.1) *above will have disjoint images when n and the set S are sufficiently large.*

Conjecture 19 implies Conjecture 16 if we assume that $Ш(J/\mathbb{Q})$ has no nontrivial infinitely divisible elements, see [52].

3.2. Satisfying the assumption on $J(\mathbb{Q})$. We are assuming here that we know explicit generators of $J(\mathbb{Q})$. For the Mordell-Weil sieve as described above, if we use it to show that C has no rational points, it is actually sufficient to know generators of a subgroup of finite index, if we can also show that the index is coprime to n. The latter is usually not so hard; see [27]. To achieve the former, we can use n-descent again, but this time on the Jacobian J. This is feasible for hyperelliptic curves when $n = 2$ and in a few other rather special cases, see [40, 37, 48, 38]. As with elliptic curves, large generators can be a problem, however.

Example 20. (See [7].) For the small genus 2 curve

$$C : y^2 = -3\,x^6 + x^5 - 2\,x^4 - 2\,x^2 + 2\,x + 3\,,$$

the Mordell-Weil group $J(\mathbb{Q})$ is infinite cyclic, generated by $[P_1 + P_2 - W]$, where the x-coordinates of P_1 and P_2 are the roots of

$$x^2 + \tfrac{37482925498065820078878366248457300623}{34011049811816647384141492487717524243}\,x + \tfrac{581452628280824306698926561618393967033}{544176796989066358146263879803480387888}\,,$$

and W is a canonical divisor.

The bound on r obtained from 2-descent on J need not be tight. The difference to the actual value of r comes from 2-torsion elements of the Shafarevich-Tate group $\text{Ш}(J/\mathbb{Q})$. In some cases, it is possible to show that there are non-trivial such elements, thereby improving the upper bound on the rank. Two techniques that have been suggested and also used are *visualization* [6] and the Brauer-Manin obstruction on certain related varieties [1, 25, 32].

For 'reasonable' curves of genus 2, generators of a finite-index subgroup of $J(\mathbb{Q})$ can usually be determined. For hyperelliptic curves of genus at least 3, it may still be possible in many cases, but the situation is already less favorable. Beyond hyperelliptic curves and variations on that theme, descent calculations appear to be rather hopeless with the currently available technology. There are some first attempts at 2-descent on Jacobians of non-hyperelliptic curves of genus 3, however, so maybe the situation will change at some point in the not-too-distant future.

3.3. An extension. If we take n in Diagram (3.1) to be a multiple of a fixed number N, then we can restrict to a given *coset* X *of* $NJ(\mathbb{Q})$ (since this coset will be a union of cosets of $nJ(\mathbb{Q})$). Therefore the Mordell-Weil sieve computation gives us a way of proving that the coset X does not meet $\iota(C)$. In this case, there are no rational points on C that are mapped into X under ι.

Conjecture 16 can be extended to this situation.

Conjecture 21. *Let $Q \in J(\mathbb{Q})$. If $(Q + NJ(\mathbb{Q})) \cap \iota(C) = \emptyset$, then there are $n \in N\mathbb{Z}$ and S such that the Mordell-Weil sieve with these parameters proves this fact.*

So if we can find an N that *separates* the rational points on C, i.e., such that the composition $C(\mathbb{Q}) \xrightarrow{\iota} J(\mathbb{Q}) \to J(\mathbb{Q})/NJ(\mathbb{Q})$ is injective, then we *can effectively determine* $C(\mathbb{Q})$ if Conjecture 21 holds for C. The procedure simply considers each coset of $NJ(\mathbb{Q})$ in turn. On the one hand, we run a search on C to find a rational point that maps into the coset under consideration; on the other hand, we run the Mordell-Weil sieve with the aim of proving that no such point exists. If Conjecture 21 holds, then one of these two computations has to produce a result. (In practice, we just run the Mordell-Weil sieve. As long as the intersection of the images of α and β is nonempty, we check the smallest representatives in $J(\mathbb{Q})$ of the elements of the intersection whether they come from the curve.)

4. Chabauty's method

4.1. The idea. Chabauty [13] used this method to prove Mordell's Conjecture in the case that the rank r of $J(\mathbb{Q})$ is smaller than the genus g of the curve. The idea is to consider the p-adic points $J(\mathbb{Q}_p)$ as a p-adic Lie group. The topological closure of $J(\mathbb{Q})$ then is a Lie subgroup of dimension at most r. One then expects that this subgroup of positive codimension has only finitely many points of intersection with the analytic curve $\iota(C(\mathbb{Q}_p))$. This is what Chabauty proves. Later, the method was taken up by Coleman [15] who used it to deduce upper bounds on the number of rational points on the curve. The method can also be used to determine the set of rational points in certain cases, see [23, 26, 57] for early examples of this. The book [12] contains a description of the method when C has genus 2.

We now describe the setting more concretely. Let p be a prime of good reduction for C (this assumption simplifies things, but is not strictly necessary). We denote by $\Omega^1_J(\mathbb{Q}_p)$ the g-dimensional $\mathbb{Q}_p$-vector space of regular 1-forms on J, and similarly for C. Then ι induces an isomorphism of $\Omega^1_J(\mathbb{Q}_p)$ and $\Omega^1_C(\mathbb{Q}_p)$ that is in fact independent of our choice of the embedding ι.

The p-adic logarithm on J is a continuous group homomorphism

$$\log : J(\mathbb{Q}_p) \longrightarrow T_0 J(\mathbb{Q}_p) = \Omega^1_J(\mathbb{Q}_p)^*$$

whose kernel consists of the elements of finite order. It induces a pairing

$$\text{(4.1)} \qquad \Omega^1_J(\mathbb{Q}_p) \times J(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p\,, \qquad (\omega, R) \longmapsto \int_0^R \omega = \langle \omega, \log R \rangle$$

that becomes perfect if we replace $J(\mathbb{Q}_p)$ by $J(\mathbb{Q}_p)^0 \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ (where $J(\mathbb{Q}_p)^0$ is a sufficiently small neighborhood of the identity). Since

$$\operatorname{rank} J(\mathbb{Q}) = r < g = \dim_{\mathbb{Q}_p} \Omega^1_J(\mathbb{Q}_p)\,,$$

there is a differential

$$0 \neq \omega_p \in \Omega^1_C(\mathbb{Q}_p) \cong \Omega^1_J(\mathbb{Q}_p)$$

that kills $J(\mathbb{Q}) \subset J(\mathbb{Q}_p)$ under the pairing (4.1).

Let $P_0 \in C(\mathbb{Q})$ be used as the base-point for the embedding ι. Then the above implies that every point $P \in C(\mathbb{Q})$ must satisfy

$$\lambda(P) = \int_{P_0}^P \omega_p = 0\,.$$

The function λ is a p-adic analytic function on $C(\mathbb{Q}_p)$. On each residue class mod p, it can be represented by an explicit converging power series. This makes it possible to bound the number of zeros of λ on such a residue class. If we find the same number of rational points within the residue class, then we know that we have found them all. Some of the zeros of λ may occur at transcendental points, however; in this case the upper bound on the number of points is not tight. We can use information from the Mordell-Weil sieve to rule out the spurious zeros; see [38] for some examples.

4.2. Combination with the Mordell-Weil sieve. We can also switch the roles of Chabauty's method and the Mordell-Weil sieve and use Chabauty's method in a helping function. We still need to assume that $r < g$. The idea is to use Chabauty's approach to find a *separating* number N. The key to this is the following result (see for example [51]).

Theorem 22. *Suppose that p is a prime of good reduction for C and that $\omega_p \in \Omega^1_C(\mathbb{Q}_p)$ is a differential that kills the Mordell-Weil group $J(\mathbb{Q})$. We can assume that ω_p is scaled so that it has a well-defined reduction $\bar{\omega}_p \neq 0$ mod p. If $\bar{\omega}_p$ does not vanish on $C(\mathbb{F}_p)$ and $p > 2$, then each residue class mod p on C contains at most one rational point.*

In this case, the number $N = \#J(\mathbb{F}_p)$ is separating, since we know that the map $C(\mathbb{Q}) \to C(\mathbb{F}_p)$ is injective (this is the statement of the theorem), that $\iota : C(\mathbb{F}_p) \to J(\mathbb{F}_p)$ is injective, and that $J(\mathbb{Q})/NJ(\mathbb{Q})$ maps to $J(\mathbb{F}_p)$.

Heuristic considerations indicate that the theorem applies for a set of primes p of positive density whenever $r < g$ and J is simple. (If J splits, we can use one of the factors of J to do a similar computation.)

The most accessible case is when $g = 2$, since then we have a good chance to determine $J(\mathbb{Q})$. The 'Chabauty condition' $r < g$ then reduces to $r = 1$. (When $r = 0$, the group $J(\mathbb{Q})$ is finite, and we can easily find its intersection with $\iota(C)$, so this case is essentially trivial.) In this case, the differentials $\bar{\omega}_p$ can be computed very easily, and we quickly find suitable primes p. The search for a suitable separating number N can be integrated with the Mordell-Weil sieve computation. This leads to a very efficient implementation that determines $C(\mathbb{Q})$ quite fast for genus 2 curves C such that $\operatorname{rank} J(\mathbb{Q}) = 1$. See [9] for a discussion.

Example 23. (See [54]) For the 46 436 small genus 2 curves with rational points and such that $r = 1$, we determined $C(\mathbb{Q})$. This computation takes about 8–9 hours on current hardware (as of 2009).

5. Some odds and ends

In this section, we collect some remarks on extensions and variants of the methods discussed above, and on some other approaches.

5.1. Larger rank. When $r \geq g$, we can still use the Mordell-Weil Sieve to show that we know all rational points up to very large height. For this, we increase n in the sieving procedure until we can prove that none of the remaining cosets of $nJ(\mathbb{Q})$ contains a point on C of height smaller than a given bound, except for the points we know. Once the bulk of the computation is done, we can increase the height bound without much extra cost.

If the desired height bound is not so large, it may be more efficient to use lattice point enumeration. For this, we use the fact that the torsion-free quotient $J(\mathbb{Q})/J(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}^r$ is endowed with a positive definite quadratic form $\hat{h}$, the *canonical height.* The height bound for $P \in C(\mathbb{Q})$ translates into a bound for $\hat{h}(\iota(P))$; we can then enumerate all points in $J(\mathbb{Q})$ (mod torsion) up to that height bound and check if they come from the curve.

Example 24. (See [54]) Unless there are points of height $> 10^{100}$, the largest point on a small genus 2 curve has height (i.e., maximum absolute value of the numerator and denominator of its x-coordinate) 209 040.

For these applications, it is not enough to know generators of a finite-index subgroup of $J(\mathbb{Q})$. We really need to know generators of the full Mordell-Weil group. The 'saturation' step from a finite-index subgroup to the full group requires the computation of canonical heights on J, and we need a bound for the difference between the canonical height and a suitable 'naive height'. So far, the necessary theory and algorithms only exist for $g \leq 2$ [22, 27, 47, 49]. Therefore, we are currently limited to curves of genus 2. There is current work that aims at extending the tools so that they can also be used for higher-genus hyperelliptic curves, so we may soon be able to deal with a larger class of curves.

5.2. Integral points. If we can determine the set of rational points on C, we obviously have also found the *integral* points. However, we can determine the set of integral points in some cases even when we are not able to find $C(\mathbb{Q})$. For example, if C is hyperelliptic, we can compute bounds for integral points using *Baker's method* of 'Linear forms in logarithms'. The currently best results in this direction [10] lead to bounds of a flavor like $|x| < 10^{10^{600}}$.

If we know *generators* of $J(\mathbb{Q})$, we can use the Mordell-Weil sieve as explained in the previous subsection to prove that there are no unknown rational points below that bound. (The bound for $\hat{h}$ is something like 10^k with k of the order of several hundred or a couple of thousand. This is within reach of our current implementation of the Mordell-Weil sieve method. See [10] or [9] for details.) It follows that we already know all the integral points on C.

Example 25. (See [10]) The integral solutions to

$$\binom{y}{2} = \binom{x}{5}$$

have $x \in \{0, 1, 2, 3, 4, 5, 6, 7, 15, 19\}$.

Since we need to know generators of the full Mordell-Weil group for this application, the remarks made at the end of the previous subsection also apply here. In particular, we are currently restricted to curves of genus 2.

5.3. Genus larger than two. We have seen that there are methods available that allow us to find out a lot about the rational points on a given curve *of genus 2*. When the genus is larger, a number of difficulties arise.

If C is hyperelliptic (or perhaps of some other rather special form), it is still possible to do 2-descent on C and (to a certain extent) on J. For other curves, there is so far no feasible way to obtain provable upper bounds on the rank of $J(\mathbb{Q})$. If we are willing to assume the Birch and Swinnerton-Dyer conjecture for J (together with some related conjectures on L-series) and the conductor of J is not too large, then we can use Tim Dokchitser's code [20] to compute (an upper bound for) the order of vanishing of $L(s, J)$ at $s = 1$, which gives a conditional upper bound on r. We may then be able to find a set of generators of a finite-index subgroup of $J(\mathbb{Q})$; this suffices to apply Chabauty's method or its combination with the Mordell-Weil sieve.

Another difficulty is the missing explicit theory of heights. This prevents us from obtaining generators of the full Mordell-Weil group (or rather, it prevents us from showing that we actually have generators). This means that we cannot use the techniques described earlier in this section.

Here are some examples that show what can still be done with curves of genus at least 3.

Example 26. (See [38]) In the course of solving $x^2 + y^3 = z^7$ in coprime integers, one has to determine the set of rational points on certain twists of the Klein Quartic. These are rather special non-hyperelliptic curves of genus 3. 2-Descent on J is possible here; Chabauty and Mordell-Weil sieve techniques are successful.

Example 27. (See [53]) The curve $X_0^{\mathrm{dyn}}(6)$ classifying 6-cycles under the iteration of $x \mapsto x^2 + c$ has genus 4. Assuming the Birch and Swinnerton-Dyer conjecture for its Jacobian, we can show that $r = 3$. We can then apply Chabauty's method to determine $X_0^{\mathrm{dyn}}(6)(\mathbb{Q})$. It follows that there are no 6-cycles consisting of rational numbers (under the assumptions made).

Example 28. (See [44]) What are the arithmetic progressions in coprime integers that have the form (a^2, b^2, c^2, d^5)? This question leads to a number of hyperelliptic curves of genus 4; every solution to the original question gives rise to a rational point on one of these curves. There are three essentially different curves. For two of them, the 2-Selmer set turns out to be empty. For the last one, a 2-descent on its Jacobian is possible and shows that the rank is 2. Chabauty, combined with a little Mordell-Weil sieve information, then succeeds in showing that there are no unexpected points. This finally proves that the only arithmetic progression of the desired form is the trivial one, $(1, 1, 1, 1)$.

5.4. The method of Dem'yanenko-Manin. The method of Dem'yanenko-Manin is an alternative method that can be used to determine $C(\mathbb{Q})$ in some cases. When it applies, it gives an effective bound on the height of the rational points on C (and not just on their number, as is the case with Chabauty's method).

The requirement here is that we have m independent morphisms $C \to A$, where A is some abelian variety and $m > \operatorname{rank} A(\mathbb{Q})$. The idea is that the images of points on C under these independent morphisms want to be independent in $A(\mathbb{Q})$, but there is not enough room for them to be independent. This leads to a bound on the height of the points.

If one looks at more or less 'random' curves C that have two independent maps to an elliptic curve E, say, then the two images on E of a rational point on C usually *are* independent in $E(\mathbb{Q})$, invalidating the assumption. So the method appears to be of fairly limited applicability.

There are cases, however, when the method can be used with profit. In [19], it is applied to certain twists of the Fermat quartic that have two independent maps to an elliptic curve. However, as Serre comments in [43], it is hard to find nontrivial examples. See [28] for a more recent variation on this theme.

In [33], Manin makes use of the growing number of degeneracy maps $X_0(p^n) \to X_0(p)$ in order to show that for any given prime p, the power of p that divides the order of a rational torsion point on an elliptic curve over $\mathbb{Q}$ (or over any fixed number field) is bounded.

5.5. Covering collections and elliptic curve Chabauty. The Descent Theorem 11 tells us that we obtain all rational points on a given curve C from the rational points on the various twists D_ξ of a covering of C. If we can find this collection of twists explicitly (this is sometimes called a *covering collection* for C), then we can attempt to determine their sets of rational points instead of directly trying to find $C(\mathbb{Q})$. This can be helpful when the rank of $J(\mathbb{Q})$ is too large to apply Chabauty's method on C, since the ranks associated to the curves D_ξ may well be sufficiently small.

The downside of this approach is that the covering curves have larger genus than C, and so the methods described here are usually not applicable. In some cases, the curves D_ξ map to other curves of low genus. If we can find their rational points, we can determine those on D_ξ. A very useful variant arises when the target is an elliptic curve E; the map may be defined over some number field K. The images of rational points on D_ξ then satisfy some additional constraints. This can be used to find these images by a variant of Chabauty's method (applied to the restriction of scalars of E from K down to $\mathbb{Q}$) when the rank of $E(K)$ is less than the degree of K. This is known as *Elliptic curve Chabauty*; see [2, 3, 4, 5, 57] for details and examples.

6. Concluding remarks

The last ten or fifteen years have seen tremendous progress in our ability to determine the set of rational points on curves of higher genus, in particular on curves of genus 2. Given a curve C of genus 2 over $\mathbb{Q}$, we can now do the following.

- Search for rational points on C.
- Check if C has points everywhere locally.
- Perform a 2-descent on C, thus possibly showing that $C(\mathbb{Q})$ is empty.
- Perform a 2-descent on J, the Jacobian of C, thus obtaining an upper bound on $r = \operatorname{rank} J(\mathbb{Q})$.
- Search for rational points on J, thus obtaining a lower bound on r.
- Find generators of a finite-index subgroup of $J(\mathbb{Q})$ if both bounds agree.
- Compute canonical heights on J.
- Find generators of $J(\mathbb{Q})$ if generators of a finite-index subgroup are known, assuming that the bound for the difference between naive and canonical height is not too large.
- If $r \leq 1$, determine $C(\mathbb{Q})$ using a combination of the Mordell-Weil sieve and Chabauty's method. (Termination of this is conditional on Conjecture 21, but if the computation terminates, which is always the case in practice, the result is provably correct.)
- If $r \geq 2$ and $J(\mathbb{Q})$ is known, find all rational points on C up to very large height.
- If $J(\mathbb{Q})$ is known, find all integral points on C.

From a practical point of view, what is missing to make this really satisfying is a way of determining a separating N when $r \geq 2$ (without previous knowledge what $C(\mathbb{Q})$ is). If a separating N can be found, then the same approach as used when combining the Mordell-Weil sieve with Chabauty's method will enable us to determine $C(\mathbb{Q})$.

From a theoretical point of view, we would like to have a proof of Conjecture 21, since this will guarantee that our procedure terminates. (For practical computations, we don't really care about a proof as long as the computation terminates; the result will be correct in any case.) The other theoretical gap is that it is still open whether the rank r can be found effectively. This is related to the finiteness of $\text{Ш}(J/\mathbb{Q})$, which is only known in very special cases.

For curves of higher genus than 2, some of the items on the list above can still be done (in particular when C is hyperelliptic), but we soon reach a point where things become infeasible. However, I believe that this is only a matter of complexity and not of principle: given sufficient resources, we should be able to perform the same kind of computation also with more general curves. (Of course, some theoretical work still has to be done for this, like an extension of the explicit theory of heights that we have at our disposal when the genus is 2.)

Based on what we can actually do, on various heuristic considerations, and on fairly extensive experimental data, I am convinced that it is actually possible (in principle) to determine the set $C(\mathbb{Q})$ algorithmically, when C is a curve of genus ≥ 2. A complete proof of this statement is likely to be quite far away still, but the progress that has been made on the practical side in recent years is very encouraging.

References

[1] M.J. Bright, N. Bruin, E.V. Flynn, A. Logan, *The Brauer-Manin obstruction and* Ш$[2]$*,* LMS J. Comput. Math. **10** (2007), 354–377.

[2] N. Bruin, *Chabauty methods and covering techniques applied to generalized Fermat equations,* CWI Tract 133, 77 pages (2002).

[3] N. Bruin, *Chabauty methods using elliptic curves,* J. Reine Angew. Math. **562** (2003), 27–49.

[4] N. Bruin, N.D. Elkies, *Trinomials* ax^7+bx+c *and* ax^8+bx+c *with Galois groups of order* 168 *and* $8\cdot 168$*,* in: *Algorithmic number theory, Sydney 2002,* Lecture Notes in Comput. Sci. **2369**, Springer, Berlin (2002), pp. 172–188.

[5] N. Bruin, E.V. Flynn, *Towers of 2-covers of hyperelliptic curves,* Trans. Amer. Math. Soc. **357** (2005), 4329–4347.

[6] N. Bruin, E.V. Flynn, *Exhibiting SHA*$[2]$ *on hyperelliptic Jacobians,* J. Number Theory **118** (2006), 266–291.

[7] N. Bruin, M. Stoll, *Deciding existence of rational points on curves: an experiment,* Experiment. Math. **17** (2008), 181–189.

[8] N. Bruin, M. Stoll, *2-cover descent on hyperelliptic curves*, Math. Comp. **78** (2009), 2347–2370.

[9] N. Bruin, M. Stoll, *The Mordell-Weil sieve: Proving non-existence of rational points on curves*, LMS J. Comput. Math. **13** (2010), 272–306.

[10] Y. Bugeaud, M. Mignotte, S. Siksek, M. Stoll, Sz. Tengely, *Integral points on hyperelliptic curves,* Algebra Number Theory **2** (2008), 859–885.

[11] J.W.S. Cassels, *Second descents for elliptic curves,* J. reine angew. Math. **494** (1998), 101–127.

[12] J.W.S. Cassels, E.V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus 2,* London Math. Soc., Lecture Note Series **230**, Cambridge Univ. Press, Cambridge, 1996.

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

[14] C. Chevalley, A. Weil, *Un théorème d'arithmétique sur les courbes algébriques,* Comptes Rendus Hebdomadaires des Séances de l'Acad. des Sci., Paris **195** (1932), 570–572.

[15] R.F. Coleman, *Effective Chabauty,* Duke Math. J. **52** (1985), 765–770.

[16] J.E. Cremona, T.A. Fisher, C. O'Neil, D. Simon, M. Stoll, *Explicit* n*-descent on elliptic curves. I. Algebra,* J. reine angew. Math. **615** (2008), 121–155. *II. Geometry,* J. reine angew. Math. **632** (2009), 63–84. *III. Algorithms,* in preparation.

[17] J.E. Cremona, T.A. Fisher, M. Stoll, *Minimisation and reduction of 2-, 3- and 4-coverings of elliptic curves,* Algebra Number Theory **4** (2010), 763–820.

[18] B. Creutz, *Explicit second p-descent on elliptic curves*, PhD Thesis, Jacobs University Bremen, 2010.

[19] V.A. Dem'janenko, *Rational points of a class of algebraic curves* (Russian), Izv. Akad. Nauk SSSR Ser. Mat. **30** (1966), 1373–1396.

[20] T. Dokchitser, *Computing special values of motivic L-functions,* Experiment. Math. **13** (2004), 137–149.

[21] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern,* Invent. Math. **73** (1983), 349–366.

[22] E.V. Flynn, *An explicit theory of heights,* Trans. Amer. Math. Soc. **347** (1995), 3003–3015.

[23] E.V. Flynn, *A flexible method for applying Chabauty's theorem,* Compositio Math. **105** (1997), 79–94.

[24] E.V. Flynn, *The Hasse Principle and the Brauer-Manin obstruction for curves,* Manuscripta Math. **115** (2004), 437–466.

[25] E.V. Flynn, *Homogeneous spaces and degree 4 del Pezzo surfaces,* Manuscripta Math. **129** (2009), 369–380.

[26] E.V. Flynn, B. Poonen, E.F. Schaefer, *Cycles of quadratic polynomials and rational points on a genus-2 curve,* Duke Math. J. **90** (1997), 435–463.

[27] E.V. Flynn, N.P. Smart, *Canonical heights on the Jacobians of curves of genus* 2 *and the infinite descent,* Acta Arith. **79** (1997), 333–352.

[28] M. Girard, L. Kulesz, *Computation of sets of rational points of genus-3 curves via the Dem'janenko-Manin method,* LMS J. Comput. Math. **8** (2005), 267–300.

[29] Su-Ion Ih, *Height uniformity for algebraic points on curves,* Compositio Math. **134** (2002), 35–57.

[30] V.A. Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and $Ш(E,\mathbb{Q})$ for a subclass of Weil curves,* Izv. Akad. Nauk SSSR Ser. Mat., Vol. **52** (1988), 522–540.

[31] A.K. Lenstra, H.W. Lenstra, Jr., L. Lovász, *Factoring polynomials with rational coefficients,* Math. Ann. **261** (1982), 515–534.

[32] A. Logan, R. van Luijk, *Nontrivial elements of Sha explained through K3 surfaces,* Math. Comp. **78** (2009), 441–483.

[33] Y. Manin, *The p-torsion of elliptic curves is uniformly bounded* (Russian), Izv. Akad. Nauk SSSR Ser. Mat. **33** (1969), 459–465.

[34] J.R. Merriman, S. Siksek, N.P. Smart, *Explicit* 4*-descents on an elliptic curve,* Acta Arith. **77** (1996), 385–404.

[35] L.J. Mordell, *On the rational solutions of the indeterminate equations of the 3rd and 4th degrees,* Proc. Camb. Phil. Soc. **21** (1922), 179–192.

[36] B. Poonen, *Heuristics for the Brauer-Manin obstruction for curves,* Experiment. Math. **15** (2006), 415–420.

[37] B. Poonen, E.F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line,* J. reine angew. Math. **488** (1997), 141–188.

[38] B. Poonen, E.F. Schaefer, M. Stoll, *Twists of $X(7)$ and primitive solutions to $x^2+y^3=z^7$,* Duke Math. J. **137** (2007), 103–158.

[39] B. Poonen, M. Stoll, *A local-global principle for densities,* in: Scott D. Ahlgren (ed.) et al.: *Topics in number theory. In honor of B. Gordon and S. Chowla.* Kluwer Academic Publishers, Dordrecht. Math. Appl., Dordr. **467** (1999), 241–244.

[40] E.F. Schaefer, *Computing a Selmer group of a Jacobian using functions on the curve,* Math. Ann. **310** (1998), 447–471.

[41] V. Scharaschkin, *Local-global problems and the Brauer-Manin obstruction,* Ph.D. thesis, University of Michigan (1999).

[42] J.-P. Serre, *Algebraic groups and class fields*, Springer GTM **117**, Springer Verlag, 1988.

[43] 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.

[44] S. Siksek, M. Stoll, *On a problem of Hajdu and Tengely,* in: G. Hanrot, F. Morain, and E. Thomé (Eds.): *ANTS-IX 2010*, LNCS 6197, pp. 316–330. Springer Verlag, Heidelberg, 2010.

[45] D. Simon, *Solving quadratic equations using reduced unimodular quadratic forms,* Math. Comp. **74** (2005), 1531–1543.

[46] S. Stamminger, *Explicit 8-descent on elliptic curves,* PhD thesis, International University Bremen (2005).

[47] M. Stoll, *On the height constant for curves of genus two,* Acta Arith. **90** (1999), 183–201.

[48] M. Stoll, *Implementing 2-descent on Jacobians of hyperelliptic curves,* Acta Arith. **98** (2001), 245–277.

[49] M. Stoll, *On the height constant for curves of genus two, II,* Acta Arith. **104** (2002), 165–182.

[50] M. Stoll, *Descent on Elliptic Curves.* Short Course taught at IHP in Paris, October 2004. arXiv:math/0611694v1 [math.NT].

[51] M. Stoll, *Independence of rational points on twists of a given curve,* Compositio Math. **142** (2006), 1201–1214.

[52] M. Stoll, *Finite descent obstructions and rational points on curves,* Algebra Number Theory **1** (2007), 349–391.

[53] M. Stoll, *Rational 6-cycles under iteration of quadratic polynomials,* LMS J. Comput. Math. **11** (2008), 367–380.

[54] M. Stoll, *On the average number of rational points on curves of genus 2,* Preprint (2009), arXiv:0902.4165v1 [math.NT].

[55] M. Stoll, *Documentation for the ratpoints program,* Manuscript (2009), arXiv:0803.3165 [math.NT].

[56] A. Weil, *L'arithmétique sur les courbes algébriques,* Acta Math. **52** (1929), 281–315.

[57] J.L. Wetherell, *Bounding the number of rational points on certain curves of high rank,* Ph.D. thesis, University of California (1997).

Michael Stoll
Mathematisches Institut
Universität Bayreuth
95440 Bayreuth, Germany.
E-mail: `Michael.Stoll@uni-bayreuth.de`
URL: `http://www.mathe2.uni-bayreuth.de/stoll/`