Deciding Existence of Rational Points on Curves: An Experiment

Nils Bruin and Michael Stoll

CONTENTS

In this paper we gather experimental evidence related to the question of deciding whether a curve has a rational point. We consider all genus-2 curves over $\mathbb{Q}$ given by an equation $y^2 = f(x)$ with f a square-free polynomial of degree 5 or 6, with integral coefficients of absolute value at most 3. For each of these roughly 200 000 isomorphism classes of curves, we decide whether there is a rational point on the curve by a combination of techniques that are applicable to hyperelliptic curves in general.

In order to carry out our project, we have improved and optimized some of these techniques. For 42 of the curves, our result is conditional on the Birch and Swinnerton-Dyer conjecture or on the generalized Riemann hypothesis.

1. INTRODUCTION

The problem to decide whether a given algebraic variety defined over the rational numbers has rational points is fundamental in arithmetic geometry. Abstracting from concrete examples, this leads to the question whether there exists an algorithm that is able to perform this task for any given variety. This is probably too much to ask for: we know that Hilbert's tenth problem, which asks the same question for integral points on general affine varieties, has a negative answer. But we can hope for a more favorable outcome if we restrict the class of varieties we consider.

It is then most natural to look at curves first, since they have been studied very intensively, resulting in good theoretical knowledge and a very rich supply of algorithmic methods. Also, it makes sense to consider the geometrically nicest class of varieties, namely those that are projective. Since it is easy to check whether a curve has rational singular points, we can assume that the curve is smooth. Therefore, the question we are specifically interested in is the following.

2000 AMS Subject Classification: Primary 11D41, 11G30, 11Y50
Secondary 14G05, 14G25, 14H25, 14H45, 14Q05

Keywords: Rational points, curves, solvability, local-to-global obstruction, descent

1058-6458/2008 $ 0.50 per page

Question 1.1. Is there an algorithm that decides for any given smooth projective curve $C/\mathbb{Q}$ whether C has rational points?

Since we can always algorithmically prove that $C(\mathbb{Q}) \neq \varnothing$ if rational points exist by simply enumerating all rational points of the relevant projective space and checking for each point whether it is on C until we find a rational point on C, our question is equivalent to the following, seemingly more restricted, version.

Question 1.2. Is there an algorithm that verifies that $C(\mathbb{Q}) = \varnothing$ for any given smooth projective curve $C/\mathbb{Q}$ without rational points?

"Verification" here means that the algorithm constructs a proof of some kind.

For curves of genus 0, our question has a positive answer, since the Hasse principle holds for these curves: a curve of genus 0 has rational points if and only if it is "everywhere locally solvable" (ELS), i.e., it has real points and p-adic points for all primes p. Since for a general curve C, we can check algorithmically whether it has points everywhere locally, we can assume that C is ELS. The main problem is then to show that $C(\mathbb{Q})$ is empty even though C is ELS.

If C is a curve of genus 1 with Jacobian elliptic curve E, then we can perform descent calculations (on E or on C), which will succeed in proving that $C(\mathbb{Q})$ is empty if C represents an element of $Ш(E)$, the Tate–Shafarevich group of E, that is not divisible. In particular, if we assume (as is generally believed) that $Ш(E)$ is finite for all elliptic curves $E/\mathbb{Q}$, then our question has a positive answer for curves of genus 1 as well.

We will therefore focus our attention on curves of higher genus. It is only since fairly recently that there is some confidence that the question might have a positive answer, spurred by progress on the theoretical side [Stoll 07, Stoll 05] and also by heuristic considerations [Poonen 05]. In this paper, we attempt to give supporting evidence of a more practical kind, by applying the available algorithms (with some new improvements and additions) to a large number of curves in order to see whether we actually can decide for each of them whether it has rational points.

The obvious class of curves to look at for a first attempt at gathering evidence is the class of curves of genus 2. Their main advantage is that quite a variety of algorithms is available for them, and so we can hope to use them as adequate test cases. In order to keep the computational effort within reasonable limits, we decided to consider "small" genus-2 curves. More precisely, our initial set of curves consists of all genus-2 curves over $\mathbb{Q}$ that have a model of the form

$$y^2 = f(x) = f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0$$

with integral coefficients $f_0, f_1, \ldots, f_6$ satisfying $|f_j| \leq 3$. Excluding non-square-free f and f of degree ≤ 4 and identifying isomorphic curves, our initial set contains 196 171 isomorphism classes of curves.

In Section 2, we describe our findings, and in Section 3, we give an overview of the methods we have used. The details on the new methods and the improvements on existing methods we have made can be found in a series of forthcoming papers [Bruin and Stoll 08a, Bruin and Stoll 08b, Bruin and Stoll 08c].

2. RESULTS

As a first step, we searched for a small rational point on each curve C. Note that C has one or two obvious points if $f_0 \in \{0, 1\}$ or $f_6 \in \{0, 1\}$ (C is considered to have one or two rational points "at infinity" if f_6 is respectively zero or a nonzero square). At a later stage, we searched for larger rational points on those curves that were not yet decided. The largest points found at that stage were $(1519/601, 4816728814/601^3)$ on

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

and $(193/436, 165847285/436^3)$ on

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

This left us with 58 681 curves C without (apparent) rational points, for which we need to prove that $C(\mathbb{Q}) = \varnothing$. Among these, there are 29 278 curves with points everywhere locally. Together with the curves that do have rational points, this means that we found 166 768 with points everywhere locally, which is about 85% of all the curves we considered. In [Poonen and Stoll 99b] (see also [Poonen and Stoll 99a, Section 9]), it is shown that the set of polynomials f giving rise to an everywhere locally solvable curve has a well-defined positive density δ. Numerical estimates of the local densities involved lead to a value close to 0.85 for δ, which fits well with our observations. This good agreement is a bit surprising, since our set of curves certainly does not provide an even coverage of polynomials over $\mathbb{Z}_p$, except perhaps for $p = 7$.

The next stage in the procedure is to perform a 2-cover descent on each of the remaining curves. This constructs

(implicitly) a finite collection of curves D_j that cover C and are such that every rational point on C is the image of a rational point on some D_j. So if we obtain an empty covering collection $\{D_j\}$, this proves that C has no rational points. For a more precise description of the computation, see Section 3.1. With this method, we were able to prove that $C(\mathbb{Q})$ is empty for all but 1492 curves.

For these 1492 curves, we wanted to perform a "Mordell–Weil sieve" computation. The idea is as follows. Let J be the Jacobian variety of C, and assume that we can embed C into J. Assume also that we can determine generators of the Mordell–Weil group $J(\mathbb{Q})$, which is a finitely generated abelian group. By abuse of notation, we call its free abelian rank the *rank* of the curve C. Now consider the following commutative diagram:

$$\begin{array}{ccc} C(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q}) \\ \downarrow & & \downarrow \alpha \\ \prod_{p\in S} C(\mathbb{F}_p) & \xrightarrow{\beta} & \prod_{p\in S} J(\mathbb{F}_p) \end{array}$$

Here S is some finite set of primes (of good reduction for C, say). Since we know $J(\mathbb{Q})$ and can find the finite sets $C(\mathbb{F}_p)$, we can compute the images of α and β. If these images do not meet, this proves that $C(\mathbb{Q})$ is empty.

First, we had to find generators of the Mordell–Weil group. To do this, we performed a 2-descent (see [Stoll 01]) on J to get an upper bound, called the *Selmer rank*, for the rank of the finitely generated abelian group $J(\mathbb{Q})$. Then we needed to find the correct number of independent points in $J(\mathbb{Q})$. In order to be able to do this successfully, we had to come up with new strategies, involving a search for points on (quotients of) 2-covering spaces for J. See Section 3.2 for more details. In this way, we were able to find generators of a finite-index subgroup of $J(\mathbb{Q})$ for all but 47 curves. It is then a fairly easy matter to check that we actually had generators of $J(\mathbb{Q})$ (modulo torsion); see [Stoll 02].

In the course of these computations, we also found a rational point on the 2-covering space Pic^1_C for J, which provides an embedding of C into J. So for these 1445 curves (3 of rank 0, 516 of rank 1, 772 of rank 2, 152 of rank 3, and 2 of rank 4), the assumptions for the application of the Mordell–Weil sieve are satisfied.

After several improvements of the algorithm performing the actual sieve computation (the problem here is combinatorial explosion), we were finally able to run the procedure successfully for all these curves. With the current version of the algorithm, the maximal computation time for a single curve was roughly 16 hours on a 1.7-GHz processor; this curve is one of the two with rank 4. The computations for all the other curves together can be performed in about the same time.

For the remaining 47 curves (36 of Selmer rank 2, 10 of Selmer rank 3, and one of Selmer rank 4), the number of independent points we found fell short of the Selmer rank by 2. Therefore, we suspect that there is nontrivial 2-torsion in $Ш(J)$ in these cases. In 5 out of the 10 cases of Selmer rank 3, we found a rational point on Pic^1_C. Here we expect that $Ш(J)[2] = (\mathbb{Z}/2\mathbb{Z})^2$. This was confirmed by an ad hoc visualization argument. See [Bruin 04, Bruin and Flynn 06] for a description and detailed analysis of this method for hyperelliptic curves with a rational branch point.

For these 5 curves, we know that $\operatorname{rank} J(\mathbb{Q}) = 1$, and we have an embedding of C into J, so that we can run the Mordell–Weil sieve procedure, which confirms that there are no rational points on these curves.

One of these curves is

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

For the visualization argument we consider a quadratic twist of this curve,

$$C^{(-1)} : y^2 = -f(x)\,.$$

We find that $J^{(-1)}(\mathbb{Q})$ is of rank 4, where $J^{(-1)}$ is the Jacobian of $C^{(-1)}$. A slightly more involved computation gives that $J(\mathbb{Q}(\sqrt{-1}))$ is of rank at most 5. Since this rank is the sum of the ranks of $J(\mathbb{Q})$ and $J^{(-1)}(\mathbb{Q})$, this means that the rank of $J(\mathbb{Q})$ can be at most 1. This is less than the rank bound of 3 we obtain from a 2-descent on J directly.

In the remaining 42 cases, we did not find a rational point on Pic^1_C. On the other hand, from the 2-cover descent, we know that C has everywhere locally solvable 2-coverings; the same must then be true for Pic^1_C, since C has a canonical embedding into Pic^1_C. This means that the class of Pic^1_C in $Ш(J)$ is divisible by 2. If $\mathrm{Pic}^1_C(\mathbb{Q}) = \varnothing$, this then implies that there are elements of order 4 in $Ш(J)$. The computations necessary for a visualization argument are hardly feasible in this situation: one needs to compute the 2-Selmer group of J over a quartic number field. This involves finding an S-unit group in a degree-24 number field.

Still, assuming the generalized Riemann hypothesis (GRH) to make the number field computations feasible, we were successful for four curves in showing that the

true Mordell–Weil rank is smaller than the bound obtained from a 2-descent. One of these curves is

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

The Jacobians of the quadratic twists by 2, -3, -6 can easily be shown to have Mordell–Weil ranks $4, 4, 3$ respectively. Furthermore, a 2-descent shows, conditional on GRH, that $J(\mathbb{Q}(\sqrt{2}, \sqrt{-3}))$ is of rank at most 11. It follows that $J(\mathbb{Q})$ must be of rank 0.

We do not expect that results along these lines can be extended much further. To complement the above computations, assuming that the Birch and Swinnerton-Dyer conjecture (BSD) holds for the Jacobians of our curves, we computed the analytic rank of the Jacobian and the analytic order of $Ш(J)$. For this we had to assume that the L-series $L(C, s)$ can be analytically continued and satisfies the usual functional equation.

The results of our computations are consistent with this assumption. First of all, we verified that the rth derivative of $L(C, s)$ at $s = 1$ is nonzero, where r is the conjectured rank of $J(\mathbb{Q})$ (i.e., the number of independent points we have found). Secondly, the analytic order of $Ш(J)$ comes out to be 16 for the 42 curves for which we expect elements of order 4, and it is 4 for the 5 curves mentioned above, where we expect $Ш(J) = (\mathbb{Z}/2\mathbb{Z})^2$. Hence, assuming standard conjectures on L-series and the Birch and Swinnerton-Dyer conjecture, we find that $\mathrm{Pic}^1_C(\mathbb{Q}) = \varnothing$ for our 42 curves, and therefore $C(\mathbb{Q}) = \varnothing$ as well. See Tables 1 and 2 for a summary of our findings.

All curves	196 171	100.00%
Curves with rational points	137 490	70.09%
Curves without rational points	58 681	29.91%
ELS curves total	166 768	85.01%
ELS curves without rational points	29 278	14.92%
Curves with ELS 2-covers among these	1 492	0.76%
Curves that need GRH or BSD	42	0.02%

TABLE 1. Curve statistics (ELS = everywhere locally solvable).

conj. $Ш(J)$	0	$(\mathbb{Z}/2\mathbb{Z})^2$	$(\mathbb{Z}/4\mathbb{Z})^2$	Total
rank $J(\mathbb{Q}) = 0$	3		36	39
rank $J(\mathbb{Q}) = 1$	516	5	5	526
rank $J(\mathbb{Q}) = 2$	772		1	773
rank $J(\mathbb{Q}) = 3$	152			152
rank $J(\mathbb{Q}) = 4$	2			2
all ranks	1445	5	42	1492

TABLE 2. Ranks and conjectural Ш for the curves surviving 2-cover descent.

2.1 Discussion

The main result of our experiment is that we were successful in deciding the existence of rational points unconditionally for all but 42 of our curves. If we assume standard conjectures, we can prove that there are no rational points on these remaining 42 curves as well.

Let us explain these statements in more detail. If we find a rational point on one of the curves, we are obviously done, and the result can easily be verified. If a curve turns out not to have real points, or not to have p-adic points for some specific prime p, this can also easily be verified. For the 2-cover descent procedure, we have to compute the class group of (in general) a sextic number field. A distinctive feature of MAGMA is that by default, it computes this information *unconditionally*; this is different from the behavior of PARI, which by default uses a heuristic assumption that is even stronger than the generalized Riemann hypothesis. So, assuming that our hardware was working correctly and the implementation is correct, the results of the 2-cover descent computations are unconditional as well. The same applies to the computation of the rank bound by 2-descent on the Jacobian; this uses essentially the same information. If we find rational points on the Jacobian, we can compute the rank of the subgroup they generate and check that this subgroup is saturated, using the canonical height on the Jacobian. If this rank reaches the upper bound, this verifies that we have found generators of the Mordell–Weil group. In this case, the Mordell–Weil sieve computation, if successful, will prove that the curve has no rational points.

When the rank bound is not reached, we try to get a better bound. One approach is to visualize elements of the 2-torsion in the Shafarevich–Tate group. For this, we need to compute the class group of a number field of degree 12. For the small coefficient sizes we are using, this can still be done unconditionally, and was successful for 5 curves.

For 42 curves, we expect 4-torsion elements in the Shafarevich–Tate group. In these cases, to reduce the upper bound for the rank by visualization requires the computation of class groups in number fields of degree 24, which is beyond current technology. Therefore, we had to assume some standard conjectures (Birch and Swinnerton-Dyer, analytic continuation and functional equation of the L-function) in order to get the required result. However, it should be possible in principle (and very likely at some point also in practice) to remove this dependence on conjectures by actually performing the

computations in these big number fields. We have done so successfully in a few cases, assuming the generalized Riemann hypothesis in order to speed up the class group computation.

To what extent does our result provide evidence that existence of rational points on curves of genus 2 should be decidable in general? It can be argued (and this point was raised by both referees) that our curves are "too small" to allow such conclusions. It is probably true that with our set of curves, we do not yet reach the "typical" regime (rational points abound, and only few curves remain unresolved after the 2-cover descent). So it was suggested that to work on a random sample of 200 000 larger curves would (if successful) provide more convincing evidence. But against this, one can argue that counterexamples may be extremely rare and of a special kind, so that they are unlikely to show up in such a random sample. We see the strength of our result in its *completeness*: we have looked at each and every curve in our "box" and dealt successfully with it. It is this completeness that we think justifies the claim that our experiment does indeed give strong evidence in favor of a positive answer to Question 1.1.

Let us discuss the prospects of actually performing a similar experiment on a large random sample of larger curves. Some preliminary computations indicate that the fraction of curves that remain unresolved after the 2-cover descent grows slowly with the size of the coefficients; it reaches ca. 14% for coefficients bounded by 100. See [Bruin and Stoll 08a] for more information. The 2-cover descent requires the computation of the class group of the sextic number field given by the defining polynomial of the curve. This is still possible unconditionally for coefficient sizes of about 20, but is already quite time-consuming.

For even larger curves, one would have to assume GRH in order to keep the computations feasible. The 2-descent on the Jacobians of the remaining curves uses the same information. The next obstacle here is the search for generators of the Mordell–Weil group, since they can be very large and may be impossible to find with current methods. There are some very large ones even on our "small" Jacobians.

The other problem is that the 2-Selmer group may not provide a sharp bound on the rank, and so one needs to use visualization or other methods in order to improve it. Visualization becomes impractical soon, since it requires computations with number fields of degree 12 or 24, and application of the Birch–Swinnerton-Dyer conjecture will also become infeasible quickly, since the conductors of the curves will be too large to allow the computation of sufficiently many coefficients of the L-series. The Mordell–Weil sieve computation itself seems to work quite reliably on curves of rank up to 4; higher ranks may be problematic.

Note that all these problems are of a practical nature; given sufficient computing power and time, we should be able to overcome them. We hope to be able to perform such computations with larger curves in the future.

Moreover, our results also provide evidence for the conjecture that the Brauer–Manin obstruction should be the only obstruction against rational points on curves. For all but the 1492 curves surviving a 2-cover descent, we verify this unconditionally. For the remaining curves, we need to assume that $Ш(J)$ has trivial divisible subgroup, plus whatever assumptions were necessary in addition for individual curves. See [Scharaschkin 99, Flynn 04, Stoll 07] for details on how our computations relate to the Brauer–Manin obstruction.

A complete list of all curves considered and indications on how to prove that each curve does or does not have rational points are available at [Bruin and Stoll 06]. The file `AllCurves.m` lists all the curves, represented by the polynomial f and ordered according to isomorphism classes. The first polynomial listed in each class is taken as a representative for the class. The file `Solvable.m` gives the curves that have rational points. In the file `LocalObstruction.m`, we list the curves that fail to have a point over $\mathbb{R}$ or over $\mathbb{Q}_p$ for some prime p. The file `DescentObstruction.m` contains the curves that have points everywhere locally, but can be shown not to have rational points by a 2-cover descent. The files `MWSieve-rankr.m`, where $r \in \{0, 1, 2, 3, 4\}$, list the curves with Jacobian of Mordell–Weil rank r that were proved not to have rational points by a Mordell–Weil sieve computation. We also provide data that should make it fairly easy to check the computations. Finally, the file `BSD-data.txt` gives some information related to the computation of the analytic order of Ш, which we performed for some of the curves.

3. METHODS

In this section, we give an overview of the methods we have used. Detailed descriptions will be provided in [Bruin and Stoll 08a, Bruin and Stoll 08b, Bruin and Stoll 08c].

3.1 2-Cover Descent

Let the curve C be given by the equation $y^2 = f(x)$, and let L denote the étale $\mathbb{Q}$-algebra $\mathbb{Q}[T]/(f(T))$. We let θ

be the image of T in L. If f has a rational root or is of odd degree, then C has a rational point. Therefore, we can assume in the following that f is of degree 6 and has no rational roots. Let a be the leading coefficient of f. Let $k = \mathbb{Q}$ or $k = \mathbb{Q}_v$, where v is a prime p or ∞ and $\mathbb{Q}_\infty = \mathbb{R}$. We have a map

$$F : C(k) \longrightarrow \frac{(L \otimes_{\mathbb{Q}} k)^*}{k^*(L \otimes_{\mathbb{Q}} k)^{*2}}\,,$$
$$P = (x, y) \longmapsto (x - \theta) \cdot k^*(L \otimes_{\mathbb{Q}} k)^{*2}\,,$$

whose image is contained in the subset of elements whose norm in k^*/k^{*2} is the class of a. Note that $y^2 = f(x) = aN_{L\otimes k/k}(x - \theta)$.

As in the case of 2-descent on the Jacobian J of C, one shows that $F(C(\mathbb{Q}_p))$ is contained in the image of the p-adic units for all odd p not dividing a or the discriminant of f (see [Stoll 01]). Let $H' \subset L^*/\mathbb{Q}^*L^{*2}$ be the (finite) group of elements that come from p-adic units for this set of primes, and let $H \subset H'$ be the subset of elements whose norm is $a\mathbb{Q}^{*2}$; then $F(C(\mathbb{Q})) \subset H$. There are cases in which H is already the empty set; we can then immediately conclude that $C(\mathbb{Q}) = \varnothing$. An example of this is

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

For this curve it can be checked that $2\mathbb{Q}^{*2}$ is not the norm of an element of H'.

We denote $L\otimes_{\mathbb{Q}}\mathbb{Q}_v$ by L_v. Let $H_v \subset L_v^*/\mathbb{Q}_v^*L_v^{*2}$ denote the subset of elements whose norm is $a\mathbb{Q}_v^{*2}$. We have the following commutative diagram:

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{F} & H \\ \downarrow & & \downarrow \rho \\ \prod_{v\in S} C(\mathbb{Q}_v) & \xrightarrow{F} & \prod_{v\in S} H_v \end{array}$$

Here, S is a suitable finite set of places. One can show that $F(C(\mathbb{Q}_p)) = H_p$ for $p > 1154$ if p does not divide $\mathrm{disc}(f)$. Therefore, we obtain the maximal amount of information when we choose

$$S = \{\infty\} \cup \{p : p < 1154\} \cup \{p : p \mid \mathrm{disc}(f)\}\,.$$

Note that the sets H_v are finite and that F is v-adically continuous, hence locally constant. Therefore we can compute $F(C(\mathbb{Q}_v)) \subset H_v$ explicitly for every v. Following [Poonen and Schaefer 97], we define the *fake* 2-*Selmer set* of C, $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(C)$, to be the preimage in H under ρ of the image of the lower F map. Then F maps $C(\mathbb{Q})$ into $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(C)$, and hence if $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(C) = \varnothing$, then we know that $C(\mathbb{Q})$ is empty as well.

The geometric interpretation of the elements of $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(C)$ is that they correspond to everywhere locally solvable 2-covering curves of C. If $\xi \in L$ represents an element of $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(C)$, then the corresponding covering $D_\xi \to C$ can be obtained as follows. We write $z = z_0 + z_1\theta + \cdots + z_5\theta^5$ for a generic element of L. The condition for a rational point $P = (x, y)$ on C to be in the image of $D_\xi(\mathbb{Q})$ is that

$$(x - \theta) \cdot \mathbb{Q}^*L^{*2} = F(P) = \xi \cdot \mathbb{Q}^*L^{*2}\,.$$

So $x - \theta = c\xi z^2$ for some $c \in \mathbb{Q}$, $z \in L$.

Expanding the right-hand side in terms of powers of θ, we obtain four quadrics in the six variables $z_0, \ldots, z_5$ that express the condition that the coefficients of $\theta^2, \ldots, \theta^5$ have to vanish. These four quadrics define the curve $D_\xi \subset \mathbb{P}^5$ of degree 16 and genus 17. To obtain the covering map, note that x can be recovered from the coefficients of 1 and θ in ξz^2, and y can be recovered from these, the norm of z, and a square root of $N(\xi)/a$. One has to make a sign choice here, so that there are really two different covering maps in most cases. See also [Bruin 02, 5.3] and [Bruin and Flynn 05] for a description of the cover. For details on how to compute $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(C)$ efficiently, see [Bruin and Stoll 08a].

3.2 Finding Generators

Since the simplest generally available projective model of the Jacobian J is given by 72 quadrics in $\mathbb{P}^{15}$ [Cassels and Flynn 96], it is usually not a good idea to search for rational points directly on J. A better alternative is to consider the Kummer surface $K = J/\{\pm 1\}$, which sits naturally as a quartic surface in $\mathbb{P}^3$. We now can search for rational points on K that lift to rational points on J. A fairly efficient implementation of this idea that uses mod-p information for several primes p in order to rule out many candidates is obtainable as `j-points` from M. Stoll's homepage; this program is also incorporated in MAGMA. This approach is feasible for points of naive (nonlogarithmic) height around 10 000 or a little bit more, where the height is that of the image point on $K \subset \mathbb{P}^3$.

However, there are many cases in our list for which there is a much bigger generator. In order to find these, we use the idea (by now in common use in the context of elliptic curves) that rational points on J lift to usually much smaller rational points on a 2-covering of J. Therefore we attempt to search for rational points on these 2-coverings. However, these coverings are as complicated

geometrically as J itself, and therefore we consider a suitable quotient again.

Recall [Poonen and Schaefer 97, Stoll 01] that the fake 2-Selmer group of J is a finite subgroup of $L^*/\mathbb{Q}^*L^{*2}$. It contains the image of $J(\mathbb{Q})$ under a map that sends a rational point P to an element represented by $x_0 - x_1\theta + \theta^2 \in L$, for certain $x_0, x_1 \in \mathbb{Q}$ depending on P. Let ξ be an element of the fake Selmer group. We use the same idea as in the previous section to construct a surface K_ξ: we are looking for $z \in L$ such that ξz^2 does not involve $\theta^3, \theta^4, \theta^5$. This gives us an intersection K_ξ of three quadrics in $\mathbb{P}^5$. We simplify the defining equations as far as possible by a change of projective coordinates so that they have small coefficients. Then we perform a search for rational points on K_ξ using a p-adic variant of Elkies' lattice-based point-searching techniques [Elkies 00]. For each point found, we check whether it corresponds to a rational point on J. In this way, we can find points in $J(\mathbb{Q})$ whose image in the fake Selmer group is nontrivial.

However, note that Pic^1_C is a 2-covering of J via the map $D \mapsto 2D - W$, where $D \in \mathrm{Pic}^1_C$ and W is the canonical class. Its image in the fake Selmer group is trivial, so the method above will not help in finding rational points on it. Instead, in analogy to the use of the Kummer surface in searching for points on J, we can use the dual Kummer surface [Cassels and Flynn 96, Chapter 4]. We can even go a step further and consider 2-coverings of Pic^1_C. In this case, we obtain 3-dimensional varieties, given as intersections of two quadrics in $\mathbb{P}^5$, that are quotients of $\mathbb{P}^1$-bundles over the coverings we are interested in. We can search for rational points on these 3-folds and check whether they give rise to a rational point on J. This amounts to a partial explicit 4-descent on J. It is therefore perhaps not surprising that we were able to find some quite large generators in this way. The record example is

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

with $J(\mathbb{Q})$ infinite cyclic generated by $P_1 + P_2 - W$, where the x-coordinates of P_1 and P_2 are the roots of

$$x^2 + \frac{3748292549806582007887836624845730062 3}{3401104981181664738414149248771752424 3}\,x + \frac{5814526282808243066989265616183939670 33}{5441767969890663581462638798034803878 88}\,;$$

the canonical logarithmic height of this generator is 95.26287. The second-largest example is

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

with $J(\mathbb{Q})$ generated by a point coming from

$$x^2 + \frac{836283543413625628607991530 63}{267798119543522958491436140 59}\,x + \frac{852972547276507286513269157689}{321357743452227550189723368708}\,.$$

The canonical height of this generator is 77.33265. For details, see [Bruin and Stoll 08b].

3.3 Mordell–Weil Sieve

As mentioned in Section 2, we consider the commutative diagram

$$\begin{array}{ccc} C(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q}) \\ \downarrow & & \downarrow{\scriptstyle \alpha} \\ \prod_{p\in S} C(\mathbb{F}_p) & \xrightarrow{\beta} & \prod_{p\in S} J(\mathbb{F}_p) \end{array}$$

with a suitable finite set S of (good) primes. In some cases, it can be helpful to use some more general finite quotient of $J(\mathbb{Q}_p)$ instead of $J(\mathbb{F}_p)$, for example to make use of information modulo higher powers of p, or also in order to use information at primes of bad reduction. In the following discussion, we will assume for simplicity that we are working with $J(\mathbb{F}_p)$.

Our goal is to prove that the images of α and β above do not meet for some set S, which implies that $C(\mathbb{Q}) = \varnothing$. This approach was (to our knowledge) first suggested by Scharaschkin [Scharaschkin 99, Scharaschkin 98]. Flynn [Flynn 04] used it for more extensive calculations. We would like to mention here that in the course of improving the algorithms, we were able to prove all the curves marked "Unresolved" in the tables of [Flynn 04] to have no rational points. All but five of these already succumb to a 2-cover descent, while the remaining five, all of which have Jacobians of Mordell–Weil rank 3, can be dealt with using our Mordell–Weil sieve implementation.

The basic algorithmic problem one has in this computation is that the product of the $J(\mathbb{F}_p)$ can be a very large group. One approach to keeping the combinatorics in check is to work with $J(\mathbb{Q})/BJ(\mathbb{Q})$ and $\prod_p J(\mathbb{F}_p)/BJ(\mathbb{F}_p)$ for a suitable choice of B. In practice, we compute the subset of $J(\mathbb{Q})/BJ(\mathbb{Q})$ that maps under α into the image of β. We first need to choose a promising set S of primes. Since we can hope to arrive at a contradiction only when the group orders of the $J(\mathbb{F}_p)$ have (preferably large) common factors, we select those primes p for which the order of $J(\mathbb{F}_p)$ is sufficiently smooth. We then compute the image of $C(\mathbb{F}_p)$ in $J(\mathbb{F}_p)$ and the image of the generators of $J(\mathbb{Q})$. Note that this involves a discrete logarithm computation in $J(\mathbb{F}_p)$ for each point in $C(\mathbb{F}_p)$ and each generator of $J(\mathbb{Q})$. While

this is a hard problem in general, it is harmless here, since the group order is smooth and we can reduce to several discrete logs in small groups.

In the following discussion, the set S is fixed. For a given B, we can find the image $C_{B,p}$ of $C(\mathbb{F}_p)$ in $J(\mathbb{F}_p)/BJ(\mathbb{F}_p)$, and we can then compute the expected size

$$n(B) = \#\big(J(\mathbb{Q})/BJ(\mathbb{Q})\big) \prod_{p\in S} \frac{\#C_{B,p}}{\#\big(J(\mathbb{F}_p)/BJ(\mathbb{F}_p)\big)}$$

of the subset $A(B)$ of $J(\mathbb{Q})/BJ(\mathbb{Q})$ that maps into these images for all $p \in S$. We now search for a sequence $1 = B_0, B_1, \ldots, B_m$ such that $B_{j+1} = B_j q_j$ for some prime q_j, such that $n(B_m) \ll 1$, and such that $\max_j n(B_j)$ is not too large. (See [Poonen 05] for heuristics on why there should exist B with $n(B) \ll 1$, at least when S is sufficiently large.)

After we have fixed our sequence (B_j), we successively compute the sets $A(B_j)$ for $j = 1, 2, \ldots$ until $A(B_j) = \varnothing$. If we reach $j = m$ and $A(B_m) \neq \varnothing$, then we can check whether this is caused by an exhibitable rational point. The set $A(B_m)$ will give a very good indication of which elements of $J(\mathbb{Q})$ could give rise to such a point. If we cannot find a point, we can extend the sequence or choose a bigger set S. This situation never occurred in our computations, however.

To obtain $A(B_{j+1})$ from $A(B_j)$, we run through the elements of $A(B_j)$. For each element, we run through its possible lifts to $J(\mathbb{Q})/B_{j+1}J(\mathbb{Q})$, and check for each lift whether it maps into the image of C mod p for all relevant p (i.e., such that the largest power of q_{j+1} dividing B_{j+1} also divides the exponent of $J(\mathbb{F}_p)$). The largest set $A(B_j)$ that we encountered in our computations had a size of about 10^6. It is perhaps worth mentioning that the estimate $n(B)$ for $\#A(B)$ was in most cases accurate up to a factor of 2 to 5, so that a value $n(B_m) < 10^{-3}$ (say) virtually guarantees success in practice. For details see [Bruin and Stoll 08c].

3.4 BSD Computations

Finally, let us give some indications of how to compute the analytic order of Ш. Dokchitser [Dokchitser 04] describes how the numbers $L^{(r)}(C,1)$ can be computed numerically, given (i) the coefficients a_n of the L-series for sufficiently many n, (ii) the conductor N of C (or J), and (iii) the sign ε in the (conjectured) functional equation. The last of these is determined by the parity of the rank.

The coefficients a_p and a_{p^2} for good primes p can be computed by counting the points in $C(\mathbb{F}_p)$ and $C(\mathbb{F}_{p^2})$; these coefficients then determine a_{p^k} for all $k \geq 1$. For bad primes p, the coefficients can be deduced from a minimal proper regular model of C over $\mathbb{Z}_p$; a description of the computation of such a model can be found in [Flynn et al. 01]. The most frequent case is that an odd prime p divides the discriminant of the polynomial f just once; then

$$f(x) \equiv (x-a)^2 g(x) \bmod p\,,$$

and the Euler factor at p of $L(C,s)$ depends on whether $g(a)$ is a square and on the number of $\mathbb{F}_p$-points on the genus-1 curve $y^2 = g(x)$. In most other cases, the original model is already regular. For all of the curves, we computed $5 \cdot 10^5$ or even 10^6 coefficients; this led to an error in the value of $\#Ш(J)$ predicted by the Birch and Swinnerton-Dyer conjecture of less than 10^{-3} in all cases.

We can find the odd part of the conductor N using Q. Liu's `genus2reduction` program [Liu 94b], based on [Liu 94a]. If the given model of the curve is regular at 2, then the power of 2 dividing N is that dividing the discriminant of C. Otherwise, we use the approach described in [Dokchitser 04, Section 7] to determine the right power of 2 (which is then less than that in the discriminant). We can then verify the functional equation for the inverse Mellin transform of $L(C,s)$ numerically, thus corroborating our computations.

Given the value of $L^{(r)}(C,1)$, we compute the analytic order of Ш by solving the conjectural equality between $L^{(r)}(C,1)/r!$ and a combination of invariants of C and J for $\#Ш$. See [Flynn et al. 01] for how to compute the other invariants. As already mentioned, the values we obtain were always close to an integer, which was 4 in the five cases in which we expect $Ш(J) \cong (\mathbb{Z}/2\mathbb{Z})^2$ and 16 in the remaining cases, where we expect $Ш(J) \cong (\mathbb{Z}/4\mathbb{Z})^2$.

ACKNOWLEDGMENTS

We would like to thank Victor Flynn and Bjorn Poonen for useful discussions related to our project. Michael Stoll thanks the Computational Laboratory for Analysis, Modeling and Visualization (CLAMV) of the Jacobs University Bremen for computing time on the CLAMV Teaching Lab machines. This was used for substantial parts of the computations that were done in the course of this project. For the computations, the MAGMA system was used.

Nils Bruin's research was supported by NSERC.

REFERENCES

[Bruin 02] N. Bruin. *Chabauty Methods and Covering Techniques Applied to Generalized Fermat Equations*, CWI Tract 133. Amsterdam: Stichting Mathematisch Centrum voor Wiskunde en Informatica, 2002.

[Bruin 04] N. Bruin. "Visualisation of Sha[2] in Abelian Surfaces." *Math. Comp.* 73:247 (2004), 1459–1476.

[Bruin and Flynn 05] N. Bruin and E. V. Flynn. "Towers of 2-Covers of Hyperelliptic Curves." *Trans. Amer. Math. Soc.* 357 (2005), 4329–4347.

[Bruin and Flynn 06] N. Bruin and E. V. Flynn. "Exhibiting Sha[2] on Hyperelliptic Jacobians. *Journal of Number Theory* 118 (2006), 266–291.

[Bruin and Stoll 06] N. Bruin and M. Stoll. Electronic data, available online (http://www.cecm.sfu.ca/~nbruin/smallgenus2curves/).

[Bruin and Stoll 08a] N. Bruin and M. Stoll. "2-Cover Descent on Hyperelliptic Curves." ArXiv:0803.2052v1, 2008.

[Bruin and Stoll 08b] N. Bruin and M. Stoll. "Finding Mordell–Weil Generators on Genus-2 Jacobians. In preparation, 2008.

[Bruin and Stoll 08c] N. Bruin and M. Stoll. "The Mordell–Weil Sieve: Proving Nonexistence of Rational Points on Curves." In preparation, 2008.

[Cassels and Flynn 96] J. W. S. Cassels and E. V. Flynn. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*. Cambridge: Cambridge University Press, 1996.

[Dokchitser 04] T. Dokchitser. "Computing Special Values of Motivic L-Functions." *Experiment. Math.* 13:2 (2004), 137–149.

[Elkies 00] N. D. Elkies. "Rational Points near Curves and Small Nonzero $|x^3 - y^2|$ via Lattice Reduction. In *Algorithmic Number Theory (Leiden, 2000)*, edited by W. Bosma, pp. 33–63, Lecture Notes in Comput. Sci. 1838. Berlin: Springer, 2000.

[Flynn 04] E. V. Flynn. "The Hasse Principle and the Brauer–Manin Obstruction for Curves." *Manuscripta Math.* 115 (2004), 437–466.

[Flynn et al. 01] E. V. Flynn, F. Leprévost, E. F. Schaefer, W. A. Stein, M. Stoll, and J. L. Wetherell. "Empirical Evidence for the Birch and Swinnerton-Dyer Conjectures for Modular Jacobians of Genus 2 Curves." *Math. Comp.* 70 (2001), 1675–1697.

[Liu 94a] Q. Liu. "Conducteur et discriminant minimal de courbes de genre 2." *Compositio Math.* 94 (1994), 51–79.

[Liu 94b] Q. Liu. `genus2reduction`. Computer program, available online (http://www.math.u-bordeaux.fr/~liu/G2R/).

[Magma 1997] MAGMA is described in W. Bosma, J. Cannon and C. Playoust: *The Magma Algebra System I: The User Language*, *J. Symb. Comp.* 24 (1997), 235–265. (Also see the Magma home page at http://www.maths.usyd.edu.au:8000/u/magma/ .)

[Poonen 05] B. Poonen. "Heuristics for the Brauer–Manin Obstruction for Curves." *Experiment. Math.* 15 (2006), 415–420.

[Poonen and Schaefer 97] B. Poonen and E. F. Schaefer. "Explicit Descent for Jacobians of Cyclic Covers of the Projective Line." *J. Reine Angew. Math.* 488 (1997), 141–188.

[Poonen and Stoll 99a] B. Poonen and M. Stoll. "The Cassels–Tate Pairing on Principally Polarized Abelian Varieties." *Ann. of Math. (2)* 150 (1999), 1109–1149.

[Poonen and Stoll 99b] B. Poonen and M. Stoll. "A Local–Global Principle for Densities." In *Topics in Number Theory. In Honor of B. Gordon and S. Chowla*, edited by Scott D. Ahlgren et al., pp. 241–244, Math. Appl. Dordr. 467. Dordrecht: Kluwer Academic Publishers, 1999.

[Scharaschkin 98] V. Scharaschkin. "The Brauer–Manin Obstruction for Curves." Manuscript, 1998.

[Scharaschkin 99] V. Scharaschkin. "Local–Global Problems and the Brauer–Manin Obstruction." PhD thesis, University of Michigan, 1999.

[Stoll 01] M. Stoll. "Implementing 2-Descent on Jacobians of Hyperelliptic Curves." *Acta Arith.* 98 (2001), 245–277.

[Stoll 02] M. Stoll. "On the Height Constant for Curves of Genus Two, II." *Acta Arith.* 104 (2002), 165–182.

[Stoll 05] M. Stoll, "Finite Coverings and Rational Points." Oberwolfach Report 32/2005, 2005.

[Stoll 07] M. Stoll. "Finite Descent Obstructions and Rational Points on Curves." *Algebra and Number Theory* 1 (2007), 349–391.

Nils Bruin, Department of Mathematics, Simon Fraser University, Burnaby, BC, Canada V5A 1S6 (nbruin@cecm.sfu.ca)

Michael Stoll, School of Engineering and Science, Jacobs University Bremen, Campus Ring 1, 28759 Bremen, Germany (m.stoll@jacobs-university.de)

Received June 15, 2006; accepted in revised form, April 18, 2007.