On powers as sums of two cubes

Nils Bruin*

March 24, 2000

Abstract

In a paper of Kraus, it is proved that $x^3 + y^3 = z^p$ for $p \geq 17$ has only trivial primitive solutions, provided that p satisfies a relatively mild and easily tested condition. In this article we prove that the primitive solutions of $x^3 + y^3 = z^p$ with $p = 4, 5, 7, 11, 13$, correspond to rational points on hyperelliptic curves with Jacobians of relatively small rank. Consequently, Chabauty methods may be applied to try to find all rational points. We do this for $p = 4, 5$, thus proving that $x^3 + y^3 = z^4$ and $x^3 + y^3 = z^5$ have only trivial primitive solutions. In the process we meet a Jacobian of a curve that has more 6-torsion at any prime of good reduction than it has globally. Furthermore, some pointers are given to computational aids for applying Chabauty methods.

1 Introduction

In this paper we consider for given $p = 2, 3, \ldots$ the Diophantine equation

$$x^3 + y^3 = z^p,\ x, y, z \in \mathbb{Z},\ \gcd(x, y, z) = 1. \tag{1}$$

To emphasise that we look at solutions with $\gcd(x, y, z) = 1$, we refer to such solutions as *primitive solutions*.

First, we review what is known. This equation is a special case of the generalised Fermat equation $x^r + y^s = z^t$. For fixed exponent triples r, s, t, a theorem of Darmon and Granville (see [8]) gives a classification of what the solution set looks like. If we apply their result to our equation, we get that for each $p \geq 4$, $x^3 + y^3 = z^p$ has only finitely many primitive solutions. If we assume the ABC-conjecture (see [23]), then we even get that for p big enough, $x^3 + y^3 = z^p$ only has the trivial primitive solutions, i.e. with $xyz = 0$. This has led (together with the lack of counterexamples) to the very bold conjecture

Conjecture 1 (Tijdeman, Zagier, Beal Prize Problem) *Let x, y, z, r, s, t be positive integers with $r, s, t > 2$. If $x^r + y^s = z^t$ then x, y, z have a factor in common.*

*funded by NWO grant "Groot project getaltheorie".

which even has a reward attached to its resolution (see [13]).

For $p = 2$, the result by Darmon and Granville does not give information. In fact, there are infinitely many primitive solutions to $x^3 + y^3 = z^2$. A paper by Beukers (see [2]) guarantees that these solutions can be finitely parametrised. That means that one can give a finite number of polynomial solutions to $x^3 + y^3 = z^2$ such that each primitive solution can be obtained from one of the polynomial solutions by specialisation. In Lemma 1 we give these parametrisations.

For $p = 3$, the Darmon and Granville result is also inconclusive. However, Euler and maybe even Fermat already proved that the equation $x^3 + y^3 = z^3$ has only trivial rational solutions.

For $p \geq 4$, Darmon and Granville predict that there are only finitely many primitive solutions and it is generally believed that they are all trivial. Once we verify this for $p = 4$, it suffices to prove triviality only for prime p, since any composite $p \geq 4$ is either divisible by 4 or by a prime number≥ 3. This justifies that the exponent is tendenciously designated by p, hinting at primality. In this light, one may consider 4 as a composite number with primal tendencies.

For $17 \leq p < 10000$, Kraus (see [12]) has proved that there are no nontrivial primitive solutions, assuming the Taniyama-Weil conjecture that is now considered proved by many. His proof resembles Frey's and Ribet's construction of a nonmodular elliptic curve assuming the existence of a nontrivial solution. For this, however, he needs the existence of a prime number with certain properties. While it seems plausible that such a prime exists for any p, Kraus failed at proving so. Therefore, he checked the condition for all prime numbers in the given range individually.

It is the purpose of this paper to sketch how the cases with $p < 17$ can be dealt with and carry out the procedure in a couple of cases. We will prove

Theorem 1 *Integer solutions to $x^3 + y^3 = z^4$ with $xyz \neq 0$ have* $\gcd(x, y, z) > 1$.

Theorem 2 *Integer solutions to $x^3 + y^3 = z^5$ with $xyz \neq 0$ have* $\gcd(x, y, z) > 1$.

Alternatively, one may try to extend the method of Kraus to smaller p. In his paper, he assumes there is a nontrivial solution and constructs a non-CM elliptic curve from it. He then analyses the Galois-representation on the p torsion and concludes it is not modular. One step consists of showing that the representation should be irreducible. Since the curve constructed by Kraus has a rational 2-torsion point, the curve would correspond to a rational point on the modular curve $X_0(2p)$ if the representation were reducible. Following [9], such curves are either singular or CM for prime $p \geq 7$. The curve $X_0(10)$, however, has genus 0 and has infinitely many rational points. It may be possible to prove irreducibility in this case using other arguments, however. Although the details are not (yet) available in the literature, it seems doable to extend Kraus's methods to $p = 5, 7, 11, 13$ (see [11]). The number 4 still has enough composite features to completely break down Kraus's method for $p = 4$, however.

2 Parametrising curves; Chabauty methods

If we use the word *curve*, we mean a smooth projective geometrically irreducible variety of dimension 1. We will often work with singular, planar models of these curves. Some of these models will have singularities at their unique point at infinity. If the smooth curve has only one point there, we will refer to that as ∞ and if it has two, we call them ∞^+ and ∞^- (arbitrarily but fixed).

In this section, we will construct hyperelliptic curves over $\mathbb{Q}$ such that a primitive solution of $x^3 + y^3 = z^p$ corresponds to a rational point on one of the curves. Furthermore, we will give an estimate for the Mordell-Weil rank of the Jacobians of these curves and sketch how one may proceed in finding all rational points on these curves. The sketched method is not an algorithm, but in practice these methods often work.

Suppose that we have $x, y, z \in \mathbb{Z}$ with $\gcd(x, y, z) = 1$ and $x^3 + y^3 = z^p$. Note that $\gcd(x + y, x^2 - xy + y^2) \mid 3$ (an elementary resultant computation). Therefore, we have $t \in \{-1, 0, 1\}$ and $z_1, z_2 \in \mathbb{Q}$ such that

$$\begin{aligned} x + y &= 3^t z_1^p, \\ x^2 - xy + y^2 &= 3^{-t} z_2^p, \\ z &= z_1 z_2. \end{aligned}$$

We solve for y in the first equation and substitute the value in the second equation and divide by z_1^{2p}. This gives an equation that is of degree p in $\frac{z_2}{z_1^2}$ and quadratic in $\frac{x}{z_1^p}$. For each solution and given t, this gives us a rational point on a fixed curve $\mathcal{C}_{p,t}$ in the following way.

t	X	Y	$\mathcal{C}_{p,t}$	$A_{p,t}$
-1	$\frac{z_2}{z_1^2}$	$54\frac{x}{z_1^p} + 9$	$Y^2 = 324X^p - 3$	$-2^{2p-2}3^{2p-3}$
0	$\frac{z_2}{z_1^2}$	$6\frac{x}{z_1^p} + 3$	$Y^2 = 12X^p - 3$	$-2^{2p-2}3^p$
1	$\frac{z_2}{z_1^2}$	$6\frac{x}{z_1^p} + 9$	$Y^2 = 4X^p - 27$	$-2^{2p-2}3^3$

For odd $p \geq 5$, the curves $\mathcal{C}_{p,t}$ are of genus $(p-1)/2$ and also have a model of the form $Y^2 = X^p + A_{p,t}$. By Faltings' theorem, we have that the number of rational points on a curve of genus ≥ 2 is finite. Finding those points or, if you have them, proving that the list of points is complete, is a different matter. Faltings' proof is not constructive, so it is of little help.

There is an earlier, partial proof by Chabauty (see [6]) that uses a construction that, if adapted in a proper way, might yield sharp bounds on the number of points. Suppose we have a (smooth) curve $\mathcal{C}$ of genus g over $\mathbb{Q}$ that has a known rational point $P_0 \in \mathcal{C}(\mathbb{Q})$.

The *Jacobian variety* of $\mathcal{C}$ is an abelian variety $\mathcal{J}$ over $\mathbb{Q}$ of dimension g. That means that it is a complete variety with a point $O \in \mathcal{J}(\mathbb{Q})$ together with a morphism $\mathcal{J} \times \mathcal{J} \to \mathcal{J}$ over $\mathbb{Q}$ that defines a group operation on the points of $\mathcal{J}$ with O as a neutral element. The points of $\mathcal{J}$ coincide with the degree 0 divisor classes $\mathrm{Pic}^0(\mathcal{C})$ and the fact that $\mathcal{C}(\mathbb{Q}) \neq \emptyset$

guarantees that $\mathcal{J}(\mathbb{Q}) \simeq \mathrm{Pic}^0(\mathcal{C})(\mathbb{Q})$, i.e. the group of degree 0 divisors over $\mathbb{Q}$ modulo linear equivalence.

Also, the map $P \mapsto [P - P_0]$ gives an injective morphism $\mathcal{C} \to \mathcal{J}$ over $\mathbb{Q}$. Therefore, we can consider $\mathcal{C}$ as a subvariety of $\mathcal{J}$ over $\mathbb{Q}$. As such, we have $\mathcal{C}(\mathbb{Q}) \subset \mathcal{J}(\mathbb{Q})$. Chabauty's method applies to any curve in an abelian variety, so for the sequel it is sufficient to consider $\mathcal{J}$ an abelian variety of dimension g over $\mathbb{Q}$ with a curve $\mathcal{C}$ as a subvariety over $\mathbb{Q}$.

The set of rational points $\mathcal{J}(\mathbb{Q})$ forms a finitely generated abelian group, the Mordell-Weil group. Therefore, there exist an $r \in \mathbb{Z}_{\geq 0}$ and a finite group T such that $\mathcal{J}(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus T$. The number r is called the rank of $\mathcal{J}(\mathbb{Q})$.

Let p be a rational prime. Then $\mathcal{J}(\mathbb{Q}_p)$ is a g-dimensional p-adic analytic abelian Lie-group. Such groups are locally isomorphic to $(\mathbb{Z}_p)^g$. The topological closure of a finitely generated subgroup of rank r in such a variety will be of dimension $\leq r$. Therefore, if the Mordell-Weil rank r of $\mathcal{J}(\mathbb{Q})$ is smaller than g, then the topological closure $\overline{\mathcal{J}(\mathbb{Q})}$ of the Mordell-Weil group will be a proper analytic subvariety of $\mathcal{J}(\mathbb{Q}_p)$. Since both $\mathcal{C}(\mathbb{Q}) \subset \mathcal{J}(\mathbb{Q})$ and $\mathcal{C}(\mathbb{Q}) \subset \mathcal{C}(\mathbb{Q}_p) \subset \mathcal{J}(\mathbb{Q}_p)$, we see that

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

The right hand side is the intersection of analytic subvarieties. If $\mathcal{J}$ is indeed the Jacobian of $\mathcal{C}$, then Chabauty has proved that $\mathcal{C}(\mathbb{Q}_p)$ does not have dimension 1 intersections with proper analytic subvarieties of $\mathcal{J}(\mathbb{Q}_p)$. Therefore, the intersection is of dimension 0 and, since $\mathcal{J}(\mathbb{Q}_p)$ is compact, is finite.

This proves that $\mathcal{C}(\mathbb{Q})$ is finite and that $\#\mathcal{C}(\mathbb{Q}_p) \cap \overline{\mathcal{J}(\mathbb{Q})}$ gives an upper bound for $\#\mathcal{C}(\mathbb{Q})$. In practise, it turns out that p can often be chosen such that the bound is sharp. Furthermore, if one can find $G_1, \ldots, G_m \in \mathcal{J}(\mathbb{Q})$ such that $\overline{\langle G_1, \ldots, G_m \rangle} = \overline{\mathcal{J}(\mathbb{Q})}$, then one can often approximate the points in $\mathcal{C}(\mathbb{Q}_p) \cap \overline{\mathcal{J}(\mathbb{Q})}$ well enough to count them.

Thus, to be able to apply this method to $\mathcal{C}_{p,t}(\mathbb{Q})$, we must estimate the Mordell-Weil ranks of the corresponding Jacobians. A theorem of Stoll (see [19] and [20]) helps.

Let l be an odd prime, let A be a non-zero, $2l$-th power free integer prime to l and let $\mathcal{C}$ be the smooth, complete curve with an affine model $Y^2 = X^l + A$. Let ζ_l be a primitive lth root of unity and define $q_l(A) := (A^{l-1} - 1)/l$. We assume that $-A/4^{l-1}$ is an odd, positive integer in which each prime factor occurs to an odd power.

Define

$$d_l(A) := \begin{cases} \left\lfloor \frac{1}{4}(l-1) \right\rfloor - (-1)^{\frac{1}{2}(l-1)} & \text{if } A \cdot q_l(A) \bmod l \text{ is a nonzero square in } \mathbb{F}_l, \\ \left\lfloor \frac{1}{4}(l-1) \right\rfloor & \text{otherwise.} \end{cases}$$

Theorem 3 (Stoll) *Let $\mathcal{C}$ be the smooth, complete curve with model $Y^2 = X^l + A$ satisfying the conditions above. If the ideal class number of $\mathbb{Q}(\sqrt{A}, \zeta_l)$ is prime to l, then the rank of the Mordell-Weil group of the Jacobian of $\mathcal{C}$ is bounded above by $d_l(A)$.*

It should be noted that Stoll's original theorem gives a more precise statement for many more values of A, but this result suffices for us. The proof is based on a descent argument utilising the ζ_l-action on the Jacobian, described by Schaefer (see [17] and [16]).

In order to apply the theorem to our situation, we have to check that the ideal class number of $\mathbb{Q}(\sqrt{-3}, \zeta_p) = \mathbb{Q}(\zeta_{3p})$ is not divisible by p. We do this using lower bounds on discriminants together with a little bit of class field theory.

Let K be a number field. Let $\Delta(K)$ be the discriminant of the ring of integers of K. We define the *root discriminant* by $\mathrm{rd}(K) := |\Delta(K)|^{1/[K:\mathbb{Q}]}$. If p divides the ideal class number of K, then there is a degree p unramified relative extension L of K. Such an extension has $[L : \mathbb{Q}] = p[K : \mathbb{Q}]$ and $\mathrm{rd}(L) = \mathrm{rd}(K)$. One can compute lower bounds on $\mathrm{rd}(K)$, increasing in $[K : \mathbb{Q}]$ (see [15]). Thus, if $\mathrm{rd}(K)$ is small enough, this puts a bound on the ideal class number of K.

So, if the ideal class number of $\mathbb{Q}(\zeta_{3p})$ is divisible by p. then there is a number field L with $[L : \mathbb{Q}] = 2p(p-1)$ and $\mathrm{rd}(L) = \mathrm{rd}\mathbb{Q}(\zeta_{3p})$. In [14] we find the following lower bounds on $\mathrm{rd}(L)$.

p	$\mathrm{rd}(\mathbb{Q}(\zeta_{3p}))$	$[L : \mathbb{Q}]$	lower bound on $\mathrm{rd}(L)$	
5	5.79	40	12.96	
7	8.77	84	15.87	
11	14.99	220	18.59	
13	18.18	312	> 19.23	
17	24.66	544	< 23	(> 26.48 under GRH)

So, obviously, for $p = 5, 7, 11, 13$ such L cannot exist. Therefore, Theorem 3 applies to $\mathcal{C}_{p,t}$ and we find

p	t	$d_p(A_{p,t})$	genus$(\mathcal{C}_{p,t})$
5	-1	1	2
5	0	1	2
5	1	0	2
7	-1	1	3
7	0	1	3
7	1	1	3

p	t	$d_p(A_{p,t})$	genus$(\mathcal{C}_{p,t})$
11	-1	3	5
11	0	3	5
11	1	3	5
13	-1	3	6
13	0	2	6
13	1	2	6

So, we have proved that for $p = 5, 7, 11, 13$, Chabauty methods may be applied to bound the number of primitive solutions to $x^3 + y^3 = z^p$.

Amusingly, the root discriminant argument breaks down for $p = 17$ (although not under assumption of the generalised Riemann hypothesis). This is blissfully irrelevant for the equation $x^3 + y^3 = z^p$, since Kraus's result applies.

3 The equation $x^3 + y^3 = z^4$

The construction of the curves $\mathcal{C}_{p,t}$ does not depend on $p \geq 5$. In constructing the model $Y^2 = X^p + A_{p,t}$ we did use that p is odd, though, so we cannot use those models for $p = 4$. As it turns out, $\mathcal{C}_{4,-1}$, $\mathcal{C}_{4,0}$ and $\mathcal{C}_{4,1}$ are genus 1 curves with a rational point. Therefore, they are elliptic curves over $\mathbb{Q}$. Unfortunately, $\mathcal{C}_{4,-1}$ and $\mathcal{C}_{4,0}$ have Mordell-Weil groups of rank 1, so they have infinitely many rational points. This is useless if we want to bound the number of primitive solutions to $x^3+y^3=z^4$. For this case, we find other parametrising curves, of higher genus. We use that fourth powers are squares. Thus, a solution to $x^3+y^3=z^4$ is also a solution of $x^3+y^3=v^2$, with $v=z^2$. We use Zagier's result to describe those solutions.

Lemma 1 (Zagier) *Let $x,y,z \in \mathbb{Z}$ be coprime integers satisfying $x^3+y^3=z^2$. Then there exist $s,t \in \mathbb{Z}_{\{2,3\}}$ with $(s,t) \neq (0,0) \bmod p$ for any prime $p \nmid 6$ such that*

$$\left\{\begin{array}{rcl} x \text{ or } y &=& s^4+6s^2t^2-3t^4 \\ y \text{ or } x &=& -s^4+6s^2t^2+3t^4 \\ z &=& 6st(s^4+3t^4) \end{array}\right. \quad \textit{or} \quad \left\{\begin{array}{rcl} x \text{ or } y &=& \frac{1}{4}(s^4+6s^2t^2-3t^4) \\ y \text{ or } x &=& \frac{1}{4}(-s^4+6s^2t^2+3t^4) \\ z &=& \frac{3}{4}st(s^4+3t^4) \end{array}\right.$$

$$\textit{or} \quad \left\{\begin{array}{rcl} x \text{ or } y &=& s(s^3+8t^3) \\ y \text{ or } x &=& 4t(t^3-s^3) \\ \pm z &=& s^6-20s^3t^3-8t^6 \end{array}\right.$$

See [2]. A detailed account of how to arrive at the parametrisations for $x^2+y^4=z^3$ can be found in [3, Section 3.2]. The proof of Lemma 1 proceeds similarly.

For a solution of $x^3+y^3=v^2$ to be a solution of $x^3+y^3=z^4$ as well, we see that the z in Lemma 1 should be a square. So, by change of variables, we see that a primitive solution to $x^3+y^3=z^4$ gives rise to a rational point on one of the genus 2 curves

$$\begin{array}{rcl} \mathcal{C}_1 &:& Y^2=6X(X^4+3) \\ \mathcal{C}_2 &:& Y^2=3X(X^4+3) \\ \mathcal{C}_3 &:& Y^2=X^6-20X^3-8 \\ \mathcal{C}_4 &:& -Y^2=X^6-20X^3-8. \end{array}$$

So we can determine the primitive solutions of $x^3+y^3=z^4$ by finding those rational points and tracing them back to solutions of $x^3+y^3=z^4$. We hope that Chabauty methods apply to these curves and, as it turns out, things work out very well.

Lemma 2 *The Mordell-Weil groups of the Jacobians of the curves $\mathcal{C}_1$, $\mathcal{C}_2$, $\mathcal{C}_3$ and $\mathcal{C}_4$ are finite.*

Proof: This can be showed by determining the size of $\mathrm{jac}(\mathcal{C}_i)(\mathbb{Q})/2\mathrm{jac}(\mathcal{C}_i)(\mathbb{Q})$ by means of a 2-descent as described in, for instance [5]. This is quite a complicated procedure to carry out by hand but, fortunately, completely automated (see [21]). We will not bother the reader with boring details. $\square$

Therefore, it is sufficient to determine the torsion part of the Mordell-Weil groups. For that, we use a trick that often works and is computationally very easy. Consider a curve $\mathcal{C}$ of genus g over $\mathbb{Q}_p$, given by a smooth projective model over $\mathbb{Z}_p$. Suppose that the reduction of that model, $\mathcal{C} \bmod p$, is again a smooth curve over $\mathbb{F}_p$. Let $\mathcal{J}$ be the Jacobian of $\mathcal{C}$. Then reduction modulo p induces a splitting of $\mathcal{J}(\mathbb{Q}_p)$

$$0 \to \mathcal{J}^{(1)}(\mathbb{Q}_p) \to \mathcal{J}(\mathbb{Q}_p) \to (\mathcal{J} \bmod p)(\mathbb{F}_p) \to 0.$$

The kernel of reduction, denoted by $\mathcal{J}^{(1)}(\mathbb{Q}_p)$, is a $\mathbb{Z}_p$-module. Consequently, it has only p-power torsion. By a more involved argument (see [18, Theorem IV.6.4] or [5, Theorem 7.4.1]), it follows that the kernel of reduction is actually free of torsion. We will only use that all torsion of $\mathcal{J}(\mathbb{Q}_p)$ prime to p maps injectively to $(\mathcal{J} \bmod p)(\mathbb{F}_p)$. Since $\mathcal{J}(\mathbb{Q})$ injects in $\mathcal{J}(\mathbb{Q}_p)$ for all p, we have for any pair of primes p, q of good reduction that

$$\#J(\mathbb{Q})^{\mathrm{tor}} \mid \gcd(p^r \#(\mathcal{J} \bmod p)(\mathbb{F}_p), q^s \#(\mathcal{J} \bmod q)(\mathbb{F}_q)) \text{ for some } r, s.$$

If $\mathcal{C}$ is given by $Y^2 = F(X)$, where F is some squarefree polynomial over $\mathbb{Z}_p$, where p is an odd prime not dividing the discriminant of F, then $\mathcal{C}$ can be given by a smooth model with smooth reduction, so the same principle holds (see [5, Theorem 7.4.1] for an even stronger result).

In order to count points on Jacobians, we first have to represent them. We briefly review some standard results that can be found in [5]. Let $\mathcal{C}$ be a genus 2 curve over a field K and let $\mathcal{J}$ be its Jacobian. A point in $\mathcal{J}(K)$ can be represented by a divisor of $\mathcal{C}$ over K - i.e., a formal linear combination of points on $\mathcal{C}$. Suppose we either have one Weierstrass point $\infty \in \mathcal{C}(K)$ or two points ∞^+, ∞^- rational over K or conjugate quadratic over K that are interchanged by the hyperelliptic involution on $\mathcal{C}$. Then we can represent each divisor class by $[P + Q - 2\infty]$ or $[P + Q - \infty^+ - \infty^-]$, where $P, Q \in \mathcal{C}(K)$ or quadratic conjugate over K. This representation is even unique (apart from interchanging P and Q) for all divisor classes apart from the trivial one. The trivial divisor class, the neutral element of $\mathcal{J}(K)$, is represented by any divisor that counts the zeros of a function on $\mathcal{C}$ with multiplicity, where poles are counted as zeros with negative multiplicity.

Lemma 3 *Let $\mathcal{C}$ be a genus 2 curve over a finite field $\mathbb{F}_q$ and let $\mathcal{J}$ be its Jacobian. Then*

$$\mathcal{J}(\mathbb{F}_q) = \frac{1}{2}(\#\mathcal{C}(\mathbb{F}_q))^2 + \frac{1}{2}\#\mathcal{C}(\mathbb{F}_{q^2}) - q$$

Proof: Some simple combinatorics using the fact that divisor classes are either represented by a pair of rational points or a pair of quadratic conjugate points prove this fact. Alternatively, evaluate the characteristic polynomial of the Frobenius endomorphism at 1. See [5, Section 8.2]. □

For $i = 1, 2, 3, 4$, we write $\mathcal{J}_i$ for the Jacobian of $\mathcal{C}_i$.

Lemma 4 $\mathcal{J}_1(\mathbb{Q}) = \mathcal{J}_2(\mathbb{Q}) = \{0, [(0,0) - \infty]\}$, *so* $\mathcal{C}_1(\mathbb{Q}) = \mathcal{C}_2(\mathbb{Q}) = \{(0,0), \infty\}$.

Proof: The two divisor classes given, are clearly defined over $\mathbb{Q}$. We find using Lemma 3 that $\#(\mathcal{J} \bmod 5)(\mathbb{F}_5) = 26$ and $\#(\mathcal{J} \bmod 7)(\mathbb{F}_7) = 64$ for both Jacobians. Since we have already seen that the Mordell-Weil groups consist solely torsion (Lemma 2), we see that $\#\mathcal{J}(\mathbb{Q}) \mid \gcd(5^r \cdot 26, 7^s \cdot 64) = 2$, which concludes the proof. □

Lemma 5 $\mathcal{J}_4(\mathbb{Q}) := \{0, [(1 + \sqrt{3}, 0) + (1 - \sqrt{3}, 0) - \infty^+ - \infty^-]\}$, *so* $\mathcal{C}_4(\mathbb{Q}) = \emptyset$.

Proof: We find $\#(\mathcal{J}_4 \bmod 5)(\mathbb{F}_5) = 36$ and $\#(\mathcal{J}_4 \bmod 19)(\mathbb{F}_{19}) = 484$. Therefore, $\#\mathcal{J}_4(\mathbb{Q}) \mid 4$. Put $F_1 = X^2 - 2X - 2$, $F_2 = X^4 + 2X^3 + 6X^2 - 4X + 4$. Then $X^6 - 20X^3 - 8 = F_1 F_2$. Furthermore, the extension of $\mathbb{Q}$ generated by a root of F_2 is $\mathbb{Q}(\sqrt{3}, \sqrt{-1})$. A localisation of this field at a prime not above $p = 2, 3$ is at most a quadratic extension of $\mathbb{Q}_p$. Therefore, we have x_1, x_2, roots of F_2, that are either rational or quadratic conjugate over $\mathbb{Q}_p$. In reduction, we have $[(\bar{x}_1, 0) + (\bar{x}_2, 0) - \infty^+ - \infty^-] \in (\mathcal{J}_4 \bmod p)(\mathbb{F}_p)$. Note that two times this divisor is the divisor of the function $(X - x_1)(X - x_2)$, so it represents a 2-torsion point on $(\mathcal{J}_4 \bmod p)(\mathbb{F}_p)$. So, we see that $\mathcal{J}(\mathbb{Q}) \subset \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Using $-[(x_1, y_1) + (x_2, y_2) - \infty^+ - \infty^-] = [(x_1, -y_1) + (x_2, -y_2) - \infty^+ - \infty^-]$, we see that a divisor represents a point of order 2 *only* if $y_1 = y_2 = 0$. As we have already seen, there is only one rational divisor class with that property. $\square$

Note. The above proof shows that it is impossible to bound the torsion of $\mathcal{J}_4(\mathbb{Q})$ purely by local data at primes of good reduction, since $\mathcal{J}_4$ has extra 2-torsion at all good primes. An alternative proof would be the following. Upon closer inspection, $(\mathcal{J}_4 \bmod 5)(\mathbb{F}_5)$ has the structure $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Therefore, $\mathcal{J}_4(\mathbb{Q})$ is either $\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. From the data used to prove Lemma 2, we know that $\mathcal{J}_4(\mathbb{Q})/2\mathcal{J}_4(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$.

Incidentally, this curve is a nice example of the fact that local means are not always sufficient to determine torsion. This adds importance to the height theory on genus 2 curves, which does give an effective procedure, as is described in [5, page 82] and [22]). For determining $\mathcal{C}_4(\mathbb{Q})$, however, it is entirely unnecessary to consider $\mathcal{J}_4(\mathbb{Q})$. It is straightforward to check that $\mathcal{C}_4(\mathbb{Q}_2) = \mathcal{C}_4(\mathbb{Q}_3) = \emptyset$.

Lemma 6 *$\mathcal{J}_3(\mathbb{Q}) = \langle [(1+\sqrt{3}, 0) + (1-\sqrt{3}, 0) - \infty^+ - \infty^-], [\infty^+ - \infty^-] \rangle$ and $\#\mathcal{J}_3(\mathbb{Q}) = 6$. Furthermore, $\mathcal{C}_3(\mathbb{Q}) = \{\infty^+, \infty^-\}$.*

Proof: Note that the divisor of the rational function $y - x^3 + 10$ is $\pm(3\infty^+ - 3\infty^-)$. Therefore, $3[\infty^+ - \infty^-] = 0$.

This proves that the points mentioned in the lemma generate a group of 6 elements. It remains to show that there are no other points. Upon inspection, we find $\#(\mathcal{J}_3 \bmod 5)(\mathbb{F}_5) = \#(\mathcal{J}_3 \bmod 7)(\mathbb{F}_7) = 36$, and the group structures are $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Using the same argument as in Lemma 5, we find that $\mathcal{J}_3(\mathbb{Q})$ has only one point of order 2. This means that either $\mathcal{J}_3(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$ or $\mathcal{J}_3(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

First we prove that $\mathcal{C}(\mathbb{Q})$ has no affine point. Suppose $P = (x, y) \notin \{\infty^+, \infty^-\}$ with $y^2 = x^6 - 20x^3 - 8$. If $P \in \mathcal{C}_3(\mathbb{Q})$, then $[P - \infty^+] \in \mathcal{J}_3(\mathbb{Q})$, so $0 = 6[P - \infty^+] = [6P - 3\infty^+ - 3\infty^-] - 3[\infty^+ - \infty^-] = 3[2P - \infty^+ - \infty^-]$. We construct a function g that has (at least) a quadruple zero in P and has triple poles in ∞^+ and ∞^-. As it turns out, this fixes the location of the other two zeros. Therefore, if $6[P - \infty^+] = 0$, then g has a zero of order 6 in P.

Put $F(X) = X^6 - 20X^3 - 8$ and let $g(X, Y) = Y - (g_3X^3 + g_2X^2 + g_1X + g_0)$ be a function on $\mathcal{C}_3$ with a quadruple zero at P and a triple pole at both ∞^+ and ∞^-. Since $F(X)$ has no rational roots, without loss of generality, $y^2 = F(x) \neq 0$, so $t = X - x$ is a uniformising coordinate at P. We compute a power series expansion of g in t at P.

$$\theta_P := \theta_P^{(0)} + \theta_P^{(1)} t \cdots + \theta_P^{(5)} t^5 + O(t^6) = g(x + t, \sqrt{F(x + t)}).$$

Since $g(P)=0$, we have $g_0 = y - g_3x^3 - g_2x^2 - g_1x$. We solve g_1, g_2, g_3 from the equations $\theta_P^{(1)} = \theta_P^{(2)} = \theta_P^{(3)} = 0$, which must hold for P to be a quadruple zero of g. We find

$$\begin{aligned}\theta_P^{(4)} &= 1620\frac{x^2(x-1)^2(x+2)^2(x^2-2x+4)^2(x^2+x+1)^2}{F(x)^3},\\ \theta_P^{(5)} &= 648x(x-1)(x+2)(x^2-2x+4)(x^2+x+1)(x^3+2)\\ &\quad (4x^9-111x^6-168x^3+32)/F(x)^4.\end{aligned}$$

Thus, we see that the only P with $6[P-\infty^+]=0$ and $X(P)\in\mathbb{Q}$ are $(0,2\sqrt{-2})$, $(1,3\sqrt{-3})$ and $(-2,6\sqrt{6})$, and none of these points has $Y(P)\in\mathbb{Q}$. Therefore, $\mathcal{C}_3(\mathbb{Q}) = \{\infty^+,\infty^-\}$.

It follows that any 3-torsion point in $\mathcal{J}_3(\mathbb{Q})$ other than $\pm[\infty^+-\infty^-]$, is of the form $[(x_1,y_1)+(x_2,y_2)-\infty^+-\infty^-]$, where (x_1,y_1) and (x_2,y_2) are quadratic conjugate points over $\mathbb{Q}$ and $y_1\neq 0$. We use the same construction to show that such points do not exist. We determine $g_0,\ldots,g_3$ such that the function $Y-g_3X^3-g_2X^2-g_1X-g_0$ has double zeros in (x_1,y_1) and (x_2,y_2). Then we determine for which point the function has in fact zeros of order 3 in those points. One can do this by computing the conditions x_1+x_2 and x_1x_2. The computer algebra involved in this computation, is too bulky to display here, but completely straightforward. There turns out to be no other 3-torsion. □

Note. The proof of Lemma 6 exhibits that $6[(0,2\sqrt{-2})-\infty^+] = 6[(1,3\sqrt{-3})-\infty^+] = 6[(-2,6\sqrt{6})-\infty^+] = 0$. For any prime $p\neq 2$, this yields an extra 6-torsion point over $\mathbb{Q}_p$. This gives another example of a curve for which the torsion of the Jacobian cannot be determined solely by information at primes of good reduction.

Proof of Theorem 1: Lemmas 4 through 6 give us the rational points on the curves $\mathcal{C}_1$ through $\mathcal{C}_4$. These points all correspond to trivial solutions of $x^3+y^3=z^4$. Thus, by construction of the curves, the only primitive solutions are trivial. □

4 The equation $x^3+y^3=z^5$

As was shown in Section 2, it is sufficient to determine the rational points on the curves

$$\begin{aligned}\mathcal{C}_1 &: Y^2 = X^5 - 559872\\ \mathcal{C}_2 &: Y^2 = X^5 - 62208\\ \mathcal{C}_3 &: Y^2 = X^5 - 6912\end{aligned}$$

in order to find all primitive solutions to $x^3+y^3=z^5$. Let $\mathcal{J}_i$ be the Jacobian of $\mathcal{C}_i$. As a result of Theorem 3, we have seen that $\mathrm{rk}(\mathcal{J}_1(\mathbb{Q}))\leq 1$, $\mathrm{rk}(\mathcal{J}_2(\mathbb{Q}))\leq 1$ and that $\mathrm{rk}(\mathcal{J}_3(\mathbb{Q}))=0$. The procedure of determining the rational points on curves of genus 2 is, provided that generators of the appropriate Mordell-Weil groups can be found, almost a standard one, although not guaranteed to be successful. Instead of providing a lot of hard to check numerical data to make up the proof, we will describe a session with the available software to give an idea how one can perform these computations in practice nowadays.

Lemma 7 $\mathcal{C}_1(\mathbb{Q}) = \{\infty\}$

We will prove this lemma using Chabauty techniques as described in [5], [10] and [4]. In these articles, the curve is embedded in the Jacobian using the map $P \mapsto [2P - \infty^+ - \infty^-]$ or $[2P - 2\infty]$. We describe a session with the software mentioned in [4].

```
> read`divcalc.mpl`;
> initcurve(x^5+A);
`current curve is `, y^2 = x^5+A
> s_nG:=locexp([n*L[1],n*L[2]]):
> k_nG:=loccoord2kummer(s_nG):
> theta_nG:=factor(series(kummer2theta(k_nG),n,11));
theta_nG := series((4*L[2]^5*(A*L[2]^5+L[1]^5))*n^10+O(n^12),n,12)
> coeff_theta:=factor(coeff(theta_nG,n,10));
coeff_theta := 4*L[2]^5*(A*L[2]^5+L[1]^5)
```

Let $G \in \mathcal{J}(\mathbb{Q})$ be a point in the kernel of reduction mod p of the Jacobian of a curve $Y^2 = X^5 + A$. The two quantities L_1 and L_2 can be computed from G and if the quantity `coeff_theta` does not vanish mod p^{12}, then nG is not of the form $[2P - 2\infty]$ for any $n \neq 0$. Below, G will be a point in $\mathcal{J}(\mathbb{Q})$. It is a generator of the Mordell-Weil group, but we will only need and check that it generates a group of finite index not divisible by certain primes.

```
> alias(alpha=RootOf(x^2+3));
I, alpha
> F:=x^5-559872;
F := x^5-559872
> P:=[12*alpha,1296+864*alpha];
P := [12*alpha, 1296+864*alpha]
> G:=[P,conj(P)];
G := [[12*alpha, 1296+864*alpha], [-12*alpha, 1296-864*alpha]]
> initcurve(F);
`current curve is `, y^2 = x^5-559872
> njac(11,F);
131
> njac(19,F);
400
```

The last two instructions count the number of points on the Jacobian in reduction. The values are coprime, so there is no rational torsion.

```
> alpham19:=(Roots(op(alpha))mod 19);
alpham19 := [[15, 1], [4, 1]]
> Gred19:=subs(alpha=alpham19[1][1],G)mod 19:
> tbl19:=maketablep(19,F mod 19,[[]],Gred19):
> rowdim(tbl19);
20
```

```
> select(i->tbl19[i+1,2][1][1]=tbl19[i+1,2][2][1],
     [i$i=1..rowdim(tbl19)-1]);
[8, 12]
> G7red29:=adp(29,mlp(29,3,G),mlp(29,4,G));
G7red29 := [[21, 27], [25, 15]]
> tbl29:=maketablep(29,F mod 29,[[]],G7red29):
> rowdim(tbl29);
30
> select(i->tbl[i+1,2][1][1]=tbl[i+1,2][2][1],
               [i$i=1..rowdim(tbl29)-1]);
[]
> alpham7:=(Roots(op(alpha))mod 7);
alpham7 := [[2, 1], [5, 1]]
> Gred7:=subs(alpha=alpham7[1][1],G)mod 7:
> njac(7,F);
50
> mlp(7,10,Gred7);mlp(7,25,Gred7);
[[0, 4], [0, 4]]
[[3, 0], [infinity, 0]]
```

This shows that $20G \in \mathcal{J}^{(1)}(\mathbb{Q}_{19})$ and that any divisor $nG = [2P - 2\infty]$ has $n = 20m$ or $n = 8 + 20m$ or $n = 12 + 20m$ for some $m \in \mathbb{Z}$. However, the reduction data at 29 shows that any such point has $n = 30m$ for some $m \in \mathbb{Z}$, so this rules out the last two options. We see that G generates the full group $(\mathcal{J} \bmod 7)(\mathbb{F}_5)$ of order 50. Therefore, the group generated by G has index prime to 10 in the Mordell-Weil group.

```
> Gml20:=ml(20,G):
> sGml20:=div2loccoord(Gml20):
> lGml20:=loclog(sGml20)mod 19^3;
lGml20 := [4636, 2660]
> subs(A=-559872,L[1]=lGml20[1]/19,L[2]=lGml20[2]/19,
     coeff_theta)mod 19;
14
```

Here, we compute $20G$ and its 19-adic logarithm. The fact that $[4636, 2660] \neq [0, 0] \bmod 19^2$, proves that $19 \nmid [\mathcal{J}(\mathbb{Q}) : \langle G \rangle]$. Furthermore, we check that indeed the coefficient of n^{10} in θ does not vanish mod 19^{11}. This proves that $0G$ is the only multiple of $20G$ of the form $[2P - 2\infty]$. See [4] for details on how this power series argument works.

Lemma 8 $\mathcal{C}_2(\mathbb{Q}) = \{\infty\}$.

Although in principle the same procedure applies to this curve as well, we will use another method, described in [3]. An advantage of this method is that it might still work if $\mathrm{rk}(\mathcal{J}(\mathbb{Q})) > 1$. Put $\alpha^5 = 2$. We use that if $x, y \in \mathbb{Q}$ with $y^2 = x^5 - 62208$, then there is a

δ in some finite set and $y_1, y_2 \in K = \mathbb{Q}(\alpha)$ such that

$$\begin{aligned} x - 6\alpha^3 &= \delta y_1^2 \\ x^4 + 6\alpha^3 x^3 + 72\alpha x + 432\alpha^4 x + 5184\alpha^2 &= \delta y_2^2 \end{aligned}$$

We can therefore suffice in finding the K-rational points on genus 1 curves with an X-coordinate in $\mathbb{Q}$. It turns out we can suffice in proving

Lemma 9 *The K-rational points on the genus 1 curve $Y^2 = X^4 + 6\alpha^3 X^3 + 72\alpha X + 432\alpha^4 X + 5184\alpha^2$ with rational X-coordinate have $X \in \{\infty, 0, -12\}$.*

Lemma 10 *The K-rational points on the genus 1 curve $(1 + 2\alpha - 2\alpha^2 + 2\alpha^3 - 2\alpha^4)Y^2 = X^4 + 6\alpha^3 X^3 + 72\alpha X + 432\alpha^4 X + 5184\alpha^2$ with rational X-coordinate have $X \in \{12\}$.*

Note that all finite X-coordinates found satisfy $X^5 < 62208$, so they do not correspond to rational point on $\mathcal{C}_2$. Therefore, $\mathcal{C}_2(\mathbb{Q}) = \{\infty\}$. More details on how to do this can be found in [3]. Here, we describe a session with a package that does these computations for you.

```
kash> Read("ell.g");
ell package loaded.
kash> pol:=x^5-62208;
x^5 - 62208
kash> O:=OrderMaximal(x^5-2);
Generating polynomial: x^5 - 2
Discriminant: 50000
kash> OrderClassGroup(O);
[ 1, [ 1 ] ]
kash> alpha:=XOrderPrimElt(O);
[0, 1, 0, 0, 0]
kash> theta:=PolyRoots(pol+RingZero(O))[1];
[0, 0, 0, 6, 0]
kash> Qpol:=x-theta;
x + [0, 0, 0, -6, 0]
kash> Rpol:=pol/Qpol;
x^4+[0,0,0,6,0]*x^3+[0,72,0,0,0]*x^2+[0,0,0,0,432]*x+[0,0,5184,0,0]
deltas:=FilterTwists(Qpol,Rpol);
[ 1, [1, 2, -2, 2, -2] ]
```

The last result shows that indeed we only need consider two twists of the genus 1 curve (`FilterTwists` checks which twists have points with the desired property locally).

```
kash> ec:=Quar(x^3-5*x^2+Elt(O,5)*x);
kash> EllAddHint(ec,1);EllAddHint(ec,1-2*alpha+alpha^3);
kash> EllGensMod2(ec);
Finding generators of 2-isogeny selmer group on curve...
```

$\vdots$

```
Found global basis using hints.
[(0:0:1),([1,-2,0,1,0]:[3,0,-2,-2,1]:1),(1:1:1)]
kash> EllGenInit([EllXtoPnt(ec,1),
>    EllXtoPnt(ec,1-2*alpha+alpha^3),EllXtoPnt(ec,0)],2);
```

The function `Quar` initialises an elliptic curve in Weierstrass form from a model of the form $Y^2 = F(X)$. Since in this call, F is cubic, transforming to Weierstrass form is trivial. The next commands give hints to the system about where to look for X-coordinates of Mordell-Weil generators. The command `EllGensMod2` tries to find generators of $E(K)/2E(K)$. First it bounds the rank using a 2-descent or a 2-isogeny descent (see [18]), depending on the curve. Then it makes a feeble attempt at finding generators. This is where giving hints helps tremendously. We register the found points. We will only prove that certain primes do not divide the index of the generated group in the full Mordell-Weil group. Note that we already know that the index is odd.

```
kash> cov:=QuarCov(Rpol,ec);;
kash> p151:=PlaceSupport(151*O);;
kash> List(p151,p->EllGrpIndex(ec mod p));
[ 2, 2, 2, 1, 1 ]
```

This shows that the images of the group we have determined in the reductions at the several places over 151 (this is the smallest completely split prime. It is not necessary to use a split prime, but it does reduce the amount of needed computations) are at most 2. Since we know the index to be odd from the descent, we know that the image surjects on the reduction of the Mordell-Weil group. Finally, we check which points P have a rational X-coordinate on the original quartic model. Note that for such a point, the values of $X(P)$ under all 5 embeddings $K \to \mathbb{Q}_{151}$ should agree. This gives 4 equations. Since the Mordell-Weil rank is 2, there are essentially only two variables, so we expect only finitely many solutions. See [3] for details.

```
kash> EllCovChab(cov,[0,[-12,1],[1,0]],p151);
Result of FibStrict:[151,[[139,1],[0,1],[1,0]]]
Computing Theta^G for G=( 4: 2: 1 )...
G is only point in fiber if matrix has maximal rank mod 151
[  9  60]
[132 113]
[  1 115]
[ 73 101]

Computing Theta^G for G=([4,-2,-3,0,2]:[2,-9,-7,4,7]:1)...
G is only point in fiber if matrix has maximal rank mod 151
[ 44  55]
```

```
[145 147]
[140   2]
[ 12  17]

Computing Theta^G for G=( 0: 1: 0 )...
Point maps to infinity. Taking 1/phi
G is only point in fiber if matrix has maximal rank mod 151
[ 37  56]
[106  79]
[100  66]
[ 48  28]

[ [ 0, 1 ], [ -12, 1 ], [ 1, 0 ] ]
kash>
```

For the other elliptic curve, we proceed similarly.

```
kash> ec:=Quar((x^3-5*x^2+Elt(O,5)*x)/deltas[2]);
Elliptic curve [1,2,-2,2,-2]*y^2=x^3-5*x^2+5*x over order generated
by x^5 - 2
kash> cov:=QuarCov(Rpol/deltas[2],12,ec);;
kash> p3:=PlaceInit((-1+alpha-alpha^2+alpha^3-alpha^4)*O);
place [ 3, [1, 2, 1, 2, 1] ] above 3
kash> EllAddHint(ec,Elt(O,[8,6,5,4,3]));
kash> EllAddHint(Ell2Iso(ec),Elt(O,[109,128,112,80,52])/9);
kash> EllGensMod2(ec);
Finding generators of 2-isogeny selmer group on curve...
Computing 2-isogeny selmer rank.

               ⋮

Found global basis using hints.
[(0:0:1),([8,6,5,4,3]:[76,67,58,50,43]:1),
([14308,8384,9136,4952,4324]/2601:[-4461238,-3728612,-3260650,
-2970062,-2572342]/132651:1)]
kash> EllGenInit([EllXtoPnt(ec,Elt(O,[8,6,5,4,3])),
>              EllXtoPnt(ec,Elt(O,[15, -20, 5, -10, 10])/ 12),
>              EllXtoPnt(ec,0)],2);
kash> List(p151,p->EllGrpIndex(ec mod p));
[ 1, 2, 2, 1, 8 ]
kash> EllCovChab(cov,[12],p151);
Result of FibStrict:[ 151, [ [ 12, 1 ] ] ]
Computing Theta^G for G=( 0: 1: 0 )...
G is only point in fiber if matrix has maximal rank mod 151
```

```
[148  37]
[ 31  98]
[113  95]
[ 41  76]

[ [ 12, 1 ] ]
kash>
```

Lemma 11 $\mathcal{C}_3 = \{\infty\}$.

Proof: Since we already know that the Jacobian has rank 0, we only need to determine the torsion. The fact that $(\mathcal{J}_3 \bmod 7)(\mathbb{F}_7) = 43$ and $(\mathcal{J}_3 \bmod 11)(\mathbb{F}_{11}) = 375$ shows that there is none. □

5 Availability of programs

Two implementations of the descent procedure on genus 2 curves as described in [5] are available, both written by Stoll. One is based on the public domain packages PARI/GP ([1]) and CLISP, the other is a package for MAGMA. The latter also has routines for applying Chabauty methods on Jacobians of genus 2 curves. The PARI/GP based program is available in binary form for Linux/i386 systems from `http://www.math.uni-duesseldorf.de/~stoll/genus2/` and the MAGMA package can be obtained from `http://www.math.uni-duesseldorf.de/~stoll/programs/HC/`.

Routines for doing computations on Jacobians of genus 2 curves are available from several locations. There are some routines referred to in [5] at `ftp:// ftp.liv.ac.uk/pub/genus2` for Maple V. The author has also made available some routines for the commercial computer algebra package Maple V for doing computations. An example session is described in Section 4. In the same location, there are also some rudimentary routines for doing 2-descents, written for KASH ([7]).

An elliptic curve package for elliptic curves over arbitrary number fields based on KASH is also available. It can do 2-descent and 2-isogeny descent on elliptic curves over number fields, also with even class number. Furthermore, as demonstrated, there are facilities for Chabauty-arguments.

The computations needed to determine the 3-torsion in Section 3, can be found in `tor334.mpl`. The proof of Lemma 7 can be found in `prf335.mpl`, but the Maple program in `divcalc.sh`, available from the same location, is also necessary. The elliptic curve Chabauty method can be found in `prf335.g`, together with the KASH package `ell.sh` which it is based on.

Electronic locations have a very temporary nature. All these files are presently located at `http://www.math.uu.nl/people/Bruin/`, but this will probably not be permanent. The author will attempt to have a home page somewhere with links to the relevant files.

Acknowledgments

I wish to thank Frits Beukers for the stimulating discussions and pointing out a much more efficient parametrisation of the solutions of $x^3 + y^3 = z^p$. The rank computation programs and the quick and accurate replies of Michael Stoll have also been a great help. The remarks of Alain Kraus have helped to put the work in perspective. Furthermore, I would like to thank Utrecht University for supplying the facilities and stimulating scientific environment that made this paper possible.

References

[1] C. Batut, K. Belabas, D. Bernardi, H. Cohen, and M. Olivier. PARI-GP. Avaliable from `ftp://megrez.math.u-bordeaux.fr/pub/pari`.

[2] Frits Beukers. The Diophantine equation $Ax^p + By^q = Cz^r$. *Duke Math. J.*, 91(1):61–88, 1998.

[3] Nils Bruin. *Chabauty Methods and Covering Techniques applied to Generalised Fermat Equations*. PhD thesis, Universiteit Leiden, 1999.

[4] Nils Bruin. The diophantine equations $x^2 \pm y^4 = \pm z^6$ and $x^2 + y^8 = z^3$. *Compositio Math.*, 118:305–321, 1999.

[5] J.W.S. Cassels and E.V. Flynn. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*. LMS–LNS 230. Cambridge University Press, Cambridge, 1996.

[6] Claude Chabauty. Sur les points rationnels des variétés algébriques dont l'irrégularité est supérieure à la dimension. *C. R. Acad. Sci. Paris*, 212:1022–1024, 1941.

[7] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörnig, and K. Wildanger. KANT V4. *J. Symbolic Comput.*, 24(3-4):267–283, 1997. Available from `ftp://ftp.math.tu-berlin.de/pub/algebra/Kant/Kash`.

[8] Henri Darmon and Andrew Granville. On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$. *Bull. London Math. Soc.*, 27(6):513–543, 1995.

[9] Henri Darmon and Loïc Merel. Winding quotients and some variants of Fermat's last theorem. *J. Reine Angew. Math.*, 490:81–100, 1997.

[10] E.V. Flynn. A flexible method for applying chabauty's theorem. *Compositio Mathematica*, 105:79–94, 1997.

[11] Alain Kraus. private communication.

[12] Alain Kraus. Sur l'équation $a^3 + b^3 = c^p$. *Experiment. Math.*, 7(1):1–13, 1998.

[13] R. Daniel Mauldin. A generalization of Fermat's last theorem: the Beal conjecture and prize problem. *Notices Amer. Math. Soc.*, 44(11):1436–1437, 1997.

[14] A. M. Odlyzko. Tables of discriminant bounds. available at `http://www.research.att.com/~amo/unpublished/index.html`, 1976.

[15] A. M. Odlyzko. Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results. *Sém. Théor. Nombres Bordeaux (2)*, 2(1):119–141, 1990.

[16] Bjorn Poonen and Edward F. Schaefer. Explicit descent for jacobians of cyclic covers of the projective line. *J. reine angew. Math.*, 488:141–188, 1997.

[17] Edward F. Schaefer. Computing a Selmer group of a Jacobian using functions on the curve. *Math. Ann.*, 310(3):447–471, 1998.

[18] Joseph H. Silverman. *The Arithmetic of Elliptic Curves.* GTM 106. Springer-Verlag, 1986.

[19] Michael Stoll. On the arithmetic of the curves $y^2 = x^l + A$ and their Jacobians. *J. Reine Angew. Math.*, 501:171–189, 1998.

[20] Michael Stoll. On the arithmetic of the curves $y^2 = x^l + A$, II. available from `http://www.math.uiuc.edu/Algebraic-Number-Theory`, 1998.

[21] Michael Stoll. Implementing 2-descent for jacobians of hyperelliptic curves. available from `http://www.math.uiuc.edu/Algebraic-Number-Theory`, 1999.

[22] Michael Stoll. On the height constant for curves of genus two. *Acta Arith.*, 90(2):183–201, 1999.

[23] R. Tijdeman. Diophantine equations and Diophantine approximations. In *Number theory and applications (Banff, AB, 1988)*, pages 215–243. Kluwer Acad. Publ., Dordrecht, 1989.

Utrecht University, PO box 80010, 3508 TA Utrecht, The Netherlands