Compositio Mathematica **118:** 305–321, 1999.
© 1999 *Kluwer Academic Publishers. Printed in the Netherlands.*

The Diophantine Equations $x^2 \pm y^4 = \pm z^6$ and $x^2 + y^8 = z^3$

NILS BRUIN
Department of Mathematics and Computer Science, University of Leiden, Leiden, The Netherlands[⋆]
e-mail: nbruin@wi.leidenuniv. nl

(Received: 9 October 1997; accepted in final form: 4 June 1998)

Abstract. In this article we determine all solutions to the equation $x^p + y^q = z^r, (p, q, r) \in \{(2, 4, 6), (2, 6, 4), (4, 6, 2), (2, 8, 3)\}$ in coprime integers x, y, z. First we determine a set of curves of genus 2, such that every solution corresponds to a rational point on one of these curves. Then we determine the rational points on these curves using either covers of rank 0 elliptic curves or a method known as effective Chabauty which works if the Mordell–Weil rank of the Jacobian is smaller than the dimension.

Mathematics Subject Classification (1991): 11D41.

Key words: rational points on algebraic curves, effective Chabauty, generalised Fermat equations, genus 2 curves.

1. Introduction

The diophantine equation $x^p + y^q = z^r$ in integers $p > 1, q > 1, r > 1, x, y, z$ is a generalisation of the well-known Fermat equation $x^n + y^n = z^n$. We will refer to it as the *generalised Fermat equation*.

The homogeneity of the Fermat equation implies that it is sufficient to know the coprime solutions in order to determine all rational solutions. The generalised Fermat equation is only weighted homogeneous. That means that not all integer solutions reduce to coprime integer solutions. The identity $2160^2 - 36^4 = 12^6$ is an example of this phenomenon. We exclude these from our considerations and we limit ourselves to the determination of the *primitive* solutions: solutions with x, y and z coprime.[⋆⋆]

The quantity $\chi = 1/p + 1/q + 1/r$ determines the general shape of the set of primitive solutions. In the case $\chi > 1$, Beukers proved in [Beu98] that, for fixed A, B, C, the equation $Ax^p + By^q = Cz^r$ has either none or infinitely many primitive solutions. He described the solutions quite explicitly by proving that there exists a finite set of polynomial solutions $x, y, z \in \mathbb{Z}[s, t]$, so called

[⋆] Address for correspondence: PO Box 9512, 2300 RA Leiden, The Netherlands.

[⋆⋆] The techniques used also apply to the situation where one allows $\gcd(x, y, z)$ to factor over a fixed, finite set of primes.

https://doi.org/10.1023/A:1001529706709 Published online by Cambridge University Press

parametrisations, such that each primitive solution can be obtained by specialising s and t in one of the parametrisations.

For the equations $x^2 \pm y^2 = z^r$ with $r \geqslant 2$, $x^3 + y^3 = z^2$, $x^2 + y^3 = z^4$ and $x^2 + y^4 = z^3$, these parametrisations can be determined using factorisation. Zagier has done that and the results for $(p, q, r) = (3, 3, 2), (2, 3, 4), (2, 4, 3)$ can be found in an appendix to [Beu98].

The case $x^2 + y^3 = z^5$ is harder. Thiboutot bounded the number of needed parametrizations in [Thi96], but explicitly determining them seems beyond the feasable at the moment. These are the only cases with $\chi > 1$.

For $\chi = 1$, the solutions are parametrised by elliptic curves. No nontrivial solutions exist for $(p, q, r) = (2, 3, 6), (2, 6, 3), (3, 3, 3), (4, 4, 2), (4, 2, 4)$ except $2^3 + 1^6 = 3^2$ and obvious modifications of it.

For $\chi < 1$, Darmon and Granville proved in [DG95] that there are only finitely many primitive solutions. For the case $p = q$ they describe a procedure that generates a finite set of parametrizing curves such that each solution corresponds to a rational point on one of the curves.

The ABC conjecture implies an even stronger finiteness result. Consider the following.

CONJECTURE 1. (ABC Conjecture) For every $\varepsilon > 0$ there are only finitely many coprime positive integers A, B, C satisfying the relation $A + B = C$ such that

$$\frac{\log C}{\log(\text{product of prime divisors of } ABC)} > 1 + \varepsilon.$$

If $1/p + 1/q + 1/r < 1$, then $1/p + 1/q + 1/r \leqslant 41/42$. Applying the ABC-Conjecture with $\varepsilon < 1/41$ gives that there are only finitely many triples $(A, B, C) = (x^p, y^q, z^r)$ satisfying $A + B = C$ and $\gcd(A, B, C) = 1$.[⋆]

The case $p = q = r$ was treated by Wiles. There are no nontrivial primitive solutions in this case. Darmon and Merel [DM96] proved the same for $p = q \geqslant 7$, $r = 2$ and, under the Shimura–Tanayama–Weil conjecture, for $p = q \geqslant 7$, $r = 3$. The cases with $p = q < 7$, $r = 2, 3$ are treated by Poonen in [Poo97].

In [Beu98], a list of small solutions to the generalised Fermat-equation with $\chi < 1$ is given. Since the number of primitive solutions to $x^p + y^q = z^r$ with $\chi < 1$ is conjecturally finite, it is tempting to try to provably list them all. We make a modest start by proving that for some equations, there are no solutions apart from the ones already known.

THEOREM 1. *The only solutions to* $x^p + y^q = z^r$ *with* $\gcd(x, y, z) = 1$, $xyz \neq 0$ *and* $(p, q, r) \in \{(2, 4, 6), (2, 6, 4), (4, 6, 2), (2, 8, 3)\}$ *are*

$$(\pm 1549034)^2 + (\pm 33)^8 = 15613^3.$$

[⋆] One is easily tempted to conclude that the equation $x^p + y^q = z^r$ has only finitely many solutions (x, y, z, p, q, r) with $\gcd(x, y, z) = 1$, $xyz \neq 0$ and $1/p + 1/q + 1/r < 1$. A counterexample is given by $2^3 + 1^q = 3^2$.

https://doi.org/10.1023/A:1001529706709 Published online by Cambridge University Press

In each case, we use the parametrisations of primitive solutions to $x^2 + y^2 = z^2$, $x^2 + y^2 = z^3$ and $x^2 + y^4 = z^3$ to derive curves of genus two such that primitive solutions to the equations investigated correspond to rational points on these curves. In some cases the curve covers an elliptic curve of rank 0. Thus, the rational points can be determined by lifting the torsion points on the elliptic curve to the cover.

In the other cases, the Jacobian turns out to be of rank 1. We embed the curve in the Jacobian and use a method known as effective Chabauty to determine the rational points. The calculations involved are too bulky to display here. The interested reader can obtain scripts to check these using a computer. See Section 6 for more information.

Note that the curves for $x^2 + y^4 = z^6$, $x^2 + y^6 = z^4$ and $x^4 + y^6 = z^2$ are all isomorphic to one another over some finite algebraic extension of $\mathbb{Q}$ and so are the curves for $x^2 + y^8 = z^3$. Thus, when examining the different cases, we are examining different arithmetic structures on one and the same geometric object. This is essential to the method, as can be seen in the equation $x^3 + y^8 = z^2$, which is geometrically equivalent to $x^2 + y^8 = z^3$. When determining the underlying curves using the parametrisations of $x^3 + y^4 = z^2$, we run into the curves

$$\begin{aligned} Y^2 &= X^6 - 6X^5 + 45X^4 - 180X^3 + 135X^2 + 162X - 405, \\ Y^2 &= X^6 + 6X^5 - 15X^4 + 20X^3 + 15X^2 + 30X - 17 \end{aligned}$$

which turn out to have Jacobians of Mordell–Weil rank 2 over $\mathbb{Q}$. This prevents us from using the present method to solve the equation $x^3 + y^8 = z^2$. However, these curves are geometrically equivalent to the curves encountered for $x^2 + y^8 = z^3$, so their Jacobians are nonsimple, as are the Jacobians we will meet in the present article. It turns out that they split over a degree 12 extension of $\mathbb{Q}$.

2. Preliminaries

We shall use the parametrisations of some equations with $\chi > 1$.

LEMMA 1. *Let x, y, z be coprime integers such that $x^2 + y^2 = z^2$. Possibly by interchanging x and y, we can assume that x is divisible by 2. Then there are coprime integers s and t, not both odd, such that*

$$x = 2st, \qquad \pm y = s^2 - t^2, \qquad \pm z = s^2 + t^2.$$

Sketch of proof. This is a classical result. That x and y are not both odd can be seen mod 4. The polynomials can be obtained by observing that $y^2 = z^2 - x^2 = (z + x)(z - x)$. □

LEMMA 2. *Let x, y, z be coprime integers such that $x^2 + y^2 = z^3$. Then there are coprime integers s, t such that*

$$x = s(s^2 - 3t^2), \qquad y = t(t^2 - 3s^2), \qquad z = s^2 + t^2.$$

https://doi.org/10.1023/A:1001529706709 Published online by Cambridge University Press

Sketch of proof. This result can be obtained by considering $(x+iy)(x-iy)=z^3$. □

LEMMA 3 (Zagier, [Beu98]). *Let x, y, z be coprime integers such that $x^2+y^4=z^3$ Then there are rational numbers s, t such that one of the following holds.*

$$\begin{aligned}
&x = 4st(s^2-3t^2)(s^4+6s^2t^2+81t^4)(3s^4+2s^2t^2+3t^4),\\
&\pm y = (s^2+3t^2)(s^4-18s^2t^2+9t^4),\\
&z = (s^4-2s^2t^2+9t^4)(s^4+30s^2t^2+9t^4),
\end{aligned}$$

$$\begin{aligned}
&\pm x = (s^4+12t^4)(s^8-408s^4t^4+144t^8),\\
&y = 6st(s^4-12t^4),\\
&z = s^8+168s^4t^4+144t^8,
\end{aligned}$$

$$\begin{aligned}
&\pm x = (3s^4+4t^4)(9s^8-408s^4t^4+16t^8),\\
&y = 6st(3s^4-4t^4),\\
&z = 9s^8+168s^4t^4+16t^8,
\end{aligned}$$

$$\begin{aligned}
&\pm x = (1/8)(s^4+3t^4)(s^8-102s^4t^4+9t^8),\\
&y = (3/2)st(s^4-3t^4),\\
&z = (1/4)(s^8+42s^4t^4+9t^8).
\end{aligned}$$

Sketch of proof. First observe that $x^2+(y^2)^2=z^3$. Using Lemma 2, we see that $y^2=t(t^2-3s^2)$. This implies that $t=Au^2$, $t^2-3s^2=Au^2$ for some $A\in\{1,-1,3,-3\}$. Parametrise the latter ternary quadratic equations to get a list of quadratic expressions for s and t (for $A=3$ and $A=-1$ there are no solutions at all). Substitute each expression for t in $t=Au^2$ to obtain a ternary quadratic equation. Parametrisation again results in quadratic forms, which can be substituted back. Care should be taken to eliminate parametrisations that do not produce coprime solutions. □

3. The Equations $x^2+y^4=z^6$, $x^2+z^6=y^4$ and $y^4+z^6=x^2$

The equations with exponents 2, 4 and 6 turn out to be easy to solve. Essentially, the solutions are parametrised by genus 2 curves that admit a morphism to a rank 0 elliptic curve.

THEOREM 2. *If $x, y, z\in\mathbb{Z}$ are coprime such that $x^2+y^4=z^6$, then $xyz=0$.*

Proof. Suppose we have a primitive solution x, y, z. Then, by applying Lemma 2 to $x^2+(y^2)^2=(z^2)^3$, we have coprime $a, b\in\mathbb{Z}$ such that

$$x=b(3a^2-b^2), \tag{1}$$

https://doi.org/10.1023/A:1001529706709 Published online by Cambridge University Press

$$y^2 = a(a^2 - 3b^2), \tag{2}$$

$$z^2 = a^2 + b^2. \tag{3}$$

Equation (3) implies that either $a = s^2 - t^2, b = 2st$ or $a = 2st, b = s^2 - t^2$. We treat each of the possibilities separately.

$\mathbf{a = s^2 - t^2, b = 2st}$. By substitution in Equation (2), we get

$$y^2 = (s^2 - t^2)(s^4 - 14s^2t^2 + t^4).$$

Note that $t = 0$ implies that $b = 0$ and thus $x = 0$. We can therefore safely put $Y = y/t^3, X = s^2/t^2$. Solutions with $x \neq 0$ correspond to affine rational points on the elliptic curve

$$Y^2 = (X - 1)(X^2 - 14X + 1).$$

Using GP/Pari or Apecs, one can calculate the minimal model and the conductor of this curve. From this, we see that it is isomorphic to 144A2 from Cremona's tables [Cre92]. These tables show that this curve has only one affine rational point, namely $(1, 0)$. This corresponds to solutions with $y = 0$.

$\mathbf{a = 2st, b = s^2 - t^2}$. Put $s - t = u, s + t = v$. This gives $a = (v^2 - u^2)/2, b = uv$. Substitution in Equation (2) yields

$$8y^2 = (v^2 - u^2)(v^4 - 14v^2u^2 + u^4).$$

Note that $u = 0$ implies that $b = 0$ and thus $x = 0$. By putting $Y = y/u^3$, $X = v^2/u^2$, other solutions correspond to affine rational points on the elliptic curve

$$8Y^2 = (X - 1)(X^2 - 14X + 1).$$

This curve is isomorphic to 576A2 in [Cre92] and has only one affine rational point, namely $(1, 0)$. This corresponds to solutions with $y = 0$. □

THEOREM 3. *If $x, y, z \in \mathbb{Z}$ are coprime such that $x^2 = z^6 + y^4$, then $xyz = 0$.*

Proof. Suppose we have a primitive solution x, y, z. Then Lemma 1 states that there exist coprime s, t of distinct parity such that $y^2 = 2st, z^3 = s^2 - t^2$ or $y^2 = s^2 - t^2, z^3 = 2st$. We treat these cases separately.

$\mathbf{y^2 = 2st, z^3 = (s + t)(s - t)}$. Since $\gcd(y, x) = 1$ and $s + t$ and $s - t$ are both odd, we have that $s + t$ and $s - t$ are coprime. Therefore, there exist $u, v \in \mathbb{Z}$ such that $u^3 = s - t, v^3 = s + t$. Rewriting y^2 in u, v gives

$$2y^2 = v^6 - u^6.$$

https://doi.org/10.1023/A:1001529706709 Published online by Cambridge University Press

$u = 0$ implies that $s = t$ and thus $z = 0$. Other solutions correspond to the affine rational points on the elliptic curve curve $2Y^2 = X^3 - 1$, which is isomorphic to 576E1 and has just $(1, 0)$ as affine rational point.

$\mathbf{y^2 = s^2 - t^2, z^3 = 2st}$. Since y is odd, we have $y^2 = 1 \bmod 4$. Therefore, s is odd. From $z^3 = 2st$ we then conclude that $s = v^3$, $t = 4u^3$. Rewriting y^2 in u, v gives

$$y^2 = v^6 - 16u^6.$$

Note that $u = 0$ implies $t = 0$ and thus $z = 0$. Other solutions correspond to affine rational points on the elliptic curve $Y^2 = X^3 - 16$, which is is 432A1 in [Cre92]. The curve has no affine rational points at all. □

THEOREM 4. *If $x, y, z \in \mathbb{Z}$ are coprime such that $x^2 + z^6 = y^4$, then $xyz = 0$.*

Proof. Suppose we have a primitive solution x, y, z. If $z \neq 0$ then $y^4 - x^2 > 0$. Therefore, both $y^2 - x > 0$ and $y^2 + x > 0$. Since x and y are coprime, $\gcd(y^2 - x, y^2 + x) \mid 2$. Possibly after change of sign of x we have $y^2 - x = 2u^6$, $y^2 + x = 2^5v^6$ or $y^2 - x = u^6$, $y^2 + x = v^6$. We treat these cases separately.

$\mathbf{y^2 - x = 2u^6, y^2 + x = 2^5v^6}$. Eliminating x gives

$$y^2 = u^6 + 16v^6.$$

$v = 0$ implies that $z = 0$. Other solutions correspond to affine rational points on the elliptic curve $Y^2 = X^3 + 16$, which is isomorphic to 27A3 and has only the two affine rational points $(0, 4), (0, -4)$. The corresponding solutions have $u = z = 0$.

$\mathbf{y^2 - x = u^6, y^2 + x = v^6}$. It follows that u and v are odd and coprime. Eliminating x gives $2y^2 = u^6 + v^6$. Proceeding as before does not work, as the elliptic curve $2Y^2 = X^3 + 1$ has infinitely many rational points. However, we remark that

$$2y^2 = (u^2 + v^2)(u^4 - u^2v^2 + v^4)$$

implies that

$$u^2 + v^2 = \alpha\, y_1^2, \qquad u^4 - u^2v^2 + v^4 = \beta\, y_2^2,$$

where $\alpha\beta = 2y_0^2$ and α, β consist only of factors 2 and 3. Positivity shows that $\alpha, \beta > 0$ and modulo 3 we see that $3 \nmid \alpha$. Furthermore, the parity of u and v implies that $u^4 - u^2v^2 + v^4$ is odd. Therefore we have

$$u^2 + v^2 = 2y_1^2, \tag{4}$$

$$u^4 - u^2v^2 + v^4 = y_2^2. \tag{5}$$

https://doi.org/10.1023/A:1001529706709 Published online by Cambridge University Press

Solutions of (5) correspond to rational points on the elliptic curve $Y^2 = X^4 - X^2 + 1$, which is isomorphic to 27A1. (The smooth model of) this curve has 8 rational points: $\{\infty^+, \infty^-, (0, \pm 1), (\pm 1, \pm 1)\}$. The points at infinity and $(0, \pm 1)$ correspond to solutions with $v = 0$ and $u = 0$ respectively. Equation (4) has no solution for those points. Solutions corresponding to $(\pm 1, \pm 1)$ have $u^6 = v^6$, which implies that $x = 0$. □

4. Rational Points on Genus 2 Curves

The exponent triples 2-4-6, 2-6-4 and 4-6-2 are easy to handle, since the corresponding genus 2 curves cover elliptic curves of rank 0. The following method works for the cases we encounter for 2-8-3.

We use the fact that the p-adic topological closure of a rank r subgroup of a p-adic abelian variety is a p-adic subvariety of dimension at most r. Chabauty used this observation in [Cha41] to prove the finiteness of the number of rational points on curves of genus $g > 0$ with a Jacobian of Mordell–Weil rank $< g$ over $\mathbb{Q}$. Flynn has adapted this idea in [CF96] and [Fly97] to get bounds on the number of rational points on curves of genus 2 with a Jacobian of rank 1 over $\mathbb{Q}$. We present and use a version that is restricted to the type of curves we will encounter.

4.1. NOTATION AND STANDARD RESULTS

This section is a summary of the objects and results we need from, for example, [CF96]. Let $\mathcal{C}$ denote a smooth curve of genus 2 with a singular model $Y^2 = F(X)$, where $F(X)$ is a square-free polynomial over $\mathbb{Z}$ of degree 5[⋆]. We denote the hyperelliptic involute of a point (x, y) by $\widehat{(x, y)} = (x, -y)$. Note that, because the degree of F is odd, we have a unique place ∞ on $\mathcal{C}$ corresponding to the intersection of the model with the line at infinity. We have $\hat{\infty} = \infty$.

We write $\mathcal{J} = \mathcal{J}_{\mathcal{C}}$ for the Jacobian. As a set, $\mathcal{J}$ is the same as the collection of divisor-classes of degree 0, the Pic^0. It is a standard result that $\mathcal{J} \simeq \mathcal{C} \times \mathcal{C} / \sim$, where $(P_1, Q_1) \sim (P_2, Q_2)$ if $\{P_1, Q_1\} = \{P_2, Q_2\}$ or if $P_1 = \hat{Q}_1$, $P_2 = \hat{Q}_2$. We write $[P + Q]$ for the point on $\mathcal{J}$ corresponding to the divisor-class represented by $\{P + Q - 2\infty\}$.

Note that ∞ is defined over $\mathbb{Q}$, so $\mathcal{C}(K)$ is nonempty for any extension K of $\mathbb{Q}$. That means that all points in $\mathcal{J}(K)$ can be represented by divisors defined over K. That means that every point in $\mathcal{J}(K)$ can be written as $[P + Q]$, where P, Q are points on $\mathcal{C}$, either rational of quadratic conjugate over K (in fact, this is true for all curves of genus 2 and number fields K).

On this representation of $\mathcal{J}$, the description of the group law bears great resemblance to the chord-tangent method on elliptic curves. The point $[P_3 + Q_3]$

[⋆] In general, a model exists with deg $F \in \{5, 6\}$. We limit ourselves to the special case deg $F = 5$, but this is not essential to the method used.

such that $[P_1+Q_1]+[P_2+Q_2]+[P_3+Q_3]=0$ is characterised by the fact that the points P_3, Q_3 are the other points of intersection of $\mathcal{C}$ with the curve $Y=a_3X^3+a_2X^2+a_1X+a_0$ through P_1, Q_1, P_2, Q_2. The inverse of $[P+Q]$ is $[\hat{P}+\hat{Q}]$.

Let p be a prime of good reduction (i.e. $p>2$ and does not divide the discriminant of F). Denote with $\mathcal{J}(\mathbb{Q}_p)^0$ the kernel of reduction $\bmod p$

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

By the corollary to Theorem 7.4.1 in [CF96] we have that $\mathcal{J}(\mathbb{Q}_p)^0$ is free of torsion. Since $\mathcal{J}(\mathbb{Q})$ injects into $\mathcal{J}(\mathbb{Q}_p)$, this implies that $\#\mathcal{J}_{\mathrm{tor}}(\mathbb{Q}) \mid \#\mathcal{J}(\mathbb{F}_p)$. The latter quantity can be calculated using

$$\#\mathcal{J}_{\mathcal{C}}(\mathbb{F}_p)=\tfrac{1}{2}(\#\mathcal{C}(\mathbb{F}_p))^2+\tfrac{1}{2}\#\mathcal{C}(\mathbb{F}_{p^2})-p. \tag{6}$$

(see Section 8.2 in [CF96]). Completely analogous to the elliptic curves case, this gives us a way to bound $\mathcal{J}_{\mathrm{tor}}(\mathbb{Q})$.

4.2. COMPUTING THE RANK AND THE GROUP STRUCTURE

We compute the rank of $\mathcal{J}(\mathbb{Q})$ by a complete 2-descent as described in, for example, 11.2 of [CF96]. Let K be an extension of $\mathbb{Q}$. Denote by Θ the image of X in $K[X]/(F(X))$. Then $K[\Theta]$ is a finite, square-free commutative K-algebra and thus the direct sum of finite field-extensions of K. Write M_K for $K[\Theta]^*/(K[\Theta]^*)^2$. This is a commutative group of exponent 2 and therefore an $\mathbb{F}_2$-vector space. The group homomorphism $\mu_K\colon \mathcal{J}(K)/2\mathcal{J}(K) \to M_K$ partially given by $[(x,y)+(u,v)] \mapsto (x-\Theta)(u-\Theta)$, is injective. Let S be the set of primes dividing $2\,\mathrm{Disc}(F)$ together with a set of primes such that the class groups of the irreducible factors of $\mathbb{Q}(\Theta)$ can be represented by ideals that are unitary outside S. In our case, we will only meet trivial classgroups, so the latter condition is void. Let $\mathcal{G}$ be the subspace of $M_{\mathbb{Q}}$ of quadratic classes that can be represented by elements of $\mathbb{Q}[\Theta]$ that are unitary outside S in each of the factors of $\mathbb{Q}[\Theta]$. It is shown in [FPS95] that $\mu_{\mathbb{Q}}(\mathcal{J}(\mathbb{Q}))$ lies in $\mathcal{G}$. Furthermore, note that $\mathcal{G}$ is finite and effectively computable given F. We make use of the commutative diagram

$$\begin{tikzcd}
\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q}) \arrow[r, "\mu_{\mathbb{Q}}"] \arrow[d] & \mathcal{G} \arrow[d] \\
\mathcal{J}(\mathbb{Q}_p)/2\mathcal{J}(\mathbb{Q}_p) \arrow[r, "\mu_{\mathbb{Q}_p}"] & M_{\mathbb{Q}_p}.
\end{tikzcd}$$

We use that $\#\mathcal{J}(\mathbb{Q}_p)/2\mathcal{J}(\mathbb{Q}_p)=\#\mathcal{J}[2](\mathbb{Q}_p)/|2|_p^2$ to compute the dimension of $\#\mathcal{J}(\mathbb{Q}_p)/2\mathcal{J}(\mathbb{Q}_p)$ as an $\mathbb{F}_2$-vector space and search for generators (p-adic points

https://doi.org/10.1023/A:1001529706709 Published online by Cambridge University Press

are not too hard to find). The intersection $\mathcal{G}$ in $M_{\mathbb{Q}_p}$ with the pullback of the image of $\mu_{\mathbb{Q}_p}$ to $M_{\mathbb{Q}}$ gives a bound on the dimension of $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$ and thus on the rank of $\mathcal{J}(\mathbb{Q})$. Provided that we can find $\mathcal{J}_{\mathrm{tor}}(\mathbb{Q})$, this gives us the group structure.

4.3. THE JACOBIAN AS A p-ADIC VARIETY

In [CF96], Chapter 2, Cassels and Flynn give an explicit embedding $z\colon \mathcal{J} \hookrightarrow \mathbb{P}_{15}$. Note for future reference that

$$(z_{12} : z_{13} : z_{14})([(x, y) + (u, v)]) = (xu : x + u : 1).$$

The affine coordinates $(s_1, \ldots, s_{15}) = (z_1/z_0, \ldots, z_{15}/z_0)$ are normalized such that for a prime p of good reduction we have $D \in \mathcal{J}(\mathbb{Q}_p)^0$ exactly if $s_1(D), s_2(D) \in p\mathbb{Z}_p$. Thus s_1 and s_2 are local coordinates around the origin. The power series expansions of $s_3, \ldots, s_{15}$ in s_1, s_2 are convergent for such D. Furthermore, the formal logarithm and exponential map describe the group law on $\mathcal{J}(\mathbb{Q}_p)^0$ and are expressible in terms of s_1, s_2. Thus, for $D_1, D_2 \in \mathcal{J}(\mathbb{Q}_p)^0$ we have

$$(s_1, s_2)(D_1 + D_2) = \mathrm{Exp}(\mathrm{Log}(D_1) + \mathrm{Log}(D_2)).$$

Here, the $+$ on the left-hand side is on $\mathcal{J}$ and on the right-hand side on $p\mathbb{Z}_p \oplus p\mathbb{Z}_p$.

4.4. APPLYING CHABAUTY'S METHOD

Consider the map

$$\mathcal{C} \to \mathcal{J},$$
$$P \mapsto [P + P].$$

It maps $\mathcal{C}(\mathbb{Q})$ into $\mathcal{J}(\mathbb{Q})$, so determining the rational points on $\mathcal{C}$ reduces to finding all $n \in \mathbb{Z}$ such that $nG = [P + P]$ or $T + nG = [P + P]$. We will assume that using a variety of ad hoc finite-field arguments, we have found a prime p of good reduction such that any $P \in \mathcal{C}(\mathbb{Q})$ has $[P + P] = 0 \bmod p$ and that $T + G$ is not of the form $[P + P]$ for any $n \in \mathbb{Z}$.

Let m be the order of $G \bmod p$. We define

$$\theta_{mG}(n) = (s_{13}^2 - 4\, s_{12}s_{14})(nmG).$$

This function has a zero at n if $nmG = [P + P]$. We can express this as a power series in n, since $(s_1, s_2)(nmG) = \mathrm{Exp}(n\,\mathrm{Log}(mG))$ and $mG \in \mathcal{J}(\mathbb{Q}_p)^0$. We then use Strassmann's theorem to bound the number of $n \in \mathbb{Z}_p$ for which $\theta_{mG}(n) = 0$.

THEOREM 5 (Strassman). *Let $A(X) = \sum_{i=0}^{\infty} a_n X^n$ be a nonzero power series over $\mathbb{Q}_p$ such that*

$$\lim_{n\to\infty} |a_n|_p = 0.$$

https://doi.org/10.1023/A:1001529706709 Published online by Cambridge University Press

Let N be such that $|a_n|_p \leqslant |a_N|_p$ for $n = 0, \ldots, N-1$ and $|a_n|_p < |a_N|_p$ for $n = N+1, \ldots$. Then $A(X) = 0$ for at most N values of $X \in \mathbb{Z}_p$. If the zeros are counted with the appropriate multiplicity, then the bound still holds.

Sketch of proof. This is Theorem 4.1 in [Cas86]. The stronger statement about multiplicity follows from the proof given there or from the Preparation Theorem of Weierstrass, which says that A(X) can be written as the product of an Nth degree polynomial and a power-series without zeros in $\mathbb{Z}_p$. (Theorem 5.1 in [Cas86]). □

For convenience, we do this calculation once for the type of curve we will encounter. Note that the restriction on the model of the curve is purely to limit the size of the computer algebra involved.

LEMMA 4. *Consider the genus 2 curve $\mathcal{C}: Y^2 = X^5 + aX$ ($a \in \mathbb{Z}$). Choose a prime $p > 2$ not dividing a. Let $G \in \mathcal{J}(\mathbb{Q})$ be a point on the Jacobian and let m be its order $\bmod p$. If $(L_1, L_2) = \operatorname{Log}(mG)$ satisfies $L_2 \neq 0 \bmod p^2$, then the following holds. If $L_1^4 + a\,L_2^4 = 0 \bmod p^6$, then there is at most one $n \in \mathbb{Z}_{\geqslant 0}$ such that $nmG = [P + P]$. Otherwise, only $n = 0$ is a solution.*

Proof. Using the formulas described by [CF96] and available by anonymous ftp, we compute

$$\begin{aligned}\theta_{mG}(n) \;=\; & 4\,L_1L_2^5\left(L_1^4 + aL_2^4\right)n^{10} - \\ & -\tfrac{1}{3}\,L_2^4(17\,L_1^8 + 2a\,L_1^4L_2^4 + a^2L_2^8)n^{12} + \mathrm{O}(n^{14}).\end{aligned}$$

From [CF96] we know that power series for $s_{12}, s_{13}, s_{14} \in \mathbb{Z}[a][[s_1, s_2]]$ and that the denominators of coefficients of terms of total degree n in the power series for Exp and Log have their denominators bounded by $n!$. This means that for $p \geqslant 7$, the available terms are sufficient to compute $(L_1, L_2) \bmod p^7$ and that the coefficient of n^t in $\theta_{mG}(n)$ is divisible by p^{13} for $t > 12$. Note that $n = 0$ is at least a 10-fold zero of θ_{mG}. If $L_1^4 + a\,L_2^4 = 0 \bmod p^6$, then $\theta_{mG}(n) = -\frac{16}{3}a^2L_2^{12}n^{12} \bmod p^{13}$, which is nonzero by the assumption on L_2. So, by Strassman's lemma we have that $\theta_{mG}(n)$ has at most 12 zeros in $\mathbb{Z}_p$ counted with multiplicity. Apart from $n = 0$, this leaves room for at most two more zeros. Since $\mathbb{Z} \subset \mathbb{Z}_p$, this bound surely holds for $n \in \mathbb{Z}$. By construction we know that if n is a zero, so is $-n$. Therefore there can be at most one such $n > 0$.

If $L_1^4 + a\,L_2^4 \neq 0 \bmod p^6$, we have that $\theta_{mG}(n) = 4L_1L_2^5(L_1^4 + aL_2^4)n^{10} \bmod p^{12}$ is nonzero, so again by Strassman's lemma we see that there is no $n \in \mathbb{Z}_p$ apart from $n = 0$ that is a zero of θ_{mG}. □

https://doi.org/10.1023/A:1001529706709 Published online by Cambridge University Press

5. The Equation $x^2 + y^8 = z^3$

Observe that any primitive solution of the diophantine equation $x^2 + y^8 = z^3$ must also satisfy $x^2 + (y^2)^4 = z^3$. Lemma 3 gives us a finite set of formulae describing such x, y^2, z. We see that

$$\begin{aligned}
&\pm y^2 = (s^2 + 3t^2)(s^4 - 18s^2t^2 + 9t^4) \quad \text{or}\\
&y^2 = 6st(s^4 - 12t^4) \quad \text{or}\\
&y^2 = 6st(3s^4 - 4t^4) \quad \text{or}\\
&y^2 = (3/2)st(s^4 - 3t^4).
\end{aligned}$$

Remark that in each case, $t = 0$ implies either $x = 0$ or $y = 0$. Therefore, non-trivial solutions correspond (after some transformations) to affine rational points on one of the curves

$$\begin{aligned}
&\mathcal{C}_1 : Y^2 = -(X^2 + 3)(X^4 - 18X^2 + 9),\\
&\mathcal{C}_2 : Y^2 = (X^2 + 3)(X^4 - 18X^2 + 9),\\
&\mathcal{C}_3 : Y^2 = X^5 - 15552X,\\
&\mathcal{C}_4 : Y^2 = X^5 - 139968X,\\
&\mathcal{C}_5 : Y^2 = X^5 - 3888X.
\end{aligned}$$

The rational points on the first two curves can be determined using covers of elliptic curves.

PROPOSITION 1. *The curve $\mathcal{C}_1$ has no affine rational points.*

Proof. The curve $\mathcal{C}_1$ is a double cover of the elliptic curve $Y^2 = -(X+3)(X^2 - 18X + 9)$ by the map $X \mapsto X^2$. The elliptic curve is of conductor 2304 and has rank 0, which can be verified by performing a 2-descent on the curve. The only affine torsion-point is $(-3, 0)$, which lifts to $(\pm\sqrt{-3}, 0)$ on $\mathcal{C}_1$. □

PROPOSITION 2. *The curve $\mathcal{C}_2$ has no affine rational points.*

Proof. Unfortunately, the elliptic curve we get by applying the map $X \mapsto X^2$ has rank 1. We observe that, because $(X^2 + 3)(X^4 - 18X^2 + 9)$ has no rational roots and $\mathrm{Res}(X^2 + 3, X^4 - 18X^2 + 9) = 2^6 3^4$, any rational solution must satisfy

$$\mu Y_1^2 = X^2 + 3, \tag{7}$$

$$\mu Y_2^2 = X^4 - 18X^2 + 9, \tag{8}$$

for one $\mu \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$. Equation (7) shows that $\mu \geqslant 0$. A simple computer search shows that there are no solutions to $\mu Y_2^2 = X^4 - 18X^2Z^2 + 9Z^4 \bmod 128$ for $\mu = 2, 3, 6$ with $(X, Z) \in \mathbb{Z}^2$, $(X, Z) \not\equiv (0, 0) \bmod 2$, which only leaves $\mu = 1$.

https://doi.org/10.1023/A:1001529706709 Published online by Cambridge University Press

For $\mu = 1$, (8) is isomorphic to 288D1, which is a curve with 4 rational points. For our model, these are ∞^+, ∞^-, $(0, 3)$, $(0, -3)$. The affine points clearly do not satisfy (7). □

PROPOSITION 3. $\mathcal{C}_3(\mathbb{Q}) = \{(0, 0), \infty\}$.

Proof. Fix α_3 such that $\alpha_3^2 + 3\alpha_3 + 36 = 0$. Then $P_3 = (\alpha_3, 33\alpha_3 - 180) \in \mathcal{C}(\mathbb{Q}(\alpha_3))$. Write $\bar{P}_3$ for the quadratic conjugate point of P_3. Then $G_3 = [P_3 + \bar{P}_3] \in \mathcal{J}(\mathbb{Q})$. Another point is $T = [(0, 0) + \infty] \in \mathcal{J}(\mathbb{Q})$. Using the notation from Section 4.2, we have

$$\mu_{\mathbb{Q}_2}(\mathcal{J}(\mathbb{Q}_2)/2\mathcal{J}(\mathbb{Q}_2)) = \mu_{\mathbb{Q}_2}(\langle T, G_3, [(4, 2^4\sqrt{-239}) + \infty]\rangle),$$

$$\mu_{\mathbb{R}}(\mathcal{J}(\mathbb{R})/2\mathcal{J}(\mathbb{R})) = \mu_{\mathbb{R}}(\langle T\rangle).$$

Calculation shows that the intersection of $\mathcal{G}$ with the pullbacks of these spaces to $M_{\mathbb{Q}}$ is two dimensional. Furthermore, $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q}) = \langle T, G_3\rangle$.

Table I. Image of $\mathcal{J}_{\mathcal{C}_3}(\mathbb{Q})$ in $\mathcal{J}_{\mathcal{C}_3}(\mathbb{F}_7)$

G_3	$[(\alpha_3, -2\alpha_3 + 2) + (-3 - \alpha_3, 1 + 2\alpha_3)]$
$2G_3$	$[(3, 2) + (6, 5)]$
$3G_3$	$[(\gamma, -\gamma - 3) + (-\gamma, \gamma - 3)]$
$4G_3 = T$	$[(0, 0) + \infty]$
$5G_3$	$[(\gamma, \gamma + 3) + (-\gamma, -\gamma + 3)]$
$6G_3$	$[(3, 5) + (6, 2)]$
$7G_3$	$[(\alpha_3, 2\alpha_3 - 2) + (-3 - \alpha_3, -1 - 2\alpha_3)]$
$8G_3$	$[2\infty]$

$\gamma^2 + 2 = 0$

Table II. $T + nG_3$ in $\mathcal{J}_{\mathcal{C}_3}(\mathbb{F}_{13})$

T	$[(0, 0) + \infty]$
$T + G_3$	$[(-1, 4) + (3, 6)]$
$T + 2G_3$	$[(\gamma, 5\gamma + 5) + (-\gamma - 4, -5\gamma - 2)]$
$T + 3G_3$	$[(1, -6) + (-3, -4)]$
$T + 4G_3$	$[(1, 6) + (-3, 4)]$
$T + 5G_3$	$[(\gamma, -5\gamma - 5) + (-\gamma - 4, 5\gamma + 2)]$
$T + 6G_3$	$[(-1, -4) + (3, -6)]$

$\gamma^2 + 4\gamma - 3 = 0$

Using (6) we determine that $\#\mathcal{J}(\mathbb{F}_5) = 26$ and that $\#\mathcal{J}(\mathbb{F}_7) = 64$. Thus, $\mathcal{J}_{\mathrm{tor}}(\mathbb{Q})$ has at most two elements and since $2T = 0$, is $\{0, T\}$. This means that $\mathcal{J}(\mathbb{Q}) \simeq$

https://doi.org/10.1023/A:1001529706709 Published online by Cambridge University Press

$\mathbb{Z}/(2) \times \mathbb{Z}$. For future reference we observe that $G_3 \bmod 7$ and $[(3, 2) + \infty] \bmod 7$ generate order 8 subgroups of $\mathcal{J}(\mathbb{F}_7)$ with trivial intersection. Therefore, $\mathcal{J}(\mathbb{F}_7) \simeq \mathbb{Z}/(8) \times \mathbb{Z}/(8)$. As Table I shows, $T = 4G_3 \bmod 7$, so $\mathcal{J}(\mathbb{Q}) \bmod 7$ is a cyclic group containing $G_3 \bmod 7$. Taking into account the group-structure, this implies that $\mathcal{J}(\mathbb{Q}) \bmod 7 = \langle G_3 \bmod 7\rangle$. It follows that G_3 is not in $2\mathcal{J}(\mathbb{Q})$ (but we already knew that, since G_3 is nontrivial in $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$).

An inspection of Table I yields that any point $[P + P] \in \mathcal{J}(\mathbb{Q})$ lies in $\mathcal{J}(\mathbb{Q}_7)^0$ or in $T+4G_3+\mathcal{J}(\mathbb{Q}_7)^0$. However, the following argument mod 13 rules out $[P+P] = T + 4G + n8G$.

We have that $\{0, T, [(\sqrt{2}, 0) + (-\sqrt{2}, 0)], [(\sqrt{10}, 0) + (-\sqrt{10}, 0)]\}$ form a subgroup of $\mathcal{J}(\mathbb{F}_{13})$ isomorphic to $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$. Furthermore, $G_3 \bmod 13$ and $[(1, 6) + (1, 6)] \bmod 13$ generate cyclic subgroups of order 7 with trivial intersection. It follows that $\mathcal{J}(\mathbb{F}_{13}) \simeq \mathbb{Z}/(2) \times \mathbb{Z}/(2) \times \mathbb{Z}/(7) \times \mathbb{Z}/(7)$, and thus that G_3 is not in $7\mathcal{J}(\mathbb{Q})$. Furthermore, $\mathcal{J}(\mathbb{Q}) \bmod 13$ is generated by T and G_3 (since we already saw that G_3 is not in $2\mathcal{J}(\mathbb{Q})$). Table II shows that no point $T + nG_3$ can be of the form $[2P]$. We have not proved that G_3 is a generator and we do not need to either. It is enough to know that G_3 is not twice or seven times a point in $\mathcal{J}(\mathbb{Q})$. Upon choice of a generator, we get

$$\mathcal{J}(\mathbb{Q}) \cap \mathcal{J}(\mathbb{Q}_7)^0 \subset \{n8G_3 : n \in \mathbb{Q} \cap \mathbb{Z}_7 \cap \mathbb{Z}_2\}.$$

We compute $8G_3$ represented as a divisor on $\mathcal{C}_3$ using the genus 2 analogon of the chord-tangent method for computing on elliptic curves. The result is too large to print here, but using a computer algebra package, we can calculate it and substitute it in the formulas by Flynn. We get $\operatorname{Log}(8G_3) = (133, 14) \bmod 7^3$. Lemma 4 yields that the only $n \in \mathbb{Z}$ such that $8nG_3 = [P + P]$ is $n = 0$. However, note that if $G_3 = kG'$, we know that $2, 7 \nmid k$, so the order of $G' \bmod 7$ will also be 8 and $\operatorname{Log}(8G') = k \operatorname{Log}(8G_3)$. Thus, only $0 \in \mathcal{J}(\mathbb{Q}_7)^0 \cap \mathcal{J}(\mathbb{Q})$ is of the form $[P + P]$. The only points P on $\mathcal{C}$ such that $[P + P] = 0$ are points with $Y(P) = 0$ or $P = \infty$. The only rational points with this property are $P = \infty$ and $P = (0, 0)$. □

PROPOSITION 4. $\mathcal{C}_4(\mathbb{Q}) = \{(0, 0), \infty\}$.

Proof. Fix α_4 such that $\alpha_4^2 - 36\alpha_4 - 648 = 0$. We have that $P_4 = (\alpha_4, 288\alpha_4 + 2592)$ is a point on $\mathcal{C}_4$ and

$$G_4 = [P_4 + \bar{P}_4], T = [(0, 0) + \infty] \in \mathcal{J}(\mathbb{Q}) = \mathcal{J}_{\mathcal{C}_4}(\mathbb{Q}).$$

It is straightforward to verify that

$$\mu_{\mathbb{Q}_2}(\mathcal{J}(\mathbb{Q}_2)/2\mathcal{J}(\mathbb{Q}_2)) = \mu_{\mathbb{Q}_2}(\langle T, G_4, [(4, 2^4\sqrt{-2183}) + \infty]\rangle).$$

The intersection $\mathcal{G}$ with the pullback of this set to $M_{\mathbb{Q}}$ is two-dimensional. Since $2T = 0$, this bounds the rank of $\mathcal{J}(\mathbb{Q})$ to one. By (6), we have $\#\mathcal{J}(\mathbb{F}_7) = 26$ and that $\#\mathcal{J}(\mathbb{F}_{13}) = 196$. Therefore, $\mathcal{J}_{\mathrm{tor}}(\mathbb{Q}) = \{0, T\}$ and $\mathcal{J}(\mathbb{Q}) \simeq \mathbb{Z}/(2) \times \mathbb{Z}$.

https://doi.org/10.1023/A:1001529706709 Published online by Cambridge University Press

By some computations in $\mathcal{J}(\mathbb{F}_{13})$, we see that $T \bmod 13$ and $[(\sqrt{6}, 0)+(-\sqrt{6}, 0)]$ generate a $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$ subgroup of $\mathcal{J}(\mathbb{F}_{13})$ and that $[(2, 5) + (2, 5)]$ and $2G_4$ generate distinct order 7 subgroups. It follows that $\mathcal{J}(\mathbb{F}_{13}) \simeq \mathbb{Z}/(2) \times \mathbb{Z}/(2) \times \mathbb{Z}/(7) \times \mathbb{Z}/(7)$. We know that $\mathcal{J}(\mathbb{Q}) \bmod 13$ is a subgroup with 2 generators, one of which has order 2 and contains T and G_4. Computations show that $\#\langle T, G_4\rangle = 28$, and therefore T and G_4 generate $\mathcal{J}(\mathbb{Q}) \bmod 13$, since such a group is maximal under the given properties. Table III shows that the only point in $\mathcal{J}(\mathbb{Q})$ of the form $[P + P]$ is $[2\infty]$ (use that if $D = [P + P]$, then $-D = [\hat{P} + \hat{P}]$). Therefore, every point of the form $[P + P] \in \mathcal{J}(\mathbb{Q})$ must lie in $\mathcal{J}(\mathbb{Q}_{13})^0$.

Table III. (half of) Image of $\mathcal{J}_{\mathcal{C}_4}(\mathbb{Q})$ in $\mathcal{J}_{\mathcal{C}_4}(\mathbb{F}_{13})$

0	$[2\infty]$
G_4	$[(-2, 1) + (-1, 3)]$
$2G_4$	$[(-2, -1) + (2, 5)]$
$3G_4$	$[(-1, 3) + (2, 5)]$
$4G_4$	$[(\gamma_1, 5\gamma_1 + 6) + (-4 - \gamma_1, -1 - 5\gamma_1)]$
$5G_4$	$[(\gamma_2, 4\gamma_2 + 4) + (-3 - \gamma_2, 5 - 4\gamma_2)]$
$6G_4$	$[(\gamma_3, 6\gamma_3 + 3) + (5 - \gamma_3, -6 - 6\gamma_3)]$
$7G_4$	$[(\gamma_4, 0) + (-\gamma_4, 0)]$
T	$[(0, 0) + \infty]$
$T + G_4$	$[(2, -5) + (4, -3)]$
$T + 2G_4$	$[(1, -2) + (-4, -2)]$
$T + 3G_4$	$[(-2, -1) + (4, -3)]$
$T + 4G_4$	$[(-1, 3) + (4, -3)]$
$T + 5G_4$	$[(\gamma_5, -5\gamma_5 + 4) + (2 - \gamma_5, 5\gamma_5 - 6)]$
$T + 6G_4$	$[(\gamma_6, -4\gamma_6 - 3) + (-2 - \gamma_6, 4\gamma_6 + 5)]$
$T + 7G_4$	$[(\gamma_7, 0) + (-\gamma_7, 0)]$
	$\gamma_1^2 + 4\gamma_1 - 4 = 0$
	$\gamma_2^2 + 3\gamma_2 + 6 = 0$
	$\gamma_3^2 - 5\gamma_3 - 4 = 0$
	$\gamma_4^2 + 6 = 0$
	$\gamma_5^2 - 2\gamma_5 - 6 = 0$
	$\gamma_6^2 + 2\gamma_6 - 4 = 0$
	$\gamma_7^2 - 6 = 0$

We compute that $\mathrm{Log}(14G_4) = (1456, 1534) \bmod 13^3$. This is not congruent to $(0, 0) \bmod 13^2$, so we see G_4 is not in $13\mathcal{J}(\mathbb{Q})$. This means

$$\mathcal{J}(\mathbb{Q}) \cap \mathcal{J}(\mathbb{Q}_{13})^0 \subset \{14nG_4 : n \in \mathbb{Q} \cap \mathbb{Z}_{13}\}.$$

https://doi.org/10.1023/A:1001529706709 Published online by Cambridge University Press

Lemma 4 proves that 0 is the only point in $\mathcal{J}(\mathbb{Q})$ of the form $[P + P]$. The only $P \in \mathcal{C}(\mathbb{Q})$ such that $[P + P] = 0$ are ∞ and points with $Y(P) = 0$, i.e. $(0, 0)$. □

PROPOSITION 5. $\mathcal{C}_5(\mathbb{Q}) = \{(0, 0), \infty, (-2, 88), (-2, -88)\}$

Proof. We write $P_5 = (-2, 88)$, $T = [(0, 0) + \infty]$ and $G_5 = [P_5 + \infty]$. We have that

$$\mu_{\mathbb{Q}_2}(\mathcal{J}(\mathbb{Q}_2)/2\mathcal{J}(\mathbb{Q}_2)) = \mu_{\mathbb{Q}_2}(\langle T, G_5, [(-12, 2^3 3^2\sqrt{-39}) + \infty]\rangle)$$

and that the intersection of $\mathcal{G}$ with the pullback of this space to $M_{\mathbb{Q}}$ is two-dimensional. Thus, $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q}) = \langle T, G_5\rangle$. Using (6) we find that $\#\mathcal{J}(\mathbb{F}_{17}) = 2{\cdot}89$ and $\#\mathcal{J}(\mathbb{F}_{43}) = 2^2{\cdot}3^3{\cdot}17$. We see that $\mathcal{J}_{\mathrm{tor}}(\mathbb{Q}) = \{0, T\}$ and $\mathcal{J}(\mathbb{Q}) \simeq \mathbb{Z}/(2) \times \mathbb{Z}$. Furthermore, from the fact that $108G_5 \bmod 43 \neq 0$, we conclude that G_5 is not in $17\mathcal{J}(\mathbb{Q})$. Some computation shows that $\mathcal{J}(\mathbb{F}_{11}) = (\mathbb{Z}/(2))^3 \times \mathbb{Z}/(17)$. Since $G_5 \bmod 11 = [(-2, 0) + \infty]$ and G_5 is not in 17-divisible, we see that $\mathcal{J}(\mathbb{Q}) \bmod 11$ is completely 2-torsion. A 2-torsion point being of the form $[P + P]$ means that $\hat{P} = P$ and thus $[P + P] = 0$. Therefore, any rational point $P \in \mathcal{C}_5(\mathbb{Q})$ has $[P + P] \in \mathcal{J}(\mathbb{Q}_{11})^0$. We have $2G_5 \in \mathcal{J}(\mathbb{Q}_{11})^0$. However, the formulas available for s_1, s_2 are not defined for points of the form $[P + P]$. We could compute $(s_1, s_2)(2G_5)$ by taking limits, but for our purposes, $(s_1, s_2)(6G_5)$ are also sufficient, so we will compute these. We find $\mathrm{Log}(6G_5) = (649, 341) \bmod 11^3$. These values satisfy $L_1^4 - 3888L_2^4 = 0 \bmod 11^6$. Since $\mathrm{Log}(6G_5) \neq (0, 0) \bmod 11^2$, we see that $6G_5$ (and therefore G_5) is not 11-divisible. Upon choice of a generator we have $\mathcal{J}(\mathbb{Q}) \cap \mathcal{J}(\mathbb{Q}_{11})^0 \subset \{n2G_5 : n \in \mathbb{Q} \cap \mathbb{Z}_{11}\}$. and we see that the Log of that generator also satisfies $L_1^4 - 3888L_2^4 = 0 \bmod 11^6$. By Lemma 4, there is at most one pair of nontrivial points in $\mathcal{J}(\mathbb{Q})$ of the form $[P + P]$. Together with the points $P \in \mathcal{C}(\mathbb{Q})$ with $[P + P] = 0$, these are the points mentioned in the proposition. □

THEOREM 6. *The only solutions to* $x^2 + y^8 = z^3$ *with* $x, y, z \in \mathbb{Z}$ *and* $\gcd(x, y, z) = 1$ *are* $(x, y, z) = (\pm 1, 0, 1), (0, \pm 1, 1)$ and $(\pm 1549034, \pm 33, 15613)$.

Proof. The solutions with $xyz = 0$ are clear. Solutions with $xyz \neq 0$ correspond to affine rational points on the curves $\mathcal{C}_1, \ldots, \mathcal{C}_5$. Proposition 1 and 2 show that $\mathcal{C}_1$ and $\mathcal{C}_2$ contain no such points. The point $(0, 0)$ on $\mathcal{C}_3, \mathcal{C}_4, \mathcal{C}_5$ gives rise to solutions with $y = 0$. By Proposition 3, 4 and 5, $\mathcal{C}_5$ is the only curve that contains other affine rational points. It contains two such points. Taking into account the sign of x, these give rise to four more solutions of $x^2 + y^8 = z^3$. Therefore, the list stated in the theorem is complete. □

6. References for Computations and Further Reading

The computations necessary for the proofs presented in this article are clearly undoable with pencil and paper. While Lemma 1 and 2 may be checked by hand,

https://doi.org/10.1023/A:1001529706709 Published online by Cambridge University Press

for Lemma 3 it is necessary to compute fundamental units and (trivial) ideal class groups in quadratic orders.

The computer algebra package KASH [DKF97] has good support for this. Versions 1.6 through 1.8 were used to obtain all algebraic-number theoretic results used in this article. The package is maintained by the group of Pohst and is free. It can be obtained from `ftp://ftp.math.tu-berlin.de/pub/algebra/Kant`.

Determining conductor, minimal model, rank and torsion of elliptic curves are also tasks better left to a computer. The Maple package Apecs 3.8 by Connell was used for this. It can be obtained from `ftp://math.mcgill.ca/pub/apecs`.

Doing a 2-descent on genus 2 curves requires information on class-groups, units, factorisation of ideals and squares in number fields up to degree 6 (for the curves in this article, degree 4). Kash provides ample support for this kind of calculations. The ranks computed in this article were verified by calculations using Kash and by Stoll [Sto96] who uses a program not based on Kash.

The computations on Jacobians were done in Maple Vr3 using the cubic fitting algorithm described in Section 1.2 of [CF96]. The formulas mentioned in Section 4.3 are available from `ftp://ftp.liv.ac.uk/~ftp/pub/genus2`. In this article, these were used in Maple Vr3 to obtain local coordinates and approximations to $\theta(n)$.

In all cases, calculations took at most a couple of minutes on a HP712/60 workstation. The interested reader can download the scripts `prfs283.mpl` and `dscnt283.g`. See for more information `README` in

`ftp://ftp.wi.leidenuniv.nl/pub/GM/Publications/N.Bruin/`

Most of the required theory for applying effective Chabauty can be found in [CF96]. The history of the formulas can be found in [Fly90] and [Fly93]. Notation in these article slightly differs from the one used here and in [CF96]. For people interested in doing this kind of computations themselves, [FPS95] is a valuable source. Further references for determining Mordell–Weil ranks are [Sch95] and [PS97].

Note that the curves in this article, all having a rational Weierstrass-point, can in principle be analysed as suggested in [Gra90] and [GG93]. While this method may be theoretically simpler, the availability of the formulas in Flynn's case makes it easier to use his (more general) method. Also, the reader might be interested in [Col85], which offers an alternative treatment of Chabauty's method.

Acknowledgements

I would like to thank Frits Beukers for his critical proof-reading and for suggesting the present form of the proof of the 2-4-6, 2-6-4 and 4-6-2 cases and Prof. Tijdeman for thoroughly checking the formulation of the text. Furthermore, I am indebted to Bjorn Poonen for pointing out to me the principles of effective Chabauty and to Michael Stoll for providing me with all the Mordell–Weil ranks I required. The

https://doi.org/10.1023/A:1001529706709 Published online by Cambridge University Press

quick responses of the Kant group have made my work considerably easier, as did the symbolic computing capabilities of Maple.

References

[Beu98] Beukers, Frits: The diophantine equation $Ax^p + By^q = Cz^r$, *Duke Math. J.* **91** (1998), 61–88.

[Cas86] Cassels, J. W. S.: *Local Fields*, London Math. Soc. Stud. Texts 3, Cambridge University Press, 1986.

[CF96] Cassels, J. W. S. and Flynn, E. V.: *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*, London Math. Soc. Lecture Notes Ser. 230, Cambridge Univ. Press, Cambridge, 1996.

[Cha41] Chabauty, C.: Sur les points rationels des variétés algebriques dont l'irregularité est supérieur à la dimension, *C. R. Acad. Sci. Paris* **212** (1941), 1022–1024.

[Col85] Coleman, R. F.: Effective chabauty, *Duke Math. J.* **52** (1985), 765–770.

[Cre92] Cremona, J.E.: *Algorithms for Modular Elliptic Curves*, Cambridge University Press, 1992.

[DKF97] Daberkow, M., Fieker, C., Klueners, J., Pohst, M., Roegner, K., Schoernig, M. and Wildanger, K.: Kant v4, *J. Symb. Comp.* **24** (1997), 267–284.

[DG95] Darmon, Henri and Granville, A.: On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$, *Bull. London Math. Soc.* **27** (1995), 513–543.

[DM96] Darmon, Henri and Merel, Loïc: Winding quotients and some variants of Fermat's Last Theorem, to appear in *J. Reine Angew. Math.*, 1996.

[Fly90] Flynn, E. V.: The Jacobian and formal group of a curve of genus 2 over an arbitrary ground field, *Math. Proc. Cambridge Philos. Soc.* **107** (1990), 425–441.

[Fly93] Flynn, E. V.: The group law on the Jacobian of a curve of genus 2. *J. Reine Angew. Math.* **439** (1993), 45–69.

[Fly97] Flynn, E. V.: A flexible method for applying Chabauty's theorem, *Compositio Math.* **105** (1997), 79–94.

[FPS95] Flynn, E. V., Poonen, B. and Schaefer, E. F.: Cycles of quadratic polynomials and rational points on a genus-two curve, Preprint No. 062-95, MSRI, 1995. To appear in *Duke Math J.*

[GC93] Gordon, Daniel M. and Grant, David: Computing the Mordell–Weil rank of Jacobians of curves of genus two, *Trans. Amer. Math. Soc.* **337**(2) (1993), 807–824.

[Gra90] Grant, David: Formal groups in genus two. *J. Reine Angew. Math.* **411** (1990), 96–121.

[Poo97] Poonen, B.: Some diophantine equations of the form $x^n + y^n = z^m$, Preprint, 1997.

[PS97] Poonen, Bjorn and Schaefer, Edward F.: Explicit descent for Jacobians of cyclic covers of the projective line, *J. Reine Angew. Math.* **488** (1997), 141–188.

[Sch95] Schaefer, Edward F.: 2-descent on the Jacobians of hyperelliptic curves, *J. Number Theory* **51** (1995), 219–232.

[Sto96] Stoll, Michael.: Implementing 2-descent in genus 2, In preparation, 1996.

[Thi96] Thiboutot, Steve: Courbes elliptiques, représentations galoisiennes et l'équation $x^2+y^3 = z^5$, Master's thesis, Université McGill, Montréal, 1996.

https://doi.org/10.1023/A:1001529706709 Published online by Cambridge University Press