Canad. Math. Bull. Vol. **52** (1), 2009 pp. 117–126

On the Rational Points of the Curve $f(X,Y)^q = h(X)g(X,Y)$

Dimitrios Poulakis

Abstract. Let $q = 2,3$ and $f(X,Y)$, $g(X,Y)$, $h(X)$ be polynomials with integer coefficients. In this paper we deal with the curve $f(X,Y)^q = h(X)g(X,Y)$, and we show that under some favourable conditions it is possible to determine all of its rational points.

1 Introduction

Let K be a number field and $F(X,Y)$ an absolute irreducible polynomial of $K[X,Y]$ such that the algebraic curve C defined by the equation $F(X,Y) = 0$ has genus ≥ 2. Faltings proved that the set of rational points of C over K is finite (see [10]). Faltings' proof and its simplifications (see [1, 27]) do not give us a method for determining all the rational points of C. For this task, there are only three methods which are applicable to particular families of curves, except for showing that C has no rational points because $C(\mathbb{Q}_p)$ is empty for some completion $\mathbb{Q}_p$ of $\mathbb{Q}$. Chabauty's method (see [4, 6, 11]) is applicable in the case where the Mordell–Weil rank of the Jacobian of C over K is smaller than the genus of C. Some generalizations of it are given in [2, 3, 9, 12–14, 28]. The method of Dem'janenko and Manin (see [8, 20]) is applicable in the case where there are m independent morphisms from C to an elliptic curve with rank over K smaller than m. Some applications of it are given in [16, 26]. Finally, the method of heterogeneous spaces [7], which is influenced by Chevalley–Weil theorem [18, page 45], [5]), can be applied in some cases to reduce the problem to some curves whose arithmetic is known. The above methods have been applied mainly to curves of the form $F(X,Y) = Y^q - f(X)$, where $f(X) \in \mathbb{Q}[X]$ and $q = 2$ or 3. Some examples of non-superelliptic equations can be found in [24], which handles the equation $X^4 + (Y^2+1)(X+Y) = 0$, in [15], which deals with a higher genus curve that cover a genus 2 curve, and in [22], which studies some plane quartics.

In this paper, we reduce the problem of the determination of rational points of the curve $f(X,Y)^q = h(X)g(X,Y)$, where $f(X,Y), g(X,Y), h(X) \in \mathbb{Z}[X,Y]$ and $q = 2,3$, to the same problem for a finite family of curves of the form $aY^q = b(X)$, where a divides a fixed integer and $b(X) \in \mathbb{Z}[X]$. If the sets of rational points of curves $aY^q = b(X)$ are finite and we are able to determine them, then we can find all the rational points of $f(X,Y)^q = h(X)g(X,Y)$. Note that sometimes it is possible after the reduction to complete the solution using elementary methods (see, for instance, the proof of Proposition 4.3). Bounds for the integral points of these curves have been calculated using Baker's method (see [23]).

Received by the editors June 26, 2006; revised March 7, 2007.
AMS subject classification: Primary: 11G30; secondary: 14G05, 14G25.

To state our results we begin with some notation. Let $h(X) \in \mathbb{Z}[X] \setminus \mathbb{Z}$, $g(X,Y) \in \mathbb{Z}[X,Y] \setminus \{0\}$, and $f(X,Y) \in \mathbb{Z}[X,Y] \setminus \mathbb{Z}$. Suppose that $f(X,Y)$ and $g(X,Y)h(X)$ have no common factor and $g(X,Y)$ is not divisible by a polynomial of $\mathbb{Z}[X] \setminus \mathbb{Z}$. We denote by $R(X)$ the resultant of $f(X,Y)$ and $g(X,Y)$ with respect to Y. Let $h(X) = h_1(X)h_2(X)$, where $h_1(X)$, $h_2(X)$ are polynomials of $\mathbb{Z}[X] \setminus \{0\}$ without common roots and with relatively prime coefficients, such that the multiplicities of the roots of $h_1(X)$ are prime to q and $q | \deg h_1$. Further, we suppose that $h_2(X)g(X,Y)$ is not a constant. Write $h_1(X) = \eta(X-a_1)^{k_1} \cdots (X-a_m)^{k_m}$, where the roots $a_1, \dots, a_m$ are pairwise distinct. We suppose that $R(a_i) \neq 0$ $(i = 1, \dots, m)$ and put

$$\Theta = \eta^{m \deg R} \prod_{i=1}^{m} R(a_i).$$

Let h_0 be the leading coefficient of $h(X)$ and $R(h_1, h_2)$ the resultant of $h_1(X)$ and $h_2(X)$. We suppose that $f(X,Y)$, considered as a polynomial with coefficients in $\mathbb{Z}[X]$, has leading coefficient an integer f_0 (so the monomial with the highest power of Y is not divisible by X). Finally, let γ be the greatest common divisor of the coefficients of $g(X,Y)$. Consider now the polynomial $F(X,Y) = f(X,Y)^q - h(X)g(X,Y)$. We prove the following theorem.

Theorem 1.1 *Let $(x,y) \in \mathbb{Q}^2$ with $F(x,y) = 0$ and $xh(x)f(x,y) \neq 0$. Put $A(q) = qh_0 f_0 R(h_1,h_2)\Theta\gamma$. If $q = 2$, then there is a square-free integer b with $b|A(2)$ and $r \in \mathbb{Q}$ such that $br^2 = h_1(x)$. If $q = 3$, then there are relatively prime square-free integers c_1, c_2 with $c_1c_2|A(3)$ and $s \in \mathbb{Q}$ such that $c_1c_2^2s^3 = h_1(x)$.*

Corollary 1.2 *Let B_2 be the set of square-free divisors of $A(2)$ and B_3 the set of cube-free integers such that its prime divisors divide $A(3)$. Suppose that for every $b \in B_q$ either the set of rational points of curve $bT^q = h_1(X)$ or the set of rational points of surface $b^{-1}T^q = h_2(X)g(X,Y)$ is finite and explicitly determined. Then the set of rational points of $F(X,Y) = 0$ is explicitly determined.*

Note that the polynomial $F(X,Y)$ is not always irreducible. For instance, take $f(X,Y) = Y^a$, $h(X) = 1 - X^2$ and $g(X,Y) = Y^{2a} - X$, where a is a positive integer. Then $f(X,Y)^2 - h(X)g(X,Y) = X(1 + XY^2 - X^2)$.

The method of proof of Theorem 1.1 is based on the Chevalley–Weil theorem. By this theorem, if $\phi\colon D \to C$ is an unramified morphism of projective smooth curves defined over $\mathbb{Q}$, then there is a number field K such that $\phi^{-1}(C(\mathbb{Q})) \subseteq D(K)$. Suppose that the curves defined by $F(X,Y) = 0$ and by $F(X,Y) = T^q - h_1(X) = 0$ are irreducible. Thus, in our case, C and D are the desingularizations of these curves, respectively. In the proof of Theorem 1.1 we determine K and so we conclude that the rational solutions to $F(X,Y) = 0$ are covered by the rational points of finitely many twists of $T^q = h_1(X)$ which are explicitly given.

This paper is organized as follows. Section 2 is devoted to the proof of Theorem 1.1. In Section 3, we prove that the desingularization of the curve defined by $F(X,Y) = T^q - h_1(X) = 0$ is a an unramified cover of the desingularization of the curve defined by $F(X,Y) = 0$, provided that these two curves are irreducible. In Section 4, we present some applications of Theorem 1.1, solving equations of the form

$f(X,Y)^q = h(X)g(X,Y)$ over $\mathbb{Q}$. Finally, in Section 5, we obtain, with a completely elementary method, the rational solutions of the equation studied in [24].

2 Proof of Theorem 1.1

Consider an algebraic number w such that $w^q = h_1(x)$ and let $L = \mathbb{Q}(w)$. Suppose that $L \neq \mathbb{Q}$. We denote by S the set of prime numbers p such that $p|A(q)$. We denote by $\mathbb{Z}_{(p)}$ the local ring of $\mathbb{Z}$ at p and by D_p the discriminant of the integral closure of $\mathbb{Z}_{(p)}$ in L. If $z = p^r u/v$, where $u, v \in \mathbb{Z} \setminus \{0\}$ with $\gcd(u,v) = 1$ and $r \in \mathbb{Z}$, then we set $\mathrm{ord}_p(z) = r$. Furthermore we denote by $\bar{x}$, $\bar{y}$, $\bar{f}(X,Y)$, $\bar{g}(X,Y)$ and $\bar{h}_i(X)$ the reductions of x, y, $f(X,Y)$, $g(X,Y)$ and $h_i(X)$ modulo p, respectively. Since $p \nmid f_0 h_0 \gamma$, we have that the polynomials $\bar{f}(X,Y)$, $\bar{g}(X,Y)$ and $\bar{h}_i(X)$ are nonzero. Let $b_{i,j}$ ($j = 1, \dots, n(i)$) be the distinct roots of $f(a_i, Y) = 0$. Since $p \nmid f_0 h_0$, we deduce that a_i and b_{ij} are integral elements over $\mathbb{Z}_{(p)}$. Let K be the field generated over $\mathbb{Q}$ by the elements a_i, $b_{i,j}$ ($i = 1, \dots, m,\ j = 1, \dots, n(i)$). We denote by O_K the ring of integers of K.

Let $p \notin S$. We prove that p is not ramified in L. Suppose first that $\mathrm{ord}_p(x) \geq 0$. We separate the following two cases:

(i) $h_1(x) \not\equiv 0 \pmod p$. The discriminant of the polynomial $Q(T) = T^q - h_1(x)$ is $\Delta(Q) = (-q)^q h_1(x)^{q-1}$. Since $\mathrm{ord}_p(x) \geq 0$, $h_1(x) \not\equiv 0 \pmod p$ and $p \neq q$, we deduce that $\Delta(Q) \not\equiv 0, \infty \pmod p$. Thus, $\Delta(Q)$ is a unit in $\mathbb{Z}_{(p)}$. Since D_p divides $\Delta(Q)$, it follows that D_p is a unit in $\mathbb{Z}_{(p)}$ and so p is not ramified in L.

(ii) $h_1(x) \equiv 0 \pmod p$. Let $\wp$ be a prime ideal of O_K such that $\wp \cap \mathbb{Z} = (p)$. We denote by $\bar{a}_i$ and $\bar{b}_{ij}$ the reduction of a_i and b_{ij} modulo $\wp$ ($i = 1, \dots, m$), respectively. Since a_i and b_{ij} are integral elements over $\mathbb{Z}_{(p)}$, we get $\bar{a}_i, \bar{b}_{ij} \in O_K/\wp$. The equality $\bar{h}_1(\bar{x}) = 0$ implies that $(\bar{x}, \bar{y}) = (\bar{a}_i, \bar{b}_{ij})$ for some i and j.

Next, we consider the element $z = h_1(x)/f(x,y)^q$.

We have $h_1(x) f(x,y) \neq 0$ and so z is a nonzero rational number. The reduction of z modulo p is

$$\bar{z} = \frac{\bar{h}_1(\bar{x})}{\bar{f}(\bar{x}, \bar{y})^q} = \frac{1}{\bar{h}_2(\bar{a}_i)\bar{g}(\bar{a}_i, \bar{b}_{ij})}.$$

Since $p \nmid R(h_1, h_2)\Theta$, we deduce that $\bar{h}_2(\bar{a}_i) \neq 0$ and $\bar{g}(\bar{a}_i, \bar{b}_{ij}) \neq 0$. So, $\bar{z}$ is a nonzero element of the finite field $\mathbb{F}_p$ and hence z is a unit in $\mathbb{Z}_{(p)}$. Putting $\omega = w/f(x,y)$ we have $L = \mathbb{Q}(\omega)$ and $\omega^q = z$. The discriminant of the polynomial $P(T) = T^q - z$ is $\Delta(P) = (-q)^q z^{q-1}$ and, since $p \neq q$, $\Delta(P)$ is a unit in $\mathbb{Z}_{(p)}$. The discriminant D_p divides $\Delta(P)$ and so it follows that D_p is also a unit in $\mathbb{Z}_{(p)}$. Therefore p is not ramified in L.

Suppose now that $\mathrm{ord_p}(x) < 0$. Thus $1/x$ lies in the maximal ideal of $\mathbb{Z}_{(p)}$. Since $q|\deg h_1$, we have $\deg h_1 = qs$, where $s \in \mathbb{Z}$. Set $\theta = w/x^s$ and $H(X) = X^{qs} h_1(1/X)$. We have $L = \mathbb{Q}(\theta)$ and $\theta^q = H(1/x)$. The discriminant of $B(T) = T^q - H(1/x)$ is $\Delta(B) = (-q)^q H(1/x)^{q-1}$. Thus $\Delta(B) \equiv (-q)^q \eta \not\equiv 0 \pmod p$ and so $\Delta(B)$ is a unit in $\mathbb{Z}_{(p)}$. Since D_p divides $\Delta(B)$, we obtain that D_p is also a unit in $\mathbb{Z}_(p)$. Therefore p is not ramified in L.

Let $q = 2$ and write $h_1(x) = r^2 b$, where $b, r \in \mathbb{Z}$ and b is square-free. Then

https://doi.org/10.4153/CMB-2009-014-1 Published online by Cambridge University Press

$L = \mathbb{Q}(\sqrt{b})$. Since every $p \notin S$ is not ramified in L and the discriminant of L is either b or $4b$, we deduce that b is a divisor of $A(2)$. Finally, let $q = 3$ and set $h_1(x) = s^3c$, where $c, s \in \mathbb{Z}$ and c is cube-free. Write $c = c_1c_2^2$, where c_1, c_2 are relatively prime square-free integers. Then $L = \mathbb{Q}(\sqrt[3]{c})$ and the discriminant of L is $-27c_1^2c_2^2$, if $c_1c_2 \not\equiv 1 \pmod 9$ and $-3c_1^2c_2^2$, otherwise. Since every $p \notin S$ is not ramified in L, c_1c_2 divides $A(3)$.

3 Geometrical Interpretation

Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$. Suppose that $F(X,Y)$ is absolutely irreducible and denote by C a smooth projective model of the curve defined by $F(X,Y) = 0$ and by D a smooth projective curve with function field $\overline{\mathbb{Q}}(C)(t)$, where $t^q = h_1(X)$. We prove that D is an unramified cover of C. This is an immediate consequence of the following result.

Proposition 3.1 *The field extension $\overline{\mathbb{Q}}(C)(t)/\overline{\mathbb{Q}}(C)$ is unramified.*

Proof Let $R = \overline{\mathbb{Q}}(X)$. If $a \in \overline{\mathbb{Q}}$, then we denote by $\hat{R}_a$ the completion of R under the discrete valuation ring V_a of R defined by $X - a$. Similarly, we denote by $\hat{R}_\infty$ the completion of R under the discrete valuation ring V_∞ of R defined by $1/X$. Let $F(X,Y) = F_1(Y)\cdots F_r(Y)$ be the decomposition of $F(X,Y)$ in irreducible factors over $\hat{R}_b$, where $b \in \overline{\mathbb{Q}} \cup \{\infty\}$. The discrete valuation rings V_i $(i = 1,\dots,r)$ of $\overline{\mathbb{Q}}(C)$ which extend V_b correspond to F_i $(i = 1,\dots,r)$ and theirs completions are $\hat{R}_b(y_i) \cong \hat{R}_a[Y]/(F_i(Y))$ $(i = 1,\dots,r)$, respectively (see [19, Chapter 14, §4]).

Let μ_i be the ramification degree of V_i above V_b. By [17, Proposition 12, page 52], we have $\hat{R}_b(y_i) = \hat{R}_b(\pi^{1/\mu_i})$, where $\pi = X - b$ if $b \in \overline{\mathbb{Q}}$ and $\pi = 1/X$ otherwise. Let b be one of the roots $a_1,\dots,a_m$ of $h_1(X)$ with multiplicity k. Then V_i dominates the local ring of C at a point (b,c) with $f(b,c) = 0$. Since $R(b) \neq 0$, we get $g(b,c) \neq 0$ and so, $g(X,Y)$ defines a unit into V_i. Thus, from the equation $f(X,Y)^q = h(X)g(X,Y)$, taking the orders at V_i of functions defined by $f(X,Y)$, $h(X)$ and $g(X,Y)$ on C, we deduce that $q|\mu_i$.

On the other hand, the extension $R(t)/R$ is ramified only above $a_1,\dots,a_m$ with ramification index equal to q. Thus, if V is a discrete valuation ring of $R(t)$, then the completion of $R(t)$ at V is $\hat{R}_a(t) = \hat{R}_a((X - a_i)^{1/q})$ if V lies above $X = a_i$ and $\hat{R}_a$ otherwise (see [19, Chapter 14, §4] and [17, Proposition 12, page 52]).

Let U be a discrete valuation ring of $\overline{\mathbb{Q}}(C)(t)$ which extends V_b. If $b \neq a_i$ $(i = 1,\dots,m)$, then the completion of $\overline{\mathbb{Q}}(C)(t)$ at U is $\hat{R}_b(y_i)$ which coincides with the completion of $\overline{\mathbb{Q}}(C)$ at $U \cap \overline{\mathbb{Q}}(C)$. If $b = a_j$, then the completion of $\overline{\mathbb{Q}}(C)$ at $U \cap \overline{\mathbb{Q}}(C)$ is $\hat{R}_b((X - a_j)^{1/\mu_i})$. Since $q|\mu_i$, we have $\hat{R}_b((X - a_j)^{1/q}) \subseteq \hat{R}_b((X - a_j)^{1/\mu_i})$ and so the completion of $\overline{\mathbb{Q}}(C)(t)$ at U is $\hat{R}_b((X - a_j)^{1/\mu_i})$. Therefore, the extension $\overline{\mathbb{Q}}(C)(t)/\overline{\mathbb{Q}}(C)$ is unramified. ■

4 Applications

In this section we give some applications of Theorem 1.1, determining the rational solutions of equations of the form $f(X,Y)^q = h(X)g(X,Y)$. In Propositions 4.1 and

4.2, in order to compute the rank of the elliptic curves involved, we used the package "algcurves[Weierstrassform]" of Maple 7 for the calculation of a normal form and next J. Cremona's program *mwrank*.

Proposition 4.1 *Let $n, m \in \mathbb{Z}$ with $n \geq 3$ and $m \geq 1$. Then the only rational solutions to the equation*

$$Y^{2m} = (X^{2^n} - 1)(XY - 1)$$

are $(X,Y) = (\pm 1, 0), (0, \pm 1)$.

Proof We have $X^{2^n} - 1 = (X^4)^{2^{n-2}} - 1 = (X^4 - 1)[(X^4)^{2^{n-2}-1} + \cdots + 1]$. The discriminant of $X^{2^n} - 1$ is -2^{n2^n} and so, the resultant of $X^4 - 1$ and $(X^4)^{2^{n-2}-1} + \cdots + 1$ is not divisible by primes > 2. Furthermore the resultant of Y^m and $XY - 1$ with respect to X is equal to 1. Let $(x,y) \in \mathbb{Q}^2$ be a solution of the above equation with $y \neq 0$. By Theorem 1.1 we obtain there is $r \in \mathbb{Q}$ such that $br^2 = x^4 - 1$, where $b = 1$ or 2. Thus, we consider the elliptic curves $E_b \colon bY^2 = X^4 - 1$, where $b = 1, 2$. The curve E_1 is birational equivalent to the curve $C_1 \colon Y_0^2 = X_0^3 + 4X_0$. The birational equivalence is given by

$$(X_0, Y_0) = \Big(2\frac{X-1}{X+1}, 4\frac{Y}{(X+1)^2}\Big), \quad (X,Y) = \Big(\frac{X_0+2}{-X_0+2}, \frac{4Y_0}{(-X_0+2)^2}\Big).$$

We have $C_1(\mathbb{Q}) = \{(0,0), (2, \pm 4), \infty\}$ and so we obtain the rational point of E_1, $(X,Y) = (1,0)$. The curve E_2 is birational equivalent to the curve $C_2 \colon Y_0^2 = X_0^3 + 16X_0$ by the relations

$$(X_0, Y_0) = \Big(4\frac{X-1}{X+1}, 16\frac{Y}{(X+1)^2}\Big), \quad (X,Y) = \Big(\frac{X_0+4}{-X_0+4}, \frac{4Y_0}{(-X_0+4)^2}\Big).$$

We have $C_2(\mathbb{Q}) = \{(0,0), \infty\}$ and we obtain again the rational point of E_1, $(X,Y) = (1,0)$. ∎

Proposition 4.2 *The rational solutions of the equation*

$$(1 + XY + X^2 + Y^3)^3 = X(X-1)(X+1)(X-Y)^2$$

are $(X,Y) = (0,-1), (1,-1)$.

Proof The resultant of $1 + XY + X^2 + Y^3$ and $(X-Y)^2$ with respect to X is equal to $R(X) = (1 + 2X^2 + X^3)^2$. Furthermore we have $R(0)R(1)R(-1) = 64$. Let $(x,y) \in \mathbb{Q}^2$ be a solution of the above equation with $x \neq 0, \pm 1$ and $x \neq y$. By Theorem 1.1, there is an integer b with $b|4$ and $r \in \mathbb{Q}$ such that $br^3 = x(x^2 - 1)$. Thus we consider the elliptic curves $E_b \colon bY^3 = X(X^2 - 1)$, where $\pm b = 1, 2, 4$. The correspondence $(x,y) \mapsto (-x, y)$ defines an isomorphism between the curves E_b and E_{-b}. So, we have to deal only with the following three cases:

(i) $b = 1$. The curve E_1 is birational equivalent to $C_1 \colon Y_0^2 = X_0^3 + 1$. The set of rational points of C_1 is $C_1(\mathbb{Q}) = \{(-1,0), (0, \pm 1), (2, \pm 3), \infty\}$. The birational equivalence between E_1 and C_1 is given by the relations

$$(X_0, Y_0) = (3X^2 - 1 + 3YX + 3Y^2, 9X^3 - 6X + 9YX^2 - 3Y + 9Y^2X)$$

https://doi.org/10.4153/CMB-2009-014-1 Published online by Cambridge University Press

and
$$(X,Y)=\left(\frac{Y_0(X_0+1)}{3-3X_0+3X_0^2},\frac{Y_0(X_0-2)}{3-3X_0+3X_0^2}\right).$$
Thus we obtain $E_1(\mathbb{Q})=\{(0,0),(1/3,-2/3),(-1/3,2/3),(\pm 1,0),\infty\}$. It follows that $E_{-1}(\mathbb{Q})=\{(0,0),(-1/3,-2/3),(1/3,2/3),(\pm 1,0),\infty\}$.

(ii) $b=2$. The curve E_2 is birational equivalent to $C_2\colon Y_0^2=X_0^3+4$ and the birational equivalence is given by the relations:
$$(X_0,Y_0)=\left(\frac{-2Y}{X},\frac{2}{X}\right),\quad (X,Y)=\left(\frac{2Y_0}{4+{X_0}^3},\frac{-X_0Y_0}{4+{X_0}^3}\right).$$
We have $C_2(\mathbb{Q})=\{(0,\pm 2),\infty\}$ and so we deduce that $E_2(\mathbb{Q})=\{(\pm 1,0),\infty\}$. It follows that $E_{-2}(\mathbb{Q})=\{(\pm 1,0),\infty\}$.

(iii) $b=4$. The curve E_4 is birational equivalent to $C_4\colon Y_0^2=X_0^3+16$ and this equivalence is given by the relations:
$$(X_0,Y_0)=\left(\frac{-4Y}{X},\frac{4}{X}\right),\qquad (X,Y)=\left(\frac{4Y_0}{16+{X_0}^3},\frac{-X_0Y_0}{16+{X_0}^3}\right).$$
We have $C_4(\mathbb{Q})=\{(0,\pm 4),\infty\}$ and so, we get
$$E_4(\mathbb{Q})=E_{-4}(\mathbb{Q})=\{(\pm 1,0),\infty\}$$
.

By the above procedure we obtain $x\in\{0,\pm 1,\pm 1/3\}$. ■

The following equation is solved using only Theorem 1.1 and some elementary arithmetic.

Proposition 4.3 *The only rational solution of the equation*
$$(X+Y)^{20}=(7X^2-2)(X^2+Y^2)$$
is $(X,Y)=(0,0)$.

Proof The resultant of $(X+Y)^{10}$ and X^2+Y^2 as polynomials with coefficients in $\mathbb{Z}[X]$ is equal to $R(X)=1024X^{20}$. The roots of the polynomial $7X^2-2$ are the numbers $\pm\sqrt{2/7}$. We have $R(\sqrt{2/7})R(\sqrt{2/7})=2^{30}/7^{20}$. Let $(x,y)\in\mathbb{Q}^2$ be a solution of the above equation with $x+y\neq 0$. By Theorem 1.1, there is an integer $b>0$ dividing 14 and $r\in\mathbb{Q}$ such that $br^2=7x^2-2$. We separate the following cases:

(i) If $b=1$, then there are $u,v,z\in\mathbb{Z}$ with $\gcd(u,v,z)=1$ such that $u^2=7v^2-2z^2$. Thus $u^2\equiv -2z^2 \pmod 7$. If $7|u$, then $7|z$ and we obtain $7|v$. Thus $\gcd(u,v,z)>1$ which is a contradiction. So $7\nmid u$. Similarly, we have $7\nmid z$. Hence -2 is a quadratic residue modulo 7, which is a contradiction.

(ii) If $b=2$, then there are $u,v,z\in\mathbb{Z}$ with $\gcd(u,v,z)=1$ such that $2u^2=7v^2-2z^2$. It follows that v is even and so there is $w\in\mathbb{Z}$ such that $u^2=14w^2-z^2$, whence $u^2\equiv -z^2 \pmod 7$. As in the previous case, we have $7\nmid u$ and $7\nmid z$. Thus we deduce that -1 is a quadratic residue modulo 7, which is a contradiction.

https://doi.org/10.4153/CMB-2009-014-1 Published online by Cambridge University Press

(iii) If $b = 7$, then there is $a \in \mathbb{Q}$ such that $7^{(2k+1)e}a^2 = x^2 + y^2$, where $e = \pm 1$ and $\mathrm{ord}_7(a) = 0$. Let $a = a_1/a_2$, $x = x_1/x_2$, $y = y_1/y_2$, with $a_i, x_i, y_i \in \mathbb{Z}$ $(i = 1, 2)$, $\gcd(a_1, a_2) = \gcd(x_1, x_2) = \gcd(y_1, y_2) = 1$ and $7 \nmid a_1a_2$. Suppose that $e = 1$. Thus we have

$$7^{2k+1}(a_1x_2y_2)^2 = (x_1y_2a_2)^2 + (y_1x_2a_2)^2,$$

and since $7 \nmid a_2$ we obtain that $7|(x_1y_2)^2 + (y_1x_2)^2$. If x_1y_2 and y_1x_2 are not divisible by 7, then we obtain -1 is a quadratic residue modulo 7, which is a contradiction. Consider the case $7|x_1y_2$ and $7|x_2y_1$. Then either $7|x_1$ and $7|y_1$ or $7|x_2$ and $7|y_2$. If $7|x_1$ and $7|y_1$, then we deduce that $7|x_2y_2$ and so either $7|x_2$ or $7|y_2$, which is a contradiction. Suppose that $7|x_2$ and $7|y_2$. If $\mathrm{ord}_7(x_2) \neq \mathrm{ord}_7(y_2)$, then the above equality gives

$$2\min\{\mathrm{ord}_7(x_2), \mathrm{ord}_7(y_2)\} > 2\mathrm{ord}_7(x_2) + 2\mathrm{ord}_7(y_2),$$

which is a contradiction. If $\mathrm{ord}_7(x_2) = \mathrm{ord}_7(y_2)$, then $x_2 = 7^r x_3$ and $y_2 = 7^r y_3$, where $x_3, y_3, r \in \mathbb{Z}$, $7 \nmid x_3y_3$ and $r > 0$. Thus $7|(x_1y_3)^2 + (y_1x_3)^2$ and x_1y_3, y_1x_3 are not divisible by 7. It follows that -1 is quadratic residue modulo 7, which is a contradiction. Finally, we consider the case $e = -1$. We have

$$(a_1x_2y_2)^2 = [(x_1y_2a_2)^2 + (y_1x_2a_2)^2]7^{2k+1}.$$

Since $7 \nmid a_1$, we have $7^{2k+1}|(x_2y_2)^2$. It follows that $7|(x_1y_2)^2 + (y_1x_2)^2$. Working as previously, we deduce a contradiction.

(iv) If $b = 14$, then, working as in case (iii), we obtain a contradiction.

Therefore there is no solution $(x, y) \in \mathbb{Q}^2$ with $x + y \neq 0$. If $x + y = 0$, then we obtain $x = y = 0$. ∎

Next, we determine the rational solutions of two classes of equations.

Proposition 4.4 *Let p be an odd prime number $\equiv 17 (\mathrm{mod} 24)$ for which 2 is not a quartic residue. Then the equation*

$$(X^2 + Y^2)^2 = (4pX^4 - 1)(3X^2 + Y^2)$$

has no rational solution.

Proof Let $(x, y) \in \mathbb{Q}^2$ be a solution of the above equation. The resultant of $X^2 + Y^2$ and $3X^2 + Y^2$ with respect to X is $R(X) = 4X^4$. We have

$$R(1/\sqrt[4]{4p})R(-1/\sqrt[4]{4p})R(1/i\sqrt[4]{4p})R(-1/i\sqrt[4]{4p}) = 1/p^4.$$

By Theorem 1.1, there is an integer $b > 0$ dividing $2p$ and $r \in \mathbb{Q}$ such that $br^2 = 4px^4 - 1$. Hence, we have the following cases:

(i) If $b = 1$, the since $p \equiv 1 (\mathrm{mod} 8)$ and 2 is not a quartic residue modulo p, the equation $Y^2 = 4pX^4 - 1$ has no solution in rational numbers (see [25, Proposition 6.5, page 316]).

https://doi.org/10.4153/CMB-2009-014-1 Published online by Cambridge University Press

(ii) If $b = 2$, then it follows that there are $u, v, z \in \mathbb{Z}$ with $\gcd(u, v, z) = 1$ such that $2v^2z^2 = 4pu^4 - z^4$. If $\mathrm{ord}_2(4pu^4) = \mathrm{ord}_2(z^4)$, then $2 + 4\mathrm{ord}_2(u) = 4\mathrm{ord}_2(z)$, whence $4|2$ which is a contradiction. Thus $\mathrm{ord}_2(4pu^4) \neq \mathrm{ord}_2(z^4)$ and so

$$1 + 2\mathrm{ord}_2(vz) = \min\{2 + 4\mathrm{ord}_2(u), 4\mathrm{ord}_2(z)\},$$

whence we deduce that $2|1$, which is a contradiction.

(iii) If $b = p$, then there is $a \in \mathbb{Q}$ such that $p^{(2k+1)e}a^2 = 3x^2 + y^2$, where $e = \pm 1$ and $\mathrm{ord}_p(a) = 0$. Let $a = a_1/a_2$, $x = x_1/x_2$, $y = y_1/y_2$, with $a_i, x_i, y_i \in \mathbb{Z}$ $(i = 1, 2)$, $\gcd(a_1, a_2) = \gcd(x_1, x_2) = \gcd(y_1, y_2) = 1$ and p does not divide a_1a_2. Suppose that $e = 1$. Thus we have

$$p^{2k+1}(a_1x_2y_2)^2 = 3(x_1y_2a_2)^2 + (y_1x_2a_2)^2.$$

Since $p \nmid a_2$ it follows that $p|3(x_1y_2)^2 + (y_1x_2)^2$. If $p \nmid x_1y_2$ and $p \nmid y_1x_2$, then -3 is a quadratic residue modulo p. But since $p \equiv -1 \pmod 6$ this is impossible. Suppose that $p|x_1y_2$ and $p|y_1x_2$. Then either $p|x_1$ and $p|y_1$ or $p|x_2$ and $p|y_2$. If $p|x_1$ and $p|y_1$, then we deduce that $p|x_2y_2$ and so either $p|x_2$ or $p|y_2$, which is a contradiction. Next, we suppose that $p|x_2$ and $p|y_2$. If $\mathrm{ord}_p(x_2) \neq \mathrm{ord}_p(y_2)$, then we have

$$2\min\{\mathrm{ord}_p(x_2), \mathrm{ord}_p(y_2)\} > 2\mathrm{ord}_p(x_2) + 2\mathrm{ord}_p(y_2),$$

which is a contradiction. If $\mathrm{ord}_p(x_2) = \mathrm{ord}_p(y_2)$, then $x_2 = p^s x_3$ and $y_2 = p^s y_3$, where $x_3, y_3, s \in \mathbb{Z}$, $p \nmid x_3y_3$ and $s > 0$. We have $p|3(x_1y_3)^2 + (y_1x_3)^2$ and $p \nmid x_1y_3$, $p \nmid y_1x_3$. It follows that -3 is quadratic residue modulo p, which is a contradiction. Finally, we consider the case $e = -1$. We have

$$(a_1x_2y_2)^2 = [(x_1y_2a_2)^2 + (y_1x_2a_2)^2]p^{2k+1}.$$

Since $p \nmid a_1$, we have $7^{2k+1}|(x_2y_2)^2$ and we deduce that $p|(x_1y_2)^2 + (y_1x_2)^2$. Working as previously, we get a contradiction.

(iv) If $b = 2p$ then, working as in case 2, we obtain a contradiction. ■

Proposition 4.5 *Let p be a prime $\equiv 7$ or $11 (\mathrm{mod} 16)$, a be a nonzero integer with $(a/p) = 1$ and μ be a positive integer. Furthermore, if $p \equiv 7 (\mathrm{mod} 16)$, then we suppose that a has a prime divisor q with $q \equiv 3$ or $5 (\mathrm{mod} 8)$. Then the only rational solution to the equation*

$$Y^2 = (X^4 + p)(X^{2\mu} + aY^2)$$

is $(X, Y) = (0, 0)$. Here (a/p) denotes the usual Legendre symbol.

Proof The resultant of Y and $X^{2\mu} + aY^2$, as polynomials with coefficients in $\mathbb{Z}[X]$, is equal to $R(X) = X^{2\mu}$. We have

$$R(\sqrt[4]{-p})R(-\sqrt[4]{-p})R(i\sqrt[4]{-p})R(-i\sqrt[4]{-p}) = p^{2\mu}.$$

Let $(x, y) \in \mathbb{Q}^2$ be a solution of the above equation with $xy \neq 0$. By Theorem 1.1, there is an integer $b > 0$ dividing $2p$ and $r \in \mathbb{Q}$ such that $br^2 = x^4 + p$. We have the following cases:

https://doi.org/10.4153/CMB-2009-014-1 Published online by Cambridge University Press

(i) $b = 1$. The curve E: $Y^2 = X^4 + p$ defines a principal homogeneous space for the elliptic curve F: $Y^2 = X^3 - 4pX$ which has exactly two rational points at infinity (see [25, page 310]) and so, it is isomorphic to F over $\mathbb{Q}$. Furthermore, F is isogenous to G: $Y^2 = X^3 + pX$ (see [25, page 310]). By [25, Proposition 6.2, page 311], we have rang $G(\mathbb{Q}) = 0$. Thus $F(\mathbb{Q}) = \{(0,0), \infty\}$. It follows that the affine curve E has no rational point.

(ii) $b = 2$. Suppose first that $p \equiv 11(\text{mod}16)$. Multiplying $2r^2 = x^4 + p$ by an appropriate integer, we deduce that $2u^2 = v^2 + pw^2$, where u, v, w are relatively prime positive integers. Thus $(2/p) = 1$. Since $p \equiv 3(\text{mod}8)$, we obtain a contradiction. Suppose $p \equiv 7(\text{mod}16)$. Then there is $s \in \mathbb{Q}$ such that $2s^2 = x^{2\mu} + ay^2$. Multiplying by an appropriate integer we get $2u^2 = v^2 + aw^2$, where u, v, w are relatively prime positive integers. It follows that $(2/q) = 1$, which is a contradiction because $q \equiv 3, 5(\text{mod}8)$.

(iii) If $b = p$, then there is $s \in \mathbb{Q}$ such that $ps^2 = x^{2\mu} + ay^2$. It follows that $pu^2 = v^2 + aw^2$, where u, v, w are relatively prime positive integers. Hence $(-a/p) = 1$. Since $p \equiv 3(\text{mod}4)$, we have $(-1/p) = -1$ and so $(a/p) = -1$, which is a contradiction.

(iv) $b = 2p$. Working as above we get a contradiction. ■

5 The curve $X^4 + (Y^2 + 1)(X + Y) = 0$

In this section we determine all the rational solutions of the equation handled in [24] in a completely elementary way.

Proposition 5.1 *The rational solutions of the equation*

$$X^4 + (Y^2 + 1)(X + Y) = 0$$

are $(X,Y) = (0,0), (-1,0)$.

Proof We apply the birational transformation $X = (1 - V)/U$, $Y = -1/U$ to the above curve and we obtain the curve $(1 - V)^4 = UV(U^2 + 1)$. Let $(u, v) \in \mathbb{Q}^2$ be a point of this curve with $uv \neq 0$. Suppose that $u > 0$ (and so, $v > 0$). Then $u = u_1/u_2$ and $v = v_1/v_2$, where u_1, u_2, v_1, v_2 are positive integers with $\gcd(u_1, u_2) = \gcd(v_1, v_2) = 1$. Thus $(v_2 - v_1)^4 u_2^3 = u_1 v_1 v_2^3 (u_1^2 + u_2^2)$.

We have $\gcd(v_2 v_1, v_2 - v_1) = \gcd(u_2, u_1^2 + u_2^2) = 1$ and so $u_2^3 | v_1 v_2^3$ and $v_1 v_2^3 | u_2^3$, whence $u_2^3 = v_1 v_2^3$. Hence $(v_2 - v_1)^4 = u_1(u_1^2 + u_2^2)$. Since $\gcd(u_1, u_1^2 + u_2^2) = 1$, there are $A, B \in \mathbb{Z}$ such that $u_1 = A^4$ and $u_2^2 = B^4 - (A^4)^2$. Thus $u_2^2 = B^4 - (A^2)^4$. We have either $B^2 = A^4 = 1$ or $B^2 = 1$ and $A = 0$ (see [21, Chapter 4, page 17]). Thus $(u_1, u_2) \in \{(1,0), (0, \pm 1)\}$, which is a contradiction. If $u < 0$, working as previously, we get a contradiction. ■

Acknowledgement The author wishes to thank the referee for helpful comments.

References

[1] E. Bombieri, *The Mordell conjecture revisited.* Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **17**(1990), no. 4, 615–640.
[2] N. Bruin, *On Generalised Fermat Equations.* PhD Dissertation, Leiden 1999. http://www.cecm.sfu.ca/~nbruin/oldindex.html
[3] N. Bruin and E.V. Flynn, *Towers of 2-covers of hyperelliptic curves.* Trans. Amer. Math. Soc. **357**(2005), no. 11, 4329–4347.
[4] C. Chabauty, *Sur les points rationnels des variétés algébriques dont l'irrégularité est supérieure à la dimension.* C. R. Acad. Sci. Paris **212**(1941), 1022–1024.
[5] C. Chevalley and A. Weil, *Un théorème d' arithmétique sur les courbes algébriques.* C. R. Acad. Sci. Paris **195**(1932), 570–572.
[6] R.F. Coleman, *Effective Chabauty.* Duke Math. J. **52**(1985), no. 3, 765–770.
[7] K.R. Coombes and D.R. Grant, *On heterogeneous spaces.* J. London Math. Soc. (2) **40**(1989), no. 3, 385–397.
[8] V. Dem'janenko, *Rational points of a class of algebraic curves* Amer. Math. Soc. Trasl. 66, American Mathematical Society, Providence, RI, 1968, pp. 246–272.
[9] S. Duquesne, *Points rationnels et méthode de Chabauty elliptique.* J. Théor. Nombres Bordeaux **15**(2003), no. 1, 99–113.
[10] G. Faltings, *Endlichkeitssäatze für abelsche Varietäten über Zahlkörpern.* Invent. Math. **73**(1983), no. 3, 349–366.
[11] E. V. Flynn, *A flexible method for applying Chabauty's theorem.* Compositio Math. **105**(1997), no. 1, 79–94.
[12] E. V. Flynn and J. L. Wetherell, *Finding rational points on bielliptic genus 2 curves.* Manuscripta Math. **100**(1999), no. 4, 519–533.
[13] ———, *Covering collections and a challenge problem of Serre.* Acta Arith. **98**(2001), no. 2, 197–205.
[14] E. V. Flynn and J. Redmond, *Application of covering techniques to families of curves.* J. Number Theory **101**(2003), no. 2, 376–397.
[15] E. V. Flynn, B. Poonen, and E. F. Schaefer, *Cycles of quadratic polynomials and rational points on a genus-*2 *curve.* Duke Math. J. **90**(1997), no. 3, 435–463.
[16] L. Kulesz, *Application de la méthode de Dem'janenko–Manin à certaines familles de courbes de genre 2 et 3.* J. Number Theory **76**(1999), no. 1, 130–146.
[17] S. Lang, *Algebraic Number Theory.* Addison-Wesley, Reading, Mass., 1970.
[18] S. Lang, *Fundamentals of Diophantine Geometry.* Springer-Verlag, New York, 1983.
[19] M. P. Malliavin, *Algèbre commutative.* Applications en géomŕrie et théorie des nombres. Masson, Paris, 1985.
[20] Y. Manin, *The p-torsion of elliptic curves is uniformly bounded.* Izv. Akad. Nauk SSSR Ser. Mat. **33**(1969), 459–465.
[21] L. J. Mordell, *Diophantine Equations.* Pure and Applied Mathematics 30, Academic Press, New York, 1969.
[22] B. Poonen, E. F. Schaefer, and M. Stoll, *Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$.* http://math.berkeley.edu/~poonen/papers/pss.pdf.
[23] D. Poulakis, *Solutions entières de l'équation $f(X, Y)^a = p(X)g(X, Y)$.* C. R. Acad. Sci. Paris Sér. I Math. **315**(1992), no. 9, 963–968.
[24] E. F. Schaefer and J. L. Wetherell, *Computing the Selmer group of an isogeny between abelian varieties using a further isogeny to a Jacobian.* J. Number Theory **115**(2005), no. 1, 158–175.
[25] J. H. Silverman, *The arithmetic of elliptic curves.* Graduate Texts in Mathematics 106, Springer-Verlag, New York, 1986.
[26] ———, *Rational points on certain families of curves of genus at least 2.* Proc. London Math. Soc. (3) **55**(1987), no. 3, 465–481.
[27] P. Vojta, *Siegel's theorem in compact case.* Ann. of Math. (2) **133**(1991), no. 3, 509–548.
[28] J. L. Wetherell, *Bounding the Number of Rational Points on Certain Curves of Hight Rank,* PhD Dissertation, University of California at Berkeley, 1997.

Aristotle University of Thessaloniki, Department of Mathematics, 54124 Thessaloniki, Greece,
e-mail: poulakis@math.auth.gr