J. Symbolic Computation (2000) **30**, 573–582
doi:10.1006/jsco.2000.0420
Available online at http://www.idealibrary.com on IDEAL

On the Practical Solution of Genus Zero Diophantine Equations

DIMITRIOS POULAKIS† AND EVAGGELOS VOSKOS

Aristotle University of Thessaloniki, Department of Mathematics, 54006 Thessaloniki, Greece

Let $f(X, Y)$ be an absolutely irreducible polynomial with integer coefficients such that the curve defined by the equation $f(X, Y) = 0$ is of genus 0 having at least three infinite valuations. This paper describes a practical general method for the explicit determination of all integer solutions of the diophantine equation $f(X, Y) = 0$. Some elaborated examples are given.

1. Introduction

Let $f(X, Y)$ be an absolutely irreducible polynomial with integer coefficients such that the curve C defined by the equation $f(X, Y) = 0$ is of genus 0. We denote by $\overline{\mathbf{Q}}$ an algebraic closure of the field of rational numbers $\mathbf{Q}$ and by $\overline{\mathbf{Q}}(C)$ the function field of C. We suppose that there are at least three discrete valuation rings of $\overline{\mathbf{Q}}(C)$ which dominate the local rings of C at the points at infinity. Maillet (1918, 1919), using the finiteness of the integer solutions of Thue equations established in 1908, proved that the equation $f(X, Y) = 0$ has only finitely many integer solutions (see also, Lang, 1978, Theorem 6.1, p. 146 and 1983, Chapter 8, Section 5). The first effective upper bound for the solutions of Thue equations was obtained in 1968 by A. Baker as a consequence of his study of linear forms in the logarithms of algebraic numbers. Poulakis (1993) calculated the first effective upper bound for the integer solutions of $f(X, Y) = 0$ using an effective version of the Riemann–Roch theorem and an effective upper bound for the solutions of Thue equations. For other results see Bilu (1993, Theorem 5B) and Poulakis (1997, Theorem 2). Unfortunately, since the bounds obtained so far are too large, they cannot provide us with a practical method for solving the equation $f(X, Y) = 0$.

In this paper we give a practical general method for the explicit determination of all integer solutions of a particular equation $f(X, Y) = 0$ satisfying the above properties. It is rested merely on the construction of a parametrization defined over $\mathbf{Q}$ for the points of C (if it exists) and on the practical solution of Thue equations. Since there are efficient algorithms to carry out these two tasks (see for instance Tzanakis and de Weger, 1989; Bilu and Hanrot, 1996; Sendra and Winkler, 1997), we can obtain all the integer solutions to $f(X, Y) = 0$ in a reasonable time.

The paper is organized as follows. In Section 2 we obtain some useful results for the discussion of our method. Section 3 is devoted to the description of the algorithm for

†E-mail: poulakis@ccf.auth.gr

numerical solution of any particular equation $f(X,Y)=0$ defining a curve of genus 0 having at least three infinite valuations. Finally, in the last section we apply this method to find all the integer solutions of a one-parameter family of cubic equations, a two-parameter family of quartic equations and two equations of degrees 4 and 5, respectively.

2. Auxiliary Results

Let $F(X,Y,Z) \in \mathbf{Q}[X,Y,Z]$ be an absolutely irreducible homogeneous polynomial of degree $N \geq 3$ such that the curve C defined by the equation $F(X,Y,Z)=0$ is of genus 0. We suppose that C has a non-singular point defined over $\mathbf{Q}$. (If N is odd or if N is even and C has a singularity over $\mathbf{Q}$ of odd multiplicity, then it is always the case (Sendra and Winkler, 1997, Corollary 2.1).) This is equivalent to the existence of a birational map, over $\mathbf{Q}$, between C and the projective line $\mathbf{P}^1$ (see Mordell, 1969, Chapter 17, pp. 150-152, and Poulakis, 1998).

Lemma 2.1. *Let $u(S,T), v(S,T), w(S,T) \in \mathbf{Z}[S,T]$ be homogeneous polynomials of the same degree with no common non-constant factor (in $\mathbf{Q}[S,T]$) such that the correspondence*

$$(S,T) \to (u(S,T), v(S,T), w(S,T))$$

defines a birational map ϕ over $\mathbf{Q}$ of $\mathbf{P}^1$ to C. Then ϕ is a birational morphism of $\mathbf{P}^1$ onto C and $\deg u(S,T) = \deg v(S,T) = \deg w(S,T) = N$. Furthermore, if $(x:y:1)$ is a non-singular point of $C(\mathbf{Q})$, then there exist $s,t \in \mathbf{Z}$ with $s \geq 0$ and $\gcd(s,t)=1$ such that $x = u(s,t)/w(s,t)$ and $y = v(s,t)/w(s,t)$.

Proof. Let $(s:t) \in \mathbf{P}^1(\overline{\mathbf{Q}})$ such that $u(s,t)=v(s,t)=w(s,t)=0$. We can suppose, without loss of generality, that $t \neq 0$ and we denote by $P(S)$ the irreducible polynomial of s/t over $\mathbf{Q}$. Then, $P(S)$ divides the polynomials $u(S,1)$, $v(S,1)$, $w(S,1)$ in $\mathbf{Q}[S]$ and we find that the homogenization $P_h(S,T)$ of $P(S)$ is a common factor of $u(S,T)$, $v(S,T)$ and $w(S,T)$, contradicting the fact that $u(S,T)$, $v(S,T)$ and $w(S,T)$ have no common non-constant factor in $\mathbf{Q}[S,T]$. Hence, the birational map ϕ is a morphism. Since ϕ is a birational map, the set $\phi(\mathbf{P}^1)$ is dense in C and by Shafarevich (1977, Theorem 2, p. 45), we have that $\phi(\mathbf{P}^1)$ is a closed subset of C. Hence ϕ is surjective.

Let ψ be the inverse birational map of ϕ. The domain of ψ contains all the non-singular points of C (Fulton, 1969, Corollary 1, p. 160). Thus, if $(x:y:1)$ is a non-singular point of $C(\mathbf{Q})$, then $\psi((x:y:1)) = (s:t)$, where s and t are integers with $s \geq 0$ and $\gcd(s,t)=1$, whence we obtain $x = u(s,t)/w(s,t)$ and $y = v(s,t)/w(s,t)$. Finally, Gao and Chou (1992, Theorem 4.4) implies that $\deg u(S,T) = \deg v(S,T) = \deg w(S,T) = N$. □

Let $\overline{\mathbf{Q}}(C)$ be the function field of C. If P is a point on C, we denote by $O_P(C)$ the local ring at P. We call, as usual, the points $(x:y:z)$ on C, with $z=0$, *points at infinity*. Furthermore, we denote by C_∞ the set of discrete valuation rings V of $\overline{\mathbf{Q}}(C)$ which dominate the local rings of C at the points at infinity.

Lemma 2.2. *Let $u(S,T)$, $v(S,T)$ and $w(S,T)$ be as in Lemma 2.1. The number of elements of C_∞ is equal to the number of distinct zeros of $w(S,T)$. The point $(0:1:0)$ (respectively $(1:0:0)$) is not on C if and only if $u(S,T)$ (respectively $v(S,T)$) and $w(S,T)$ have no common zero. If $(0:1:0)$ (respectively $(1:0:0)$) is a point on C, then* *the number of discrete valuation rings of* $\overline{\mathbf{Q}}(C)$ *lying above the local ring at* $(0:1:0)$ *(respectively* $(1:0:0)$*) is equal to the number of distinct common zeros of* $u(S,T)$ *(respectively* $v(S,T)$*) and* $w(S,T)$*.*

Proof. We denote by $\overline{\mathbf{Q}}(\mathbf{P}^1)$ the function field of $\mathbf{P}^1$ and if $Q \in \mathbf{P}^1$ we denote by $O_Q(\mathbf{P}^1)$ the local ring at Q. Let $\phi : \mathbf{P}^1 \to C$ be the birational morphism of Lemma 2.1. The correspodence $f \to f \circ \phi$ induces an isomorphism $\tilde{\phi}$ from $\overline{\mathbf{Q}}(C)$ onto $\overline{\mathbf{Q}}(\mathbf{P}^1)$. Let $P = (x:y:0)$ be a point on C at the infinity. We denote by V_i $(i = 1,\dots,k)$ the discrete valuation rings of C_∞ dominating $O_P(C)$. Then, $\tilde{\phi}(V_i)$ is a discrete valuation ring of $\overline{\mathbf{Q}}(\mathbf{P}^1)$ and so there is $P_i \in \mathbf{P}^1$ such that $\tilde{\phi}(V_i) = O_{P_i}(\mathbf{P}^1)$ $(i = 1,\dots,k)$. Since $O_{P_i}(\mathbf{P}^1)$ dominate $\tilde{\phi}(O_P(C))$, Fulton (1969, Proposition 11(2), p. 153) implies that $\phi(P_i) = P$. Thus, $w(P_i) = 0$ $(i = 1,\dots,k)$.

Conversely, let $Q \in \mathbf{P}^1$ with $w(Q) = 0$. Then $\phi(Q) = P$ is a point on C at infinity and by Fulton (1969, Proposition 11(2), p. 153) the discrete valuation ring $O_Q(\mathbf{P}^1)$ dominates $\tilde{\phi}(O_P(C))$. Thus, $\tilde{\phi}^{-1}(O_Q(\mathbf{P}^1))$ dominates $O_P(C)$. Hence, the number of distinct zeros of $w(S,T)$ is equal to $|C_\infty|$.

By Lemma 2.1, the morphism ϕ is surjective. Thus, we obtain that $(0:1:0)$ (respectively $(1:0:0)$) is not on C if and only if $u(S,T)$ (respectively $v(S,T)$) and $w(S,T)$ have no common zero. Suppose next that $(0:1:0)$ (respectively $(1:0:0)$) is a point on C. The above procedure yields that the number of discrete valuation rings dominating the local ring at $(0:1:0)$ (respectively $(1:0:0)$) is exactly the number of points $Q \in \mathbf{P}^1$ with $\phi(Q) = (0:1:0)$ (respectively $\phi(Q) = (1:0:0)$) and hence the number of distinct common zeros of $u(S,T)$ (respectively $v(S,T)$) and $w(S,T)$. □

Lemma 2.3. *Let* $F_N(X,Y)$ *be the homogeneous part of degree* N *of polynomial* $F(X,Y,1)$*. Suppose that* $F_N(X,Y) = X^aY^bG(X,Y)$*, where* a*,* b *are positive integers and* $G(X,Y)$ *is a homogeneous polynomial with* k *distinct linear factors which is not divisible by* X *or* Y*. Then,* $w(S,T)$ *has at least* $k+1$ *zeros which are not zeros of* $u(S,T)$ *(respectively of* $v(S,T)$*).*

Proof. Since $G(X,Y)$ has k distinct zeros, there are k distinct points on C of the form $(x:y:0)$ with $x \neq 0$ and $y \neq 0$. Hence there exist at least k distinct elements of C_∞ which do not dominate the local rings at $(0:1:0)$ and $(1:0:0)$. Thus, Lemma 2.2 implies that $w(S,T)$ has at least $k+1$ zeros which are not zeros of $u(S,T)$ (respectively of $v(S,T)$). □

Let

$$f(X) = a_0 + a_1X + \cdots + a_nX^n, \qquad a_n \neq 0,$$
$$g(X) = b_0 + b_1X + \cdots + b_mX^m, \qquad b_m \neq 0,$$

be two polynomials with integer coefficients and degrees ≥ 1. We recall that the resultant $R(f,g)$ of $f(X)$ and $g(X)$ is defined to be the determinant of the matrix

$$M(f,g) = \begin{bmatrix} a_0 & a_1 & \dots & a_n & 0 & 0 & \dots \\ 0 & a_0 & a_1 & \dots & a_n & 0 & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & a_0 & a_1 & \dots & a_n \\ b_0 & b_1 & \dots & b_m & 0 & 0 & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & b_0 & b_1 & \dots & b_m \end{bmatrix}$$

where there are m rows of a's and n rows of b's. We denote by $A_1, \dots, A_{m+n}$ the cofactors of the first column of matrix $M(f,g)$.

LEMMA 2.4. *The greatest common divisor $\delta(f,g)$ of $A_1, \dots, A_{m+n}$ divides $R(f,g)$ and there are polynomials $A(X), B(X) \in \mathbf{Z}[X]$ of degrees at most $n-1$ and $m-1$, respectively, such that*

$$A(X)f(X) + B(X)g(X) = R(f,g)/\delta(f,g).$$

PROOF. By the proof of Walker (1978, Theorem 9.6, p. 25), we obtain

$$(A_1 + \dots + A_m X^{m-1})f(X) + (A_{m+1} + \dots + A_{m+n}X^{n-1})g(X) = R(f,g).$$

Dividing the two parts by $\delta(f,g)$ the result follows. □

3. Description of the Method

Let $F(X,Y,Z)$ be an absolutely irreducible homogeneous polynomial in $\mathbf{Z}[X,Y,Z]$ of degree $N \geq 3$ such that the projective curve C defined by the equation $F(X,Y,Z) = 0$ is of genus 0 and the set C_∞ has at least three (distinct) elements. Set $f(X,Y) = F(X,Y,1)$. In this section, following Maillet (1919), Lang (1978, Theorem 6.1, p. 146) and Lang (1983, Chapter 8, Section 5), we describe an algorithm for the determination of all integer solutions of the diophantine equation $f(X,Y) = 0$.

We suppose first that if the two points $(0:1:0)$ and $(1:0:0)$ are on C, we have $|C_\infty| - n_1 \geq 3$ or $|C_\infty| - n_2 \geq 3$, where n_1 and n_2 are the numbers of elements of C_∞ dominating the local rings at $(0:1:0)$ and $(1:0:0)$, respectively. The algorithm is as follows:

Step 1. Determine the singularities of the projective curve C.

Step 2. Decide if there is a non-singular rational point on C. If there is not, the integer singular points on the curve $f(X,Y) = 0$ are the only integer solutions of the equation $f(X,Y) = 0$. Otherwise, find homogeneous polynomials $u(S,T), v(S,T), w(S,T) \in \mathbf{Z}[S,T]$ of the same degree, with no common non-constant factor (in $\mathbf{Q}[S,T]$), such that the correspondence

$$(S,T) \to (u(S,T), v(S,T), w(S,T))$$

defines a birational map ϕ over $\mathbf{Q}$ of $\mathbf{P}^1$ to C. Write

$$\frac{u(S,T)}{w(S,T)} = \frac{U(S,T)}{W_1(S,T)}, \qquad \frac{v(S,T)}{w(S,T)} = \frac{V(S,T)}{W_2(S,T)},$$

where $U(S,T), V(S,T), W_1(S,T), W_2(S,T)$ are homogeneous polynomials in $\mathbf{Z}[S,T]$ with

$\gcd(U(S,T), W_1(S,T)) = \gcd(V(S,T), W_2(S,T)) = 1$. Since we have $|C_\infty| - n_1 \geq 3$ or $|C_\infty| - n_2 \geq 3$, Lemma 2.2 implies that either $W_1(S,T)$ or $W_2(S,T)$ has at least three distinct linear factors. We suppose, without loss of generality, that $W_1(S,T)$ has this property.

Step 3. Set $u_1(S) = U(S,1)$, $w_1(S) = W_1(S,1)$, $u_2(T) = U(1,T)$ and $w_2(T) = W_1(1,T)$. Since $U(S,T)$ and $W_1(S,T)$ have no common factor, the resultant R_i of u_i and w_i is non-zero ($i = 1, 2$). Compute the resultants R_i and the integers $\delta_i = \delta(u_i, w_i)$ ($i = 1, 2$). Next, compute the least common multiple $l = \operatorname{lcm}((R_1/\delta_1), (R_2/\delta_2))$.

Step 4. Determine the set Σ of integer solutions (s,t) with $\gcd(s,t) = 1$ and $s \geq 0$ of all the Thue equations $W_1(s,t) = k$, where k is an integer dividing l.

Step 5. Compute the values $x = U(s,t)/W_1(s,t)$ and $y = V(s,t)/W_2(s,t)$, where $(s,t) \in \Sigma$. The integer points obtained in this way and the integer singular points on the curve $f(X,Y) = 0$ are all the integer solutions to the equation $f(X,Y) = 0$.

Remark. In case where $W_2(S,T)$ has exactly two distinct linear factors and the equation $W_2(S,T) = A$, where A is an integer, has only a finite number of integer solutions easily determined, it is more convenient to proceed with $W_2(S,T)$ instead of $W_1(S,T)$. Furthermore, in some cases the integer solutions of $f(X,Y) = 0$ can be determined using only the parametrization of C and some ad hoc arguments.

Proof of correctness of the algorithm. Let $U(S,T)$ and $W_2(S,T)$ be as in Step 2. By Lemma 2.4, there are polynomials $A(S)$, $B(S)$, $\Gamma(T)$, $\Delta(T)$ with integer coefficients, such that

$$A(S)u_1(S) + B(S)w_1(S) = R_1/\delta_1, \qquad \Gamma(T)u_2(T) + \Delta(T)w_2(T) = R_2/\delta_2.$$

Thus, we obtain

$$\begin{aligned} A(S,T)U(S,T) + B(S,T)W_1(S,T) &= (R_1/\delta_1)T^\mu, \\ \Gamma(S,T)U(S,T) + \Delta(S,T)W_1(S,T) &= (R_2/\delta_2)S^\nu, \end{aligned}$$

where μ and ν are positive integers and $A(S,T)$, $B(S,T)$, $\Gamma(S,T)$, $\Delta(S,T)$ are homogeneous polynomials with integer coefficients.

If (x,y) is an integer non-singular point on $f(X,Y) = 0$, then Lemma 2.1 implies that there are integers $s \geq 0$, t with $\gcd(s,t) = 1$ such that $x = U(s,t)/W_1(s,t)$. Setting $S = s$ and $T = t$ in the two above homogeneous equations, we deduce that $W_1(s,t)$ divides $(R_1/\delta_1)t^\mu$ and $(R_2/\delta_2)s^\nu$, whence $W_1(s,t)$ divides l. □

Supppose now that the points $(0:1:0)$ and $(1:0:0)$ are on C and $|C_\infty| - n_1 \leq 2$, $|C_\infty| - n_2 \leq 2$. Then, the polynomials $W_1(S,T)$ and $W_2(S,T)$ provided by the above method have at most two distinct linear factors. Thus, the equations $W_i(s,t) = k$ ($i = 1, 2$) do not always have a finite number of integer solutions and therefore we cannot determine the integer solutions to $f(X,Y) = 0$. In this case Lemma 2.3 yields that the homogeneous part of degree N of $f(X,Y)$ has the form $X^\alpha Y^\beta (aX + bY)^\gamma$, where α, β are positive integers, a, b are non-zero integers and γ is an integer ≥ 0. We consider the polynomial $g(X,Y) = f(X + cY, Y)$, where c is an integer such that $ac + b \neq 0$. Thus, we reduce the problem of computation of the integer solutions of $f(X,Y) = 0$ to the same problem for $g(X,Y) = 0$. Since $(0:1:0)$ is not on the projective closure of the curve $g(X,Y) = 0$, we can apply the above method to solve the equation $g(X,Y) = 0$ and therefore $f(X,Y) = 0$.

The hypothesis $|C_\infty| - n_1 \geq 3$ or $|C_\infty| - n_2 \geq 3$ enters in the algorithm only in Step 2 and it is a necessary and sufficient condition for $W_1(S,T)$ or $W_2(S,T)$ to have at least three distinct linear factors. On the other hand, the problem of the determination of integer points on a curve E of genus 0, defined over $\mathbf{Q}$, is reduced to the same problem for a curve with the above property only if $|E_\infty| \geq 3$. Thus, the hypothesis $|E_\infty| \geq 3$ is used only to show that the equations at which our problem is reduced are Thue equations.

Step 1 of the above method can be achieved by the algorithm of Sakkalis and Farouki (1990) or in many cases it is enough to use the resultants of the derivatives of first order of $f(X,Y)$ with respect to X and Y and check the points at infinity. For Step 2 one can use the algorithms of Abhyankar and Bajaj (1988), Sendra and Winkler (1991, 1997, 1999) and van Hoeij (1997). Note that the algorithm DIOPHANTINE-SOLVER of Sendra and Winkler (1997) is very useful for our purpose. The computation of the resultant of two polynomials can be carried out by the algorithm of Cohen (1993, Algorithm 3.3.7, p. 121) and for the computations of the integers δ_i $(i = 1, 2)$ we can use the algorithms of Cohen (1993, Section 2.2.4, p. 49, and Section 1.3, p. 12). Finally, the solution of Thue equations can be achieved by the methods of Tzanakis and de Weger (1989) and Bilu and Hanrot (1996, 1999), or in many cases by more elementary methods (see Mordell, 1969). Note that in numerous cases we do not actually need a computer to carry out all necessary computations; see the numerical examples in Section 4.

4. Applications

In this section we illustrate the above method by solving some diophantine equations. In the first two examples we deal with two families of equations of degree 3 and 4, respectively. The solution of the corresponding families of Thue equations are given in Mignotte (1996) and Wakabayashi (1997), respectively. Note however that the solution of a family of Thue equations is a very difficult task and this can only be achieved in a very small number of situations. In the other two examples we deal with two particular equations of degree 4 and 5.

EXAMPLE 4.1. *Let n be a non-negative integer. The only integer solutions of the equation*

$$f_n(X,Y) = X^3 - (n-1)X^2Y - (n+2)XY^2 - Y^3 - 2nY(X+Y) = 0,$$

are $(X,Y) = (0,0), (0,-2n)$.

The equation $f_n(X,Y) = 0$ defines a curve of genus 0 having three infinite valuations. Setting $X = SY$, we obtain the parametrization

$$X = \frac{2nS^2 + 2nS}{S^3 - (n-1)S^2 - (n+2)S - 1}, \qquad Y = \frac{2nS + 2n}{S^3 - (n-1)S^2 - (n+2)S - 1}.$$

Put

$$W(S,T) = S^3 - (n-1)S^2T - (n+2)ST^2 - T^3, \qquad U(S,T) = 2nS^2T + 2nST^2.$$

The resultant of $U(S,1)$ and $W(S,1)$ is $R_1 = -8n^3$. The cofactors of the first column of matrix $M(U(S,1), W(S,1))$ are $A_1 = 8n^3$, $A_2 = 16n^3$, $A_3 = 4n^2(n+4)$, $A_4 = 4n^2(2n-1)$ $A_5 = -8n^2$ and their greatest common divisor (g.c.d.) is $\delta_1 = 4n^2$. Thus $R_1/\delta_1 = -2n$. On the other hand, the resultant of $U(1,T)$ and $W(1,T)$ is $R_2 = -8n^3$. The cofactors of the first column of matrix $M(U(1,T),W(1,T))$ are $B_1 = -8n^3$, $B_2 = -16n^3$, $B_3 = 4n^2(-n+3)$, $B_4 = -4n^2(2n+3)$, $B_5 = -8n^2$ and their greatest common divisor is $\delta_2 = 4n^2$. Therefore $R_2/\delta_2 = -2n$. Hence $\operatorname{lcm}(R_1/\delta_1, R_2/\delta_2) = 2n$.

Now we have to estimate the integer solutions (s,t) with $\gcd(s,t) = 1$ and $s \geq 0$ of the Thue equations $W(S,T) = k$, where k is a divisor of $2n$. By Mignotte (1996, Theorem 3), it follows that $(s,t) = (1,0)$, $(0,1)$, $(1,-1)$, $(1,1)$, $(1,-2)$, $(2,-1)$,$(1,-n-1)$, $(n,1)$, $(n+1,-n)$. In the case where $n = 2$, the previous list also contains the couples $(4,-3)$,$(8,3)$,$(1,-4)$,$(3,1)$, $(3,-11)$. We easily deduce that the integer solutions to $f_n(X,Y) = 0$ are the obvious ones $(X,Y) = (0,0),(0,-2n)$ which correspond to the couples $(S,T) = (1,0),(0,1)$, respectively.

EXAMPLE 4.2. *Let a and b be integers such that $a \geq 8$ and $b \neq 0$. Then, the only integer solutions of the equation*

$$f_{a,b}(X,Y) = b(X^4 - a^2X^2Y^2 + Y^4) - 2X^3 + 2a^2XY^2 = 0$$

are $(X,Y) = (0,0)$ if $b \neq \pm 1, \pm 2$ and $(X,Y) = (0,0),(2/b,0)$ otherwise.

The curve defined by the equation $f_{a,b}(X,Y) = 0$ has genus 0 and four infinite valuations. Setting $X = SY$, we obtain the parametrization

$$X = \frac{2S(S^2 - a^2)}{b(S^4 - a^2S^2 + 1)}, \qquad Y = \frac{2S^2(S^2 - a^2)}{b(S^4 - a^2S^2 + 1)}.$$

Put

$$U(S,T) = 2ST(S^2 - a^2T^2), \qquad W(S,T) = b(S^4 - a^2S^2T^2 + T^4).$$

The resultant of $U(S,1)$ and $W(S,1)$ is $R_1 = 16b^3$. The cofactors of the first column of matrix $M(U(S,1),W(S,1))$ are $A_1 = -16b^2$, $A_2 = 0$, $A_3 = 0$, $A_4 = 0$, $A_5 = 8b^3$ and their g.c.d. is $\delta_1 = 8b^2$ if b is odd and $\delta_1 = 16b^2$ otherwise. Thus $R_1/\delta_1 = b$ or $2b$. Furthermore, the resultant of $U(1,T)$ and $W(1,T)$ is $R_2 = 16b^3$. The cofactors of the first column of matrix $M(U(1,T),W(1,T))$ are $B_1 = -16b^2$, $B_2 = 0$, $B_3 = 16a^2b^2(1-a^4)$, $B_4 = 0$, $B_5 = 8a^2b^3(-2+a^4)$, $B_6 = 0$, $B_7 = 8b^3(1-a^4)$ and their g.c.d. is $\delta_2 = 8b^2$ if b odd or a even and $\delta_2 = 16b^2$ otherwise. Thus $R_2/\delta_2 = b$ or $2b$. Hence $\operatorname{lcm}(R_1/\delta_1, R_2/\delta_2)$ divides $2b$.

Our next task is to determine the integers s and t with $\gcd(s,t) = 1$ and $s \geq 0$ such that $W(s,t)$ is a divisor of $2b$, whence $|s^4 - a^2s^2t^2 + t^4| \leq 2$. By Wakabayashi (1997, Theorem 2), it follows that $(s,t) = (1,0)$, $(0,\pm 1)$, $(a,\pm 1)$, $(1,\pm a)$, $(1,\pm 1)$. If $(s,t) = (1,\pm 1)$, then $|a^2 - 2| \leq 2$ which is a contradiction. Thus, we obtain the following solutions for the equation $f_{a,b}(X,Y) = 0$: $(X,Y) = (2/b,0)$, (b,b), $(b(1-a^4), b(1-a^4))$, $(2(1-a^4)/b, 2a(1-a^4)/b)$. Now we have to check whether these solutions are integers. First, we remark that $(2/b,0)$ is an integer solution if and only if b divides 2. The equation $f_{a,b}(b,b) = 0$ implies $b^2 = 2 + 2/(a^2-2)$. As the right-hand side of this equality is not an integer, we have a contradiction. Hence the couple (b,b) is not an integer solution. Similarly, if $f_{a,b}(b(1-a^4), b(1-a^4)) = 0$, then $-b^3(a-1)^4(a+1)^4(a^2+1)^3(2-2a^2-2b^2+a^2b^2) = 0$ which leads to the same contradiction. Finally, if $f_{a,b}(2(1-a^4)/b, 2a(1-a^4)/b) = 0$, then $16a^4(a-1)^4(a+1)^4(a^2+1)^4/b^3 = 0$ which is a contradiction with $a \geq 8$. Hence, the only integer solutions to the equation $f_{a,b}(X,Y) = 0$ are $(X,Y) = (0,0)$ if $b \neq \pm 1, \pm 2$ and $(X,Y) = (0,0),(2/b,0)$ otherwise.

EXAMPLE 4.3. *The only integer solutions of the equation*

$$g(X,Y) = 2X^4 - 4X^3Y + 6X^2Y^2 - 4XY^3 + 6Y^4 - 16X^3 + 9X^2Y - 21XY^2 - 2Y^3 + 29X^2 + 7XY = 0$$

are $(X,Y) = (0,0), (1,-1), (2,-1), (2,2), (3,3), (7,5), (10,5)$.

Denote by C the curve defined by the equation $g(X,Y) = 0$. First, we determine the singular points on C. The point $P_1 = (0,0)$ is obviously a node. Let $g_X(X,Y)$ and $g_Y(X,Y)$ be the derivatives of $g(X,Y)$ with respect to X and Y. The resultants of $g_X(X,Y)$ and $g_Y(X,Y)$ with respect to X and Y are

$$\begin{aligned} A(Y) &= 8Y(Y+1)^2(335872Y^6 - 1399808Y^5 - 25440Y^4 + 2465408Y^3 - 141958Y^2 \\ &\quad -625323Y + 122598) \\ B(X) &= -16X(X-1)(X-2)(167936X^6 - 2134272X^5 + 7749392X^4 - 11635848X^3 \\ &\quad +7211033X^2 - 1257252X - 9261). \end{aligned}$$

If (x,y) is a singular point on C in finite distance, then $A(y) = B(x) = 0$. Thus, we easily conclude that the points $P_2 = (1,-1)$ and $P_3 = (2,-1)$ are double points on C. It follows that C has genus 0. On the other hand, since the polynomial $X^4 - 2X^3 + 3X^2 - 2X + 3$ is irreducible, C has four distinct points at the infinity, whence $|C_\infty| = 4$. Hence, we can apply our method to solve the equation $g(X,Y) = 0$.

We remark that $Q = (0, 1/3)$ is a point on C. Thus C has a rational parametrization. Following Abhyankar and Bajaj (1988), we consider the parametric family of conics

$$C(S) : G_S(X,Y) = -2X^3 - 3Y^2 + (S-6)XY + SX + Y = 0$$

which passes through the points P_1, P_2, P_3 and Q. The resultants of $g(X,Y)$ and $G(X,Y)$ with respect to X and Y are:

$$\begin{aligned} Res_X(g,G) &= 2Y^2(Y+1)^4(3Y-1)(2S^4Y - 60S^3Y + 658S^2Y - 3116SY + 5398Y \\ &\quad +7S^3 - 141S^2 + 870S - 1682) \\ Res_Y(g,G) &= 6X^3(X-2)^2(X-1)^2(2S^4X - 60S^3X + 658S^2X - 3116SX + 5398X \\ &\quad -7S^2 + 43S - 58). \end{aligned}$$

Hence, we deduce the following parametrization for C:

$$X = \frac{7S^2 - 43S + 58}{2(S^4 - 30S^3 + 329S^2 - 1558S + 2699)},$$

$$Y = \frac{-7S^3 + 141S^2 - 870S + 1682}{2(S^4 - 30S^3 + 329S^2 - 1558S + 2699)}.$$

Put

$$\begin{aligned} U(S,T) &= 7S^2T^2 - 43ST^3 + 58T^4, \\ W(S,T) &= 2(S^4 - 30S^3T + 329S^2T^2 - 1558ST^3 + 2699T^4). \end{aligned}$$

The resultant of $U(S,1)$ and $W(S,1)$ is $R_1 = 340807500$. The cofactors of the first column of matrix $M(U(S,1), W(S,1))$ are $A_1 = -2537190$, $A_2 = -1394820$, $A_3 = 242009640$, $A_4 = 86701860$, $A_5 = 10232460$, $A_6 = 398520$ and their g.c.d. is $\delta_1 = 270$. The resultant of $U(1,T)$ and $W(1,T)$ is $R_2 = 1363230000$. The cofactors of the first column of matrix $M(U(1,T), W(1,T))$ are $B_1 = -10148760$, $B_2 = -5579280$, $B_3 = 0$, $B_4 = 0$, $B_5 =$

968038560, $B_6 = 346807440$, $B_7 = 40929840$, $B_8 = 1594080$ and their g.c.d. is $\delta_2 = 1080$. Thus $R_1/\delta_1 = R_2/\delta_2 = 1262250 = 2 \cdot 3^3 \cdot 5^3 \cdot 11 \cdot 17$.

Set $w(S,T) = W(S,T)/2$. Now, we have to determine all the integers $s \geq 0$ and t such that $\gcd(s,t) = 1$ and $w(s,t) = d$, where d is a divisor of $3^3 \cdot 5^3 \cdot 11 \cdot 17$. We deduce that for every real z we have $w(z,1) > 5,81$. Thus

$$|d| = |w(s/t,1)|t^4 > 5,81t^4,$$

whence $|t| < \sqrt[4]{|d|/5.81} \leq 18.2$. It follows that $(s,t) = (7,1)$, $(8,1)$, $(9,1)$, $(19,2)$, whence we obtain the solutions $(X,Y) = (2,2)$, $(3,3)$, $(7,5)$, $(10,5)$. Hence, all the solutions of $g(X,Y) = 0$ are $(X,Y) = (0,0)$, $(1,-1)$, $(2,-1)$, $(2,2)$, $(3,3)$, $(7,5)$, $(10,5)$.

EXAMPLE 4.4. *The only integer solutions of the equation*

$$f(X,Y) = X^2Y^3 - 2XY^3 + X^3 - 3XY^2 + 3Y^3 = 0$$

are $(X,Y) = (0,0), (1,1), (-3,1)$.

Denote by C the algebraic curve defined by the equation $f(X,Y) = 0$. By Sendra and Winkler (1999), C is of genus 0 and has a parametrization given by

$$X = -\frac{-8 + 36S - 78S^2 + 55S^3}{8S^3}, \qquad Y = \frac{-8 + 36S - 78S^2 + 55S^3}{2S(4 - 12S + 17S^2)}.$$

Furthermore, the only singular points of C in finite distance are $(0,0)$ and $(1,1)$. By Lemma 2.1, we have $|C_\infty| = 3$.

Put

$$U(S,T) = -8T^3 + 36ST^2 - 78S^2T + 55S^3, \qquad W(S,T) = 2S(4T^2 - 12ST + 17S^2).$$

The resultant of $U(S,1)$ and $W(S,1)$ is $R_1 = -786432$ and the cofactors of the first column of matrix $M(U(S,1), W(S,1))$ are $A_1 = 98304$, $A_2 = 171008$, $A_3 = -2289152$, $A_4 = -271360$, $A_5 = -2914304$, $A_6 = 3703040$. In addition, the resultant of $U(1,T)$ and $W(1,T)$ is $R_2 = 98304$ and the cofactors of the first column of $M(U(1,T), W(1,T))$ are $B_1 = -10240$, $B_2 = 4096$, $B_3 = 19456$, $B_4 = -16384$, $B_5 = 4096$. The g.c.d. of A_i $(i = 1,\ldots,6)$ is $\delta_1 = 256$ and the g.c.d. of B_j $(j = 1,\ldots,5)$ is $\delta_2 = 1024$. The least common multiple of $R_1/\delta_1 = 3072$ and $R_2/\delta_2 = 96$ is equal to 3072.

Next, we shall determine the integers s,t with $s \geq 0$ and $\gcd(s,t) = 1$ such that $W(s,t)$ is a divisor of 3072. Since $4t^2 - 12st + 17s^2 = 8s^2 + (3s - 2t)^2$, we have $16s^3 \leq 3072$, whence $s \leq 5,8$. Further, we have that s is a divisor of $1536 = 2^93$. Thus, $s = 1,2,3,4$. If s is odd, then $8s^2 + (3s - 2t)^2$ is odd. Hence, we obtain $8 \leq 8s^2 + (3s - 2t)^2 \leq 3$ which is a contradiction. Hence $s = 2,4$. If $s = 2$, then $8 + (3 - t)^2$ divides 2^63, whence $t = -1,1,3,5,7$. If $s = 4$, then $32 + (6 - t)^2$ divides 2^53, whence it follows that t is even which is a contradiction. Therefore $(s,t) = (2,\pm1), (2,3), (2,5), (2,7)$. We deduce that the only integer solution to $f(X,Y) = 0$ obtained by the above couples is $(-3,1)$ which correspond to $(s,t) = (2,1)$. Hence, the integer solutions of $f(X,Y) = 0$ are $(X,Y) = (0,0), (1,1), (-3,1)$.

References

Abhyankar, S. S., Bajaj, C. L. (1988). Automatic parametrization of rational curves and surfaces III: Algebraic plane curves. *Comput. Aided Geom. Des.*, **5**, 309–321.

Bilu, Y. (1993). Effective analysis of integral points on algebraic curves. Thesis, Beer Sheva.

Bilu, Y., Hanrot, G. (1996). Solving Thue equations of high degree. *J. Number Theory*, **60(2)**, 373–392.
Bilu, Y., Hanrot, G. (1999). Thue equations with composite fields. *Acta Arith.*, **LXXXVIII. 4**, 311–326.
Cohen, H. (1993). *A Course in Computational Algebraic Number Theory.* Springer-Verlag.
Fulton, W. (1969). *Algebraic Curves.* New York, Benjamin.
Gao, X. S., Chou, S. C. (1992). On the Parametrization of Algebraic Curves. *AAECC*, **3**, 27–38.
van Hoeij, M. (1997). Rational Parametrizations of Algebraic Curves using a Canonical Divisor. *J. Symb. Comput.*, **23**, 209–227.
Lang, S. (1978). *Elliptic Curves. Diophantine Analysis.* Springer-Verlag.
Lang, S. (1983). *Fundamentals of Diophantine Geometry.* Springer-Verlag.
Maillet, E. (1918). Détermination des points entiers des courbes algébriques unicursales à coefficients entiers. *C. R. Acad. Sci. Paris*, **168(4)**, 217–220.
Maillet, E. (1919). Détermination des points entiers des courbes algébriques unicursales à coefficients entiers. *J. Ecole Polytech.*, **2, 20**, 115–156.
Mignotte, M., Pethő, A, Lemmermeyer, F. (1996). On the family of Thue equations $x^3 - (n-1)x^2y - (n+2)xy^2 - y^3 = k$. *Acta Arithm.*, **LXXVI.3**, 245–269.
Mordell, L. J. (1969). *Diophantine Equations.* Academic Press.
Poulakis, D. (1993). Points entiers sur les courbes de genre 0. *Colloq. Math.*, **LXVI. 1**, 1–7.
Poulakis, D. (1997). Integer points on algebraic curves with exceptional units. *J. Aust. Math. Soc.*, **63**, 145–164.
Poulakis, D. (1998). Bounds for the minimal solution of genus zero diophantine equations. *Acta Arithm.*, **LXXXVI. 1**, 51–90.
Sakkalis, T., Farouki, R. (1990). Singular points of Algebraic curves. *J. Symb. Comput.*, **9**, 405–421.
Sendra, J. R., Winkler, F. (1991). Symbolic Parametrization of curves. *J. Symb. Comput.*, **12**, 607–631.
Sendra, J. R., Winkler, F. (1997). Parametrization of Algebraic Curves over Optimal Field Extensions. *J. Symb. Comput.*, **23**, 191–207.
Sendra, J. R., Winkler, F. Algorithms for Rational Real Algebraic Curves. *Fundam. Inform.*, special issue on "Symbolic Computation and AI" 1999.
Shafarevich, I. R. (1977). *Basic Algebraic Geometry.* Springer-Verlag.
Tzanakis, N., de Weger, B. M. M. (1989). On the practical solution of the Thue equation. *J. Number Theory*, **31(2)**, 99–132.
Wakabayashi, I. (1997). On a Family of Quartic Inequalities I. *J. Number Theory*, **66**, 70–84.
Walker, R. (1978). *Algebraic Curves.* Springer-Verlag.

Originally Received 15 March 2000
Accepted 15 June 2000