Solving Genus Zero Diophantine Equations with at Most Two Infinite Valuations

DIMITRIOPOULAKIS AND EVAGGELOS VOSKOS

Department of Mathematics, Aristotle University of Thessaloniki, 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 most two infinite valuations. This paper describes a practical general method for the explicit determination of all integer solutions of the diophantine equation \( f(X, Y) = 0 \). Several elaborated examples are given. Furthermore, a necessary and sufficient condition for a curve of genus 0 to have infinitely many integer points is obtained.

1. Introduction

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. We denote by \( C \) the projective curve defined by \( F(X, Y, Z) = 0 \), where \( F(X, Y, Z) \) is the homogenization of \( f(X, Y) \). Let \( \overline{Q} \) be an algebraic closure of the field of rational numbers \( Q \) and \( \overline{Q}(C) \) 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 \((x : y : 0)\) on \( C \) points at infinity and we denote by \( C_{\infty} \) the set of discrete valuation rings \( U \) of \( \overline{Q}(C) \) such that \( U \) dominates the local ring \( O_P(C) \) at a point \( P \) at infinity (i.e. \( U \) contains \( O_P(C) \) and the maximal ideal of \( U \) contains the maximal ideal of \( O_P(C) \)). In the case where \( |C_{\infty}| \geq 3 \) Maillet (1918, 1919) proved that the equation \( f(X, Y) = 0 \) has only finitely many integer solutions (see also Lang, 1978, Theorem 6.1, p. 146 and Lang, 1983, Chapter 8, Section 5). The first effective upper bound for the solutions of \( f(X, Y) = 0 \) was obtained by Poulakis (1993). For a more recent result see Poulakis (2001). In Poulakis and Voskos (2000) we gave an algorithm for the explicit determination of all integer solutions of \( f(X, Y) = 0 \).

The aim of this paper is the study of the remaining case where \( |C_{\infty}| \leq 2 \). As it is well known in this case the equation \( f(X, Y) = 0 \) may have infinitely many integer solutions. Our main task is the description of a practical method for the explicit determination of all integer solutions of the equation \( f(X, Y) = 0 \). It is based on the construction of a parametrization of \( C \) over \( Q \) (if it exists), the resolution of polynomial congruences and the resolution of generalized Pellian equations. Moreover, using these ideas, we obtain a necessary and sufficient condition for a rational curve to have infinitely many integer points.

The plan of the paper is the following. In Section 2 we recall two lemmas on the parametrization of algebraic curves which will be useful for the discussion of our results.
In Sections 3 and 4 we give two algorithms for the determination of the integer points on a rational plane curve $C$ with $|C_\infty| = 1$ and 2, respectively. Furthermore, we solve some diophantine equations defining curves with these properties. In the last section we prove that the rational plane curve $C$ has infinitely many integer points if and only if $C$ has at least one simple integer point and either $|C_\infty| = 1$ or $|C_\infty| = 2$ and the two elements of $C_\infty$ are conjugate over a real quadratic field.

2. Auxiliary Results

Let $F(X,Y,Z) \in \mathbb{Q}[X,Y,Z]$ be an absolutely irreducible homogeneous polynomial of degree $N \geq 2$ such that the curve $C$ defined by the equation $F(X,Y,Z) = 0$ is of genus 0. The existence of a simple point on $C$ defined over $\mathbb{Q}$ is equivalent to the existence of a birational map, over $\mathbb{Q}$, between $C$ and the projective line $\mathbb{P}_1$ (see Mordell, 1969, Chapter 17, pp. 150–152 and Poulakis, 1998). Note that if $N$ is odd or if $N$ is even and $C$ has a singularity over $\mathbb{Q}$ of odd multiplicity, then $C$ always has a simple point defined over $\mathbb{Q}$ (Sendra and Winkler, 1997, Corollary 2.1).

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

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

defines a birational map $\phi$ over $\mathbb{Q}$ of $\mathbb{P}_1$ to $C$. Then $\phi$ is a birational morphism of $\mathbb{P}_1$ onto $C$ and $\deg u(S,T) = \deg v(S,T) = \deg w(S,T) = N$. If $(x : y : 1)$ is a non-singular point of $C(\mathbb{Q})$, then there exist $s,t \in \mathbb{Z}$ 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. See Poulakis and Voskos (2000, Lemma 2.1)

We denote by $\mathbb{Q}(\mathbb{P}_1)$ and $\mathbb{Q}(C)$ the function fields of $\mathbb{P}_1$ and $C$, respectively. Let $\phi$ be as in Lemma 2.1. The correspondence $f \mapsto f \circ \phi$ induces an isomorphism $\tilde{\phi}$ defined over $\mathbb{Q}$ from $\mathbb{Q}(C)$ onto $\mathbb{Q}(\mathbb{P}_1)$.

Lemma 2.2. The correspondence $P \mapsto \tilde{\phi}^{-1}(O_P(\mathbb{P}_1))$ defines a bijection between the set of zeros of $w(S,T)$ and $C_\infty$.

Proof. See the proof of Poulakis and Voskos (2000, Lemma 2.2)

Remark 2.1. The Lemmas 2.1 and 2.2 of Poulakis and Voskos (2000) are stated for $N \geq 3$. As one can easily verify they are also valid for $N = 2$.

3. Rational Curves with One Valuation at Infinity

Let $f(X,Y)$ and $C$ be as in the Introduction. Further, let $\deg f = N \geq 2$. In this section we suppose that the set $C_\infty$ has only one element and we describe an algorithm for the determination of all integer solutions of the diophantine equation $f(X,Y) = 0$. 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 to the equation \( f(X, Y) = 0 \). Otherwise, find homogeneous polynomials \( u(S, T), v(S, T), w(S, T) \in \mathbb{Z}[S, T] \) of degree \( N \), with no common non-constant factor, such that the correspondence

\[
(S, T) \rightarrow (u(S, T), v(S, T), w(S, T))
\]

defines a birational map \( \phi \) over \( \mathbb{Q} \) of \( \mathbb{P}^1 \) to \( C \). Since \( |C_\infty| = 1 \), Lemma 2.2 implies that \( w(S, T) = a(bS + cT)^N \), where \( a, b, c \in \mathbb{Z} \) with \( a \neq 0 \) and \( \gcd(b, c) = 1 \).

Step 3. Put \( U = bS + cT \) and \( V = S \). Then, we have a birational morphism \( \psi \) over \( \mathbb{Q} \) of \( \mathbb{P}^1 \) to \( C \) given by the correspondence

\[
(U, V) \rightarrow (p(U, V), q(U, V), dU^N),
\]

where \( p(U, V), q(U, V) \) are homogeneous polynomials in \( \mathbb{Z}[U, V] \) of degree \( N \) and \( d \) a non-zero integer. Let \( a_0 \) and \( b_0 \) be the coefficients of \( V^N \) in the polynomials \( p(U, V) \) and \( q(U, V) \), respectively. Since \( \gcd(p(U, V), q(U, V), dU^N) = 1 \), it follows that \( (a_0, b_0) \neq (0, 0) \).

Step 4. Find \( \delta = \gcd(a_0, b_0) \).

Step 5. Determine the set \( \Sigma \) of integers \( \eta \) such that

\[
p(\delta, \eta) \equiv 0 \pmod{d\delta^N} \quad \text{and} \quad q(\delta, \eta) \equiv 0 \pmod{d\delta^N}.
\]

Step 6. Compute the values

\[
x = \frac{p(\delta, \eta)}{d\delta^N} \quad \text{and} \quad y = \frac{q(\delta, \eta)}{d\delta^N},
\]

where \( \eta \in \Sigma \).

The couples \((x, y)\) with the integer singular points of the affine curve \( f(X, Y) = 0 \) are all the integer solutions to the equation \( f(X, Y) = 0 \).

Proof of correctness of the algorithm.

Let \((x, y)\) be an integer simple point on the curve \( f(X, Y) = 0 \). By Lemma 2.1 there are \( u, v \in \mathbb{Z} \) with \( u > 0 \) and \( \gcd(u, v) = 1 \) such that \( x = p(u, v)/du^N \) and \( y = q(u, v)/du^N \). (If \( u = 0 \), then we obtain a point at infinity on \( f(X, Y) = 0 \).) Then, \( u \) divides \( \delta \) and \( v\delta/u \in \Sigma \). Hence, multiplying the nominators and denominators of \( x \) and \( y \) by \((\delta/u)^N\), we see that \((x, y)\) is obtained by the above algorithm.

Note that there are efficient algorithms to carry out all the steps of this method. The determination of the singularities of \( C \) can be achieved by the algorithm of Sakkalis and Farouki (1990) or in many cases 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. The examination of the existence of a simple rational point on \( C \) and the construction of a parametrization for \( C \) can be carried out by the methods of Abhyankar and Bajaj (1988), Sendra and Winkler (1991), Sendra and Winkler (1997), van Hoeij (1997) and Sendra and Winkler (1999). The resolution of a polynomial congruence is obtained by the algorithm of Cohen (1993, Section 1.6, p. 36).

Next, we illustrate the above method by solving two diophantine equations defining rational curves with one valuation at infinity. The first has no integer solution while the second has infinitely many integer solutions.
Example 3.1. The equation
\[ f(X, Y) = (X - 3Y)^4 + 7X^3 - 23X^2Y + 109XY^2 - 181Y^3 - 2X^2 - 24XY + 182Y^2 - 2X - 94Y + 19 = 0 \]
does not have any integer solution.

Let \( F(X, Y, Z) \) be the homogenization of \( f(X, Y) \). We denote by \( C \) the projective curve defined by \( F(X, Y, Z) = 0 \). The singularities of \( C \) are the double points \( P_1 = (-1/2, 1/2), \ P_2 = ((25 + 6\sqrt{7})/16, (23 + 6\sqrt{7})/16), \ P_3 = ((25 - 6\sqrt{7})/16, (23 - 6\sqrt{7})/16) \). It follows that \( C \) is a rational curve. The only point at infinity \( P_\infty = (3 : 1 : 0) \) is a simple point defined over \( \mathbb{Q} \). Thus \( C \) possesses a parametrization over \( \mathbb{Q} \) and \( C_\infty \) has only one element.

A birational morphism over \( \mathbb{Q} \) of \( \mathbb{P}^1 \) to \( C \) is given by the correspondence
\[
(U, V) \rightarrow (p(U, V), q(U, V), 2U^4),
\]
where
\[
p(U, V) = -(U^4 + 8U^3V + 4U^2V^2 + 11UV^3 + 3V^4),
\]
\[
q(U, V) = U^4 - 4U^3V - 8U^2V^2 - 5UV^3 - V^4.
\]

We have \( \delta = \gcd(3, 1) = 1 \). Let \( \eta \) be an integer such that
\[
p(1, \eta) \equiv 0 \pmod{2} \quad \text{and} \quad q(1, \eta) \equiv 0 \pmod{2}.
\]
It follows that \( 11\eta^3 + 3\eta^4 + 1 \) is even which is a contradiction. Hence, the equation \( f(X, Y) = 0 \) does not have any integer solution.

Example 3.2. The integer solutions of the equation
\[
f(X, Y) = 9(2X - 3Y)^3 - 288X^4 + 1632X^3Y - 3216X^2Y^2 + 2392XY^3 - 386Y^4 + 72X^3 - 276X^2Y + 254XY^2 + 29Y^3 = 0
\]
are \( (X, Y) = (0, 0), (2, 1) \) and for every \( k \in \mathbb{Z} \)

1. \[
X = 10712 + 182733k + 1248372k^2 + 4271616k^3 + 7324992k^4 + 5038848k^5,
\]
\[
Y = 2(3848 + 64503k + 433620k^2 + 1461888k^3 + 2472768k^4 + 1679616k^5).
\]
2. \[
X = 53489 + 662389k + 3283956k^2 + 8149248k^3 + 3405888k^4 + 1679616k^5,
\]
\[
Y = 2(18779 + 229855k + 1127124k^2 + 2768256k^3 + 3405888k^4 + 1679616k^5).
\]
3. \[
X = 479707 + 8335077k + 12269556k^2 + 19636992k^3 + 15723072k^4 + 5038848k^5,
\]
\[
Y = 330226 + 2621790k + 8332200k^2 + 13250304k^3 + 10544256k^4 + 3359232k^5.
\]
4. \[
X = 4063494 + 21200829k + 44254836k^2 + 46199808k^3 + 24121152k^4 + 5038848k^5,
\]
\[
Y = 2764708 + 14362830k + 29856168k^2 + 31041792k^3 + 16142976k^4 + 3359232k^5.
\]

We denote by \( C \) the projective curve associated to the equation \( f(X, Y) = 0 \). The singularities of \( C \) are \( P_1 = (0, 0) \) which is a triple point and \( P_2 = (2, 1), \ P_3 = (11/2, 3), \ P_4 = (1/2, 0) \) which are double points. Thus, \( C \) has genus 0. Since the only point at infinity \( P_\infty = (3/2 : 1 : 0) \) is simple and defined over \( \mathbb{Q} \), it follows that \( C \) has a parametrization over \( \mathbb{Q} \) and that \( C_\infty \) has only one element.

A birational morphism over \( \mathbb{Q} \) of \( \mathbb{P}^1 \) to \( C \) is given by the correspondence
\[
(U, V) \rightarrow (p(U, V), q(U, V), 36U^5),
\]
where
\[
p(U, V) = 18U^5 + 78U^4V + 117U^3V^2 + 74U^2V^3 + 22UV^4 + 3V^5,
\]
\[
q(U, V) = 36U^5 + 108U^4V + 114U^3V^2 + 60U^2V^3 + 16UV^4 + 2V^5.
\]

We have \( \delta = \gcd(3, 2) = 1 \). Thus, we obtain the congruences:
\[
18 + 78\eta + 117\eta^2 + 74\eta^3 + 22\eta^4 + 3\eta^5 \equiv 0 \pmod{36},
\]
\[
18 + 54\eta + 57\eta^2 + 30\eta^3 + 8\eta^4 + \eta^5 \equiv 0 \pmod{18}.
\]

It follows that \( \eta \equiv 9, 13, 21, 33 \pmod{36} \). Thus, the values \( x = p(1, \eta)/36 \) and \( y = q(1, \eta)/36 \), where \( \eta = 9 + 36k, 13 + 36k, 21 + 36k, 33 + 36k \) and \( k \in \mathbb{Z} \) give the solutions (1)–(4), respectively.

4. Rational Curves with Two Valuations at Infinity

Let \( f(X, Y) \), \( N \), and \( C \) be as in the previous section. In this section we suppose that \( C_\infty \) has only two elements and we describe an algorithm for the solution of the diophantine equation \( f(X, Y) = 0 \). 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 to the equation \( f(X, Y) = 0 \). Otherwise, find homogeneous polynomials \( u(S, T), v(S, T), w(S, T) \in \mathbb{Z}[S, T] \) of degree \( N \), with no common non-constant factor, such that the correspondence
\[
(S, T) \mapsto (u(S, T), v(S, T), w(S, T))
\]
defines a birational map \( \phi \) over \( \mathbb{Q} \) of \( \mathbb{P}^1 \) to \( C \). Since \(|C_\infty| = 2\), Lemma 2.2 implies that \( w(S, T) \) has two distinct zeroes. We have the following two cases:

**(i)** \( w(S, T) = k(aS + bT)^\mu(cS + dT)^\nu \) with \( \mu + \nu = N \) and the factors \( aS + bT, cS + dT \) are non-proportional.

**Step 3.** Put \( U = aS + bT \) and \( V = cS + dT \). Since \( aS + bT \) and \( cS + dT \) are non-proportional, we have a birational morphism \( \psi \) over \( \mathbb{Q} \) of \( \mathbb{P}^1 \) to \( C \) given by the correspondence
\[
(U, V) \mapsto (p(U, V), q(U, V), lU^\mu V^\nu),
\]
where \( p(U, V), q(U, V) \) are homogeneous polynomials in \( \mathbb{Z}[U, V] \) of degree \( N \) and \( l \) a non-zero integer. Write
\[
p(U, V) = a_N U^N + a_{N-1} U^{N-1} V + \cdots + a_0 V^N,
\]
\[
q(U, V) = b_N U^N + b_{N-1} U^{N-1} V + \cdots + b_0 V^N.
\]
Since \( \gcd(p(U, V), q(U, V), lU^\mu V^\nu) = 1 \), we have \( (a_0, b_0) \neq (0, 0) \) and \( (a_N, b_N) \neq (0, 0) \).

**Step 4.** Compute \( \delta_1 = \gcd(a_0, b_0) \) and \( \delta_2 = \gcd(a_N, b_N) \).

**Step 5.** Determine the set \( \Sigma = \{(u, v) \in \mathbb{Z}^2 | \gcd(u, v) = 1, u > 0, u|\delta_1, v|\delta_2 \} \).
Step 6. Compute the values

\[ x = \frac{p(u, v)}{lu^m v^r} \quad \text{and} \quad y = \frac{q(u, v)}{lu^m v^r}, \]

where \((u, v) \in \Sigma\).

(ii) \(w(S, T) = k(aS^2 + bST + cT^2)^{N/2}\) and \(\delta = b^2 - 4ac\) is not a perfect square.

Step 3. Put \(U = 2aS + bT\) and \(V = T\). Then, we have a birational morphism \(\psi\) over \(\mathbb{Q}\) of \(\mathbb{P}^1\) to \(C\) given by the correspondence

\[ (U, V) \rightarrow (p(U, V), q(U, V), m(U^2 - \delta V^2)^{N/2}), \]

where \(p(U, V), q(U, V)\) are homogeneous polynomials in \(\mathbb{Z}[U, V]\) of degree \(N\) and \(m\) is a non-zero integer.

Step 4. Compute \(D = \gcd(R_1, R_2)\), where \(R_1\) is the resultant of \(p(U, 1)\) and \(U^2 - \delta\) and \(R_2\) the resultant of \(q(U, 1)\) and \(U^2 - \delta\). Since \(p(U, V), q(U, V)\) and \(U^2 - \delta V^2\) have no common non-constant factor, it follows that \(R_1 \neq 0\) or \(R_2 \neq 0\), whence \(D \neq 0\).

Step 5. Determine the set

\[ \Sigma = \{(u, v) \in \mathbb{Z}^2| \gcd(u, v) = 1, u \geq 0, u^2 - \delta v^2|D\}. \]

Step 6. Compute the values

\[ x = \frac{p(u, v)}{m(u^2 - \delta v^2)^{N/2}} \quad \text{and} \quad y = \frac{q(u, v)}{m(u^2 - \delta v^2)^{N/2}}, \]

where \((u, v) \in \Sigma\).

The integer points \((x, y)\) obtained in this way and the integer singular points of the affine curve \(f(X, Y) = 0\) are all the integer solutions to the equation \(f(X, Y) = 0\).

Proof of correctness of the algorithm.

Let \((x, y)\) be an integer simple point on the curve \(f(X, Y) = 0\). We first consider case (i). By Lemma 2.1 there are \(u, v \in \mathbb{Z}\) with \(u > 0\) and \(\gcd(u, v) = 1\) such that \(x = p(u, v)/lu^m v^r\) and \(y = q(u, v)/lu^m v^r\). It follows that \((u, v) \in \Sigma\). Therefore, \((x, y)\) is obtained by the above algorithm.

Next we consider case (ii). Suppose that \(R_1 \neq 0\). Write

\[ R_1 = p(U, 1)B(U) + \Gamma(U)(U^2 - \delta), \]

where \(B(U)\) and \(\Gamma(U)\) are polynomials in \(\mathbb{Z}[U]\). Homogenizing this equation, we obtain

\[ R_1 V^r = p(U, V)B(U, V) + \Gamma(U, V)(U^2 - \delta V^2), \]

where \(r\) is a positive integer and \(B(U, V), \Gamma(U, V)\) are homogeneous polynomials such that their dehomogenizations with respect to \(V\) are \(B(U)\) and \(\Gamma(U)\), respectively. By Lemma 2.1 there are \(u, v \in \mathbb{Z}\) with \(u \geq 0\) and \(\gcd(u, v) = 1\) such that

\[ x = \frac{p(u, v)}{m(u^2 - \delta v^2)^{N/2}} \quad \text{and} \quad y = \frac{q(u, v)}{m(u^2 - \delta v^2)^{N/2}}. \]

If \((u, v) \neq (1, 0)\), then \(u^2 - \delta v^2\) divides \(R_1 V^r\) and since \(\gcd(u^2 - \delta v^2, v) = 1\), it follows that \(u^2 - \delta v^2\) divides \(R_1\). Similarly, if \(R_2 \neq 0\), then \(u^2 - \delta v^2\) divides \(R_2\). Hence \(u^2 - \delta v^2\) divides \(D\) and it follows that \((u, v) \in \Sigma\). Therefore, \((x, y)\) is given by the above method.
Remark 4.1. In cases (i) and (ii) with $\delta < 0$ the equation $f(X, Y) = 0$ has only finitely many integer solutions, since the set $\Sigma$ is finite.

All steps of this method can be achieved by efficient algorithms. One can use the algorithms mentioned in the previous section. Furthermore, the fundamental solution of a Pellian equation can be found using the algorithm for the continuous fraction expansion of a real number of Cohen (1993, Section 1.3.4, p. 21) and the solution of a generalized Pellian equation is obtained by the method of Mollin (1998, Section 6.2).

Next, we apply the above method to find all the integer solutions of three equations defining rational curves with two infinite valuations.

Example 4.1. The integer solutions of the equation
$$f(X, Y) = 15(X - 3Y)^3(3X + Y)^2 - 44145X^4 + 128646X^3Y + 20027X^2Y^2 - 72926XY^3 + 16128Y^4 = 0$$
are $(X, Y) = (0, 0), (1, 4), (93, -62), (3, 5), (329, 0), (737, 603), (-4, 5), (-4, -9)$.

Let $F(X, Y, Z)$ be the homogenization of $f(X, Y)$. We denote by $C$ the projective curve defined by the equation $F(X, Y, Z) = 0$. The point $(0 : 0 : 1)$ is the only singular point of $C$ and its multiplicity is 4. It follows that $C$ is a rational curve. Furthermore, $C$ has two points at infinity which are simple, whence we deduce that $|C_{\infty}| = 2$.

We easily obtain that a birational map $\phi$ from $P^1$ to $C$ is given by $\phi(S : T) = (u(S, T) : v(S, T) : w(S, T))$, where
$$u(S, T) = -44145T^5 + 128646T^4S + 20027T^3S^2 - 72926T^2S^3 + 16128TS^4,$$
$$v(S, T) = -44145T^4S + 128646T^3S^2 + 20027T^2S^3 - 72926TS^4 + 16128S^5,$$
$$w(S, T) = 15(S + 3T)^2(2S - T)^3.$$

Setting $U = S + 3T$ and $V = 2S - T$ we have the birational map $\psi : P^1 \to C$ defined by $\psi(U : V) = (p(U, V) : q(U, V) : 15U^2V^3)$, where
$$p(U, V) = 32U^5 + 260UV^4 - 980V^2U^3 + 625V^3U^2 + 258V^4U - 180V^5,$$
$$q(U, V) = 16U^5 + 186UV^4 - 7V^2U^3 - 1161V^3U^2 + 486UV^4 + 54V^5.$$

We have gcd(180, 540) = 180 and gcd(32, 16) = 16. The couples $(u, v) \in \mathbb{Z}^2$ satisfying $p(u, v)/15u^2v^3, q(u, v)/15u^2v^3 \in \mathbb{Z}$, gcd$(u, v) = 1$, $u > 0$, gcd$(v, 16) = 1, (u, v) = (1, 1), (1, -1), (2, 1), (3, -1), (6, 1), (1, -2), (3, 2)$ which give, respectively, the solutions $(X, Y) = (1, 4), (93, -62), (3, 5), (329, 0), (737, 603), (-4, 5), (-4, -9)$ for the equation $f(X, Y) = 0$. The above solutions with $(0, 0)$ are all the integer solutions of $f(X, Y) = 0$.

Example 4.2. The integer solutions of the equation
$$g(X, Y) = (2X^2 + 12XY + 19Y^2)^2 - 13X^3 - 117X^2Y - 356XY^2 - 366Y^3 + 10X^2 + 60XY + 89Y^2 = 0$$
are $(X, Y) = (3, -1), (2, 0), (-3, 1), (0, 0), (-2, 1), (4, -1)$.

Let $C$ be the projective curve defined by the equation $g(X, Y) = 0$. Since the singularities of $C$ are the double points $P_1 = (0, 0), P_2 = (-2, 1), P_3 = (4, -1)$, it follows that $C$ is rational. The points at infinity are the simple points $((-6 \pm i\sqrt{2})/2 : 1 : 0)$. Thus $|C_{\infty}| = 2$. 
We obtain the following parametrization for the curve $g(X, Y) = 0$:

\[
X = \frac{p(U)}{12(U^2 + 2)^2}, \quad Y = \frac{q(U)}{6(U^2 + 2)^2},
\]

where

\[
p(U) = -21U^4 - 94U^3 + 516U^2 + 240U - 160, \quad q(U) = 6U^4 + 5U^3 - 84U^2 - 24U + 32.
\]

We denote by $P(U, V)$ and $Q(U, V)$ the homogenizations of $p(U)$ and $q(U)$, respectively.

The resultant of $p(U)$ and $U^2 + 2$ is $R_1 = 1994544$ and the resultant of $q(U)$ and $U^2 + 2$ is $R_2 = 52488$. We have $\gcd(R_1, R_2) = 2^{3}3^{8}$. Next we shall determine the set $\Sigma$ of $(u, v) \in \mathbb{Z}^2$ such that $\gcd(u, v) = 1$, $u \geq 0$, and $u^2 + 2v^2 = 2^{a}3^{b}$, where $a$, $b$ are integers with $0 \leq a \leq 3$ and $0 \leq b \leq 8$. If $a > 1$, then $2|u$ and it follows that $2|v$. Hence $\gcd(u, v) > 1$ which is a contradiction. If $a = 0$, then $u$ is odd and we deduce that $P(u, v)/12(u^2 + 2v^2)$ is not an integer. If $a = 1$, then we have $(u, v) = (0, \pm 1), (2, \pm 1), (4, \pm 1), (2, \pm 5), (8, \pm 7), (22, \pm 1), (20, \pm 23), (26, \pm 43), (112, \pm 17)$. Finally, we deduce that $P(u, v)/12(u^2 + 2v^2)$ and $Q(u, v)/6(u^2 + 2v^2)$ are integers only for $(u, v) = (2, 1), (4, -1), (2, -5)$. Thus, we obtain the simple points : $(3, -1), (2, 0), (-3, 1)$, respectively. The result follows.

**Example 4.3.** The integer solutions to the equation

\[
h(X, Y) = 2(X^2 - 3Y^2)^3 + 8X^5 - 55X^4Y + 242X^3Y^2 - 360X^2Y^3
\]

\[
- 90XY^4 + 351Y^5 + 8X^4 - 110X^3Y + 114X^2Y^2 + 430XY^3 - 586Y^4 = 0
\]

are

\[
(X, Y) = (0, 0), (-2, 0), (3, 3), (1, 3), (-5, -3), (P(u, v)/2a^3, Q(u, v)/2a^3),
\]

where

\[
P(u, v) = 692u^6 - 7119u^5v + 30444u^4v^2 - 69192u^3v^3 + 88002u^2v^4 - 59265uv^5 + 16470v^6,
\]

\[
Q(u, v) = -3(173u^6 - 1650u^5v + 6460u^4v^2 - 13278u^3v^3 + 15999u^2v^4 - 9000uv^5 + 2196v^6),
\]

\[
(a, u, v) = (1, A_{2k+1}, B_{2k+1}), (-2, s(k)(A_k + 3B_k), s(k)(A_k + B_k)),
\]

\[
(-3, s(k)3B_{2k}, s(k)A_{2k}), (6, 3(A_k + B_k), A_k + 3B_k),
\]

\[
(13, 4A_{156k+96} - 3B_{156k+96}, 4B_{156k+96}, A_{156k+96}),
\]

\[
(-39, s(k)(12B_{78k+57} - 3A_{78k+57}), s(k)(4A_{78k+57} - 3B_{78k+57})),
\]

with $k \in \mathbb{Z}$ and $s(k)$ is the sign of $k$ if $k \neq 0$ and $s(0) = 1$. Moreover

\[
A_n = \frac{1}{2}(2 + \sqrt{3})^n + (2 - \sqrt{3})^n, \quad B_n = \frac{1}{2\sqrt{3}}((2 + \sqrt{3})^n - (2 - \sqrt{3})^n).
\]

Let $C$ be the projective curve defined by the homogenization of $h(X, Y)$. The singular points of $C$ are the double points $P_1 = (-2, 0), P_2 = (3, 3), P_3 = (1, 3), P_4 = (-5, -3)$ and the point $P_5 = (0, 0)$ with multiplicity 4. It follows that $C$ is a rational curve. Its points at infinity are $(\pm \sqrt{3} : 1 : 0)$ which are simple. Thus $|C_\infty| = 2$.

We obtain the following parametrization for the curve $C$:

\[
X = \frac{p(U)}{2(U^2 - 3)^3} \quad \text{and} \quad Y = \frac{q(U)}{2(U^2 - 3)^3},
\]
where
\[ p(U) = 692U^6 - 7119U^5 + 30444U^4 - 69192U^3 + 88002U^2 - 59265U + 16470, \]
\[ q(U) = -3(173U^6 - 1650U^5 + 6460U^4 - 13278U^3 + 15099U^2 - 9000U + 2196). \]

We denote by \( P(U, V) \) and \( Q(U, V) \) the homogenizations of \( p(U) \) and \( q(U) \), respectively.

Let \( R_1 \) be the resultant of \( p(U) \) and \( U^2 - 3 \) and \( R_2 \) be the resultant of \( q(U) \) and \( U^2 - 3 \).

We have \( R_1 = -454896 \) and \( R_2 = 151632 \) and the greatest common divisor of \( R_1 \) and \( R_2 \) is equal to 151632 = \( 2^4 \cdot 3^6 \cdot 13 \).

We consider the couples \((u, v) \in \mathbb{Z}^2\) such that \( \gcd(u, v) = 1 \), \( u \geq 0 \), and \( u^2 - 3v^2 = \pm 2^a3^b13^c \), where \( a, b, c \) are integers with \( 0 \leq a \leq 4 \), \( 0 \leq b \leq 6 \) and \( 0 \leq c \leq 1 \). Suppose that \( a > 1 \). Since \( \gcd(u, v) = 1 \), we have \( 0 \equiv u^2 - 3v^2 \equiv 1 \) or \( 2 \pmod{4} \) which is a contradiction. Thus \( a = 0, 1 \). If \( b > 1 \), then the equality \( u^2 - 3v^2 = 2^a3^b13^c \) implies that \( 3|u \) and hence \( 3|v \). So \( \gcd(u, v) > 1 \) which is a contradiction. Thus \( b = 0, 1 \).

We have the following cases:

1. \( a = b = c = 0 \). Then \( u^2 - 3v^2 = \pm 1 \). If \( u^2 - 3v^2 = -1 \), it follows that \( u^2 \equiv -1 \pmod{3} \) which is a contradiction. Hence, we have only the equation \( U^2 - 3V^2 = 1 \). The integer solutions \((u, v)\) of this equation with \( u > 0 \) are given by \( A_n + B_n\sqrt{3} = (2 + \sqrt{3})^n \) where \( n \in \mathbb{Z} \). Hence

\[ A_n = \frac{1}{2}((2 + \sqrt{3})^n + (2 - \sqrt{3})^n), \quad B_n = \frac{1}{2\sqrt{3}}((2 + \sqrt{3})^n - (2 - \sqrt{3})^n). \]

We have \((A_n, B_n) \equiv (1, 0) \pmod{2}\) if \( n \) is even and \((A_n, B_n) \equiv (0, 1) \pmod{2}\) otherwise.

On the other hand, the solutions of the system of congruences \( P(U, V) \equiv Q(U, V) \equiv 0 \pmod{2} \) are \((u, v) \equiv (0, 1), (1, 1) \pmod{2}\). Thus \( (P(A_n, B_n)/2, Q(A_n, B_n)/2) \) is an integer solution to \( h(X, Y) = 0 \) only in the case where \( n \) is odd.

2. \( a = 0, b = 1, c = 0 \). Then we have \( u^2 - 3v^2 = \pm 3 \). If \( u^2 - 3v^2 = 3 \), we obtain, as in previous cases, a contradiction. Consider the equation \( U^2 - 3V^2 = -3 \). Using Mollin (1998, Theorem 6.2.6, p. 300) we obtain that the integer solutions \((u, v)\) with \( u \geq 0 \) are given by

\[ u_n + v_n\sqrt{3} = s(n)(A_n + B_n\sqrt{3}), \quad n \in \mathbb{Z}, \]

where \( A_n, B_n \) are as in case (1), \( s(n) \) is the sign of \( n \) if \( n \neq 0 \) and \( s(0) = 1 \). We have \((u_n, v_n) \equiv s(n)(0, 1) \pmod{6}\) if \( n \) is even and \((u_n, v_n) \equiv s(n)(3, 2) \pmod{6}\) otherwise.

If \( n \) is odd, it follows that \((u_n, v_n)\) do not satisfy the congruence \( Q(U, V) \equiv 0 \pmod{6}\). On the other hand, if \( n \) is even, we obtain that \((u_n, v_n)/54, -Q(u_n, v_n)/54)\) is an integer solution to \( h(X, Y) = 0 \).

3. \( a = 1, b = c = 0 \). Then \( u^2 - 3v^2 = \pm 2 \). If \( u^2 - 3v^2 = 2 \), then \( u^2 \equiv 2 \pmod{3} \) which is a contradiction. So we have only to consider the equation \( U^2 - 3V^2 = -2 \). By Mollin (1998, Theorem 6.2.6, p. 300), the integer solutions \((u, v)\) of the above equation with \( u \geq 0 \) are given by

\[ u_n + v_n\sqrt{3} = s(n)(A_n + B_n\sqrt{3})(1 + \sqrt{3}), \quad n \in \mathbb{Z}, \]

where \( A_n, B_n \) are as above, \( s(n) \) is the sign of \( n \) if \( n \neq 0 \) and \( s(0) = 1 \). We have \((u_n, v_n) \equiv (1, 1) \pmod{2}\), whence we deduce that \( P(u_n, v_n) \equiv Q(u_n, v_n) \equiv 0 \pmod{16}\). So \((P(u_n, v_n)/16, -Q(u_n, v_n)/16)\) is an integer solution to \( h(X, Y) = 0 \).

4. \( a = b = 1, c = 0 \). In this case we have \( u^2 - 3v^2 = \pm 6 \). If \( u^2 - 3v^2 = 6 \), then \( u = 3u_1 \), where \( u_1 \in \mathbb{Z} \) and \( 3u_1^2 - t^2 = -2 \). Thus \( t^2 \equiv 2 \pmod{3} \) which is a contradiction. So we have to solve the equation \( U^2 - 3V^2 = 6 \). Following Mollin (1998, Theorem 6.2.5 and Proposition 6.2.1, p. 299), we obtain that the integer solutions \((u, v)\) with \( u > 0 \) of
the above equation are obtained by
\[ u_n + v_n\sqrt{3} = (A_n + B_n\sqrt{3})(3 + \sqrt{3}), \quad n \in \mathbb{Z}. \]

We deduce that \((u_n, v_n) \equiv (3, 1), (3, 5) \pmod{6}\), whence we get that the couple \((P(u_n, v_n))/432, Q(u_n, v_n)/432\) is an integer solution to \(h(X, Y) = 0\).

5. \(a = b = 0, c = 1\). Then \(u^2 - 3v^2 = \pm 13\). If \(u^2 - 3v^2 = -13\), we have that \(u^2 \equiv -1 \pmod{3}\) which is a contradiction. Thus, we have only to solve the equation \(U^2 - 3V^2 = 13\). Using Mollin (1998, Theorem 6.2.5, p. 299) we deduce that the integer solutions \((u, v)\) with \(u > 0\) of this equation are given by
\[ u_{e,n} + v_{e,n}\sqrt{3} = (A_n + B_n\sqrt{3})(4 + 3\sqrt{3}), \quad n \in \mathbb{Z}, \]

where \(e = \pm 1\) and \(A_n, B_n\) are as in case (1). We calculate the couples \((u_{e,n}, v_{e,n}) \pmod{13}\) and we deduce that \((u_{1,n}, v_{1,n})\) do not verify the congruence \(P(U, V) \equiv 0 \pmod{13}\). On the other hand, we obtain that only for \(n \equiv 96 \pmod{169}\) the couple \((P(u_{1,n}, v_{1,n}))/4394, Q(u_{1,n}, v_{1,n})/4394\) is an integer solution to \(h(X, Y) = 0\).

6. \(a = 0, b = c = 1\). Then \(u^2 - 3v^2 = \pm 39\). If \(u^2 - 3v^2 = 39\), it follows that \(v^2 \equiv 2 \pmod{3}\) which is a contradiction. The integer solutions \((u, v)\) with \(u \geq 0\) of the equation \(U^2 - 3V^2 = -39\) are given by
\[ u_{e,n} + v_{e,n}\sqrt{3} = s(e, n)(A_n + B_n\sqrt{3})(3 + 3\sqrt{3}), \quad n \in \mathbb{Z}, \]

where \(A_n, B_n\) are as above, \(e = \pm 1, s(e, n)\) is the sign of \(n\) if \(n \neq 0, s(1,0) = 1\) and \(s(-1,0) = -1\). We deduce that the couples \((u_{1,n}, v_{1,n})\) do not verify the congruence \(P(U, V) \equiv 0 \pmod{13}\) and only for \(n \equiv 57 \pmod{78}\) the couple \((P(u_{1,n}, v_{1,n}))/39^2, Q(u_{1,n}, v_{1,n})/39^2\) is an integer solution to \(h(X, Y) = 0\).

7. \(a = 1, b = 0, c = 1\). It follows that \(u^2 - 3v^2 = \pm 26\). In the case where \(u^2 - 3v^2 = 26\), we get \(u^2 \equiv 2 \pmod{3}\) which is a contradiction. Thus, we have only to consider the equation \(U^2 - 3V^2 = -26\). The integer solutions \((u, v)\) with \(u \geq 0\) are given by
\[ u_{e,n} + v_{e,n}\sqrt{3} = s(e, n)(A_n + B_n\sqrt{3})(1 + 3\sqrt{3}), \quad n \in \mathbb{Z}, \]

where \(A_n, B_n\) are as above, \(e = \pm 1, s(e, n)\) is the sign of \(n\) if \(n \neq 0, s(1,0) = 1\) and \(s(-1,0) = -1\). We determine the couples \((u_{e,n}, v_{e,n}) \pmod{169}\) and it follows that none of these couples satisfy the congruence \(P(U, V) \equiv 0 \pmod{169}\). Hence \(-P(u_{e,n}, v_{e,n})/26^2\) is not an integer.

8. \(a = b = c = 1\). Thus \(u^2 - 3v^2 = \pm 78\). If \(u^2 - 3v^2 = -78\), then we get \(u^2 \equiv 2 \pmod{3}\) which is a contradiction. Thus, we consider only the equation \(U^2 - 3V^2 = 78\). The solutions of this equation given by
\[ u_{e,n} + v_{e,n}\sqrt{3} = e(A_n + B_n\sqrt{3})(9 + 3\sqrt{3}), \quad n \in \mathbb{Z}, \]

where \(A_n, B_n\) are as above and \(e = \pm 1\), are the only integer solutions with \(u_{e,n} \geq 0\). We determine the couples \((u_{e,n}, v_{e,n}) \pmod{169}\) and we see that none of these couples verify the congruence \(P(U, V) \equiv 0 \pmod{169}\), whence it follows that \(P(u_{e,n}, v_{e,n})/78^2\) is not an integer.

5. Curves with Infinitely Many Integer Points

Let \(f(X, Y)\) and \(C\) be as in the previous sections. We denote by \(C(\mathbb{Z})\) the set of integer points of \(f(X, Y) = 0\). The methods developed in Sections 3 and 4 (see Remark 4.1) imply the following well-known result of Maillet (1919):
Theorem 5.1. Suppose that the equation \( f(X, Y) = 0 \) has infinitely many integer solutions. Then, there exists a birational map \( \phi \) of \( \mathbb{P}^1 \) to \( C \) given by the correspondence

\[
(S, T) \mapsto (u(S, T), v(S, T), w(S, T))
\]

where \( u(S, T), v(S, T), w(S, T) \) are relatively prime homogeneous polynomials in \( \mathbb{Z}[S, T] \) of degree \( N \) and \( w(S, T) = aT^N \) or \( aq(S, T)^{N/2} \) where \( a \in \mathbb{Z} \) and \( q(S, T) \) is a quadratic irreducible polynomial with positive discriminant.

We say that an element \( V \) of \( C_\infty \) is defined over a subfield \( k \) of \( \overline{\mathbb{Q}} \) if \( \tau(V) = V \) for every \( \tau \in \text{Gal}(\overline{\mathbb{Q}}/k) \). Further, we call two elements \( V \) and \( W \) of \( C_\infty \) conjugate over a quadratic field \( k \) if \( V \) and \( W \) are defined over \( k \) and there is \( \sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \) which is not the identity on \( k \) such that \( \sigma(V) = W \). Using the ideas developed in the previous sections and the above theorem 5.1 we obtain a necessary and sufficient condition for the set \( C(\mathbb{Z}) \) to be infinite.

Theorem 5.2. The set \( C(\mathbb{Z}) \) is infinite if and only if one of the following two conditions is satisfied:

(a) \( C_\infty \) consists of one element and \( C(\mathbb{Z}) \) has at least one simple integer point.

(b) \( C_\infty \) consists of two elements which are conjugate over a real quadratic field and \( C(\mathbb{Z}) \) has at least one simple integer point.

Proof. Suppose first that the set \( C(\mathbb{Z}) \) is infinite. By Lemma 2.1 and Theorem 5.1, there exists a birational morphism \( \phi : \mathbb{P}^1 \to C \) given by the correspondence

\[
(S, T) \mapsto (u(S, T), v(S, T), w(S, T))
\]

where \( u(S, T), v(S, T), w(S, T) \) are relatively prime homogeneous polynomials in \( \mathbb{Z}[S, T] \) of degree \( N \) and \( w(S, T) = aT^N \) or \( aq(S, T)^{N/2} \) where \( a \in \mathbb{Z} \) and \( q(S, T) \) is a quadratic irreducible polynomial with positive discriminant. By Lemma 2.2, it follows that \( C_\infty \) consists of one or two elements, respectively. In the second case, since \( \phi \) is defined over \( \mathbb{Q} \), the two elements of \( C_\infty \) are conjugate over the real quadratic field which is the splitting field of \( q(S, T) \).

Suppose that \( C(\mathbb{Z}) \) contains a simple point \( P_0 = (x_0, y_0) \). By Lemma 2.1, we have a birational morphism \( \psi : \mathbb{P}^1 \to C \) given by

\[
(U, V) \mapsto (p(U, V), q(U, V), r(U, V))
\]

where \( p(U, V) \), \( q(U, V) \) and \( r(U, V) \) are homogeneous relatively prime polynomials in \( \mathbb{Z}[U, V] \) of degree \( N \). Further, there are \( u_0, v_0 \in \mathbb{Z} \) with \( u_0 \geq 0 \) and \( \gcd(u_0, v_0) = 1 \) such that \( P_0 = \psi(u_0, v_0) \). Let \( |C_\infty| = 1 \). By Lemma 2.2, \( r(U, V) \) has only one zero and after a change of variables (as in Section 3) we have \( r(U, V) = dU^N \). It follows that for every \( v \in \mathbb{Z} \) with \( v \equiv v_0 \pmod{du_0^N} \) we have \( \gcd(v, u_0) = 1 \) and \( \psi(u_0, v) \) is an integer point on \( C \). Hence \( C(\mathbb{Z}) \) is infinite. Let \( |C_\infty| = 2 \) and let the two elements of \( C_\infty \) be conjugate over a real quadratic field \( K \). Lemma 2.2 yields that \( r(U, V) \) has only two zeros which are conjugate over \( K \). After a change of variables (as in Section 4) we have \( r(U, V) = a(U^2 - \delta V^2)^{N/2} \), where \( a, \delta \) are positive integers and \( \delta \) is not a perfect square. Put \( k = u_0^2 - \delta v_0^2 \). Taking \( (a|k|^{N/2} + 1)^2 \) distinct integer solutions \( (u_i, v_i) \) \((i = 1, \ldots, (a|k|^{N/2} + 1)^2)\) of the equation \( U^2 - \delta V^2 = 1 \), we deduce that there are at least two distinct couples \( (u_m, v_m) \) and \( (u_n, v_n) \) such that \( (u_m, v_m) \equiv (u_n, v_n) \pmod{a|k|^{N/2}} \).
The solution given by
\[ z + w\sqrt{\delta} = (u_m + v_m\sqrt{\delta})(u_n - v_n\sqrt{\delta}) \]
satisfies
\[ z \equiv 1 \pmod{a|\delta|^{N/2}} \quad \text{and} \quad w \equiv 0 \pmod{a|\delta|^{N/2}}. \]
Then, the solutions to the equation \( U^2 - \delta V^2 = k \) given by
\[ z_i + w_i\sqrt{\delta} = (z + w\sqrt{\delta})(u_0 + v_0\sqrt{\delta}) \quad (i = 0, 1, \ldots) \]
verify \((z_i, w_i) \equiv (u_0, v_0) \pmod{a|\delta|^{N/2}}\). Hence, \( \gcd(z_i, w_i) = 1 \) and
\[ p(z_i, w_i) \equiv q(z_i, w_i) \equiv 0 \pmod{a|\delta|^{N/2}}. \]
Therefore \( (z_i, w_i) \ (i = 0, 1, \ldots) \) are integer points of \( C \) and so \( C(\mathbb{Z}) \) is infinite.

**Remark 5.1.** In Schinzel (1969) it is proved that if \( f(X, Y) \) is an irreducible polynomial of degree \( N \) such that the equation \( f(X, Y) = 0 \) has infinitely many integer solutions, then the homogeneous part of degree \( N \) of \( f(X, Y) \) is of the form \( a(bX + cY)^N \) or \( aq(X, Y)^{N/2} \), where \( a, b, c \in \mathbb{Z} \) and \( q(X, Y) \) is a homogeneous quadratic polynomial of \( \mathbb{Z}[X, Y] \) with positive discriminant. This necessary condition is also not sufficient for the equation \( f(X, Y) = 0 \) to have infinitely many integer solutions as the following two examples show.

1. The equation \( Y^2 = (X + 1)^2(X^2 + 15) \) defines a rational curve and by Poulakis (1999) its integer solutions are \((X, Y) = (1, \pm 8), (-1, 0), (7, \pm 64), (-7, \pm 48)\).
2. Consider the rational curve defined by \( f(X, Y) = (X^2 - 2Y^2)^2 + XY = 0 \). Let \( x, y \in \mathbb{Z} \) with \( f(x, y) = 0 \). Set \( d = \gcd(x, y) \). Then \( x = dx', y = dy' \), where \( x', y' \in \mathbb{Z} \) and \( \gcd(x', y') = 1 \). Thus \( d(x'^2 - 2y'^2)^2 = |x'y'| \), whence \( |x'| = u^2 \), \( |y'| = v^2 \) with \( u, v \in \mathbb{Z} \) and \( u > 0, v > 0 \). It follows that \( d(u^4 - 2v^4) = uv \) and \( \gcd(u^4 - 2v^4, uv) \) are known (cf. Mordell, 1969) and so we finally obtain that the only integer solutions of \( f(X, Y) = 0 \) are \((X, Y) = (0, 0), (1, -1), (-1, 1)\).

**Acknowledgements**

The authors wish to thank the referees for helpful suggestions and comments.

**References**


Received 8 February 2001
Accepted 3 December 2001