POLYNOMIAL PARAMETRIZATION OF THE SOLUTIONS OF DIOPHANTINE EQUATIONS OF GENUS 0

SOPHIE FRISCH AND GÜNTER LETTL

Dedicated to Prof. Władysław Narkiewicz on the occasion of his 70th birthday.

Abstract. Let \( f \in \mathbb{Z}[X, Y, Z] \) be a non-constant, absolutely irreducible, homogeneous polynomial with integer coefficients, such that the projective curve given by \( f = 0 \) has a function field isomorphic to the rational function field \( \mathbb{Q}(T) \). We show that all integral solutions of the Diophantine equation \( f = 0 \) (up to those corresponding to some singular points) can be parametrized by a single triple of integer-valued polynomials. In general, it is not possible to parametrize this set of solutions by a single triple of polynomials with integer coefficients.

Recently, the first author and L. Vaserstein proved that the set of all Pythagorean triples can be parametrized by a single triple of integer-valued polynomials, but not by a single triple of polynomials with integer coefficients (in any number of variables) [2]. We denote by \( \text{Int}(\mathbb{Z}^m) \) the ring of integer-valued polynomials in \( m \) variables,

\[
\text{Int}(\mathbb{Z}^m) = \{ \varphi \in \mathbb{Q}[X_1, \ldots, X_m] \mid \varphi(\mathbb{Z}^m) \subset \mathbb{Z} \}.
\]

In this paper we will generalize the affirmative part of [2] to such homogeneous equations as define a (plane) projective curve with a rational function field.

Throughout this paper, \( f \in \mathbb{Z}[X, Y, Z] \setminus \{0\} \) denotes an irreducible polynomial with integer coefficients, which is homogeneous of degree \( n \geq 1 \). Let \( \overline{\mathbb{Q}} \) be an algebraic closure of \( \mathbb{Q} \) and \( C_f \subset \mathbb{P}^2(\overline{\mathbb{Q}}) \) the plane projective curve defined by \( f = 0 \),

\[
C_f = \{ (x : y : z) \in \mathbb{P}^2(\overline{\mathbb{Q}}) \mid f(x, y, z) = 0 \}.
\]

We will further suppose that the function field \( K = \mathbb{Q}(C_f) \) of \( C_f \) over \( \mathbb{Q} \) is isomorphic to the rational function field \( \mathbb{Q}(T) \). This implies that \( f \) is absolutely irreducible (i.e., irreducible in \( \overline{\mathbb{Q}}[X, Y, Z] \)). Our assumption is satisfied, for instance, if \( C_f \) has genus 0 and possesses a regular point defined over \( \mathbb{Q} \).

Recall that a point \((x : y : z) \in C_f\) is singular if and only if the local ring \( R_{(x:y:z)} \subset K \) above \( R_{(x:y:z)} \) (meaning \( R_{(x:y:z)} \subset \mathcal{O}_{P_i} \) and \( m_{(x:y:z)} \subset P_i \), where \( m_{(x:y:z)} \) and \( P_i \) denote the corresponding maximal ideals). Let \( C_f^{\text{bad}} \) denote the set of those singular points \((x : y : z) \in C_f\) for which there exists no discrete valuation ring \( \mathcal{O}_P \) above \( R_{(x:y:z)} \) with \( \mathcal{O}_P/P \simeq \mathbb{Q} \). These points will be “bad” for our main theorem.

We investigate the set of integer solutions of the Diophantine equation \( f(X, Y, Z) = 0 \),

\[
\mathcal{L}_f := \{ (x, y, z) \in \mathbb{Z}^3 \mid f(x, y, z) = 0 \},
\]

2000 Mathematics Subject Classification. Primary 11D85, secondary 13F20, 11D41, 14H05.
up to those solutions which correspond to the “bad” points of the curve. We set
\[ \mathcal{L}_{f}^{\text{bad}} = \{(x, y, z) \in \mathcal{L}_{f} \mid (x : y : z) \in C_{f}^{\text{bad}}\} . \]

**Theorem 1.** Let \( f \in \mathbb{Z}[X, Y, Z] \setminus \{0\} \) be an irreducible, homogeneous polynomial of degree \( n \geq 1 \) such that the function field \( K = \mathbb{Q}(C_{f}) \) is isomorphic to \( \mathbb{Q}(T) \).

Then there exist polynomials \( g_{1}, g_{2}, g_{3} \in \text{Int}(\mathbb{Z}^{m}) \) for some \( m \in \mathbb{N} \) such that
\[ \mathcal{L}_{f} \setminus \mathcal{L}_{f}^{\text{bad}} = \left\{ (g_{1}(\mathbf{x}), g_{2}(\mathbf{x}), g_{3}(\mathbf{x})) \mid \mathbf{x} \in \mathbb{Z}^{m} \right\} ; \]
in other words, up to the “bad” solutions, all solutions of the Diophantine equation
\[ f(X, Y, Z) = 0 \]
can be parametrized by one triple of integer-valued polynomials.

The suppositions of Theorem 1 imply that for \( n \leq 2 \) the curve \( C_{f} \) has no singular point. For \( n = 1 \), \( C_{f} \) is just a line and the result of Theorem 1 is obvious (even with \( g_{i} \in \mathbb{Z}[U, V] \)). For \( n = 2 \), we immediately obtain

**Corollary 2.** Let \( f \in \mathbb{Z}[X, Y, Z] \) be an absolutely irreducible quadratic form. Then there exist polynomials \( g_{1}, g_{2}, g_{3} \in \text{Int}(\mathbb{Z}^{m}) \) for some \( m \in \mathbb{N} \) such that
\[ \mathcal{L}_{f} = \left\{ (g_{1}(\mathbf{x}), g_{2}(\mathbf{x}), g_{3}(\mathbf{x})) \mid \mathbf{x} \in \mathbb{Z}^{m} \right\} . \]

For the proof of Theorem 1 we will use the resultant of polynomials and therefore recall some well-known results on it (cf. [5, Chap. I, §9-10]).

Given polynomials \( g, h \in \mathbb{Z}[U, V] \) in the variables \( U, V \), let \( \text{Res}_{V}(g, h) \in \mathbb{Z}[U] \) denote the resultant of \( g, h \) when considered as polynomials in the variable \( V \) over the ring \( \mathbb{Z}[U] \), and, vice versa, \( \text{Res}_{U}(g, h) \in \mathbb{Z}[V] \) the resultant of \( g, h \) as polynomials in \( U \).

**Lemma 3.** Let \( g, h \in \mathbb{Z}[U, V] \) be relatively prime polynomials.

a) Then \( \text{Res}_{V}(g, h) \neq 0 \) and \( \text{Res}_{V}(g, h) \neq 0 \), and there exist polynomials \( r, s, r', s' \in \mathbb{Z}[U, V] \) with
\[ gr + hs = \text{Res}_{V}(g, h) \quad \text{and} \quad gr' + hs' = \text{Res}_{V}(g, h). \]

b) If \( g \) and \( h \) are homogeneous of degree \( d_{1} \) and \( d_{2} \), resp., then \( \text{Res}_{V}(g, h) \) and \( \text{Res}_{V}(g, h) \) are each homogeneous of degree \( d_{1}d_{2} \), and consequently
\[ \text{Res}_{U}(g, h) = a V^{d_{1}d_{2}} \quad \text{and} \quad \text{Res}_{V}(g, h) = b U^{d_{1}d_{2}} \quad \text{with} \quad a, b \in \mathbb{Z} \setminus \{0\} . \]

We will also use the implication \((\text{D}) \Rightarrow (\text{B})\) of the main theorem of [1], which for the sake of completeness we state in the following

**Proposition 4.** Let \( k \in \mathbb{N} \) and suppose that \( S \subset \mathbb{Z}^{k} \) is the set of integer \( k \)-tuples in the range of a \( k \)-tuple of polynomials with rational coefficients, as the variables range through the integers, i.e., there exist \( h_{1}, \ldots, h_{k} \in \mathbb{Q}[X_{1}, \ldots, X_{r}] \) for some \( r \in \mathbb{N} \) such that
\[ S = \{(h_{1}(\mathbf{x}), \ldots, h_{k}(\mathbf{x})) \mid \mathbf{x} \in \mathbb{Z}^{r} \} \cap \mathbb{Z}^{k} . \]

Then \( S \) is parametrizable by a \( k \)-tuple of integer-valued polynomials, i.e., there exist \( g_{1}, \ldots, g_{k} \in \text{Int}(\mathbb{Z}^{m}) \) for some \( m \in \mathbb{N} \) such that
\[ S = \{(g_{1}(\mathbf{x}), \ldots, g_{k}(\mathbf{x})) \mid \mathbf{x} \in \mathbb{Z}^{m} \} . \]
Proof of Theorem 1 Let $f$ be as in the statement of the theorem. Then there exist homogeneous polynomials $h_1, h_2, h_3 \in \mathbb{Q}[U, V]$ such that

$$(X, Y, Z) = \left(h_1(U, V), h_2(U, V), h_3(U, V)\right)$$

defines a birational (projective) isomorphism between $C_f$ and the projective line. We may assume $h_1, h_2, h_3 \in \mathbb{Z}[U, V]$ and $\gcd(h_1, h_2, h_3) = 1$ (see, for instance, [1] Sect. 2).

For every $\mathbb{Q}$-rational point $(u : v) \in \mathbb{P}^1(\mathbb{Q})$, $(h_1(u, v) : h_2(u, v) : h_3(u, v))$ is the evaluation of the birational isomorphism at this point. This means that $(h_1(u, v) : h_2(u, v) : h_3(u, v))$ is a $\mathbb{Q}$-rational point of $C_f$ and its local ring is contained in some discrete valuation ring of $K$ of degree 1. Therefore

$$\mathcal{L}_\mathbb{Q} := \left\{ (w h_1(u, v), w h_2(u, v), w h_3(u, v)) \mid u, v, w \in \mathbb{Q} \right\} = \left\{ (w h_1(u, v), w h_2(u, v), w h_3(u, v)) \mid w \in \mathbb{Q}, u, v \in \mathbb{Z} \text{ with } \gcd(u, v) = 1 \right\}$$

is exactly the set of all rational solutions of (1) except for those corresponding to points of $C_f^{\text{bad}}$, and $\mathcal{L}_f \setminus \mathcal{L}_f^{\text{bad}} = \mathcal{L}_\mathbb{Q} \cap \mathbb{Z}^3$ is just the set of all integral triples of $\mathcal{L}_\mathbb{Q}$.

We claim that there exists some $d \in \mathbb{N}$ such that for all $u, v \in \mathbb{Z}$ with $\gcd(u, v) = 1$ it follows that

$$\gcd(h_1(u, v), h_2(u, v), h_3(u, v)) \mid d.$$ 

Let $\gcd(h_1, h_2) = t \in \mathbb{Z}[U, V]$ and put $h_i = t h_i'$ with $h_i' \in \mathbb{Z}[U, V], i = 1, 2$. Since $h_1', h_2'$ are relatively prime, we obtain that $\text{Res}_V(h_1', h_2') = a U^\delta$ with some $0 \neq a \in \mathbb{Z}$ and $\delta \geq 0$, and polynomials $\rho_1, \rho_2 \in \mathbb{Z}[U, V]$ with $\rho_1 h_1 + \rho_2 h_2 = a t U^\delta$. Since $h_1, h_2, h_3$ were assumed to be relatively prime, $\gcd(at U^\alpha, h_3) = c U^\alpha$ with $c \in \mathbb{Z}$ and $0 \leq \alpha \leq \delta$. Dividing both $at U^\delta$ and $h_3$ by $c U^\alpha$ and applying the same reasoning as above we finally obtain that there are $0 \neq a_1 \in \mathbb{Z}, \delta_1 \geq 0$ and polynomials $\varphi_1, \varphi_2, \varphi_3 \in \mathbb{Z}[U, V]$ with

$$(2) \quad \varphi_1 h_1 + \varphi_2 h_2 + \varphi_3 h_3 = a_1 U^{\delta_1}.$$ 

Using $\text{Res}_U$ in the same way, we obtain polynomials $\psi_1, \psi_2, \psi_3 \in \mathbb{Z}[U, V], 0 \neq a_2 \in \mathbb{Z}$ and $\delta_2 \geq 0$ such that

$$(3) \quad \psi_1 h_1 + \psi_2 h_2 + \psi_3 h_3 = a_2 V^{\delta_2}.$$ 

For any $u, v \in \mathbb{Z}$ with $\gcd(u, v) = 1$, (2) and (3) imply that $\gcd(h_1(u, v), h_2(u, v), h_3(u, v))$ divides both $a_1 u^{\delta_1}$ and $a_2 v^{\delta_2}$. It follows that

$$\gcd(h_1(u, v), h_2(u, v), h_3(u, v)) \mid \text{lcm}(a_1, a_2) := d.$$ 

So we obtain polynomials $k_i = \frac{1}{d} h_i \in \mathbb{Q}[U, V]$ with rational coefficients such that

$$\mathcal{L}_f \setminus \mathcal{L}_f^{\text{bad}} = \left\{ (w k_1(u, v), w k_2(u, v), w k_3(u, v)) \mid u, v, w \in \mathbb{Z} \right\} \cap \mathbb{Z}^3.$$ 

Now we apply Proposition 4, which yields the assertion of Theorem 1. \hfill \Box
Remarks. If the integers \( a_1, a_2 \) appearing in (2) and (3) in the proof of Theorem 1 are both equal to 1, then \( k_i = h_i \in \mathbb{Z}[U, V] \) and \( \mathcal{L}_f \setminus \mathcal{L}_f^{\text{bad}} \) can actually be parametrized by a triple of polynomials with integral coefficients (compare Example 2 below).

When applying Proposition 4, we have no information about the number \( m \) of variables of the integer-valued polynomials \( g_i \) appearing in Theorem 1.

Example 1. This example shows that for \( n \geq 3 \) “bad” singular points may appear. Consider

\[
f = X^3 + Y^3 + X^2Z - 2Y^2Z \in \mathbb{Z}[X, Y, Z].
\]

Then \((0 : 0 : 1) \in C_f\) is a singular point. Only one discrete valuation ring lies over the local ring \( R_{(0:0:1)} \), and this valuation ring has residue class field isomorphic to \( \mathbb{Q}(\sqrt{2}) \).

A birational (projective) isomorphism between \( C_f \) and the projective line is given by

\[
(X : Y : Z) = \left((V(2U^2 - V^2)) : (U(2U^2 - V^2)) : (V^3 + U^3)\right),
\]

but there is no \( \mathbb{Q} \)-rational point \((u : v) \in \mathbb{P}^1(\mathbb{Q})\) corresponding to the singular point \((0 : 0 : 1)\). Indeed, the corresponding point \((u : v) = (1 : \sqrt{2})\) is only defined over \( \mathbb{Q}(\sqrt{2}) \).

Example 2. In contrast to the Pythagorean triples (corresponding to the unit circle, see [2]), we know that for the equilateral hyperbola the set \( \mathcal{L}_f \) can be parametrized by a single triple of polynomials with integer coefficients. Let

\[
f = XY - Z^2 \in \mathbb{Z}[X, Y, Z].
\]

All \( \mathbb{Q} \)-rational points of \( C_f \) are given by \((u^2 : v^2 : uv)\) with \((u : v) \in \mathbb{P}^1(\mathbb{Q})\). If \( u, v \in \mathbb{Z} \) with \( \gcd(u, v) = 1 \) then also \( \gcd(u^2, v^2, uv) = 1 \). So the set of all integral solutions of

\[
XY - Z^2 = 0
\]

is given by

\[
\{(u^2w, v^2w, uvw) \mid u, v, w \in \mathbb{Z}\}.
\]

References

[1] S. Frisch, Remarks on polynomial parametrization of sets of integer points, Comm. Algebra 36 (2008), 1110-1114.

[2] S. Frisch and L. Vaserstein, Parametrization of Pythagorean triples by a single triple of polynomials, J. Pure Appl. Algebra 212 (2008), 271-274.

[3] E. Kunz, Introduction to Plane Algebraic Curves, Birkhäuser, 2005.

[4] D. Poulakis and E. Voskos, Solving genus zero Diophantine equations with at most two infinite valuations, J. Symbolic Computation 33 (2002), 479-491.

[5] R.J. Walker, Algebraic Curves, Springer, 1978.