Mathematica Slovaca

Günter Lettl

Parametrized solutions of Diophantine equations

Mathematica Slovaca, Vol. 54 (2004), No. 5, 465--471

Persistent URL: http://dml.cz/dmlcz/133271

Math. Slovaca, **54** (2004), No. 5, 465–471

Mathematica Slovaca

PARAMETRIZED SOLUTIONS OF DIOPHANTINE EQUATIONS

GÜNTER LETTL

(Communicated by Stanislav Jakubec)

ABSTRACT. In 1993, E. Thomas conjectured that for certain families of Thue equations there are — up to solutions arising from finitely many polynomials over the integers $\mathbb{Z}$ — only finitely many further solutions over the integers. We give an example which shows that this conjecture cannot hold for arbitrary families of Thue equations where the coefficients are polynomials in one variable over the rational integers. Therefore we introduce the notion of $\mathbb{Z}$-parameter solutions of a family of Diophantine equations, which means a solution in algebraic functions which has infinitely many specializations to rational integers. With this revised setting, one might ask whether Thomas's conjecture holds for families of Thue equations. Using C. L. Siegel's theorem on integral points on an algebraic curve and an idea going back to E. Maillet, we prove some general results showing that $\mathbb{Z}$-parameter solutions generate very special function fields and have a very clear shape.

1. Introduction

For $n \geq 3$ let $a_1, \dots, a_n \in \mathbb{Z}[T]$ be polynomials in the variable T, put

$$F = F(X,Y) = X^n + a_1 X^{n-1} Y + \cdots + a_{n-1} X Y^{n-1} + a_n Y^n \in \mathbb{Z}[T][X,Y],$$

a normed, binary form of degree n over $\mathbb{Z}[T]$, and consider the Thue equation

$$F(X,Y) = b \tag{1}$$

with $0 \neq b \in \mathbb{Z}[T]$. Following Thomas [Tho], we call a pair of polynomials $(p,q) \in \mathbb{Z}[T] \times \mathbb{Z}[T]$ with $F(p,q) = b$ a *polynomial solution* of (1). So for any $t \in \mathbb{Z}$ the Diophantine equation

$$F(X,Y)\big|_{T:=t} = b(t) \tag{2}$$

2000 Mathematics Subject Classification: Primary 11D59, 14G05.
Keywords: Thue equation, Thomas's conjecture, Siegel's theorem, integral points.

This work was presented at the 16th Czech and Slovak International Conference on Number Theory in Bratislava, SK, June 30th – July 4th, 2003.

has the solutions $\big(p(t), q(t)\big)$, where (p, q) runs through the polynomial solutions of (1), as well as further solutions, which we will call *sporadic* ones. Thomas called a family of Thue equations given by (1) *stably solvable* if there exist only finitely many polynomial solutions and only finitely many sporadic ones at all. (Here we disregard those values of $t \in \mathbb{Z}$ for which the form $F(X,Y)\big|_{T:=t}$ becomes a power of a linear or of an indefinite quadratic form — the only cases where the Diophantine equation (2) might have infinitely many solutions in $\mathbb{Z} \times \mathbb{Z}$.)

Thomas conjectured that any family of Thue equations of the shape

$$\prod_{i=1}^{n}(X - b_i Y) \pm Y^n = 1\,, \tag{3}$$

with polynomials $b_1, \dots, b_n \in \mathbb{Z}[T]$ satisfying $b_1 = 0 < \deg b_2 < \dots < \deg b_n$, is stably solvable. In [Tho] he proves this conjecture for degree $n = 3$ (assuming for the polynomials b_2, b_3 some further supposition), and in [Heu2], [Heu3], C. Heuberger proved this conjecture for arbitrary degree $n \geq 3$ (again with some mild restrictions on the polynomials b_i). Although all one-parameter families of Thue equations which appeared since then in the literature are stably solvable (see e.g. [Heu1] for an overview of such families), the example of the next paragraph makes one realize that this is not so in general.

2. A non stably solvable family of Thue equations

It is easy to see that the Thue equation[1]

$$X^6 - (T-1)Y^6 = T^2 \tag{4}$$

is not stably solvable. Considering the degree (with respect to T) one checks immediately that (4) has no solutions in $\mathbb{Q}[T] \times \mathbb{Q}[T]$. On the other hand, we find infinitely many sporadic solutions, namely

for $T := t \in \{n^6 : n \in \mathbb{N}\}$ we have the solutions $(\pm n^3, \pm n^2)$;
for $T := t \in \{n^3 : n \in \mathbb{Z}\}$ we have the solutions $(\pm n, 0)$;
for $T := t \in \{-1 - n^6 : n \in \mathbb{N}_0\}$ we have the solutions $(\pm 1, \pm n)$;
for $T := t \in \{-n^6 - n^{12} : n \in \mathbb{N}\}$ we have the solutions $(\pm n^3, \pm n^2)$.

All these solutions arise from the following solutions of (4) in algebraic functions which belong to extension fields of the rational function field $\mathbb{Q}(T)$:

$(\pm \sqrt[2]{T}, \pm \sqrt[3]{T}\,)$ is a solution in $\mathbb{Q}(\sqrt[6]{T}\,)$;

[1]If the reader minds that the form is not irreducible for infinitely many values $T := t \in \mathbb{Z}$, (s)he may substitute T^2 for T.

$(\pm\sqrt[3]{T}, 0)$ is a solution in $\mathbb{Q}(\sqrt[3]{T})$;
$(\pm 1, \pm\sqrt[6]{-1-T})$ is a solution in $\mathbb{Q}(\sqrt[6]{-1-T})$;
$\left(\pm\sqrt[2]{\frac{1}{2}(\sqrt{1-4T}-1)}, \pm\sqrt[3]{\frac{1}{2}(\sqrt{1-4T}-1)}\right)$ is a solution in $\mathbb{Q}\left(\sqrt[6]{\frac{1}{2}(\sqrt{1-4T}-1)}\right)$.

Having once seen this example, it is easy to produce many more examples of non stably solvable families of Thue equations.

3. $\mathbb{Z}$-parameter solutions of families of Diophantine equations

Let $\overline{\mathbb{Q}(T)} \supset \mathbb{Q}(T)$ be an algebraic closure of $\mathbb{Q}(T)$ and $\overline{\mathfrak{O}} \subset \overline{\mathbb{Q}(T)}$ denote the integral closure of $\mathbb{Q}[T]$ in $\overline{\mathbb{Q}(T)}$. Let $n \in \mathbb{N}$, $T, X_1, \ldots, X_n$ be algebraically independent and

$$f = f(T, X_1, \ldots, X_n) \in \mathbb{Z}[T][X_1, \ldots, X_n]$$

be a polynomial with integral coefficients. The variable T will play the role of the parameter, and we will always assume that each of $T, X_1, \ldots, X_n$ really appears in f. Any n-tuple $(x_1, \ldots, x_n)$ with all $x_i \in \overline{\mathfrak{O}}$ and with $F(T, x_1, \ldots, x_n) = 0$ will be called a *solution* of

$$f = 0. \tag{5}$$

For any solution $(x_1, \ldots, x_n)$ of (5) we put $K = \mathbb{Q}(T)(x_1, \ldots, x_n)$, the field obtained by adjoining the components of the solution to $\mathbb{Q}(T)$.

For algebraic function fields in one variable we will use the notions and definitions as explained e.g. in the textbooks of H. Stichtenoth [St] or of M. Rosen [Ro]. Let K_0 denote the constant field of K, i.e. the field of all elements of K which are algebraic over $\mathbb{Q}$. A place P of K is the valuation ideal of a discrete valuation ring $\mathcal{O}_P$ with $K_0 \subset \mathcal{O}_P \subsetneqq K$. $\pi_P \colon \mathcal{O}_P \to \mathcal{O}_P/P$ denotes the evaluation map at the place P, and $\deg P := [\mathcal{O}_P/P : K_0]$ the degree of P. Let $\mathbb{P}_K$ denote the set of all places of K.

Definition 1. Let $(x_1, \ldots, x_n)$ be a solution of (5) and K be as above.

a) A place P of K is called a $\mathbb{Z}$*-realization* of the solution $(x_1, \ldots, x_n)$ if
$$\pi_P(T), \pi_P(x_1), \ldots, \pi_P(x_n) \in \mathbb{Z}.$$

b) The solution $(x_1, \ldots, x_n)$ is called a $\mathbb{Z}$*-parameter solution* of (5) if there exist infinitely many $\mathbb{Z}$-realizations of $(x_1, \ldots, x_n)$.

Remarks. If a place P is a $\mathbb{Z}$-realization of the solution $(x_1, \ldots, x_n)$, then $(\pi_P(x_1), \ldots, \pi_P(x_n)) \in \mathbb{Z}^n$ is a solution of the Diophantine equation $f|_{T:=\pi_P(T)} = 0$.

Since over each place $(T - t)$ of $\mathbb{Q}(T)$ with $t \in \mathbb{Z}$ there are only finitely many places of K, any $\mathbb{Z}$-parameter solution $(x_1, \dots, x_n)$ yields solutions for infinitely many Diophantine equations of the family given by (5).

Instead from $\mathbb{Z}[T]$ we could have taken the coefficients of the polynomial f from the ring of all integer-valued polynomials in $\mathbb{Q}[T]$, but this yields no essential generalization.

Considering again families of Thue equations as given by (1) we can ask whether any such family admits only finitely many $\mathbb{Z}$-parameter solutions. In case of an affirmative answer one might investigate the finiteness of the set of sporadic solutions of any family (1) with respect to this new setting.

4. Some results on $\mathbb{Z}$-parameter solutions

Our first result is a consequence of Siegel's theorem on integral points on a curve:

Proposition 1. *Let* $(x_1, \dots, x_n)$ *be a solution of* (5) *and put* $K = \mathbb{Q}(T)(x_1, \dots, x_n)$.

a) *If there exists a* $\mathbb{Z}$*-realization* $P \in \mathbb{P}_K$ *of* $(x_1, \dots, x_n)$, *then* $K/\mathbb{Q}(T)$ *is a geometric extension (i.e.,* $\mathbb{Q}$ *is algebraically closed in* K*); in particular,* $\mathcal{O}_P/P = \mathbb{Q}$.

b) *If* $(x_1, \dots, x_n)$ *is a* $\mathbb{Z}$*-parameter solution, then* K *is a rational function field over* $\mathbb{Q}$*; in particular,* K *has genus* 0.

Proof.

a) Let $P \in \mathbb{P}_K$ be a $\mathbb{Z}$-realization of $(x_1, \dots, x_n)$. Since K is generated over $\mathbb{Q}$ by $T, x_1, \dots, x_n$, the residue class field at P, $\mathcal{O}_P/P$, is generated over $\mathbb{Q}$ by $\pi_P(T), \pi_P(x_1), \dots, \pi_P(x_n)$, thus it equals $\mathbb{Q}$.

b) Looking at the proof of the theorem on primitive elements for field extensions (e.g. [Jac; p. 290]) one finds by an inductive argument that there exist $k_2, \dots, k_n \in \mathbb{Z}$ such that $z = x_1 + k_2 x_2 + \dots + k_n x_n$ generates K over $\mathbb{Q}(T)$. The minimal polynomial of z over $\mathbb{Q}(T)$ defines an affine curve over $\mathbb{Q}$ with infinitely many points in $\mathbb{Z} \times \mathbb{Z}$ (arising from the infinitely many $\mathbb{Z}$-realizations of $(x_1, \dots, x_n)$; here it is essential to have $k_i \in \mathbb{Z}$), thus by Siegel's theorem (see [Sie]) this curve, and therefore K, has genus 0. By a), there exist places of degree 1 in K, thus K is a rational function field with constant field $\mathbb{Q}$. $\square$

The next result gives a very clear description of $\mathbb{Z}$-parameter solutions as well as of the function fields K generated by them. The proof generalizes an idea going back to E. Maillet [Mai].

PROPOSITION 2. *Let $(x_1, \dots, x_n)$ be a $\mathbb{Z}$-parameter solution of (5), put $K = \mathbb{Q}(T)(x_1, \dots, x_n)$, let $\mathcal{R} \subset \mathbb{P}_K$ denote the (infinite) set of all $\mathbb{Z}$-realizations of this solution, and denote the pole of T in $\mathbb{Q}(T)$ by $\infty_0 = \left(\frac{1}{T}\right) \in \mathbb{P}_{\mathbb{Q}(T)}$.*

A. *If there exists a place $\infty \in \mathbb{P}_K$ of degree 1, lying over ∞_0, then there exists a $Z \in K$ such that $K = \mathbb{Q}(Z)$ and the following properties hold:*
   (i) *For every $P \in \mathcal{R}$ one has $\pi_P(Z) \in \mathbb{Z}$.*
   (ii) *$T, x_1, \dots, x_n \in \mathbb{Q}[Z]$.*
   (iii) *∞_0 is completely ramified in K, i.e., $e_{\infty/\infty_0} = [K : \mathbb{Q}(T)]$.*

B. *If there is no place of degree 1 in $\mathbb{P}_K$ lying over ∞_0, then there exists a $Z \in K$ such that $K = \mathbb{Q}(Z)$ and the following properties hold:*
   (i) *There exist polynomials $\varphi_0, \varphi_1, \dots, \varphi_n, q \in \mathbb{Z}[Z]$ with $\gcd(\varphi_0, \dots, \varphi_n, q) = 1$, $\deg_Z q = 2$, q irreducible in $\mathbb{Q}[Z]$ and $\operatorname{disc} q > 0$, and an $m \in \mathbb{N}$ such that*
$$T = \frac{\varphi_0}{q^m}, \; x_1 = \frac{\varphi_1}{q^m}, \; \dots, \; x_n = \frac{\varphi_n}{q^m} \qquad \textit{and} \qquad \deg_Z \varphi_0 = 2m.$$
   (ii) *Over ∞_0 there lies exactly one place $\infty \in \mathbb{P}_K$, and this has degree 2; i.e., $e_{\infty/\infty_0} = [K : \mathbb{Q}(T)]/2$ and $\deg \infty = 2$.*

P r o o f. By Proposition 1 we know already that K is a rational function field over $\mathbb{Q}$ and all places of $\mathcal{R}$ have degree 1.

A. Let $Q, \infty \in \mathbb{P}_K$ be places of degree 1 with $\infty \mid \infty_0$ and $Q \nmid \infty_0$, and choose $Z_0 \in K$ with principal divisor $(Z_0) = Q - \infty$; thus we have $K = \mathbb{Q}(Z_0)$. We can find $\varphi, \psi \in \mathbb{Z}[Z_0]$ with $\gcd(\varphi, \psi) = 1$ and $T = \varphi/\psi$. Since the pole of Z_0 lies over the pole of T, one has $d = \deg \varphi > \deg \psi = d'$. Let $c_d \in \mathbb{Z}$ be the leading coefficient of φ.

We claim that for all $P \in \mathcal{R}$ we have $c_d \pi_P(Z_0) \in \mathbb{Z}$.

Let $P \in \mathcal{R}$ and $\pi_P(Z_0) = z_1/z_2 \in \mathbb{Q}$ with $z_1, z_2 \in \mathbb{Z}$ and $\gcd(z_1, z_2) = 1$. Since the denominator of
$$\frac{z_2^{d'} \varphi\left(\frac{z_1}{z_2}\right)}{z_2^{d'} \psi\left(\frac{z_1}{z_2}\right)} = \frac{\varphi\left(\frac{z_1}{z_2}\right)}{\psi\left(\frac{z_1}{z_2}\right)} = \pi_P(T) \in \mathbb{Z}$$
is an integer, we obtain $z_2^{d'} \varphi\left(\frac{z_1}{z_2}\right) = c_d \frac{z_1^d}{z_2^{d-d'}} + \cdots \in \mathbb{Z}$, which yields $z_2 \mid c_d$ and so proves the above claim. Putting $Z = c_d Z_0$ concludes the proof of (i).

Now let $Z \in K$ satisfy (i). Then there exist $\varphi_0, \dots, \varphi_n, \psi \in \mathbb{Z}[Z]$ with $T = \varphi_0/\psi$, $x_1 = \varphi_1/\psi$, $\dots$, $x_n = \varphi_n/\psi$ and $\gcd(\varphi_0, \dots, \varphi_n, \psi) = 1$. Therefore we can find $\lambda_0, \dots, \lambda_{n+1} \in \mathbb{Z}[Z]$ and $l \in \mathbb{N}$ such that
$$\varphi_0 \lambda_0 + \cdots + \varphi_n \lambda_n + \psi \lambda_{n+1} = l. \tag{6}$$
For any $P \in \mathcal{R}$ denote $z = \pi_P(Z) \in \mathbb{Z}$. Now apply π_P to (6) to obtain
$$\psi(z)\big(\pi_P(T)\lambda_0(z) + \pi_P(x_1)\lambda_1(z) + \cdots + \pi_P(x_n)\lambda_n(z) + \lambda_{n+1}(z)\big) = l.$$

Since all factors in this expression are integers, we obtain infinitely many $z \in \mathbb{Z}$ with $\psi(z) \mid l$, therefore ψ must be constant and we deduce (ii). Since T is a polynomial in Z, (iii) follows at once.

B. Since $\mathcal{R}$ is infinite, we can choose places $Q, \infty \in \mathbb{P}_K$ of degree 1, where ∞ is no zero of T. Let $Z \in K$ with principal divisor $(Z) = Q - \infty$, so $K = \mathbb{Q}(Z)$ and $T = \widetilde{\varphi}/\widetilde{\psi}$ with $\widetilde{\varphi}, \widetilde{\psi} \in \mathbb{Z}[Z]$ and $\gcd(\widetilde{\varphi}, \widetilde{\psi}) = 1$. Since there exists no place of degree 1 over ∞_0, the pole of T, we see that ∞ is neither a zero nor a pole of T, thus $\pi_\infty(T) \in \mathbb{Q}^\times$ and we have $\deg \widetilde{\varphi} = \deg \widetilde{\psi} \geq 2$.

As above, there exist $\varphi_0, \ldots, \varphi_n, \psi \in \mathbb{Z}[Z]$ with $T = \varphi_0/\psi$, $x_1 = \varphi_1/\psi, \ldots$ $\ldots, x_n = \varphi_n/\psi$, $\gcd(\varphi_0, \ldots, \varphi_n, \psi) = 1$, and furthermore from $T = \widetilde{\varphi}/\widetilde{\psi} = \varphi_0/\psi$ we obtain $\deg \varphi_0 = \deg \psi = d \geq 2$. Again we can find $\lambda_0, \ldots, \lambda_{n+1} \in \mathbb{Z}[Z]$ and $l \in \mathbb{N}$ satisfying (6).

Let $\psi = c_d Z^d + \cdots + c_1 Z + c_0$ with $c_0, \ldots, c_d \in \mathbb{Z}$, put $\psi_0(Z_1, Z_2) = Z_2^d\, \psi\big(\frac{Z_1}{Z_2}\big)$ the homogenization of ψ, define $d' = \max\{\deg \lambda_i \,:\, 0 \leq i \leq n+1\}$ and put $D := d + d' \geq 2$. For any $P \in \mathcal{R}$ let $\pi_P(Z) = z_1/z_2 \in \mathbb{Q}$ with $z_1, z_2 \in \mathbb{Z}$ and $\gcd(z_1, z_2) = 1$.

We claim that

$$\psi_0(z_1, z_2) \mid l\, c_d^D\,. \tag{7}$$

Applying π_P to (6) and multiplying with z_2^D we obtain

$$\psi_0(z_1, z_2)\Big(\pi_P(T) \cdot z_2^{d'} \lambda_0\big(\tfrac{z_1}{z_2}\big) + \pi_P(x_1) \cdot z_2^{d'} \lambda_1\big(\tfrac{z_1}{z_2}\big) + \ldots$$
$$\cdots + \pi_P(x_n) \cdot z_2^{d'} \lambda_n\big(\tfrac{z_1}{z_2}\big) + z_2^{d'} \lambda_{n+1}\big(\tfrac{z_1}{z_2}\big)\Big) = l\, z_2^D,$$

from which we conclude that

$$a := \psi_0(z_1, z_2) = c_d z_1^d + \cdots + c_0 z_2^d \mid l\, z_2^D\,.$$

For any rational prime $p \in \mathbb{P}$ let $v_p(m)$ denote the exact power of p dividing $m \in \mathbb{Z} \setminus \{0\}$. If $v_p(z_2) \leq v_p(c_d)$, we have $v_p(a) \leq v_p(l\, z_2^D) \leq v_p(l\, c_d^D)$, and if $v_p(z_2) > v_p(c_d)$, we get $v_p(a) = v_p(c_d) \leq v_p(l\, c_d^D)$, which proves (7).

Since $\mathcal{R}$ is infinite we obtain infinitely many $(z_1, z_2) \in \mathbb{Z} \times \mathbb{Z}$ with $\psi_0(z_1, z_2) \mid l\, c_d^D$, so some divisor of $l\, c_d^D$ is represented infinitely often by the binary form ψ_0. By Thue's theorem, ψ_0 must be the power of a linear or of an irreducible indefinite quadratic form from $\mathbb{Q}[Z_1, Z_2]$. The former would yield a place of K over ∞_0 of degree 1, therefore the latter must hold, concluding the proof of (i).

From $T = \varphi_0/q^m$ and $\deg \varphi_0 = 2m$ we see that $(q) \in \mathbb{P}_K$ is the only place of K lying above ∞_0, thus also (ii) is proved. □

REFERENCES

[Heu1] HEUBERGER, C.: *On general families of parametrized Thue equations.* In: Algebraic Number Theory and Diophantine Analysis, Proceedings of the Internat. Conf. in Graz 1998 (F. Halter-Koch, R. F. Tichy, eds.), Walter de Gruyter, Berlin, 2000, pp. 215–238.

[Heu2] HEUBERGER, C.: *On a conjecture of E. Thomas concerning parametrized Thue equations*, Acta Arith. **98** (2001), 375–394.

[Heu3] HEUBERGER, C.: *On explicit bounds for the solutions of a class of parametrized Thue equations of arbitrary degree*, Monatsh. Math. **132** (2001), 325–339.

[Jac] JACOBSON, N.: *Basic Algebra I*, W. H. Freeman and Co, New York, 1985.

[Mai] MAILLET, E.: *Détermination des points entiers des courbes algébriques unicursales à coefficients entiers*, Comptes Rendus Paris **168** (1919), 217–220.

[Ro] ROSEN, M.: *Number Theory in Function Fields.* Grad. Texts in Math. 210, Springer Verlag, New York, 2002.

[Sie] SIEGEL, C. L.: *Über einige Anwendungen diophantischer Approximationen*, Abh. Preuss. Akad. Wiss., Phys.-Math. Kl. **1** (1929).

[St] STICHTENOTH, H.: *Algebraic Function Fields and Codes*, Springer Verlag, Berlin, 1993.

[Tho] THOMAS, E.: *Solutions to certain families of Thue equations*, J. Number Theory **43** (1993), 319–369.

Received November 12, 2003

Institut für Mathematik
Karl-Franzens-Universität
Heinrichstraße 36
A–8010 Graz
AUSTRIA
E-mail: guenter.lettl@uni-graz.at