On equal values of binary forms over finitely generated fields

By B. BRINDZA[1] (Debrecen) and Á. PINTÉR[2] (Debrecen)

As it was pointed out by Lang [4, p. 245] and others, certain finiteness results for diophantine equations over algebraic number fields can be extended, by using deep algebraic geometrical arguments, to rather general cases when the ground domain of unknowns is a finitely generated field or a finitely generated subring of it.

The purpose of this paper is to establish a surprisingly elementary method, through a concrete equation, to obtain these kind of general results.

Let $f(X,Y)$ and $g(X,Y)$ be binary forms (homogeneous polynomials in two variables) with complex coefficients of degree m and n, respectively. The binary form fg splits into linear factors (over $\mathbb{C}$) and in the sequel, we suppose that the linear factors are pairwise non-proportional. Let K be a finitely generated subfield of $\mathbb{C}$. Then K can be written in the form $\mathbb{Q}(z_1, \ldots, z_q, u)$, where $z_1, \ldots, z_q$ is a transcendence basis of K and we may assume without loss of generality that the element u is integral over the polynomial ring $\mathbb{Z}[z_1, \ldots, z_q]$.

Theorem. *If $n \geq 1$ and $m - n \geq 5$ then the equation*

$$f(x,y) = g(x,y) \tag{1}$$

in $x, y \in K$ has only finitely many solutions.

In other words, on the curve $f - g = 0$ there are only finitely many points of $K \times K$. Deeper reasons of the technical assumption $m - n \geq 5$

are related to the genus of the curve and the approximation properties of the solutions. Similar theorems can also be proved for other polynomial equations, e.g. for Thue or superelliptic equations.

Unfortunately, there seems to be no way to make the above Davenport-Roth-type theorem effective. In the algebraic number field case, when x and y are S-integers in a given number field, similar and effective results were proved by EVERTSE, GYŐRY, SHOREY and TIJDEMAN [1]. A more general, however ineffective result was given in [6]. For further references we refer to the book of SHOREY and TIJDEMAN [8, Chapter 7]. We remark that an effective method for a large class of diophantine equations over finitely generated integral domain was developed by GYŐRY [3].

Auxiliary results

Let R be an integral domain with divisor theory and let G be the quotient field of R. Denote by M_G the set of (additive) valuations of G with value group $\mathbb{Z}$, further let S be a finite set of M_G. An element $\alpha \in G$ is said to be S-integral if $v(\alpha) \geq 0$ for all $v \in M_G \backslash S$. These elements form a ring, denoted by $\mathcal{O}_{G,S}$, and the units of $\mathcal{O}_{G,S}$ are called S-units. Moreover, let $f, g \in G[X, Y]$ be binary forms of degree m, n, respectively. To avoid technical difficulties we assume that these forms split into linear factors over G. For otherwise, the whole argument can be repeated in the splitting field of fg. Furthermore, we suppose that the linear factors of fg are non-proportional.

Write

$$f(X, Y) = f_0(X - \alpha_1 Y) \cdots (X - \alpha_m Y),$$
$$g(X, Y) = g_0(X - \beta_1 Y) \cdots (X - \beta_n Y)$$

and let T be the set of the elements $\alpha_i - \alpha_j$ ($1 \leq i < j \leq m$), $\beta_i - \beta_j$ ($1 \leq i \leq n$), f_0, g_0 and $\alpha_i - \beta_j$ ($1 \leq i \leq m, 1 \leq j \leq n$).

The following simple lemma plays a crucial rôle in the proofs of further preliminaries.

Lemma 1. *Let v be an additive valuation on G such that $v(\alpha) = 0$ for every $\alpha \in T$. Moreover, let $(x, y) \in G^2$ be a solution to the equation*

$$f(x, y) = g(x, y) \quad with \quad xy \neq 0.$$

If $m > n \geq 1$, then $v\left(\frac{x - \alpha_1 y}{x - \alpha_2 y}\right)$ is divisible by $m - n$.

PROOF. Since the degree of f and g are not equal, we certainly have two factors, say $x - \gamma y$ and $x - \delta y$, $\gamma, \delta \in \{\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n\}$ with

$$v(x - \gamma y) > v(x - \delta y).$$

For an arbitrary factor $x - \varepsilon y$ distinct from $x - \gamma y$, simple properties of valuations and the Siegel-identity

$$x - \varepsilon y = \frac{\varepsilon - \delta}{\gamma - \delta}(x - \gamma y) + \frac{\gamma - \varepsilon}{\gamma - \delta}(x - \delta y)$$

yield

(3) $$v(x - \varepsilon y) = v(x - \delta y).$$

Omitting the trivial case $v(x - \alpha_1 y) = v(x - \alpha_2 y)$ we may assume that $v(x - \alpha_1 y) > v(x - \alpha_2 y)$. One can see by using (3) that the inequalities $0 > v(x - \alpha_1 y)$, $v(x - \alpha_2 y) > 0$ and $m > n$ lead to contradiction.

In the remaining case $v(x - \alpha_1 y) \geq 0$, $v(x - \alpha_2 y) < 0$ and we obtain

$$v\left(\frac{x - \alpha_1 y}{x - \alpha_2 y}\right) = v(x - \alpha_1 y) - v(x - \alpha_2 y) = (n - m)v(x - \alpha_2 y),$$

therefore, Lemma 1 is proved.

The function field case

Using the notation of Lemma 1 let, specially G be an algebraic function field with genus $\mathcal{G}$ over an algebraically closed field k of characteristic zero, that is G is a finite algebraic extension of the rational function field $k(z)$. The valuation theory on G is given by the extensions of the valuations on $k(z)$. In the sequel, we assume that the set S contains all the *infinite* valuations of G. The additive height of a non-zero element α of G is defined by

$$H_G(\alpha) = - \sum_{v \in M_G} \min\{0, v(\alpha)\}.$$

By using the well-known "sum-formula" one can rewrite the above relation as

$$H_G(\alpha) = \sum_{v \in M_G} \max\{0, v(\alpha)\},$$

that is the number of valuations for which $v(\alpha) \neq 0$ is at most $2H_G(\alpha)$. The inequality

(4) $$\max\{H_G(\alpha\beta), H_G(\alpha + \beta)\} \leq H_G(\alpha) + H_G(\beta) \quad (\alpha, \beta \in G)$$

is an immediate consequence of the definition. The height of a polynomial $P(X) = a(X - x_1) \cdots (X - x_k)$ with $a, x_1, \ldots, x_k \in G$ is defined by $H(P) = H_G(a) + \sum_{i=1}^{k} H_G(x_i)$.

An additive relation between S-units implies an upper bound for the height of these elements:

Lemma 2 (Mason [5]). *Let γ_1, γ_2 be S-units in G such that $\gamma_1+\gamma_2=1$. Then*

$$H_G(\gamma_1) \leq |S| + 2\mathcal{G} - 2.$$

($|S|$ denotes the cardinality of the set S.)

A similar result had been proved by GYŐRY [3] with larger constants. His proof is based on Schmidt's theorem on Thue equations over function fields ([7]).

Lemma 3. *Let $m - n \geq 5$ and $n \geq 1$. Then all the solutions of the equation*

(5) $$f(x, y) = g(x, y) \quad in \quad x, y \in G$$

satisfy

$$\max\{H_G(x), H_G(y)\}$$
$$\leq (m + n)(2\mathcal{G} - 2) + (m + n)(2n + 2m + 1)\{H(f) + H(g)\}.$$

The constants certainly can be improved, however from the viewpoint of the Theorem it makes no difference.

PROOF. We may assume that $xy \neq 0$, for otherwise the lemma can trivially be proved. Let $(x, y) \in G^2$ be an arbitrary but fixed non-zero solution to (5). Let S_1 denote the set of valuations v on G such that $v(\alpha) \neq 0$ for some $\alpha \in T$. An easy calculation gives

$$|S_1| \leq 2(n + m - 1)(H(f) + H(g)).$$

Let k_1, k_2, l_1, l_2 be the cardinalities of the sets of valuations $v \in M_G \backslash S_1$ for which $v\left(\frac{x-\alpha_2 y}{x-\alpha_1 y}\right) > 0, v\left(\frac{x-\alpha_2 y}{x-\alpha_1 y}\right) < 0, v\left(\frac{x-\alpha_3 y}{x-\alpha_1 y}\right) > 0, v\left(\frac{x-\alpha_3 y}{x-\alpha_1 y}\right) < 0$, respectively. Applying Lemmas 1, 2 to the identity

$$\frac{\alpha_1 - \alpha_3}{\alpha_2 - \alpha_3} \frac{x - \alpha_2 y}{x - \alpha_1 y} + \frac{\alpha_2 - \alpha_1}{\alpha_2 - \alpha_3} \frac{x - \alpha_3 y}{x - \alpha_1 y} = 1$$

we obtain that both $(k_1 + k_2)(m - n)$ and $(l_1 + l_2)(m - n)$ are bounded by

$$2H_G\left(\frac{x - \alpha_2 y}{x - \alpha_1 y}\right) \leq 2|S_1| + 2(k_1 + k_2 + l_1 + l_2) + 4\mathcal{G} - 4 + 4H(f).$$

This relation yields

$$k_1 + k_2 + l_1 + l_2 \leq 4|S_1| + 8\mathcal{G} - 8 + 8H(f)$$

and

$$H_G\left(\frac{x - \alpha_2 y}{x - \alpha_1 y}\right) \leq 5|S_1| + 10\mathcal{G} - 10 + 10H(f).$$

The inequality (4) implies

$$H_G(x/y) \le 5|S_1| + 10\mathcal{G} - 10 + 12H(f),$$

and

$$5H_G(y) \le (m-n)H_G(y) \le H_G(f(x/y, 1)) + H_G(g(x/y, 1))$$
$$\le (m+n)H_G(x/y) + H(f) + H(g)$$
$$\le 5(m+n)\{|S_1| + 2\mathcal{G} - 2\} + \{12(m+n) + 1\}H(f) + H(g).$$

Finally, a calculation completes the proof of Lemma 3.

The number field case

In this paragraph let G (see the preparation of Lemma 1) be an algebraic number field, that is a finite extension of the field of rationals. In this case the finite valuations on G are given by the prime ideals of the ring of integers of G. For an arbitrary but fixed solution $(x, y) \in G^2$ of the equation

(6) $$f(x, y) = g(x, y)$$

the fractional ideal generated by $\frac{x - \alpha_1 y}{x - \alpha_2 y}$ can be written in the form

$$\mathfrak{M}\mathfrak{P}_1^{(m-n)k_1} \cdots \mathfrak{P}_t^{(m-n)k_t},$$

where the fractional ideal $\mathfrak{M}$ belongs to a finite set (independent of x and y), $\mathfrak{P}_1, \ldots, \mathfrak{P}_t$ are distinct prime ideals ($t \ge 0$) and the exponents $k_1, \ldots, k_t$ are rational integers. By taking fixed representatives from every ideal class of G we can rewrite the above principal ideal as

$$\mathfrak{R}^{m-n}\mathfrak{M}\left(\frac{(\mathfrak{P}_1\mathfrak{Q}_1)^{k_1} \cdots (\mathfrak{P}_t\mathfrak{Q}_t)^{k_t}}{\mathfrak{R}} \mathfrak{Q}_1^{k_t} \cdots \mathfrak{Q}_t^{k_t}\right)^{m-n},$$

where $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_t$ and $\mathfrak{R}$ belong to the inverse ideal class of $\mathfrak{P}_1, \ldots, \mathfrak{P}_t$ and $\mathfrak{Q}_1^{k_1} \cdots \mathfrak{Q}_t^{k_t}$, respectively. Since the unit group of G is finitely generated, this sophisticated form shows that the element $\frac{x - \alpha_1 y}{x - \alpha_2 y}$ can be written as uz^{m-n} where $u, z \in G$ and u can be choosen from a finite set (independent of x and y) given by the generators of the ideals $\mathfrak{R}^{m-n}\mathfrak{M}$. Therefore, the Siegel-identity for the factors $x - \alpha_1 y$, $x - \alpha_2 y$, $x - \alpha_3 y$ lead to finitely many Fermat-curves of degree $m - n$, and by using Faltings' result on Mordell-conjecture (see [2]) we have

Lemma 4. *If $n \ge 1$ and $m - n \ge 4$ then the equation (5) in $(x, y) \in G^2$ has only finitely many solutions.*

Proof of the Theorem

We may suppose that $q > 0$, for otherwise our theorem is a consequence of Lemma 4. Following the notation and concepts of GYŐRY [3] let

$$k_i = \mathbb{Q}(z_1, \ldots, z_{i-1}, z_{i+1}, \ldots, z_q)$$

for an arbitrary but fixed index i with $1 \leq i \leq q$. Further, let $\overline{k}_i$ denote its algebraic closure (in a fixed algebraic closure of K). Moreover, for simplicity we write z for z_i. If ω is an element of the polynomial ring $\mathbb{Q}[z_1, \ldots, z_q]$ then we denote by ω^* the element of $k_i[z]$ obtained from ω by the substitution $z_i \mapsto z$. Let

$$F(X) = X^\delta + F_1 X^{\delta-1} + \cdots + F_\delta$$

be the minimal polynomial of u with discriminant D_F and let $u^{(1)} = u, \ldots, u^{(\delta)}$ be the conjugates of u over $\mathbb{Q}(z_1, \ldots, z_q)$. Set $M_i = \overline{k}_i(z)(u^{(1)}, \ldots, u^{(\delta)})$ and $\Delta_i = [M_i : \overline{k}_i(z)]$ and denote by $\mathcal{G}(M_i)$ the genus of $M_i/\overline{k}_i$. Then $\Delta_i \leq \delta!$ and $u^{(1)}, \ldots, u^{(\delta)}$ are integral over $\overline{k}_i[z]$. We write $\alpha \in K$ in the form

$$\alpha = \frac{P_{\alpha,0} + P_{\alpha,1}u + \cdots + P_{\alpha,\delta-1}u^{\delta-1}}{Q_\alpha},$$

where the polynomials $P_{\alpha,0}, \ldots, P_{\alpha,\delta-1}, Q_\alpha \in \mathbb{Z}[z_1, \ldots, z_q]$ are relatively prime and uniquely determined (up to sign). The *Degree* of α (with respect to the generating set $\{z_1, \ldots, z_q, u\}$) is defined by

$$\mathrm{Deg}(\alpha) = \max\{\mathrm{Deg}(P_{\alpha,0}), \ldots, \mathrm{Deg}(P_{\alpha,\delta-1}), \mathrm{Deg}(Q_\alpha)\}.$$

Set

$$\alpha^{(j)} = \frac{P_{\alpha,0}^* + P_{\alpha,1}^* u^{(j)} + \cdots + P_{\alpha,\delta-1}^* (u^{(j)})^{\delta-1}}{Q_\alpha^*}$$

for $j = 1, \ldots, \delta$. Then $\alpha^{(1)}, \ldots, \alpha^{(\delta)} \in M_i$ and the Degree of α with respect to the generating set $\{z_1, \ldots, z_q, u\}$ is equal to the Degree of $\alpha^{(j)}$ with respect to the generating set $\{z_1, \ldots, z_q, u^{(j)}\}$ of the conjugate field $\mathbb{Q}(z_1, \ldots z_q, u^{(j)})$.

Let $(x, y) \in K^2$ be an arbitrary but fixed solution to the equation (1). Then

$$f_0^{(l)} \prod_{i=1}^m (x^{(l)} - \alpha_i^{(l)} y^{(l)}) = g_0^{(l)} \prod_{j=1}^n (x^{(l)} - \beta_j^{(l)} y^{(l)}), \quad 1 \leq l \leq \delta,$$

and by Lemma 3 we obtain

$$\text{(7)} \qquad \max_{1 \le l \le \delta} \{H_{M_i}(x^{(l)}), \, H_{M_i}(y^{(l)})\} < c_1.$$

The relations

$$x^{(l)} = \frac{P^*_{x,0}}{Q^*_x} + \frac{P^*_{x,1}}{Q^*_x} u^{(l)} + \cdots + \frac{P^*_{x,\delta-1}}{Q^*_x}(u^{(l)})^{\delta-1}, \quad (1 \le l \le \delta),$$

can be considered as a linear system of equations in unknowns $\frac{P^*_{x,0}}{Q^*_x}, \ldots,$ $\frac{P^*_{x,\delta-1}}{Q^*_x}$ and Cramer's rule with (7) imply

$$\max_{0 \le l \le \delta-1} \{H_{M_i}\left(\frac{P^*_{x,l}}{Q^*_x}\right)\} < c_2.$$

Let V_i be the set of finite valuations of $M_i/\overline{k_i}$ for which $v(Q^*_x) \ne 0$ and $v(P^*_{x,i}) = 0$, $i = 0, \ldots, \delta-1$. Since the polynomials $P^*_{x,0}, \ldots, P^*_{x,\delta-1}, Q^*_x$ are relatively prime over $k_i[z]$ we have

$$\bigcup_{i=0}^{\delta-1} V_i = \{v \in M_G : v(Q^*_x) > 0\}.$$

Hence, inequality (7) and the sum-formula yield

$$\deg_{z_i} Q_x = \deg_z Q^*_x = \Delta_i^{-1} H_{M_i}(Q^*_x) = \Delta_i^{-1} \sum_{v(Q^*_x)>0} v(Q^*_x)$$

$$= \Delta_i^{-1} \sum_{i=0}^{\delta-1} \sum_{v \in V_i} v(Q^*_x) = \Delta_i^{-1} \sum_{i=0}^{\delta-1} \sum_{v \in V_i} v\left(\frac{Q^*_x}{P^*_{x,i}}\right) \le \Delta_i^{-1} \delta H_{M_i}\left(\frac{Q^*_x}{P^*_{x,i}}\right)$$

$$= \Delta_i^{-1} \delta H_{M_i}\left(\frac{P^*_{x,i}}{Q^*_x}\right) < \Delta_i^{-1} \delta c_2 = c_3.$$

Let d be a positive integer and $P \in \mathbb{Z}[z_1, \ldots, z_q]$ be a polynomial of degree less than d in each z_j. Then the polynomial

$$\Phi_P(t) = P(t, t^d, \ldots, t^{d^{q-1}})$$

(obtained by Kronecker's substitution) has the same set of non-zero co-efficients as P and $\deg \Phi_P(t) \le d^q - 1$. If $Q \in \mathbb{Z}[z_1, \ldots, z_q]$ is another polynomial with $\deg_{z_j} Q < d$ and $\deg_{z_j} PQ < d$ for every j, then $\Phi_{P+Q} = \Phi_P + \Phi_Q$ and $\Phi_{PQ} = \Phi_P \cdot \Phi_Q$. At this stage we note that the above part of our proof is kept from GYŐRY [3].

Put
$$X = \{x : (x, y) \in K^2 \quad \text{and} \quad f(x, y) = g(x, y)\}.$$

By taking $d > \max\{c_3, \text{Deg}(D_F)\}$, we have $\deg(\Phi_{D_F} \cdot \Phi_{Q_x}) < 2d^q$ for every $x \in X$. Let $\mathcal{M}$ denote the set of subsets of $(\mathbb{Z} \cap [-2d^q, 2d^q]) \setminus \{0\}$ with cardinality less than $2d^q$ (including the empty set). Moreover, for an $M \in \mathcal{M}$, let X_M be the subset of X satisfying that the set of the rational integer zeros of $\Phi_{D_F} \cdot \Phi_{Q_x}$ in $(\mathbb{Z} \cap [-2d^q, 2d^q]) \setminus \{0\}$ is M for every $x \in X_M$. Then obviously
$$X = \bigcup_{M \in \mathcal{M}} X_M.$$

In the sequel, we fix M and prove that X_M is finite. For a $t_0 \in \overline{M} = (\mathbb{Z} \cap [-2d^q, 2d^q]) \setminus (\{0\} \cup M)$ let $U_1, \ldots, U_\delta (\in \mathbb{C})$ be the zeros of the polynomial
$$F_{t_0}(X) = X^\delta + \Phi_{F_1}(t_0) X^{\delta-1} + \cdots + \Phi_{F_\delta}(t_0) \in \mathbb{Z}[X].$$

Since $\Phi_{D_F}(t_0) \neq 0$, the zeros of $F_{t_0}(X)$ are pairwise distinct. The substitutions
$$z_1 \mapsto t, \ldots z_q \mapsto t^{d^{q-1}}, \quad u \mapsto U_k \ (1 \leq k \leq \delta)$$

define homomorphisms of the field K into the algebraic number field $M_{t_0} = \mathbb{Q}(U_1, \ldots, U_\delta)$. The image of $\alpha \in K$ under this mapping is
$$\Phi_\alpha(t_0, k) = \frac{\Phi_{P_{\alpha,0}}(t_0) + \cdots + \Phi_{P_{\alpha,\delta-1}}(t_0) U_k^{\delta-1}}{\Phi_{Q_\alpha}(t_0)}, \quad (1 \leq k \leq \delta).$$

From our equation and Lemma 4 we get
$$\Phi_{f_0}(t_0, k) \prod_{i=1}^{m} (\Phi_x(t_0, k) - \Phi_{\alpha_i}(t_0, k) \Phi_y(t_0, k))$$
$$= \Phi_{g_0}(t_0, k) \prod_{j=1}^{n} (\Phi_x(t_0, k) - \Phi_{\beta_j}(t_0, k) \Phi_y(t_0, k)),$$

and the elements $\Phi_x(t_0, k)$ belong to a finite set for all $1 \leq k \leq \delta$. Using the non-vanishing Vandermonde-type matrix (U_k^j) in Cramer's rule we obtain that the δ-tuples
$$\left(\frac{\Phi_{P_{x,0}}(t_0)}{\Phi_{Q_x}(t_0)}, \ldots, \frac{\Phi_{P_{x,\delta-1}}(t_0)}{\Phi_{Q_x}(t_0)} \right)$$

also form a finite set for every $t_0 \in \overline{M}$.

If the cardinality of X_M is infinite then there are $x_1 \neq x_2$ such that

$$\frac{\Phi_{P_{x_1,i}}(t_0)}{\Phi_{Q_{x_1}}(t_0)} = \frac{\Phi_{P_{x_2,i}}(t_0)}{\Phi_{Q_{x_2}}(t_0)} \quad (0 \leq i \leq \delta - 1)$$

for every $t_0 \in \overline{M}$. Since $|\overline{M}| > 2d^q$, the rational functions

$$\frac{\Phi_{P_{x_1,i}}(t)}{\Phi_{Q_{x_1}}(t)} \quad \text{and} \quad \frac{\Phi_{P_{x_2,i}}(t)}{\Phi_{Q_{x_2}}(t)}$$

are identically equal in t, for $0 \leq i \leq \delta - 1$. Finally, we have

$$\frac{P_{x_1,i}(z_1, \ldots, z_q)}{Q_{x_1}(z_1, \ldots, z_q)} = \frac{P_{x_2,i}(z_1, \ldots, z_q)}{Q_{x_2}(z_1, \ldots, z_q)}, \quad (0 \leq i \leq \delta - 1)$$

therefore, $x_1 = x_2$. The finiteness of the sets X_M and $\mathcal{M}$ complete the proof of the theorem.

References

[1] J. H. Evertse, K. Győry, T. N. Shorey and R. Tijdeman, Equal values of binary forms at integral points, *Acta Arith.* **48** (1987), 379–396.
[2] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* **73** (1983), 349–366.
[3] K. Győry, Bounds for the solutions of norm form discriminant form and index form equations in finitely generated domains, *Acta Math. Hungar.* **42** (1983), 45–80.
[4] S. Lang, Fundamentals of Diophantine Geometry, *Springer Verlag*, 1983.
[5] R. C. Mason, Diophantine Equations over Function Fields, LMS Lecture Notes No. 96, *Cambridge University Press*, 1984.
[6] A. Schinzel, An improvement of Runge's theorem on diophantine equations, *Comment. Pontific. Acad. Sci.* **2** no. 20 (1969), 9.
[7] W. M. Schmidt, Thue's equation over function fields, *J. Austral. Math. Soc.* A **25** (1978), 385–422.
[8] T. N. Shorey and R. Tijdeman, Exponential diophantine equations Cambridge tracts in mathematics, vol. 87, *Cambridge University Press*, 1986.

B. BRINDZA AND Á. PINTÉR
MATHEMATICAL INSTITUTE
KOSSUTH LAJOS UNIVERSITY
H–4010 DEBRECEN
P.O.BOX 12
HUNGARY