COMPOSITIO MATHEMATICA

JULIA MUELLER

Binomial Thue's equation over function fields

Compositio Mathematica, tome 73, n° 2 (1990), p. 189-197
<http://www.numdam.org/item?id=CM_1990__73_2_189_0>

Compositio Mathematica **73**: 189–197, 1990.

Binomial Thue's equation over function fields*

JULIA MUELLER
Fordham University, Department of Mathematics, Bronx, NY 10458, U.S.A.

Received 12 December 1988; accepted in revised form 21 June 1989

I. Introduction

Let $F(x, y)$ be a binary form of degree $r \geqslant 3$ with rational integral coefficients which is irreducible over the field of rational numbers and which has not more than $s + 1$ monomials. The problem of providing upper bounds for the number of solutions of the classical Thue equation.

$$F(x, y) = h, \tag{1.1}$$

where h is a rational integer, has a long history, but a great deal of significant work has been done in very recent years. We refer the readers to works of Evertse [4], Bombieri and Schmidt [1], and Mueller and Schmidt [12]. One expects that (1.1) has very few solutions. Siegel [13] conjectured in 1929 that the number of integral solutions of (1.1) may be bounded in terms of s only. A modified version of this conjecture (i.e., a bound depending on s and h only) has recently been proved by Mueller and Schmidt [12]. Actually, Siegel's conjecture was intended for diophantine equations in general, where the curve defined by the equation $G(x, y) = 0$ is irreducible and of positive genus. But even in the case of cubic Thue equations, the dependency of the bound on h cannot be avoided (see [12]).

Prior to the work of [12], this modified version of Siegel's conjecture for binomial forms $F = ax^r - by^r$ was proved in different ways by Domar [3], Hyyrö [7], Evertse [5], and then by Mueller [10]. Domar [3] was the first to show that $|ax^r - by^r| = 1$ with $a > 0$, $b > 0$ and $r \geqslant 5$ has at most two integral solutions up to sign. The case $s = 2$, i.e., the case of trinomial forms F, was settled by the present author and Schmidt [11].

Let k be an algebraically closed field of characteristic zero, and let K/k be a function field of genus g. Given nonzero elements a and b of K, we are interested in the equation

$$a\xi^r + b\eta^r = c, \tag{1.2}$$

*Supported in part by NSF grant DMS-8808398.

where c is a nonzero element in K. We call (1.2) *a binomial Thue's equation in* K. We are seeking solutions of (1.2) with $\xi \neq 0$, $\eta \neq 0$.

Writing $x = \xi^r$ and $y = \eta^r$, the above equation becomes

$$ax + by = c, \tag{1.3}$$

and we seek solutions (x, y) in $K^{*r} \times K^{*r}$. Here K^{*r}, $r \geqslant 1$ denotes the group of rth powers of nonzero elements in K.

Our object is to show that (1.3) cannot have more than two solutions when either $a/c \notin K^{*r}$ or $b/c \notin K^{*r}$, and r is sufficiently large. In terms of Siegel's conjecture, this verifies the conjecture for binomial Thue equations over function fields, in the much stronger form that we deal with all solutions in K and not just integral solutions.

MAIN THEOREM. *Let k be an algebraically closed field of characteristic 0 and let K/k be a function field of genus g. Suppose $r > 30 + 20g$ and either $a/c \notin K^{*r}$ or $b/c \notin K^{*r}$, then* (1.3) *has at most two solutions in* $K^{*r} \times K^{*r}$.

We remark first that when $a/c = b/c = 1$ in (1.2), the equation

$$\xi^r + \eta^r = 1 \tag{1.4}$$

has infinitely many *trivial* solutions, i.e., solutions (ξ, η) in $K^* \times K^*$ with $\xi^r \in k$ and $\eta^r \in k$. This is because the equation $x + y = 1$ has infinitely many solutions (x, y) in $k \times k$ and since k is algebraically closed, $k \subset K^r$. Therefore, there exist (ξ, η) in $K^* \times K^*$ with $x = \xi^r$ and $y = \eta^r$.

Our second remark is that when both a/c and $b/c \in K^{*r}$, (1.2) has infinitely many solutions in $K^* \times K^*$. In fact, (1.2) has infinitely many solutions induced by the trivial solutions of (1.4), i.e., induced by the one-one map $(\xi, \eta) \mapsto (\alpha^{-1}\xi, \beta^{-1}\eta)$, where α and β are elements of K such that $\alpha^r = a/c$ and $\beta^r = b/c$.

Finally we remark the bound 2 is best possible in the sense that for every positive integer r there are a, b, c such that (1.3) has two solutions; it suffices to solve the two linear equations for a, b, c which arise in correspondence of two distinct solutions.

The proof of the Main Theorem involves a fundamental inequality (see (3.1) below) which is analogous to the celebrated *abc*-conjecture in function fields. This inequality was first introduced by Mason [8], [9], but the version stated in (3.1) is due to Brownawell and Masser [2].

Our method is to assume that (1.3) has three distinct solutions and then to derive a contradiction by using this inequality when the degree r is appropriately large. This way of counting solutions of binomial Thue equations appears to be new and is related to the method of Evertse, Győry, Stewart and Tijdeman [6] on S-unit equations. In this paper our main concern is to present this new method, therefore we have not tried to obtain the best possible results. For example, it is very likely that one could improve the constant $30 + 20g$ ($g \geqslant 0$) in the Theorem substantially.

I am indebted to Professor Enrico Bombieri for introducing this problem to me and for his generous encouragement. I wish also to thank the referee for suggesting a simplification of the arguments in section three, which led to better bounds in our results.

II. Preliminaries

Let $W = \{w_1, \ldots, w_n\}$ be a non-empty set of elements of K^*. The height of W is defined to be

$$H(W) = -\sum_v v(W) \tag{2.1}$$

where $v(W) = \min(v(w_1), \ldots, v(w_n))$ and v runs through the valuations $\mathcal{M}_K$ of K/k with the rational integers as its value group. Let us first state some simple properties of $H(W)$ which can be derived easily from (2.1) and the sum formula $\sum_v v(W) = 0$.

We have

$$H(W) \geqslant 0, \tag{2.2}$$

$$H(W') \leqslant H(W) \quad \text{if } W' \subset W, \tag{2.3}$$

and

$$H(uW) = H(W) \tag{2.4}$$

where u is an element in K^* and $uW = \{uw_1, \ldots, uw_n\}$.

DEFINITION. Two elements w and w' in K^* are said to be *proportional* and we write $w \sim w'$ if $w/w' \in k$. We remark that $w \sim w'$ if and only if w and w' are linearly dependent over k.

DEFINITION. Let W be a set containing at least three elements of K^*. We say W is *non-degenerate* if W has no proper subset whose elements are linearly dependent over k. We say W is *minimal non-degenerate* if W is non-degenerate and if the elements of W are linearly dependent over k.

LEMMA 1. *Let $n \geqslant 2$ and let $W = \{w_1, \ldots, w_n\}$ be a set of elements of K^*. Then $H(W) = 0$ if and only if the elements of W are pairwise proportional.*

Proof. We remark first that the elements of W are pairwise proportional if and only if

$$v(w_1) = \cdots = v(w_n), \quad \forall v \in \mathcal{M}_K. \tag{2.5}$$

But (2.5) implies $H(W) = -\sum_v v(w_i) = 0$. Conversely, if $H(W) = 0$, then $\sum_v v(w_i) - H(W) = \sum_v (v(w_i) - v(W)) = 0$. Hence $v(w_i) = v(W)$ for each i, $1 \leqslant i \leqslant n$. This proves (2.5).

COROLLARY. *Let W be as in Lemma* 1. *If W is non-degenerate, then $H(W) \neq 0$.*

Proof. Suppose $H(W) = 0$. Let w and w' be elements of W, then by Lemma 1, w and w' are proportional and hence are linearly dependent over k. This contradicts the assumption that W is non-degenerate.

From now on we will work with sets whose elements are formed from the solutions of (1.3). We say two solutions (x_1, y_1) and (x_2, y_2) of (1.3) are *distinct* if $x_1 \neq x_2$ and $y_1 \neq y_2$. We remark that $x_1 = x_2$ implies $y_1 = y_2$ and conversely.

DEFINITION. Two distinct solutions (x_1, y_1), (x_2, y_2) *of* (1.3) are said to be *non-proportional* if either $x_1/x_2 \notin k$ or $y_1/y_2 \notin k$.

LEMMA 2. *Suppose* (1.3) *has three solutions* (x_i, y_i), $i = 1, 2, 3$. *Then*

$$x_1y_2 - x_1y_3 + x_2y_3 - x_2y_1 + x_3y_1 - x_3y_2 = 0. \tag{2.6}$$

Proof. From (1.3) we have

$$ax_i + by_i = c, \quad i = 1, 2, 3. \tag{2.7}$$

Since the coefficients of the linear equations in (2.7) are nonzero, the determinant of its solution matrix must vanish. That is,

$$\begin{vmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{vmatrix} = 0,$$

which gives (2.6).

Denote by $\mathcal{U}$ the set whose elements are the six terms in (2.6). That is,

$$\mathcal{U} = \{x_1y_2, -x_1y_3, x_2y_3, -x_2y_1, x_3y_1, -x_3y_2\}. \tag{2.8}$$

LEMMA 3. *Suppose $a/c \notin K^{*r}$ or $b/c \notin K^{*r}$ in* (1.3). *Then any two distinct solutions of* (1.3) *are non-proportional.*

Proof. Let (x_i, y_i), $i = 1, 2$ be two distinct solutions of (1.3). From $ax_i + by_i = c$, $i = 1, 2$ we obtain

$$\frac{x_1 a}{c} = \frac{x_1 y_2 - x_1 y_1}{x_1 y_2 - x_2 y_1} = \frac{y_2/y_1 - 1}{y_2/y_1 - x_2/x_1}. \tag{2.9}$$

Since the solutions are distinct, we have $x_1 y_2 - x_2 y_1 \neq 0$. Suppose $x_1/x_2 \in k$ and $y_1/y_2 \in k$; then the right-hand side of (2.9) is in $k \subset K^r$, so that $x_1 a/c \in K^{*r}$ and therefore $a/c \in K^{*r}$ because $x_1 \in K^{*r}$. Similarly we can show that $b/c \in K^{*r}$. But this contradicts our assumption.

COROLLARY 1. *Let $\mathscr{U}$ be given by* (2.8). *Under the hypothesis of Lemma* 3, $H(\mathscr{U}) \neq 0$.

Proof. Suppose $H(\mathscr{U}) = 0$, then from Lemma 1 we know the elements of $\mathscr{U}$ are pairwise proportional. From $x_1 y_3/x_2 y_3 \in k$ and $x_3 y_1/x_3 y_2 \in k$, we get $x_1/x_2 \in k$ and $y_1/y_2 \in k$. But this contradicts Lemma 3.

COROLLARY 2. *The number of linearly independent elements in $\mathscr{U}$ is at most* 5 *and at least* 2.

Proof. The upper bound follows from (2.6). Suppose $\mathscr{U}$ has only one linearly independent element, then any two elements of $\mathscr{U}$ would be linearly dependent over k and hence proportional. But this is impossible since $H(\mathscr{U}) \neq 0$.

LEMMA 4. *Let $\mathscr{U}$ be given by* (2.8). *Suppose either $a/c \notin K^{*r}$ or $b/c \notin K^{*r}$ in* (1.3). *Then $\mathscr{U}$ has a minimal non-degenerate subset containing at least three elements.*

Proof. Let l be the maximum number of linearly independent elements in $\mathscr{U}$ and denote a maximal subset of linearly independent elements of $\mathscr{U}$ by $V = \{v_1, \ldots, v_l\}$. Since $l \leqslant 5$, there is an element $u \in \mathscr{U}$ such that $u \notin V$. We say a subset W of V is u-minimal if u is linearly dependent on W but not on any subset of W. If W is u-minimal, then $W \cup \{u\}$ is a minimal non-degenerate subset. Our object is to show that for each l, $2 \leqslant l \leqslant 5$, there is a $u \notin V$ and a subset W of V containing at least two elements such that W is u-minimal. It then follows that $\mathscr{U}$ has a minimal non-degenerate subset containing at least three elements.

(a) $l = 5$ and $V = \{v_1, \ldots, v_5\}$. Let $u \in \mathscr{U}$ such that $u \notin V$, then from (2.6) we have $u = -(v_1 + \cdots + v_5)$. This shows that V is u-minimal and $\mathscr{U} = V \cup \{u\}$ is the desired minimal non-degenerate set.

(b) $l = 4$ and $V = \{v_1, \ldots, v_4\}$. Let u_1, u_2 be the remaining elements of $\mathscr{U}$ and let W_i be a u_i-minimal subset of V, $i = 1, 2$. Since $v_1 + \cdots + v_4 + u_1 + u_2 = 0$ by (2.6), the assumption that W_i, $i = 1, 2$ consists of a single element contradicts the linear independence of $v_1, \ldots, v_4$.

(c) $l = 3$ and $V = \{v_1, v_2, v_3\}$. Let u_1, u_2, u_3 be the remaining elements of $\mathscr{U}$ and the W_i, $i = 1, 2, 3$ denote corresponding u_i-minimal subsets of V. As in (b), the assumption that each W_i consists of a single element leads to a contradiction, except possibly in the case (after reordering indices) $W_i = \{v_i\}$. Now $u_i = l_i v_i, l_i \in k$ and

$$(1 + l_1)v_1 + (1 + l_2)v_2 + (1 + l_3)v_3 = 0$$

by (2.6). By the linear independence of the v_i's we deduce $l_i = -1$ and $u_i = v_i$, $i = 1, 2, 3$. Suppose for example $u_1 = x_1 y_2$. If $v_1 = -x_1 y_3$ or $v_1 = -x_3 y_2$ then we get $y_2 = y_3$ or $x_1 = x_3$ and two equal solutions, which is impossible. If $v_1 = -x_2 y_1$ then $x_1/y_1 = x_2/y_2$ which combined with the equation $ax_i + by_i = c$ yields again two equal solutions. Hence v_1 can only be a monomial in $\mathscr{U}$ with the same sign as the monomial u_1; the same reasoning applies to each u_i. This however contradicts the fact that the number of positive and negative monomials in $\mathscr{U}$ is odd.

(d) $l = 2$ and $V = \{v_1, v_2\}$. Let u_1, u_2, u_3 and u_4 be the remaining elements in $\mathscr{U}$. We remark first that it is impossible to have

$$u_1 \sim u_2 \sim u_3 \sim u_4 \sim v_i, \qquad i = 1 \quad \text{or} \quad 2,$$

for this will contradict the linear independence of v_1 and v_2 by (2.6). Next, suppose

$$u_1 \sim u_2 \sim u_3 \sim v_i \quad \text{and} \quad u_4 \sim v_j \quad \text{with} \quad i \neq j. \tag{2.10}$$

Among u_1, u_2, u_3, v_1 two of them must have a same x_i, which we may take to be x_1; from this we get a proportionality relation $y_2 \sim y_3$. Similarly, we must have a relation $x_i \sim x_j$ for some $i \neq j$. If $x_2 \sim x_3$, we are done. Otherwise, by renumbering x_2, x_3 we may assume $x_1 \sim x_2$. Now $x_1 y_2 \sim x_1 y_3 \sim x_2 y_3$ and the fourth element proportional to them cannot be $x_2 y_1$ or $x_3 y_2$ without getting $x_1 \sim x_2 \sim x_3$ and $y_1 \sim y_2 \sim y_3$. Hence the fourth proportional element is $x_3 y_1$ and $x_1 y_2 \sim x_1 y_3 \sim x_2 y_3 \sim x_3 y_1$ and therefore $x_2 y_1 \sim x_3 y_2$. We multiply the last relation by y_3, use $x_2 y_3 \sim x_3 y_1$ and get $x_3 y_1^2 \sim x_3 y_2 y_3$, which gives $y_1^2 \sim y_2 y_3$, hence $y_1^2 \sim y_2^2 \sim y_3^2$. Since k is algebraically closed we can take square roots ad get again $y_1 \sim y_2 \sim y_3$, showing that all solutions are proportional. Thus we may assume

$$u_1 \sim u_2 \sim v_i \quad \text{and} \quad u_3 \sim u_4 \sim v_j \quad \text{with} \quad i \neq j.$$

This partitions $\mathscr{U}$ into two sets of three proportional elements each. Suppose for example x_1 appears twice in the first set of relations. Then $y_2 \sim y_3$ and either x_2 or x_3 appears twice in the second set, yielding either $y_1 \sim y_3$ or $y_1 \sim y_2$. In any case we get $y_1 \sim y_2 \sim y_3$ and all solutions are proportional. This leaves us with

$$x_1 y_2 \sim x_2 y_3 \sim x_3 y_1 \tag{2.11}$$

and

$$-x_2y_1 \sim -x_3y_2 \sim -x_1y_3 \tag{2.12}$$

Now (2.11) implies $x_1/x_2 \sim y_3/y_2$ and from (2.12) we get $x_1/x_2 \sim y_1/y_3$, therefore $y_3/y_2 \sim y_1/y_3$ and $y_3^2 \sim y_1y_2$. Similarly, $y_2^2 \sim y_1y_3$ and $y_1^2 \sim y_2y_3$ and it follows that $y_1^3 \sim y_2^3 \sim y_3^3$. Since k is algebraically closed we can take cube roots and deduce $y_1 \sim y_2 \sim y_3$ and $x_1 \sim x_2 \sim x_3$, again contradicting Lemma 3. This completes the proof of Lemma 4.

III. Proof of Main Theorem

Our indispensable tool in the proof of Main Theorem is the following inequality [2]

$$H(W) \leqslant \tfrac{1}{2}(m-1)(m-2)(|S| + 2g - 2), \tag{3.1}$$

where $W = \{w_1, \ldots, w_m\}$, $m \geqslant 3$ is a set of elements in K^* which satisfies the following three conditions:

(a) W is non-degenerate
(b) $w_1 + \cdots + w_n = 0$ (3.2)
(c) each w_i, $1 \leqslant i \leqslant m$ is an S-unit for some finite subset S of $\mathcal{M}_K$.

Our objective is to construct sets W and S as described in (3.2).

Lemma 4 assures us that for some m, $3 \leqslant m \leqslant 6$, $\mathscr{U}$ has a minimal non-degenerate subset Z_m containing m elements. We let

$$Z_m = \{z_1, \ldots, z_m\}. \tag{3.3}$$

A typical z_h is of type $\pm x_iy_j$ with $x_i, y_j \in K^{*r}$, hence we can write $z_h = w_h^r$ for suitable $w_h \in K^*$. Now we define

$$\Gamma_m = \{w_1, \ldots, w_m\}, \quad \text{with} \quad w_h^r = z_h; \tag{3.4}$$

then

$$H(Z_m) = rH(\Gamma_m).$$

Let

$$Z'_m = \{1, z_2/z_1, \ldots, z_m/z_1\}, \quad \Gamma'_m = \{1, w_2/w_1, \ldots, w_m/w_1\};$$

then

$$H(Z'_m) = H(Z_m), \quad H(\Gamma'_m) = H(\Gamma_m)$$

and

$$H(Z'_m) = rH(\Gamma'_m) = rH(\Gamma_m). \tag{3.5}$$

Let S be the set of valuations v in $\mathscr{M}_K$ such that $v(w_1), \ldots, v(w_m)$ are not all equal. Then it is easy to see that each element in Γ'_m, and hence also in Z'_m, is an S-unit. We may then apply (3.1) to Z'_m, but first we need to obtain a bound on $|S|$. For a given $w \in \Gamma_m$, define

$$S_w = \{v \in \mathscr{M}_K \mid v(w) > v(\Gamma_m)\}.$$

Then the cardinality of S_w can be shown to be

$$|S_w| = \sum_{v \in S_w} 1 \leqslant \sum_{v \in S_w} \{v(w) - v(\Gamma_m)\} = \sum_{v \in \mathscr{M}_K} \{v(w) - v(\Gamma_m)\} = -\sum_{v \in \mathscr{M}_K} v(\Gamma_m)$$
$$= H(\Gamma_m).$$

Further, it is easy to see that

$$S = \bigcup_{w \in \Gamma_m} S_w,$$

hence

$$|S| \leqslant mH(\Gamma_m). \tag{3.6}$$

However, when $m = 6$ we can show that the cardinality of S has the better bound

$$|S| \leqslant 3H(\Gamma_6). \tag{3.7}$$

One sees easily that w_h, $h = 1, \ldots, 6$ in (3.4) can be chosen such that

$$w_1 w_2 w_3 = w_4 w_5 w_6.$$

It follows that

$$S_{w_1} \cup S_{w_2} \cup S_{w_3} = S_{w_4} \cup S_{w_5} \cup S_{w_6},$$

and hence (3.7).

From (3.5), (3.6), (3.7) we get

$$rH(\Gamma_m) \leqslant \tfrac{1}{2}(m-1)(m-2)\begin{cases} mH(\Gamma_m) + 2g - 2, & 3 \leqslant m \leqslant 5, \\ 3H(\Gamma_6) + 2g - 2, & m = 6. \end{cases} \tag{3.8}$$

To obtain an upper bound on r, we divide both sides of (3.8) by $H(\Gamma_m) \geqslant 1$ and obtain $r \leqslant r(m)$ where

$$r(3) = 3 + 2g, \quad r(4) = 12 + 6g, \quad r(5) = 30 + 12g, \quad r(6) = 30 + 20g.$$

Therefore, when $r > 30 + 20g$, (1.3) cannot have more than two distinct solutions. This completes the proof of our Main Theorem.

References

[1] E. Bombieri and W.M. Schmidt, On Thue's equation. *Invent. Math.* 88, 69–81 (1987).

[2] W.D. Brownawell and D.W. Masser Vanishing sums in function fields. *Math. Proc. Camb. Phil. Soc.* 100, 427–434 (1986).

[3] Y. Domar, On the diophantine equation $|Ax^n - By^n| = 1, n \geqslant 5$. *Math. Scand.* 2, 29–32 (1954).

[4] J-H. Evertse, Upper bounds for the number of solutions of dophantine equations. *Math. Centrum, Amst.*, 1–127(1983).

[5] J-H. Evertse, On the equation $ax^n - by^n = c$. *Compositio Math.* 47, 289–315 (1982).

[6] J-H. Evertse, K. Györy, C.L. Stewart and R. Tijdeman, On S-unit equations in two unknowns. *Invent. Math.* 92, 461–477 (1988).

[7] S. Hyyrö, Über die Gleichung $ax^n - by^n = c$ und das Catalansche Problem. *Ann. Acad. Sci. Fenn., Ser. AI* 355, 1–50 (1964).