ACTA ARITHMETICA
XLVIII (1987)

Equal values of binary forms at integral points

by

J.-H. EVERTSE* (Amsterdam), K. GYŐRY* (Debrecen)
T. N. SHOREY (Bombay) and R. TIJDEMAN (Leiden)

1. Equations in rational integers. Let $F(X, Y)$ be an irreducible binary form of degree $n \geqslant 3$ with coefficients in $\mathbf{Z}$ (the ring of rational integers) and m a non-zero rational integer. In 1968, Baker [1] gave an explicit upper bound for all the solutions of the Thue equation

$$(1) \qquad F(x, y) = m \quad \text{in} \quad x, y \in \mathbf{Z}$$

which depends only on m, n and the height $H(F)$ of F (i.e. the maximal absolute value of the coefficients of F). Here the irreducibility of F can be replaced by the weaker assumption that $\omega(F) \geqslant 3$ where $\omega(F)$ denotes the maximal number of pairwise non-proportional linear factors of F in its factorisation over $\mathbf{C}$ (see e.g. [10] or [20]).

After Baker had proved the effective version of Thue's theorem on equation (1), Coates [3], [4] showed that the dependence on m can be replaced by dependence on the distinct prime divisors of m. He proved that if $F \in \mathbf{Z}[X, Y]$ is an irreducible binary form of degree $n \geqslant 3$ and if $p_1, \ldots, p_s$ are distinct prime numbers, then all solutions of the Thue–Mahler equation

$$(2) \qquad F(x, y) = p_1^{v_1} \ldots p_s^{v_s} \quad \text{in} \quad x, y, v_1, \ldots, v_s \in \mathbf{Z}$$

with $(x, y) = 1$ and $v_1 \geqslant 0, \ldots, v_s \geqslant 0$, in absolute values are less than a bound depending only on n, $H(F)$, s and $\max_i p_i$. As a consequence, he established an explicit lower bound for the greatest prime factor $P(F(x, y))$ of $F(x, y)$ in terms of $\mathscr{X} = \max(|x|, |y|)$. These estimates of Coates have been improved and generalised by others (for references see [2], [10], [21], [14], [20]). In 1977, Shorey, van der Poorten, Tijdeman and Schinzel [19] proved that if $F \in \mathbf{Z}[X, Y]$ is any binary form with $\omega(F) \geqslant 3$ then for all pairs x, y with $(x, y) = 1$ and $F(x, y) \neq 0$,

---

* The research was partly done at the University of Leiden in the academic year 1983/1984.

$$P(F(x, y)) > C_1 \log\log(\mathscr{X}+2) \tag{3}$$

where C_1 is an effectively computable positive number depending only on F.

Shorey and Tijdeman [20, Corollary 7.1] derived an effective upper bound for the solutions of the equation

$$F(x, y) = G(x, y) \quad \text{in } x, y \in \boldsymbol{Z} \text{ with } F(x, y) \neq 0 \tag{4}$$

where F, G are binary forms with rational integral coefficients such that $\deg F > \deg G$ and $\omega(F) \geqslant 3$. Since a binary form may be a constant, equation (4) is more general than equation (1). Further it follows from the arguments of their proof that if $F, G \in \boldsymbol{Z}[X, Y]$ are relatively prime binary forms with $\omega(F) \geqslant 3$, then

$$P\left(\frac{F(x, y)}{(F(x, y), G(x, y))}\right) \to \infty, \quad \text{effectively},$$

when $\mathscr{X} \to \infty$ subject to $(x, y) = 1$.

In this paper we shall give various further generalisations some of which in a quantitative form. For any rational number a, let $P(a)$ denote the maximum of the greatest prime factors of the numerator and denominator of a (in its reduced form), but $P(0) = P(1) = P(-1) = 1$.

THEOREM 1. *Let $F, G \in \boldsymbol{Z}[X, Y]$ be relatively prime binary forms. Let x and y be rational integers with $(x, y) = 1$ and $G(x, y) \neq 0$. If $\omega(FG) \geqslant 3$, then*

$$P\left(\frac{F(x, y)}{G(x, y)}\right) > C_2 \log\log(\mathscr{X}+2).$$

If $\omega(F) \geqslant 3$, then

$$P\left(\frac{F(x, y)}{(F(x, y), G(x, y))}\right) > C_3 \log\log(\mathscr{X}+2).$$

Here $\mathscr{X} = \max(|x|, |y|)$ and C_2, C_3 are effectively computable positive numbers depending only on the (constant and non-constant) irreducible factors of FG in $\boldsymbol{Z}[X, Y]$.

The second part of Theorem 1 has the following immediate consequence.

COROLLARY 1. *Let $F, G \in \boldsymbol{Z}[X, Y]$ be relatively prime binary forms such that $\omega(F) \geqslant 3$. Let $\{p_1, \ldots, p_t\}$ be a set of prime numbers. Let $x, y, z, k_1, \ldots, k_t$ be rational integers with*

$$zF(x, y) = G(x, y)\, p_1^{k_1} \ldots p_t^{k_t},$$

$$(x, y) = 1, \quad G(x, y) \neq 0, \quad (z, p_1 \ldots p_t) = 1.$$

Then $\max(|x|, |y|, |z|, |k_1|, \ldots, |k_t|)$ is bounded by an effectively computable number depending only on the primes $p_1, \ldots, p_t$ and the (constant and non-constant) irreducible factors of FG in $\boldsymbol{Z}[X, Y]$.

This is an improvement of Theorem 7.3 of Shorey and Tijdeman [20].

In the next corollaries the restrictions concerning F and G are further relaxed.

COROLLARY 2. *Let $F, G \in \mathbf{Z}[X, Y]$ be relatively prime non-zero binary forms. Suppose that F is not a constant multiple of a power of a linear or an indefinite quadratic form. If x, y are rational integers such that*

$$F(x, y) | G(x, y), \quad G(x, y) \neq 0, \quad (x, y) = 1$$

then $\max(|x|, |y|)$ is bounded by an effectively computable number which depends only on the degrees and heights of F and G.

COROLLARY 3. *Let $F, G \in \mathbf{Z}[X, Y]$ be binary forms which satisfy the conditions of Corollary 2 and also $\deg F > \deg G$. Then all pairs of rational integers x, y with*

$$F(x, y) | G(x, y), \quad G(x, y) \neq 0,$$

are such that $\max(|x|, |y|)$ is bounded by an effectively computable number which depends only on the degrees and heights of F and G.

Corollary 3 implies the result of Shorey and Tijdeman on equation (4).

COROLLARY 4. *Let $F, G \in \mathbf{Z}[X, Y]$ be distinct non-zero binary forms. Suppose that F/G is not a constant multiple of a (positive or negative) power of a linear or an indefinite quadratic form. If x, y are rational integers such that*

$$F(x, y) = G(x, y), \quad (x, y) = 1, \tag{5}$$

then $\max(|x|, |y|)$ is bounded by an effectively computable number which depends only on the degrees and heights of F and G.

Theorem 2 gives an upper bound for the magnitude of the solutions of (5) and Theorem 3 implies an upper bound for the number of solutions of (5) both of which depend only on the irreducible factors of FG in $\mathbf{Z}[X, Y]$. In order to formulate these theorems we need some further notation. Let $\mathscr{R}$ be an integral domain of characteristic 0 with quotient field K and let

$$F(X, Y) = a_0 X^p + a_1 X^{p-1} Y + \ldots + a_p Y^p,$$

$$G(X, Y) = b_0 X^q + b_1 X^{q-1} Y + \ldots + b_q Y^q \in \mathscr{R}[X, Y]$$

be binary forms. Then the resultant $R(F, G)$ of F and G is defined as follows:

$$R(F, G) = \begin{cases} 1 & \text{if} \quad p = q = 1, \\ a_0^q & \text{if} \quad p = 0,\ q > 0, \\ b_0^p & \text{if} \quad p > 0,\ q = 0; \end{cases}$$

$$R(F, G) = \begin{vmatrix} a_0 & a_1 & \dots & a_p & 0 & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_p & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & & \ddots & 0 \\ 0 & \dots & 0 & a_0 & a_1 & \dots & a_p \\ b_0 & b_1 & \dots & b_q & 0 & \dots & 0 \\ 0 & b_0 & b_1 & \dots & b_q & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & & \ddots & 0 \\ 0 & \dots & 0 & b_0 & b_1 & \dots & b_q \end{vmatrix} \quad \text{if} \quad p > 0,\ q > 0,$$

where in the determinant the first q rows contain the coefficients of F and the other p rows the coefficients of G. The forms F and G have a non-constant common factor in $K[X, Y]$ if and only if $R(F, G) = 0$.

Let $F_1, \dots, F_r, G_1, \dots, G_s \in \mathbf{Z}[X, Y]$ be non-zero binary forms with coefficients having absolute values at most H ($\geqslant 2$). Suppose that for $i = 1, \dots, r$ and $j = 1, \dots, s$ the forms F_i, G_j have no non-constant common divisor in $\mathbf{Z}[X, Y]$. Let L denote the splitting field of $F_1 \dots F_r G_1 \dots G_s$ and l, R_L, h_L the degree, regulator and class number of L, respectively. Let t be the number of distinct prime factors of

$$\prod_{\substack{1 \leqslant i \leqslant r \\ 1 \leqslant j \leqslant s}} R(F_i, G_j)$$

and let P denote the greatest of these prime factors (with the convention that $P = 2$ if $t = 0$). Finally, we define sets of binary forms $\mathscr{F}$, $\mathscr{G}$ by

$$\mathscr{F} = \{F\colon F(X, Y) = \prod_{i=1}^{r} F_i(X, Y)^{u_i} \text{ for certain } u_1, \dots, u_r \in \mathbf{N}\},$$

$$\mathscr{G} = \{G\colon G(X, Y) = \prod_{i=1}^{s} G_i(X, Y)^{v_i} \text{ for certain } v_1, \dots, v_s \in \mathbf{N}\}.$$

Here $\mathbf{N}$ denotes the set of positive rational integers.

THEOREM 2. *Let n be the degree of $F_1 \dots F_r G_1 \dots G_s$. Suppose*

$$\omega(F_1 \dots F_r G_1 \dots G_s) \geqslant 3.$$

If x, y are rational integers with

(5) $$F(x, y) = G(x, y), \qquad (x, y) = 1,$$

for some $F \in \mathscr{F}$, $G \in \mathscr{G}$, then

(6) $$\max(|x|, |y|) < \exp\{(r+s)\, n^4 \left(\left(C_4 (t+1) \log P\right)^{t+1} P\right)^{C_5} \log H\}$$

where C_4 and C_5 are effectively computable positive numbers such that C_4 depends only on l, R_l and h_l, and C_5 depends only on l.

Note that the bound in the theorem depends only of $F_1, \ldots, F_r$, $G_1, \ldots, G_s$. If F and G have a common factor, then it can be divided out. Any common factor of F and G is a binary form which yields only finitely many new solutions of (5). In the special case $r = 1$,

$$G_j(X, Y) = p_j \quad \text{for} \quad j = 1, \ldots, s,$$

where $p_1, \ldots, p_s$ are distinct prime numbers, Theorem 2 gives an upper bound for the solutions of the Thue–Mahler equation (2) for binary forms $F \in \mathbf{Z}[X, Y]$ with $\omega(F) \geqslant 3$. For this case Győry (cf. [9], Corollary 1) has proved the same estimate, but with completely explicit values of C_4 and C_5.

We call elements $a_1, \ldots, a_k$ of a field K *multiplicatively independent in* K if $a_1 a_2 \ldots a_k \neq 0$ and if the only rational integers $l_1, \ldots, l_k$ for which $a_1^{l_1} \ldots a_k^{l_k} = 1$ are $l_1 = \ldots = l_k = 0$. The following consequence of Theorem 2 relates multiplicative independence of binary forms to multiplicative independence of the values of these forms.

COROLLARY 5. *Let $F_1(X, Y), \ldots, F_r(X, Y) \in \mathbf{Z}[X, Y]$ be binary forms such that $F_1, \ldots, F_r$, P/Q are multiplicatively independent in $\mathbf{Q}(X, Y)$ for all relatively prime binary forms P, Q in $\mathbf{Z}[X, Y]$ with $\omega(PQ) \in \{1, 2\}$. Then there exists an effectively computable number C_6 depending only on $F_1, \ldots, F_r$ such that $F_1(x, y), \ldots, F_r(x, y)$ are multiplicatively independent in $\mathbf{Q}$ for all rational integers x, y with $(x, y) = 1$ and* $\max(|x|, |y|) > C_6$.

For binary forms $F \in \mathbf{Z}[X, Y]$ with $\omega(F) \geqslant 3$, Evertse [6] and Evertse and Győry [7] derived the upper bounds $2 \times 7^{n^3(2s+3)}$ and $4 \times 7^{l(2s+3)}$, respectively, for the number of solutions of (2). Here $n = \deg(F)$ and l is the degree of the splitting field of F. (Thus $1 \leqslant l \leqslant n!$.) We shall generalise Evertse's result to the more general equation (5).

THEOREM 3. *Let $\mathcal{F}, \mathcal{G}$, $F_1, \ldots, F_r$, $G_1, \ldots, G_s$ and t be as above. Let n be the degree of $F_1 \ldots F_r G_1 \ldots G_s$. Suppose $\omega(F_1 \ldots F_r G_1 \ldots G_s) \geqslant 3$. Then the number of pairs $x, y \in \mathbf{Z}$ for which* (5) *holds for some $F \in \mathcal{F}$, $G \in \mathcal{G}$ is at most* $2 \times 7^{n^3(2t+3)}$.

This bound can be compared with the estimate (6) obtained for the solutions themselves. Note that the upper bound in Theorem 3 is independent of r, s, P, H and L.

For results on exponential diophantine equations

$$Ax^m + By^m = Cx^n + Dy^n,$$

see Shorey and Tijdeman [20, Chapters 2 and 7].

2. Equations in integers from an algebraic number field. We shall prove Theorems 1, 2, 3 in the more general situation when the coefficients of the binary forms and the unknowns of the equations assume their values in the ring of integers of any given algebraic number field K. We shall refer to the general situation as the relative case, and to the case $K = Q$ which was considered in Section 1 as the absolute case.

In the sequel we shall use the following notation. If α is an algebraic number, then $\overline{|\alpha|}$ will denote the size of α, i.e. the maximum of the absolute values of the conjugates of α. If $f(X_1, \ldots, X_r)$ is a polynomial with algebraic coefficients then we denote by $\overline{|f|}$ the maximum of the sizes of the coefficients of f. The ring of integers of the algebraic number field K is denoted by $\mathcal{O}_K$ and the group of units of $\mathcal{O}_K$ by U_K. For $x, y \in \mathcal{O}_K$ we define

$$\mathscr{X}_K(x, y) = \inf_{\varepsilon \in U_K} \max(\overline{|\varepsilon x|}, \overline{|\varepsilon y|}).\text{(}^1\text{)}$$

If $\alpha_1, \ldots, \alpha_k \in K$ then the ideal (i.e. $\mathcal{O}_K$-module) generated by $\alpha_1, \ldots, \alpha_k$ is denoted by $\langle \alpha_1, \ldots, \alpha_k \rangle_K$. In $\mathscr{X}_K(x, y)$ and $\langle \alpha_1, \ldots, \alpha_k \rangle_K$ we suppress the subscript K if no confusion can arise. If $\mathfrak{a}$ is an ideal in K then we shall denote the norm of $\mathfrak{a}$ over Q by $N(\mathfrak{a})$. If $\mathfrak{a} \neq \langle 0 \rangle, \langle 1 \rangle$, then we define $P(\mathfrak{a})$ as the maximum of the norms of the prime ideals occurring in the prime ideal decomposition of $\mathfrak{a}$, while if $\mathfrak{a} = \langle 0 \rangle$ or $\mathfrak{a} = \langle 1 \rangle$ then we put $P(\mathfrak{a}) = 1$. If $\mathfrak{a} = \langle \alpha \rangle$ with some $\alpha \in K$, then we shall often write $P(\alpha)$ instead of $P(\langle \mathfrak{a} \rangle)$.

Before stating our results in this section, we remark that Coates' result [3], [4] mentioned in Section 1 was partially extended by Kotov [16] to the relative case as follows. Let K be an algebraic number field, let $F \in \mathcal{O}_K[X, Y]$ be an irreducible binary form of degree at least 5 and let $\pi_1, \ldots, \pi_s$ be non-zero non-unit elements of $\mathcal{O}_K$. Then all solutions of the equation

$$(7) \qquad F(x, y) = \pi_1^{v_1} \ldots \pi_s^{v_s} \quad \text{in} \quad x, y \in \mathcal{O}_K, \quad v_1, \ldots, v_s \in \mathbf{Z}$$
$$\text{with } N(\langle x, y \rangle) \leqslant N_0, \quad v_1 \geqslant 0, \ldots, v_s \geqslant 0$$

(where $N_0 \geqslant 1$) satisfy $\max(\overline{|x|}, \overline{|y|}) < C_7$ where C_7 is an effectively computable number depending only on $K, F, \pi_1, \ldots, \pi_s, N_0$. Kotov also proved that for $x, y \in \mathcal{O}_K$ with $N(\langle x, y \rangle) \leqslant N_0$,

$$(8) \qquad P(F(x, y)) \geqslant C_8 \log\log(\mathscr{N}+2) \text{ with } \mathscr{N} = \max(|N_{K/Q}(x)|, |N_{K/Q}(y)|).$$

Later Györy [8], [9] generalised Kotov's results to the case that $F \in \mathcal{O}_K[X, Y]$ is any binary form with $\omega(F) \geqslant 3$. Moreover, he proved that (8) can be replaced by

$$(9) \qquad P(F(x, y)) \geqslant C_9 \log\log(\mathscr{X}(x, y)+2).$$

(1) For $\alpha \in K$, let $\alpha^{(1)}, \ldots, \alpha^{(d)}$ denote the conjugates of α relative to K/Q, where $d = [K:Q]$. For $x, y \in \mathcal{O}_K$, let $H_K(x, y)$ be the maximum of the absolute values of the coefficients of the binary form $\prod_{i=1}^{d} (y^{(i)} X - x^{(i)} Y)$. Then there are computable positive numbers c'_K, c''_K, depending only on K, such that $c'_K H_K(x, y) \leqslant \mathscr{X}_K(x, y)^d \leqslant c''_K H_K(x, y)$.

Here C_8 and C_9 are effectively computable positive constants depending only on K, F and N_0. Inequality (9) is an improvement of (8) since for $x, y \in \mathcal{O}_K$ both

$$\mathcal{X}(x, y) \geqslant \{\max(|N_{K/\mathbf{Q}}(x)|, |N_{K/\mathbf{Q}}(y)|)\}^{1/[K:\mathbf{Q}]}$$

and (when U_K is infinite)

$$\sup_{x,y \in U_K} \mathcal{X}(x, y) = \infty .$$

Further, (9) is a generalisation of (3) to the relative case. For related results, see Sprindžuk [21], Győry [9], [13], [14] and Shorey and Tijdeman [20].

Let $F_1, \ldots, F_r, G_1, \ldots, G_s$ be non-zero binary forms in $\mathcal{O}_K[X, Y]$ such that F_i, G_j have no common non-constant divisors in $K[X, Y]$ for $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant s$, that the form $F_1 \ldots F_r G_1 \ldots G_s$ has degree n and that $\omega(F_1 \ldots F_r G_1 \ldots G_s) \geqslant 3$. Let

$$H = \max(2, \overline{|F_1|}, \ldots, \overline{|F_r|}, \overline{|G_1|}, \ldots, \overline{|G_s|}).$$

Denote by L the splitting field of $F_1 \ldots F_r G_1 \ldots G_s$ over K and let l, R_L, h_L be the degree, regulator and class number of L, respectively. Let $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_u\}$ be a (possibly empty) set of distinct prime ideals. Further, suppose that the number of distinct prime ideals which belong to the set $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_u\}$ or divide the ideal $\prod_{i,j} \langle R(F_i, G_j)\rangle$ is equal to t and let P be the maximum of the norms of these prime ideals (with the convention that $P = 2$ if $t = 0$.)

Finally, let $N_0 \geqslant 2$ and

$$\mathcal{F} = \{F(X, Y)\colon F(X, Y) = \prod_{i=1}^{r} F_i(X, Y)^{k_i} \text{ for certain } k_1, \ldots, k_r \in \mathbf{N}\},$$

$$\mathcal{G} = \{G(X, Y)\colon G(X, Y) = \prod_{j=1}^{s} G_j(X, Y)^{l_j} \text{ for certain } l_1, \ldots, l_s \in \mathbf{N}\}.$$

THEOREM 4. *Suppose that $x, y \in \mathcal{O}_K$ are not both zero and satisfy*

$$\frac{\langle F(x, y)\rangle}{\langle x, y\rangle^{\deg F}} = \frac{\langle G(x, y)\rangle}{\langle x, y\rangle^{\deg G}} \mathfrak{q}_1^{v_1} \ldots \mathfrak{q}_u^{v_u}, \qquad N(\langle x, y\rangle) \leqslant N_0 \tag{10}$$

for some $F \in \mathcal{F}$, $G \in \mathcal{G}$, $v_1, \ldots, v_u \in \mathbf{Z}$. Then

$$\mathcal{X}_K(x, y) < \exp\{(r+s)n^4 \big((C_{10}(t+1)\log P)^{t+1} P\big)^{C_{11}} \log(N_0 H)\} \tag{11}$$

where C_{10}, C_{11} are effectively computable positive numbers such that C_{10} depends on l, R_L, h_L and C_{11} depends only on L.

In (10) we considered expressions with powers of $\langle x, y\rangle$ in the denominator to provide a convenient generalisation of equation (5) in Theorem 2 in which the variables $x, y \in \mathbf{Z}$ satisfied the condition $(x, y) = 1$. Note that

Theorem 2 follows at once from Theorem 4 by taking $K = \mathbf{Q}$, $u = 0$, $N_0 = 1$. The condition $N(\langle x, y\rangle) \leqslant N_0$ is necessary, since if $x, y \in \mathcal{O}_K$ satisfy (10) then so do αx, αy for each $\alpha \in \mathcal{O}_K$ with $\alpha \neq 0$. We remark that from Theorem 4 we can deduce a new version of Győry's theorem on (7) in [9] with another bound.

From Theorem 4 we shall deduce the following generalisation of Theorem 1.

THEOREM 5. *Let* $F \in \mathcal{F}$, $G \in \mathcal{G}$. *Let* x, y *be elements of* $\mathcal{O}_K$ *with* $G(x, y) \neq 0$ *and* $N(\langle x, y\rangle) \leqslant N_0$.

If $\omega(FG) \geqslant 3$ *then*

$$(12) \qquad P\left(\frac{F(x, y)}{G(x, y)}\right) > C_{12} \log\log\left(\mathcal{X}(x, y)+2\right).$$

If $\omega(F) \geqslant 3$ *then*

$$(13) \qquad P\left(\frac{\langle F(x, y)\rangle}{\langle F(x, y), G(x, y)\rangle}\right) > C_{13} \log\log\left(\mathcal{X}(x, y)+2\right).$$

Here C_{12} *and* C_{13} *are effectively computable positive numbers depending only on* $K, F_1, \ldots, F_r, G_1, \ldots, G_s$ *and* N_0.

Theorem 1 follows at once from Theorem 5 with $K = \mathbf{Q}$, $N_0 = 1$ and $F_1, \ldots, F_r$ and $G_1, \ldots, G_s$ being the (constant and non-constant) irreducible factors of F and G, respectively, in $\mathbf{Z}[X, Y]$. If $F \in \mathcal{O}_K[X, Y]$ is a binary form with $\omega(F) \geqslant 3$, then (13) yields (9).

Evertse [5], [6] and later Evertse and Győry [7] derived their upper bounds for the number of solutions of (2) mentioned in Section 1 also in the relative case. We shall now give a generalisation of Theorem 3 to the relative case. If $x, y \in K$ satisfy (10) for some $F \in \mathcal{F}$, $G \in \mathcal{G}$, $v_1, \ldots, v_u \in \mathbf{Z}$ then so do αx, αy for all $\alpha \in K \setminus \{0\}$. Therefore it is natural to consider the set of points on the projective line $\mathbf{P}^1(K)$ of which the homogeneous coordinates $(x:y)$ satisfy (10) instead of considering the set of solutions of (10) itself. We shall say that a projective point satisfies (10) if its homogeneous coordinates $(x:y)$ satisfy (10). In Theorem 6 we use the same notation as in Theorems 4, 5. Moreover, let $d = d_1 + 2d_2$ be the degree of K, where d_1 is the number of real and $2d_2$ the number of complex conjugates of K.

THEOREM 6. *The number of points on* $\mathbf{P}^1(K)$ *which satisfy* (10) *for some* $F \in \mathcal{F}$, $G \in \mathcal{G}$, $v_1, \ldots, v_u \in \mathbf{Z}$ *is at most*

$$7^{n^3(d+2(d_1+d_2+t))}.$$

Theorem 3 follows immediately from Theorem 6 on using that for each point on $\mathbf{P}^1(\mathbf{Q})$ there are exactly two possible choices for the homogeneous coordinates $(x:y)$ such that $x, y \in \mathbf{Z}$ and $(x, y) = 1$.

We shall prove Theorems 4 and 6 by reducing (10) to an appropriate

Thue–Mahler equation. To this Thue–Mahler equation we shall apply certain results of Györy [11] and Evertse [6]. We note that Györy derived his result by applying Baker's method concerning linear forms in logarithms of algebraic numbers, while Evertse proved his result by applying a method of Thue and Siegel.

3. Proofs of Theorems 1, 2, 4 and 5 and their corollaries. In Lemma 1 we state some properties of resultants of binary forms which will be used throughout the paper. We define the degree of the binary form which is identically zero to be -1.

LEMMA 1. *Let $\mathscr{R}$ be an integral domain of characteristic* 0.

(i) *Let $F, G \in \mathscr{R}[X, Y]$ be binary forms of degrees $p \geqslant 0$, $q \geqslant 0$, respectively. Then for each binary form $Q \in \mathscr{R}[X, Y]$ of degree $p+q-1$ there exist binary forms A_Q, $B_Q \in \mathscr{R}[X, Y]$ such that*

$$A_Q F + B_Q G = R(F, G)Q. \tag{14}$$

(ii) *Let $F_1, F_2, G \in \mathscr{R}[X, Y]$ be binary forms of degrees $\geqslant 0$. Then*

$$\begin{aligned} R(F_1 F_2, G) &= R(F_1, G)R(F_2, G),\\ R(G, F_1 F_2) &= R(G, F_1)R(G, F_2). \end{aligned} \tag{15}$$

Proof. (i) We shall prove that (14) holds with A_Q, B_Q having degrees at most $q-1$, $p-1$, respectively. Consider the coefficients of A_Q, B_Q as $p+q$ unknowns. By equating the coefficients of the polynomials on the left and right hand side of (14), we obtain a system of $p+q$ linear equations in $p+q$ unknowns:

$$\mathscr{A}\boldsymbol{x} = \boldsymbol{b} \tag{16}$$

where $\mathscr{A}$ is a $(p+q)\times(p+q)$-matrix with entries in $\mathscr{R}$, $\boldsymbol{b} \in \mathscr{R}^{p+q}$ and $\boldsymbol{x}$ is a vector consisting of the $p+q$ unknowns. It is easy to check that the determinant of $\mathscr{A}$ is equal to $R(F, G)$ whereas all entries of $\boldsymbol{b}$ are divisible by $R(F, G)$. This shows that (16) has a solution $\boldsymbol{x} \in \mathscr{R}^{p+q}$.

(ii) Let $F, G \in \mathscr{R}[X, Y]$ be binary forms of degree $p \geqslant 1$, $q \geqslant 1$, respectively, and take some factorisations

$$F(X, Y) = \prod_{i=1}^{p} (\alpha_i X - \beta_i Y), \qquad G(X, Y) = \prod_{j=1}^{q} (\gamma_j X - \delta_j Y)$$

in some finite extension K of the quotient field of $\mathscr{R}$. Then

$$R(F, G) = \prod_{i=1}^{p} \prod_{j=1}^{q} (\alpha_i \delta_j - \beta_i \gamma_j). \tag{17}$$

A similar result for resultants of polynomials has been proved in van der Waerden [22, § 35]. Formula (17) can be obtained by a slight modification of this proof. It is not difficult to derive (15) from (17) and the definition of the resultant. ∎

We shall adopt the notations of Section 2. Further put

$$E(X, Y) = F_1(X, Y)\dots F_r(X, Y)\, G_1(X, Y)\dots G_s(X, Y)$$

and let $\mathscr{S} = \{\mathfrak{p}_1, \dots, \mathfrak{p}_t\}$ denote the set of distinct prime ideals in K which belong to $\{\mathfrak{q}_1, \dots, \mathfrak{q}_u\}$ or divide $\prod_{i,j} \langle R(F_i, G_j)\rangle$. We recall that, by assumption, $\deg E = n$. The following elementary lemma is essential in the proofs of our results.

LEMMA 2. *If* $(x, y) \in \mathcal{O}_K^2 \setminus \{0, 0\}$ *satisfies* (10) *for some* $F \in \mathscr{F}$, $G \in \mathscr{G}$, $v_1, \dots, v_u \in \mathbf{Z}$, *then there are non-negative rational integers* $u_1, \dots, u_t$ *such that*

$$\frac{\langle E(x, y)\rangle}{\langle x, y\rangle^n} = \mathfrak{p}_1^{u_1}\dots\mathfrak{p}_t^{u_t}. \tag{18}$$

Proof. Let $(x, y) \in \mathcal{O}_K^2 \setminus \{(0, 0)\}$ and let $F \in \mathscr{F}$, $G \in \mathscr{G}$. Since, by assumption, F and G have no common non-constant factor in $K[X, Y]$, we have $R(F, G) \neq 0$. Put $p = \deg F$, $q = \deg G$. We recall that an ideal $\mathfrak{a}$ divides an other ideal $\mathfrak{b}$ if and only if $\mathfrak{b} \subset \mathfrak{a}$. The greatest common divisor of two ideals $\mathfrak{a}$ and $\mathfrak{b}$ (i.e. the smallest ideal containing both $\mathfrak{a}$ and $\mathfrak{b}$) is denoted by $\mathfrak{a}+\mathfrak{b}$. Let K' be the smallest extension such that $\langle x, y\rangle_{K'}$ is a principal ideal, with generator δ say. Put $x' = x/\delta$, $y' = y/\delta$. Then $x', y' \in \mathcal{O}_{K'}$ and $\langle x', y'\rangle_{K'} = 1$. Finally, put

$$\mathfrak{c} = \frac{\langle F(x, y)\rangle_K}{\langle x, y\rangle_K^p} + \frac{\langle G(x, y)\rangle_K}{\langle x, y\rangle_K^q}.$$

By (14) there are binary forms $A(X, Y)$, $B(X, Y)$ in $\mathcal{O}_K[X, Y]$ such that

$$A(X, Y)F(X, Y) + B(X, Y)G(X, Y) = R(F, G)\, X^{p+q-1}.$$

Hence

$$\begin{aligned} \mathfrak{c}\mathcal{O}_{K'} &= \langle F(x', y'), G(x', y')\rangle_{K'} \\ &\supset \langle A(x', y')F(x', y') + B(x', y')G(x', y')\rangle_{K'} = \langle R(F, G)\, x'^{p+q-1}\rangle_{K'}. \end{aligned}$$

Similarly we have

$$\mathfrak{c}\mathcal{O}_{K'} \supset \langle R(F, G)\, y'^{p+q-1}\rangle_{K'}.$$

Therefore, $\mathfrak{c}\mathcal{O}_{K'} \supset \langle R(F, G)\rangle_{K'}$. But this implies that

$$\mathfrak{c} \supset \langle R(F, G)\rangle_K. \tag{19}$$

From now on we consider only ideals in K, so we omit the subscript K. Let $(x, y) \in \mathcal{O}_K^2 \setminus \{(0, 0)\}$ be a pair satisfying (10) for some $F \in \mathscr{F}$, $G \in \mathscr{G}$, $v_1, \dots, v_u \in \mathbf{Z}$. Let $\mathfrak{p}$ be a prime ideal not belonging to $\{\mathfrak{q}_1, \dots, \mathfrak{q}_u\}$ which divides $\langle E(x, y)\rangle / \langle x, y\rangle^n$. Then $\mathfrak{p}$ divides at least one of the ideals

$$\langle F_i(x, y)\rangle / \langle x, y\rangle^{\deg F_i} \quad (i = 1, \ldots, r), \qquad \langle G_j(x, y)\rangle / \langle x, y\rangle^{\deg G_j} \quad (j = 1, \ldots, s).$$

Therefore $\mathfrak{p}$ divides at least one of the ideals

$$\langle F(x, y)\rangle / \langle x, y\rangle^{\deg F}, \qquad \langle G(x, y)\rangle / \langle x, y\rangle^{\deg G}.$$

But by (10) this implies that $\mathfrak{p}$ divides $\mathfrak{c}$. Together with (19) this shows that $\mathfrak{p}$ divides $\langle R(F, G)\rangle$. By combining this with (15) we obtain, on noting that $F \in \mathscr{F}$, $G \in \mathscr{G}$, that $\mathfrak{p}$ divides the ideal $\prod_{i,j} \langle R(F_i, G_j)\rangle$. Hence $\langle E(x, y)\rangle / \langle x, y\rangle^n$ is composed solely of prime ideals from $\mathscr{S}$. ■

Let now $\beta, \pi_1, \ldots, \pi_q$ be non-zero elements of $\mathcal{O}_K$ such that $\pi_1, \ldots, \pi_q$ are not units. Let q' denote the number of distinct prime ideals of K dividing $\langle \pi_1 \ldots \pi_q\rangle$ and let $P' = \max(2, P(\pi_1 \ldots \pi_q))$. Further suppose that $\max_j \overline{|\pi_j|} \leqslant \mathscr{P}$ ($\mathscr{P} \geqslant 2$). Let $E_0(X, Y) \in \mathcal{O}_K[X, Y]$ be a binary form of degree n with splitting field L over K such that $\omega(E_0) \geqslant 3$. In the proofs of Lemmas 3, 4, 5 and the proof of Theorem 4, $c_1, c_2, \ldots, c_5$, c_1', c_2', c_3' will denote effectively computable positive numbers such that $c_1, c_2, \ldots, c_5$ depend only on l, R_L, h_L and c_1', c_2', c_3' only on l. As before, $N_0 \geqslant 2$.

LEMMA 3. *Let $x, y \in \mathcal{O}_K$ satisfy*

$$E_0(x, y) = \beta \pi_1^{w_1} \ldots \pi_q^{w_q}, \qquad N(\langle x, y\rangle) \leqslant N_0$$

for certain non-negative integers $w_1, \ldots, w_q$. Then

$$\max(\overline{|x|}, \overline{|y|}) < \exp\{n^2(q+1)\big((c_1(q'+1)\log P')^{q'+1} P'\big)^{c_1'}(\log \mathscr{P})\log(N_0 \overline{|E_0|}\,\overline{|\beta|})\}.$$

Proof. This is an immediate consequence of Theorem 2 of Győry [11] (see also [12]).

LEMMA 4. (i) *Let $\mathfrak{a}$ be an ideal in K. Then $\mathfrak{a}^{[L:K]h_L}$ is a principal ideal.*

(ii) *Let α be a non-zero element of K with $|N_{K/\mathbf{Q}}(\alpha)| = m$ and let v be a positive integer. Then there exists a unit ε in K such that $\overline{|\alpha\varepsilon^v|} \leqslant (mc_2^v)^{1/[K:\mathbf{Q}]}$.*

Proof. (i) The ideal $(\mathfrak{a}\mathcal{O}_L)^{h_L}$ is obviously principal in L. This implies that the ideal $\mathfrak{a}^{[L:K]h_L} = N_{L/K}\big((\mathfrak{a}\mathcal{O}_L)^{h_L}\big)$ is principal in K.

(ii) By Lemma 6 of [15], for each $\alpha' \in L$ with $|N_{L/\mathbf{Q}}(\alpha')| = m' \neq 0$ and $v' \in N$, there exists a unit η in L such that

$$\overline{|\alpha' \eta^{v'}|} \leqslant (m')^{1/[L:\mathbf{Q}]} c_3^{v}.$$

Apply this result with $\alpha' = \alpha$, $v' = v[L:K]$. Put $\varepsilon = N_{L/K}(\eta)$. Then, on taking $c_2 = c_3^l$,

$$\overline{|\alpha\varepsilon^v|} = \overline{|\alpha^{[L:K]}\varepsilon^{v[L:K]}|}^{1/[L:K]} = \overline{|N_{L/K}(\alpha\eta^{v[L:K]})|}^{1/[L:K]}$$

$$\leqslant \overline{|\alpha\eta^{v[L:K]}|} \leqslant |N_{L/\mathbf{Q}}(\alpha)|^{1/[L:\mathbf{Q}]} c_3^{v[L:K]} = (mc_2^v)^{1/[K:\mathbf{Q}]}. \quad ■$$

In the lemma below, $\mathfrak{b}$ will denote a non-zero integral ideal. As before, $N_0 \geqslant 2$ and $P = P(\mathfrak{p}_1, \ldots, \mathfrak{p}_t)$ if $t \geqslant 0$, $P = 2$ if $t = 0$.

LEMMA 5. *Suppose that $x, y \in \mathcal{O}_K$ are not both equal to zero and that*

$$(20)\qquad \frac{\langle E_0(x, y)\rangle}{\langle x, y\rangle^n} = \mathfrak{b}\mathfrak{p}_1^{u_1}\ldots\mathfrak{p}_t^{u_t}, \qquad N(\langle x, y\rangle) \leqslant N_0$$

for certain non-negative rational integers $u_1, \ldots, u_t$. Then

$$\mathscr{X}(x, y) \leqslant \exp\left\{n^3\left(\left(c_4(t+1)\log P\right)^{t+1} P\right)^{c_2'}\log\left(N_0\lceil\overline{E_0}\rceil N(\mathfrak{b})\right)\right\}.$$

Proof. Let v_i, w_i be rational integers such that

$$0 \leqslant v_i \leqslant [L:K]\,h_L - 1 \quad \text{and} \quad u_i = [L:K]\,h_L w_i + v_i \quad (1 \leqslant i \leqslant t).$$

By Lemma 4 (i), the ideals $\mathfrak{p}_i^{[L:K]h_L}$ are principal. Moreover,

$$N(\mathfrak{p}_i^{[L:K]h_L}) \leqslant P^{[L:K]h_L}.$$

Hence, by Lemma 4 (ii) with $v = 1$, there exist $\pi_1, \ldots, \pi_t \in \mathcal{O}_K$ such that $\langle \pi_i \rangle = \mathfrak{p}_i^{[L:K]h_L}$ and

$$(21)\qquad \lceil\overline{\pi_i}\rceil \leqslant P^{c_5} \quad \text{for} \quad i = 1, \ldots, t.$$

There exists a $\beta_0 \in \mathcal{O}_K$ such that $\langle \beta_0 \rangle = \mathfrak{b}\mathfrak{p}_1^{v_1}\ldots\mathfrak{p}_t^{v_t}\langle x, y\rangle^n$ and

$$(22)\qquad E_0(x, y) = \beta_0 \pi_1^{w_1}\ldots\pi_t^{w_t}.$$

Now

$$|N_{K/\mathbf{Q}}(\beta_0)| \leqslant N(\mathfrak{b})\, N_0^n\, P^{[L:K]h_L(t+1)}.$$

Hence, by Lemma 4 (ii), there exists a unit ε in K such that for $\beta = \varepsilon^n \beta_0$,

$$(23)\qquad \lceil\overline{\beta}\rceil \leqslant \left(c_2^n\, N(\mathfrak{b})\, N_0^n\, P^{[L:K]h_L(t+1)}\right)^{1/[K:\mathbf{Q}]}.$$

Moreover, by (22),

$$(24)\qquad E_0(\varepsilon x, \varepsilon y) = \beta\pi_1^{w_1}\ldots\pi_t^{w_t}.$$

Now Lemma 5 follows immediately from Lemma 3, (21), (23), (24), by taking $P' = P$, $q' = q = t$. ∎

Proof of Theorem 4. Theorem 4 follows at once from Lemmas 2 and 5 by observing that there exists a constant c_3' with

$$\lceil\overline{E}\rceil \leqslant (nH)^{c_3'(r+s)} \quad \text{where} \quad H = \max(2, \lceil\overline{F_1}\rceil, \ldots, \lceil\overline{F_r}\rceil, \lceil\overline{G_1}\rceil, \ldots, \lceil\overline{G_s}\rceil). \;∎$$

Proof of Theorem 2. Take $K = \mathbf{Q}$, $u = 0$, $N_0 = 1$ in Theorem 4. ∎

Proof of Corollary 5. Let $F_1(X, Y), \ldots, F_r(X, Y) \in \mathbf{Z}[X, Y]$ be binary forms such that $F_1, \ldots, F_r, P/Q$ are multiplicatively independent in $\mathbf{Q}(X, Y)$ for all relatively prime binary forms P, Q in $\mathbf{Z}[X, Y]$ with $\omega(PQ) \in \{1, 2\}$.

c_6 and c_7 will denote effectively computable positive numbers depending only on $F_1, \ldots, F_r$. If x and y are rational integers with $(x, y) = 1$ and $F_1(x, y) \ldots F_r(x, y) = 0$ then $\max(|x|, |y|) \leqslant c_6$. Let x and y be rational integers such that $\max(|x|, |y|) > c_6$, $(x, y) = 1$ and $F_1(x, y), \ldots, F_r(x, y)$ are multiplicatively dependent in $\boldsymbol{Q}$. Let $l_1, \ldots, l_r$ be rational integers, not all zero, such that

$$F_1(x, y)^{l_1} \ldots F_r(x, y)^{l_r} = 1. \tag{25}$$

Let

$$\prod_{i=1}^{r} F_i(X, Y)^{l_i} = P(X, Y)/Q(X, Y),$$

where $P, Q \in \boldsymbol{Z}[X, Y]$ are relatively prime binary forms. Then (25) implies that

$$P(x, y) = Q(x, y), \quad (x, y) = 1. \tag{26}$$

Since $F_1, \ldots, F_r$ are multiplicatively independent, $P \neq Q$. Moreover, P/Q can not be a constant $\neq 1$ for otherwise (26) is impossible. Therefore $\omega(PQ) \geqslant 3$. Let $G_1, \ldots, G_s$ be the (constant and non-constant) irreducible factors of PQ in $\boldsymbol{Z}[X, Y]$. Then $\omega(G_1 \ldots G_s) \geqslant 3$ and $G_1, \ldots, G_s$ are irreducible factors of $F_1 \ldots F_r$. Together with (26) and Theorem 2 this shows that $\max(|x|, |y|) \leqslant c_7$. This proves Corollary 5. ∎

Proof of Theorem 5. In what follows, $c_8, c_9, \ldots, c_{18}$ will denote effectively computable positive numbers depending only on K, N_0, $F_1, \ldots, F_r, G_1, \ldots, G_s$. We assume that $xy \neq 0$ which is no restriction in the proofs of (12) and (13).

First suppose that $F(x, y) = 0$. Then $F_i(x, y) = 0$ for some i with $1 \leqslant i \leqslant r$. Together with $xy \neq 0$, this shows that $F_i(X, Y)$ has at least two non-zero terms. Hence

$$\max(|N_{K/\boldsymbol{Q}}(x)|, |N_{K/\boldsymbol{Q}}(y)|) \leqslant c_8.$$

By Lemma 4 (ii), there is a unit ε in K such that $\overline{|\varepsilon x|} \leqslant c_9$. Now $F_i(\varepsilon x, \varepsilon y) = 0$ implies that $\overline{|\varepsilon y|} \leqslant c_{10}$. This proves (12) and (13) in case $F(x, y) = 0$.

Now suppose that $F(x, y) \neq 0$. Put $p = \deg F$, $q = \deg G$. In order to prove (12) it suffices to show that

$$P\left(\frac{\langle F(x, y)\rangle}{\langle x, y\rangle^p} \Big/ \frac{\langle G(x, y)\rangle}{\langle x, y\rangle^q}\right) \geqslant c_{11} \log\log(\mathscr{X}(x, y) + 2). \tag{27}$$

For if $\log\log(\mathscr{X}(x, y) + 2) \leqslant c_{12} := c_{11}^{-1} N_0$ then (12) holds for an appropriate value of c_{12} and otherwise (27) implies that

$$P\left(\frac{F(x, y)}{G(x, y)}\right) = P\left(\frac{\langle F(x, y)\rangle}{\langle x, y\rangle^p} \Big/ \frac{\langle G(x, y)\rangle}{\langle x, y\rangle^q}\right)$$

and (12) follows from (27).

We shall now prove (27). Let

$$Q = P\left(\frac{\langle F(x, y)\rangle}{\langle x, y\rangle^p}\Big/\frac{\langle G(x, y)\rangle}{\langle x, y\rangle^q}\right)$$

and let $\mathscr{Q} = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_u\}$ be the set of all prime ideals with norm $\leqslant Q$. Then

$$\frac{\langle F(x, y)\rangle}{\langle x, y\rangle^p} = \frac{\langle G(x, y)\rangle}{\langle x, y\rangle^q}\mathfrak{q}_1^{v_1}\ldots\mathfrak{q}_u^{v_u} \tag{28}$$

for certain rational integers $v_1, \ldots, v_u$. Note that the prime ideals dividing $\prod_{i,j}\langle R(F_i, G_j)\rangle$ have norms at most c_{13}. For each prime number p there are at most $[K:\mathbf{Q}]$ prime ideals in K dividing $\langle p\rangle$ and all of them have a norm which is a power of p. Since there are at most $2Q/\log Q$ rational primes not exceeding Q (cf. [18]) we have $u \leqslant c_{14}Q/\log Q$. Now Theorem 4 implies that

$$\log\log(\mathscr{X}(x, y)+2) < c_{15}Q.$$

This proves (27).

We shall now prove (13). Suppose that $\omega(F) \geqslant 3$. By (14) there exist binary forms A_1, A_2, B_1, B_2 in $\mathcal{O}_K[X, Y]$ such that

$$A_1(X, Y)F(X, Y)+B_1(X, Y)G(X, Y) = R(F, G)X^{p+q-1},$$

$$A_2(X, Y)F(X, Y)+B_2(X, Y)G(X, Y) = R(F, G)Y^{p+q-1}.$$

This shows that the ideal $\langle F(x, y), G(x, y)\rangle$ divides $\langle R(F, G)\rangle\langle x, y\rangle^{p+q-1}$. In view of (15) this implies that

$$P(\langle F(x, y), G(x, y)\rangle) \leqslant c_{16}. \tag{29}$$

By applying (12) with $s = 1$ and $G_1 = 1$, we obtain

$$P(F(x, y)) > c_{17}\log\log(\mathscr{X}(x, y)+2). \tag{30}$$

If $\log\log(\mathscr{X}(x, y)+2) \leqslant c_{16}c_{17}^{-1} =: c_{18}$, then (13) follows. If

$$\log\log(\mathscr{X}(x, y)+2) > c_{18}$$

then (29) and (30) give

$$P\left(\frac{\langle F(x, y)\rangle}{\langle F(x, y), G(x, y)\rangle}\right) = P(F(x, y)) > c_{17}\log\log(\mathscr{X}(x, y)+2).$$

This completes the proof of (13). ∎

Proof of Theorem 1. Take $K = \mathbf{Q}$, $N_0 = 1$ in Theorem 5. Let $F_1, \ldots, F_r$ and $G_1, \ldots, G_s$ be the (constant and non-constant) irreducible factors of F and G, respectively. ∎

Proof of Corollary 2. We have either (i) $\omega(F) \geqslant 3$ or (ii) $F = c\cdot Q^a$

where $c \in \boldsymbol{Q}^*$, $a \in \boldsymbol{Z}$, $a > 0$ and Q is a definite quadratic form with coefficients in $\boldsymbol{Z}$ or (iii) $F = cL_1^a L_2^b$ where $c \in \boldsymbol{Q}^*$, $a, b \in \boldsymbol{Z}$, $a > 0$, $b > 0$ and L_1, L_2 are non-proportional linear forms with coefficients in $\boldsymbol{Z}$. Put $p = \deg F$, $q = \deg G$.

Let x, y be integers with $(x, y) = 1$. By applying (14) with $Q = X^{p+q-1}$, we obtain that $(F(x, y), G(x, y))$ divides $R(F, G)x^{p+q-1}$. Similarly, $(F(x, y), G(x, y))$ divides $R(F, G)y^{p+q-1}$. Hence

$$(F(x, y), G(x, y)) | R(F, G). \tag{31}$$

Now suppose that x, y are integers with $(x, y) = 1$, $G(x, y) \neq 0$ and $F(x, y) | G(x, y)$. Then (31) implies that

$$F(x, y) | R(F, G).$$

We claim that $\max(|x|, |y|)$ can be bounded by an effectively computable number depending only on the heights and degrees of F and G. In case (i) this follows from Corollary 1 applied with $t = 0$. In case (ii) it follows from the fact that $|Q(x, y)| \geqslant c_{19} \{\max(|x|, |y|)\}^2$ for some effectively computable positive number c_{19} depending only on the height of Q. Finally, in case (iii) we have

$$|L_1(x, y)| \leqslant |c^{-1} R(F, G)|, \quad |L_2(x, y)| \leqslant |c^{-1} R(F, G)|.$$

Since L_1 and L_2 are non-proportional, the claim is also justified in this case. ∎

Proof of Corollary 3. We have $p > q \geqslant 0$ where $p = \deg F$, $q = \deg G$. Let x, y be integers with $G(x, y) \neq 0$ and $F(x, y) | G(x, y)$. Put $d = (x, y)$, $x_0 = x/d$, $y_0 = y/d$. Then $d^{p-q} F(x_0, y_0) | G(x_0, y_0)$. Hence, by Corollary 2, $\max(|x_0|, |y_0|)$ and therefore d are bounded by effectively computable numbers depending only on the degrees and heights of F and G. ∎

Proof of Corollary 4. Let D be the greatest common divisor of F and G in the ring $\boldsymbol{Z}[X, Y]$. Put $F_1 = F/D$ and $G_1 = G/D$. Let x, y be rational integers with $(x, y) = 1$ and $F(x, y) = G(x, y)$. If $F(x, y) = 0$, then $\max(|x|, |y|)$ does not exceed a computable number depending only on the degree and height of F. Suppose that $F(x, y) \neq 0$. Then

$$F_1(x, y) = G_1(x, y).$$

Hence $F_1(x, y) G_1(x, y)$ divides both $\{F_1(x, y)\}^2$ and $\{G_1(x, y)\}^2$. In view of (31) this implies

$$F_1(x, y) G_1(x, y) | \{R(F_1, G_1)\}^2.$$

Since F/G is a constant multiple of a power of a linear or an indefinite quadratic form if and only if $F_1 G_1$ is, Corollary 4 follows at once from Corollary 2 with $F_1 G_1$ and $\{R(F_1, G_1)\}^2$ replacing F and G, respectively. ∎

4. Proofs of Theorems 3 and 6. We shall use the notation of Section 2. Let $\mathscr{S} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$ be a finite set of prime ideals in $\mathcal{O}_K$ and let $\mathfrak{a}$ be a fixed ideal in K. Let

$$W(\mathfrak{a}, \mathscr{S}) = \{\alpha \in K\colon \exists u_1, \ldots, u_t \in \mathbf{Z} \text{ such that } \langle\alpha\rangle = \mathfrak{a}\mathfrak{p}_1^{u_1} \ldots \mathfrak{p}_t^{u_t}\}.$$

Note that $W(\langle 1\rangle, \mathscr{S})$ is just the group of S-units where S is the set of valuations containing the archimedean valuations on K and the valuations corresponding to $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$.

LEMMA 6. *Let $\mathscr{S}$ be a finite set of prime ideals in $\mathcal{O}_K$ of cardinality t and let $\mathfrak{a}$, $\mathfrak{b}$ be fixed non-zero ideals in K. Then the number of solutions of the equation*

$$x+y = 1 \quad in \quad (x, y) \in W(\mathfrak{a}, \mathscr{S}) \times W(\mathfrak{b}, \mathscr{S}) \tag{32}$$

is at most $3 \times 7^{d+2(d_1+d_2+t)}$.

Proof. Suppose that (32) is solvable and let (λ, μ) be a fixed solution of (32). Let $U = W(\langle 1\rangle, \mathscr{S})$. Then (x, y) is a solution of (32) if and only if there are $\xi, \eta \in U$ such that $x = \lambda\xi$, $y = \mu\eta$ and $\lambda\xi+\mu\eta = 1$. But by Theorem 1 of Evertse [6] there are at most $3 \times 7^{d+2(d_1+d_2+t)}$ pairs $(\xi, \eta) \in U^2$ with $\lambda\xi+\mu\eta = 1$. ∎

Let $F(X, Y) \in K[X, Y]\setminus\{0\}$ be a binary form. The content of F with respect to K, denoted by $\mathfrak{c}_K(F)$, is defined as the ideal in K generated by the coefficients of F. We shall need the following generalisation of Gauss' Lemma: if $F(X, Y)$, $G(X, Y)$ are binary forms in $K[X, Y]$ then

$$\mathfrak{c}_K(FG) = \mathfrak{c}_K(F) \cdot \mathfrak{c}_K(G). \tag{33}$$

This follows for example from Lang [17, Proposition 2.1].

For any point $(x:y) \in \mathbf{P}^1(K)$, the homogeneous coordinates x, y can be chosen so that $x, y \in \mathcal{O}_K$. Hence Theorem 6 is an immediate consequence of Lemma 1 and Lemma 7 below.

LEMMA 7. *Let $E_0(X, Y) \in K[X, Y]$ be a binary form of degree n with $\omega(E_0) \geqslant 3$ and let $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$ be a set of prime ideals in K. Then the number of points $(x:y) \in \mathbf{P}^1(K)$ satisfying*

$$\frac{\langle E_0(x, y)\rangle}{\mathfrak{c}_k(E_0)\,\langle x, y\rangle^n} = \mathfrak{p}_1^{u_1} \ldots \mathfrak{p}_t^{u_t} \tag{34}$$

for some $u_1, \ldots, u_t \in \mathbf{Z}$ is at most $7^{n^3(d+2(d_1+d_2+t))}$.

Proof. There exists a field M of degree at most $n(n-1)(n-2)$ over K which contains the coefficients of three pairwise non-proportional linear forms dividing E_0 in $M[X, Y]$, $A(X, Y)$, $B(X, Y)$, $C(X, Y)$ say. Let s_1, $2s_2$ denote the number of real and complex conjugates of M, respectively, and let $\mathfrak{q}_1, \ldots, \mathfrak{q}_u$ be the prime ideals in $\mathcal{O}_M$ lying above $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$. Then

(35) $s_1+s_2+u \leqslant n(n-1)(n-2)(d_1+d_2+t), \quad [M:Q] \leqslant n(n-1)(n-2)d.$

Let $(x:y) \in P^1(K)$ be a point satisfying (34) for certain $u_1, \ldots, u_t \in Z$. Since the left-hand side of (34) is an integral ideal, the u_i are non-negative. Since the linear forms A, B and C are linearly dependent, there are non-zero elements $\alpha, \beta \in M$ such that

$$\alpha A(X, Y)+\beta B(X, Y) = C(X, Y) \text{ identically in } X, Y.$$

Put $u = \alpha A(x, y)/C(x, y)$, $v = \beta B(x, y)/C(x, y)$. Then $u+v = 1$. Moreover, by (33), the integral ideals

$$\frac{\langle A(x, y)\rangle_M}{\mathfrak{c}_M(A)\langle x, y\rangle_M}, \quad \frac{\langle B(x, y)\rangle_M}{\mathfrak{c}_M(B)\langle x, y\rangle_M}, \quad \frac{\langle C(x, y)\rangle_M}{\mathfrak{c}_M(C)\langle x, y\rangle_M}$$

divide the left-hand side of (34) and are therefore composed of prime ideals from $\mathscr{S} = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_u\}$. It follows easily that $u \in W(\mathfrak{a}, \mathscr{S})$, $v \in W(\mathfrak{b}, \mathscr{S})$ where

$$\mathfrak{a} = \langle\alpha\rangle_M \, \mathfrak{c}_M(A)/\mathfrak{c}_M(C), \qquad \mathfrak{b} = \langle\beta\rangle_M \, \mathfrak{c}_M(B)/\mathfrak{c}_M(C).$$

Moreover the projective point $(x:y)$ is completely determined by u, v. Now a combination of Lemma 6 and (35) with the facts mentioned above yields that the number of points $(x:y) \in P^1(K)$ which satisfy (34) for certain $u_1, \ldots, u_t \in Z$ is at most

$$3 \times 7^{n(n-1)(n-2)(d+2(d_1+d_2+t))} \leqslant 7^{n^3(d+2(d_1+d_2+t))}. \; \blacksquare$$

Proof of Theorem 3. Apply Theorem 6 and use that for each point on $P^1(Q)$ there are exactly two possible choices for the homogeneous coordinates $(x:y)$ such that $x, y \in Z$ and $(x, y) = 1$. $\blacksquare$

References

[1] A. Baker, *Contributions to the theory of diophantine equations*, Philos. Trans. Roy. Soc. London A 263 (1968), pp. 173–208.

[2] – *Transcendental number theory*, 2nd ed., Cambridge University Press, Cambridge etc., 1979.

[3] J. Coates, *An effective p-adic analogue of a theorem of Thue*, Acta Arith. 15 (1969), pp. 279–305.

[4] – *An effective p-adic analogue of a theorem of Thue II, The greatest prime factor of a binary form*, ibid. 16 (1970), pp. 399–412.

[5] J.-H. Evertse, *Upper bounds for the numbers of solutions of diophantine equations*, Math. Centre Tract 168, Centr. Math. Comput. Sci., Amsterdam, 1983.

[6] – *On equations in S-units and the Thue–Mahler equation*, Invent. Math. 75 (1984), pp. 561–584.

[7] J.-H. Evertse and K. Győry, *On unit equations and decomposable form equations*, J. Reine Angew. Math. 358 (1985), pp. 6–19.

[8] K. Győry, *On the greatest prime factors of decomposable forms at integer points*, Ann. Acad. Sci. Fenn., Ser. A1, Math. 4 (1978/1979), pp. 341–355.

[9] K. Győry, *Explicit upper bounds for solutions of some diophantine equations*, ibid. 5 (1980), pp. 3–12.

[10] – *Résultats effectifs sur la représentation des entiers par des formes décomposables*, Queen's Papers in Pure and Applied Math., No. 56. Kingston, Canada, 1980.

[11] – *On the representation of integers by decomposable forms in several variables*, Publ. Math. Debrecen 28 (1981), pp. 89–98.

[12] – *On S-integral solutions of norm form, discriminant form and index form equations*, Studia Sci. Math. Hungar. 16 (1981), pp. 149–161.

[13] – *Bounds for the solutions of norm form, discriminant form and index form equations in finitely generated integral domains*, Acta. Math. Hungar. 42 (1983), pp. 45–80.

[14] – *On norm form, discriminant form and index form equations*, in: *Topics in Classical Number Theory*, Coll. Math. Soc. J. Bolyai 34, North Holland Publ. Comp., Amsterdam etc., 1984, pp. 617–676.

[15] K. Győry and Z. Z. Papp, *Effective estimates for the integer solutions of norm form and discriminant form equations*, Publ. Math. Debrecen 25 (1978), pp. 311–325.

[16] S. V. Kotov, *The Thue-Mahler equation in relative fields* (Russian), Acta. Arith. 27 (1975), pp. 293–315.

[17] S. Lang, *Fundamentals of diophantine geometry*, Springer Verlag, New York etc., 1983.

[18] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. 6 (1962), pp. 64–94.

[19] T. N. Shorey, A. J. van der Poorten, R. Tijdeman and A. Schinzel, *Applications of the Gel'fond-Baker method to diophantine equations*, in: *Transcendence Theory: Advances and Applications*, Academic Press, London etc., 1977, pp. 59–77.

[20] T. N. Shorey and R. Tijdeman, *Exponential diophantine equations*, Cambridge University Press, 1987.

[21] V. G. Sprindžuk, *Classical diophantine equations in two unknowns* (Russian), Nauka Moskva, 1982.

[22] B. L. van der Waerden, *Algebra* 1, 7. Aufl., Springer Verlag, Berlin etc., 1966.

DEPARTMENT OF PURE MATHEMATICS
CENTRE FOR MATHEMATICS
AND COMPUTER SCIENCE
1098 SJ Amsterdam
The Netherlands

MATHEMATICAL INSTITUTE
KOSSUTH LAJOS UNIVERSITY
4010 Debrecen
Hungary

SCHOOL OF MATHEMATICS
TATA INSTITUTE OF FUNDAMENTAL RESEARCH
Bombay 400005
India

MATHEMATICAL INSTITUTE
UNIVERSITY LEIDEN
2300 RA Leiden
The Netherlands

Received on 30.12.1985 (1580)