On the distribution of solutions of Thue's equation

Béla Brindza, Ákos Pintér,
Alfred J. van der Poorten and Michel Waldschmidt

To Andrzej Schinzel on his 60th birthday

1. Introduction

We consider solutions in relatively prime integers x and y of an equation

$$|F(x,y)| = m. \tag{1}$$

Here $F \in \mathbb{Z}[X,Y]$ is an irreducible binary form of degree $n \geq 3$ and m denotes a positive integer with s distinct prime factors. Solutions (x,y) and $(-x,-y)$ will be deemed the same.

Bombieri and Schmidt [1] generalised and improved several earlier results in showing that there is an effectively computable absolute positive constant c so that (1) has at most cn^{s+1} solutions in coprime integers x and y. Brindza [2] obtained a bound linear in the degree n, provided that m is large enough; however, this bound remains exponential in s.

It seems likely that almost all the solutions of the equation (1) are small, and around $m^{1/n}$ provided that m is large compared to the height of F.

Our principal result, which is based on Baker's method and a gap principle, illustrates that tendency. For brevity, we set M to denote the Mahler height of the binary form F (compare [1]).

Theorem. *Let* $\mu(n) = (n-2)^{-1} + (n-1)^{-2}$. *There are at most* $2n^2(s+1) + 13n$ *solutions of equation* (1) *with*

$$\max(|x|,|y|) \geq 21n^2M^5m^{\mu(n)}. \tag{2}$$

Remark. The binary form is not necessarily reduced. Further, one sees readily that all solutions of (1) satisfy

$$\max(|x|,|y|) \geq \tfrac{1}{2}M^{-1/n}m^{1/n}.$$

2. Preliminaries

Our proof requires several auxiliary results. The first is a gap principle. The crucial step in applying it will be provided by a different gap principle of Bombieri and Schmidt [1].

It will be convenient occasionally to use a compact notation

$$\eta^{\mathbf{k}_j} = \eta_0^{k_{0,j}} \cdots \eta_{t-1}^{k_{t-1,j}} \quad \text{and} \quad \psi^{\mathbf{k}_j} = \psi_0^{k_{0,j}} \cdots \psi_{t-1}^{k_{t-1,j}}.$$

to denote certain monomials that arise in our enunciation and argument.

Lemma 1. *Take t at least 1, and let λ, $\eta_0, \ldots, \eta_{t-1}$, μ, $\psi_0, \ldots, \psi_{t-1}$ be nonzero complex numbers. Suppose that the equation*

$$\lambda \eta_0^{\mathbf{k}_0} \cdots \eta_{t-1}^{\mathbf{k}_{t-1}} + \mu \psi_0^{\mathbf{k}_0} \cdots \psi_{t-1}^{\mathbf{k}_{t-1}} = 1$$

has at least $t+2$ solutions in t-tuples $\mathbf{k}_j = (k_{0,j}, \ldots, k_{t-1,j})$ of integers. Denote by K the maximum 'gap' between 'consecutive' such solutions; specifically

$$K = \max_{0 \le i \le t-1, 1 \le j \le t+1} \{2, |k_{i,j+1} - k_{i,j}|\}.$$

Then

$$\tfrac{1}{4}(t+1)^{t/2} K^t \ge |\lambda \eta^{\mathbf{k}_1}|,$$

provided that for $j = 1, \ldots, t+1$,

$$|\lambda \eta^{\mathbf{k}_1}| \ge 6 \quad \textit{and} \quad |\eta^{\mathbf{k}_{j+1}} / \eta^{\mathbf{k}_j}| \ge 9(t+1)^{t/2} K^t.$$

Remark. Here is the scheme of the proof: We note that each solution $\mathbf{k}_j$ gives rise to a linear combination, Λ_j say, with rational coefficients in the $t+1$ logarithms $2\pi i$, $\log(\eta_0/\psi_0)$, ..., $\log(\eta_{t-1}/\psi_{t-1})$. It follows that the $t+2$ complex numbers $\Lambda_1, \ldots, \Lambda_{t+2}$ must be linearly dependent over $\mathbb{Q}$. We recall that the Λ_j 'are small' and apply 'Siegel's Lemma', in this case just a trivial estimate of the determinants arising from solving by Cramer's rule, to complete the argument.

Proof. The conditions detailed for Lemma 1 immediately entail

$$\tfrac{1}{6} \ge |\lambda \eta^{\mathbf{k}_1}|^{-1} > |\lambda \eta^{\mathbf{k}_2}|^{-1} > \ldots > |\lambda \eta^{\mathbf{k}_{t+2}}|^{-1},$$

and, for $j = 1, \ldots, t+1$,

$$\left|\eta^{\mathbf{k}_{j+1}} / \eta^{\mathbf{k}_j}\right| \ge 9K^t \ge 18,$$

$$\left|\psi^{\mathbf{k}_j} / \psi^{\mathbf{k}_{j+1}}\right| = \left|(1 - (\lambda \eta^{\mathbf{k}_j})^{-1}) / (\eta^{\mathbf{k}_{j+1} - \mathbf{k}_j} - (\lambda \eta^{\mathbf{k}_j})^{-1})\right| \le \tfrac{1+1/6}{18-1/6} < \tfrac{1}{15},$$

$$1 - \tfrac{1}{15} < \left|1 - \psi^{\mathbf{k}_j} / \psi^{\mathbf{k}_{j+1}}\right| < 1 + \tfrac{1}{15}.$$

Furthermore, for $z \in \mathbb{C}$ with $|z| \le \frac{1}{4}$, and with $\log(\ \ )$ denoting the principal branch, the simple inequality

$$\tfrac{5}{6}|z| \le |\log(1 \pm z)| \le \tfrac{7}{6}|z|,$$

and the relation $1-\eta^{\mathbf{k}_{j+1}-\mathbf{k}_j}/\psi^{\mathbf{k}_{j+1}-\mathbf{k}_j} = \lambda^{-1}\eta^{-\mathbf{k}_j}(1-\psi^{\mathbf{k}_j-\mathbf{k}_{j+1}})$, imply

$$\tfrac{5}{6}(1-\tfrac{1}{15})|\lambda\eta^{\mathbf{k}_j}|^{-1} \le |\log\bigl(1-(1-\eta^{\mathbf{k}_{j+1}-\mathbf{k}_j}/\psi^{\mathbf{k}_{j+1}-\mathbf{k}_j})\bigr)| \le \tfrac{7}{6}(1+\tfrac{1}{15})|\lambda\eta^{\mathbf{k}_j}|^{-1}.$$

So there are rational integers $h_1, \dots, h_{t+1}$ for which

$$\tfrac{5}{6}(1-\tfrac{1}{15})|\lambda\eta^{\mathbf{k}_j}|^{-1} \le |2\pi i h_j + \sum_{i=0}^{t-1}(k_{i,j+1}-k_{i,j})\log(\eta_i/\psi_i)| \le \tfrac{7}{6}(1+\tfrac{1}{15})|\lambda\eta^{\mathbf{k}_j}|^{-1}.$$

From Siegel's Lemma we deduce that there exist rational integers $z_1, \dots, z_{t+1}$, not all zero, so that for $i=0,\dots,t-1$

$$\sum_{j=1}^{t+1} z_j(k_{i,j+1}-k_{i,j}) = 0 \quad \text{and} \quad \max_{1\le j\le t+1}|z_j| \le (t+1)^{t/2}K^t.$$

Now for $j=1,\dots,t+1$ set

$$\Lambda_j = 2\pi i h_j + \sum_{i=0}^{t-1}(k_{i,j+1}-k_{i,j})\log(\eta_i/\psi_i),$$

and write $Z=\max_{1\le j\le t+1}|z_j|$, and $K_1 = \frac{45}{8}(t+1)^{t/2}K^t$. Then $\Lambda_j \ne 0$ and

$$\sum_{j=1}^{t+1} z_j\Lambda_j = 2\pi i\sum_{j=1}^{t+1} z_j h_j.$$

Furthermore,

$$\frac{|\Lambda_j|}{|\Lambda_{j+1}|} > \frac{\frac{5}{6}(1-\frac{1}{15})}{\frac{7}{6}(1+\frac{1}{15})}\left|\frac{\eta^{\mathbf{k}_{j+1}}}{\eta^{\mathbf{k}_j}}\right| = \tfrac{5}{8}\left|\frac{\eta^{\mathbf{k}_{j+1}}}{\eta^{\mathbf{k}_j}}\right| \ge K_1 > 15,$$

for $j=1,\dots,t+1$.

Now let l be the smallest positive integer for which $z_l \ne 0$. Then

$$\begin{aligned}
|\sum_{j=1}^{t+1} z_j\Lambda_j| = |\sum_{j=l}^{t+1} z_j\Lambda_j| &\ge |z_l||\Lambda_l| - Z(|\Lambda_{l+1}|+\dots+|\Lambda_{t+1}|)\\
&\ge |\Lambda_l| - (t+1)^{t/2}K^t|\Lambda_l|\left(\frac{1}{K_1}+\frac{1}{K_1^2}+\dots\right)\\
&= |\Lambda_l|(1-(t+1)^{t/2}K^t(K_1-1)^{-1}) > 0.
\end{aligned}$$

Therefore,

$$\begin{aligned}
2\pi \le |\sum_{j=l}^{t+1} z_j\Lambda_j| &\le Z(|\Lambda_{l+1}|+\dots+|\Lambda_{t+1}|)\\
&\le Z|\Lambda_1|\left(1+\frac{1}{K_1}+\frac{1}{K_1^2}+\dots\right) \le |\Lambda_1|Z/(1-\tfrac{1}{15})\\
&\le \tfrac{7}{6}(1+\tfrac{1}{15})|\lambda\eta^{\mathbf{k}_1}|^{-1}(t+1)^{t/2}K^t \times \tfrac{15}{14},
\end{aligned}$$

which proves Lemma 1.

Of course, the absolute constants given here can certainly be improved a little, but doing that would not change the proof of the Theorem.

In the sequel m^+ denotes $\max\{|m|, 3\}$.

Lemma 2. *All solutions x, y to the equation* (1) *satisfy*

$$\log(\max\{|x|,|y|\}) < 3^{3(n+9)} n^{18(n+1)} 2^{2(n-1)^2} M^{2n-2}((n-1)\log 2 + \log M)^{2n-1} \log m^+.$$

Proof. See [4], Theorem 3, §3.3, noting that $H \le 2^{n-1} M$.

Let $\mathbb{K}$ be an algebraic number field of degree n and discriminant $D_{\mathbb{K}}$. Denote by S a finite set of absolute values of $\mathbb{K}$, including the set S_∞ of all the archimedean values. Set $t = \operatorname{Card} S$. Let P be the maximum of the norms of the prime ideals corresponding to nonarchimedean values of S (if $S = S_\infty$ we set $P = 2$). As usual, a nonzero element $\gamma \in \mathbb{K}$ is said to be an S-unit if $|\gamma|_v = 1$ for all $v \notin S$. The S-units of $\mathbb{K}$ form a finitely generated multiplicative subgroup U_S of $\mathbb{K}^*$.

The symbol $h(\ )$ denotes the absolute logarithmic height.

Lemma 3. *There are S-units $\pi_1, \ldots, \pi_{t-1}$ in $\mathbb{K}$ so that each $\gamma \in U_S$ can be written as a product*

$$\gamma = \rho \pi_1^{k_1} \cdots \pi_{t-1}^{k_{t-1}},$$

with ρ a root of unity and

$$\max_{1 \le i \le t-1} |k_i| \le (t!)^2 \big(\log(3n)\big)^3 h(\gamma).$$

Proof. This follows from relation (26) in [3].

Lemma 4. *Let α be a zero of the polynomial $F(X,1)$ and let $D_{\mathbb{K}}$, $R_{\mathbb{K}}$, $h_{\mathbb{K}}$ denote the discriminant, regulator and class number of the field $\mathbb{K} = \mathbb{Q}(\alpha)$, respectively. Then*

$$|D_{\mathbb{K}}| \le n^n M^{2n-2}, \qquad h_{\mathbb{K}} R_{\mathbb{K}} < n^{4n} M^{2(n-1)}, \quad \textit{and} \quad 0.056 < R_{\mathbb{K}}.$$

Proof. We note that $D_{\mathbb{K}}$ divides the discriminant of $F(X,1)$, so the upper bound for the discriminant follows from an estimate of Mahler [6], Theorem 1, p. 261. The upper bound for the product of the class number by the regulator may be deduced from a result of Siegel's [7], Satz 1, p. 72. Finally the lower bound for the regulator is due to Zimmert [8], Korollar, p. 375.

We denote the maximum of the absolute values of the conjugates of an algebraic number α by $\overline{|\alpha|}$ (Kurt Mahler called this 'house' of α).

Lemma 5. *Let α be a non-zero element in $\mathbb{K}$ with $N_{\mathbb{K}/\mathbb{Q}}(\alpha) = N$. There exists a unit ϵ such that*

$$\overline{|\alpha\epsilon|} \leq N^{1/n} \exp\left\{\left(6rn^2/\log n\right)^r \tfrac{1}{2} r R_{\mathbb{K}}\right\},$$

where r is the unit rank of $\mathbb{K}$.

Proof. See [5], Lemma 3.

Lemma 6. *Set $C = 2m(2\sqrt{n}M)^n$ and assume $y \neq 0$. Then*

$$\min_{\alpha, F(\alpha,1)=0} \min\left(1, |\alpha - x/y|\right) \leq \frac{C}{2(\max(|x|,|y|))^n}$$

Proof. See [1], Lemma 1.

Remark. If $y^n > C/2$ then obviously

$$\min_{\alpha, F(\alpha,1)=0} |\alpha - x/y| \leq C/2y^n.$$

Consider two distinct solutions (x, y), (x', y') with $y' \geq y > (C/2)^{1/n}$ such that

$$|\alpha_1 - x/y| = \min_i |\alpha_i - x/y| \quad \text{and} \quad |\alpha_1 - x'/y'| = \min_i |\alpha_i - x'/y'|.$$

Then we have

$$\frac{1}{yy'} \leq \left|\frac{x}{y} - \frac{x'}{y'}\right| \leq \left|\frac{x}{y} - \alpha_1\right| + \left|\alpha_1 - \frac{x'}{y'}\right| \leq \frac{C}{2y^n} + \frac{C}{2y'^n} \leq \frac{C}{y^n}.$$

Hence

$$\frac{y^{n-1}}{C} \leq y'.$$

From now on we denote the zeros of the polynomial $F(X,1)$ by $\alpha_1, \ldots, \alpha_n$. If $(x_1, y_1), \ldots, (x_j, y_j)$ are solutions to (1) satisfying $(C/2)^{1/n} < y_1 \leq \ldots \leq y_j$, and for $k = 1, \ldots, j$,

$$\min_{1 \leq i \leq n} |\alpha_i - x_k/y_k| = |\alpha_1 - x_k/y_k|,$$

then by induction we obtain, compare the *strong gap principle* at [1], p. 73,

$$\left(y_1 \,/\, C^{1/(n-2)}\right)^{(n-1)^{j-1}} \leq y_j.$$

Lemma 7. *Suppose $y_1 \geq 20n^2(M^n m)^{\mu(n)}$, where $\mu(n) = (n-2)^{-1} + (n-1)^{-2}$. Set $c_1 = n(n-1)^{j-3} - (n^2 + 3n)$, $c_2 = \frac{1}{2}n(n-1)^{j-3} - \frac{1}{2}n^2$, $c_3 = n^2(n-1)^{j-3} - n^2$, and $c_4 = n(n-1)^{j-3} - n$; and write*

$$R_j = \left|\frac{x_{j+1} - \alpha_2 y_{j+1}}{x_{j+1} - \alpha_1 y_{j+1}}\right| \Big/ \left|\frac{x_j - \alpha_2 y_j}{x_j - \alpha_1 y_j}\right|.$$

Then for $j > 4$ we have

(a) $y_j > (2\sqrt{n} m M^n)^{(n-1)^{j-3}}$;

(b) $\frac{1}{2}y_j|\alpha_i-\alpha_1| \le |x_j-\alpha_i y_j| \le \frac{3}{2}y_j|\alpha_i-\alpha_1|$ *for* $i = 2, 3. \ldots, n$;
(c) $R_j \ge 2^{c_1}n^{c_2}M^{c_3}m^{c_4}$; *and*
(d) $|\alpha_1-\alpha_3|/|\alpha_2-\alpha_3| \cdot |x_j-\alpha_2 y_j|/|x_j-\alpha_1 y_j| \ge \frac{1}{2}\cdot y_j^n/(2nM^3)^{n-1} \ge 6$.

Proof. a) On noting that, for $n \ge 3$,

$$2^{\frac{n+1}{n-2}+\frac{1}{(n-1)^2}} < 20 \quad \text{and} \quad (\sqrt{n})^{\frac{n}{n-2}+\frac{1}{(n-1)^2}} < n^2,$$

and since

$$y_1 > C^{1/(n-2)}(2\sqrt{n}mM^n)^{\frac{1}{(n-1)^2}} = 2^{\frac{n+1}{n-2}+\frac{1}{(n-1)^2}}(\sqrt{n})^{\frac{n}{n-2}+\frac{1}{(n-1)^2}}(M^n m)^{\frac{1}{n-2}+\frac{1}{(n-1)^2}},$$

we deduce that

$$\left(y_1\cdot C^{-1/(n-2)}\right)^{(n-1)^2} > 2\sqrt{n}mM^n,$$

which proves inequality (a).

b) Let a denote the leading coefficient of the polynomial $F(X,1)$. From a result of Bombieri and Schmidt [1] (p. 72, proof of Lemma 1), we deduce that

$$\prod_{i=2}^{n}|\alpha_i-\alpha_1| = |F'(\alpha_1,1)|/|a| \ge |F'(\alpha_1,1)|/M \ge n^{-(n-1)/2}M^{-(n-1)}.$$

But, for $2 \le k \le n$, we have $\prod_{i=2, i\ne k}^{n}|\alpha_i-\alpha_1| \le (2M)^{n-2}$, whence

$$|\alpha_k-\alpha_1| \ge n^{-(n-1)/2}2^{-(n-2)}M^{-2n+3}.$$

Moreover

$$y_j|\alpha_k-\alpha_1| \ge (2\sqrt{n}M^n m)^{(n-1)^{j-3}}n^{-(n-1)/2}2^{-(n-2)}M^{-2n+3} > 1.$$

Now Lemma 6 yields

$$|x_j-\alpha_1 y_j| \le \frac{C}{2(2\sqrt{n}M^n m)^{(n-1)^{j-3}(n-1)}} \le \tfrac{1}{2},$$

and, finally, the inequalities

$$|x_j-\alpha_i y_j| \le |x_j-\alpha_1 y_j| + |\alpha_i-\alpha_1|y_j \quad \text{and} \quad |x_j-\alpha_i y_j| \ge |\alpha_i-\alpha_1|y_j - |x_j-\alpha_1 y_j|$$

complete the proof of inequality (b).

c) Using the inequalities (b) we have, for $2 \le i \le n$,

$$\left|\frac{x_{j+1}-\alpha_i y_{j+1}}{x_j-\alpha_i y_j}\right| \ge \frac{\frac{1}{2}|\alpha_i-\alpha_1|y_{j+1}}{\frac{3}{2}|\alpha_i-\alpha_1|y_j} = \frac{y_{j+1}}{3y_j}.$$

Hence

$$\left|\frac{x_j-\alpha_1 y_j}{x_{j+1}-\alpha_1 y_{j+1}}\right| = \frac{\frac{m}{|a|}\prod_{i=2}^{n}|x_{j+1}-\alpha_i y_{j+1}|}{\frac{m}{|a|}\prod_{i=2}^{n}|x_j-\alpha_i y_j|} \ge \left(\frac{y_{j+1}}{3y_j}\right)^{n-1}.$$

Thus we obtain

$$R_j \ge \left(\frac{y_{j+1}}{3y_j}\right)^n \ge \left(\frac{y_j^{n-2}}{3C}\right)^n \ge \left(\frac{y_j}{3C}\right)^n > \left(\frac{(2\sqrt{n}M^n m)^{(n-1)^{j-3}}}{8(2\sqrt{n}M)^n m}\right)^n,$$

and this gives the announced values for the exponents c_1, c_2, c_3, and c_4.

d) Define

$$S_j = \frac{|\alpha_1 - \alpha_3|}{|\alpha_2 - \alpha_3|} \cdot \frac{|x_j - \alpha_2 y_j|}{|x_j - \alpha_1 y_j|}.$$

We bound S_j from below as follows. Using (b) twice, we first obtain

$$S_j \geq \frac{|\alpha_1 - \alpha_3|}{|\alpha_1 - \alpha_2| + |\alpha_1 - \alpha_3|} \cdot \frac{\frac{1}{2} y_j |\alpha_2 - \alpha_1|}{|x_j - \alpha_1 y_j|},$$

and next we find that

$$\frac{m}{|a|} = |x_j - \alpha_1 y_j| \cdot |x_j - \alpha_2 y_j| \cdots |x_j - \alpha_n y_j| \geq |x_j - \alpha_1 y_j| \cdot \frac{y_j^{n-1}}{2^{n-1}} \cdot |\alpha_2 - \alpha_1| \cdots |\alpha_n - \alpha_1|.$$

Hence we have

$$\frac{1}{|x_j - \alpha_1 y_j|} \geq \frac{y_j^{n-1}}{2^{n-1}} \cdot \frac{|a|}{m} \cdot |\alpha_2 - \alpha_1| \cdots |\alpha_n - \alpha_1| \geq \frac{y_j^{n-1}}{2^{n-1}} \cdot |F'(\alpha_1, 1)|,$$

and therefore

$$S_j \geq \frac{y_j^n}{2^n} \cdot \frac{|F'(\alpha_1, 1)|}{\frac{1}{|\alpha_2 - \alpha_1|} + \frac{1}{|\alpha_3 - \alpha_1|}}.$$

Combining this lower bound with

$$|F'(\alpha_1, 1)| \geq n^{-(n-1)/2} M^{-(n-2)}$$

and

$$\frac{1}{|\alpha_2 - \alpha_1|} + \frac{1}{|\alpha_3 - \alpha_1|} \leq 2n^{(n-1)/2} 2^{n-2} M^{2n-3},$$

we deduce that

$$S_j \geq \frac{y_j^n}{2^{2n-1} n^{n-1} M^{3n-5}}.$$

This proves the first part of the bound (d). The second part then follows from (a).

3. Proof of the Theorem

We fix an arbitrary solution (x, y) to (1) satisfying (2) and with $y > 0$. Recall that $\mu(n) = (n-2)^{-1} + (n-1)^{-2}$. We first show that

$$y \geq 20 n^2 M^4 m^{\mu(n)}. \tag{3}$$

Indeed, if $|x| \leq |y|$, then (3) is a consequence of (2), while if $\max\{|x|, |y|\} = |x|$, then there is a zero α of $F(X, 1)$ such that

$$m^{1/n} \geq (m/|a|)^{1/n} \geq |x - \alpha y| \geq |x| - |\alpha| y \geq 21 n^2 M^5 m^{\mu(n)} - My.$$

Therefore, $y \geq M^{-1}(21 n^2 M^5 m^{\mu(n)} - m^{1/n})$, which implies (3).

For $k = 1, \ldots, n$, let $(x_1, y_1), \ldots, (x_{N_k}, y_{N_k})$ be the sequence of solutions to (1) satisfying

$$20 n^2 M^4 m^{\mu(n)} \leq y_1 \leq y_2 \leq \ldots \leq y_{N_k},$$

with

$$|\alpha_k - x_j/y_j| = \min_i |\alpha_i - x_j/y_j|\,, \qquad (1 \le j \le N_k).$$

There are at most n solutions (x, y) of (1) with $y = 0$. Therefore the number of solutions of (1) is bounded by $N_1 + \cdots + N_n + n$. It now suffices to prove $N_k \le 2n(s+1) + 12$, for each k, and by symmetry, for some k. Thus we produce the desired upper bound only for N_1. Therefore, from now on, we consider only solutions (x, y) of (1) for which

$$\min_{1 \le i \le n} |\alpha_i - x/y| = |\alpha_1 - x/y|\,.$$

For clarity we divide the argument into four steps.

Step 1 (On the ideal factors of $x - \alpha_1 y$). Set $\mathbb{K} = \mathbb{Q}(\alpha_1)$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_{s_1}$ be the distinct (finite) prime divisors of m in $\mathbb{K}$. Then the integer s_1 satisfies

$$0 \le s_1 \le ns \le n \log_2 m,$$

where $\log_2$ denotes the logarithm to base 2.

Let $\mathfrak{A}$ denote the denominator of the principal ideal $\langle \alpha_1 \rangle_{\mathbb{K}}$. Then $\mathfrak{A}$ can uniquely be written in the form

$$\mathfrak{A} = \mathfrak{A}_1 \cdot \mathfrak{A}_2,$$

where $\mathfrak{A}_1$ and m are relatively prime and where every prime divisor of $\mathfrak{A}_2$ divides m (that is, $\mathfrak{A}_1$ is the m-free part of $\mathfrak{A}$). For a prime $\mathfrak{P}$ of $\mathbb{K}$, denote by $v_{\mathfrak{P}}$ the corresponding valuation (both of an element of $\mathbb{K}$, and of an ideal of $\mathbb{K}$). Since $\mathfrak{A}(x - \alpha_1 y)$ is an integral ideal of $\mathbb{K}$, we have $v_{\mathfrak{P}}(x - \alpha_1 y) \ge -v_{\mathfrak{P}}(\mathfrak{A})$ for any $\mathfrak{P}$. Further, since $\mathfrak{A} \,|\, a$, we also have $v_{\mathfrak{P}}(\mathfrak{A}) \le v_{\mathfrak{P}}(a)$. Moreover, since $F(X, Y)$ is the product of $X - \alpha_1 Y$ by a form whose coefficients are algebraic integers of $\mathbb{K}$, we must have $v_{\mathfrak{P}}(x - \alpha_1 y) \le v_{\mathfrak{P}}(m)$. Therefore we may write

$$\langle x - \alpha_1 y \rangle_{\mathbb{K}} = \mathfrak{A}_1^{-1} \mathfrak{p}_1^{l_1} \cdots \mathfrak{p}_{s_1}^{l_{s_1}}\,, \tag{4}$$

where the exponents $l_i = v_{\mathfrak{p}_{s_i}}(x - \alpha_1 y)$ are rational integers which satisfy

$$\mathfrak{p}_i^{-l_i} | a \quad \text{if} \quad l_i < 0, \quad \text{or} \quad \mathfrak{p}_i^{l_i} | m \quad \text{if} \quad l_i > 0.$$

Thus we get the bound

$$\max_{1 \le i \le s_1} |l_i| \le \log_2 |am|^n \le n \log_2 (Mm).$$

Step 2 (On the application of Lemmas 2, 3, 4, and 5). Let $h_{\mathbb{K}}$ be the ideal class number of $\mathbb{K}$. From Lemma 5 we see that there is a generator τ of the ideal $\left(\mathfrak{A}_1^{-1}\right)^{h_{\mathbb{K}}}$ satisfying

$$\overline{\lvert\tau\rvert} \le \left(N(\mathfrak{A}_1^{-1})\right)^{h_{\mathbb{K}}/n} \cdot \exp\left\{ \left(6rn^2/\log n\right)^r \tfrac{1}{2} r R_{\mathbb{K}} \right\},$$

and that for $i = 1, \ldots, s_1$ there are generators π_i of the ideals $\mathfrak{p}_i^{h_{\mathbb{K}}}$, respectively, so that

$$\overline{\lvert\pi_i\rvert} \le \left(N(\mathfrak{p}_i)\right)^{h_{\mathbb{K}}/n} \cdot \exp\left\{ \left(6rn^2/\log n\right)^r \tfrac{1}{2} r R_{\mathbb{K}} \right\}.$$

But the inequalities

$$r < n, \quad N(\mathfrak{A}_1^{-1}) \leq |a| \leq M, \quad N(\mathfrak{p}_i) \leq m, \quad R_{\mathbb{K}} \leq h_{\mathbb{K}} R_{\mathbb{K}} \leq n^{4n} M^{2(n-1)},$$
$$\text{and} \quad h_{\mathbb{K}} \leq (0.056)^{-1} n^{4n} M^{2(n-1)} < 20 n^{4n} M^{2(n-1)}$$

imply

$$\max\{\lceil\tau\rceil, \lceil\pi_i\rceil\} \leq (mM)^{h_{\mathbb{K}}/n} \exp\left\{ \left(6n^3/\log n\right)^n \tfrac{1}{2} n \cdot n^{4n} M^{2(n-1)} \right\}.$$

Hence

$$\log\max\{\lceil\tau\rceil, \lceil\pi_i\rceil\} \leq 20 n^{4n-1} M^{2(n-1)} \log(mM) + 6^n n^{7n+1} M^{2(n-1)}$$
$$\leq n^{9n} M^{2n-2} \log(m^+ M).$$

By taking the $h_{\mathbb{K}}$-th power of (4) we get

$$(x - \alpha_1 y)^{h_{\mathbb{K}}} = \epsilon \tau \pi_1^{l_1} \cdots \pi_{s_1}^{l_{s_1}}, \tag{5}$$

where ϵ is an ordinary unit in $\mathbb{K}$. We need an upper bound for the height of ϵ. First, we estimate the height of $x - \alpha_1 y$. We claim that

$$h(x - \alpha_1 y) \leq 3^{2n^2 - n + 21} n^{20(n+1)} M^{4n} \log m^+. \tag{6}$$

The proof of (6) rests on Lemma 2. Indeed, according to this Lemma, we have

$$h(x - \alpha_1 y) \leq h(\alpha_1) + \log(|x| + |y|)$$
$$\leq 2 \cdot 3^{3(n+9)} n^{18(n+1)} 2^{2(n-1)^2} M^{2n-2} ((n-1)\log 2 + \log M)^{2n-1} \log m^+.$$

The claim (6) then follows from

$$3^{3n+27} 2^{2(n-1)^2+1} ((n-1)\log 2 + \log M)^{2n-1} \leq 3^{2n^2-n+21} n^{2(n+1)} M^{2(n+1)}.$$

Next we notice that

$$h(\tau \pi_1^{l_1} \cdots \pi_{s_1}^{l_{s_1}}) \leq n^{9n+5} M^{2n-1} (\log m^+)(\log(m^+ M))^2.$$

But this is a consequence of the inequalities $s_1 \leq n \log_2 m$, $\max |l_i| \leq n \log_2(mM)$,

$$\max\{h(\tau), h(\pi_i)\} \leq n \log\max\{\lceil\tau\rceil, \lceil\pi_i\rceil\} \leq n^{9n+1} M^{2n-1} \log m^+$$

and

$$1 + n^2 (\log_2 m) \log_2(mM) \leq n^4 (\log m^+) \log(m^+ M).$$

From these two upper bounds we deduce the desired estimate for the height of ϵ, namely

$$h(\epsilon) \leq h_{\mathbb{K}} h(x - \alpha_1 y) + h(\tau \pi_1^{l_1} \cdots \pi_{s_1}^{l_{s_1}}) \leq n^{2n^2+23n+44} M^{6n-2} (\log m^+)^3.$$

Let ρ_0 be a generator of the group of roots of unity in $\mathbb{K}$. For later purposes we denote the order of ρ_0 by $w_{\mathbb{K}}$. Applying Lemma 3, we produce a fundamental system of units for $\mathbb{K}$, say $\epsilon_1, \ldots, \epsilon_r$, such that ϵ can be written in the form

$$\epsilon = \rho_0^{q_0} \epsilon_1^{q_1} \cdots \epsilon_r^{q_r},$$

with

$$\max_{0\le i\le r}(|q_i|) \le ((r+1)!)^2 (\log(3n))^3\, h(\epsilon)$$
$$\le n^{4n}\cdot n^{2n^2+23n+44}M^{6n-2}(\log m^+)^3$$
$$\le n^{2n^2+27n+44}M^{6n-2}(\log m^+)^3.$$

We choose an automorphism σ_i of $\mathbb{C}$ for each $i = 1, \ldots, n$, such that $\sigma_i(\alpha_1) = \alpha_i$. Then we obtain

$$\left(\frac{x-\alpha_i y}{x-\alpha_1 y}\right)^{h_{\mathbb{K}}} = \frac{\sigma_i(\epsilon\tau\pi_1^{l_1}\cdots\pi_{s_1}^{l_{s_1}})}{\epsilon\tau\pi_1^{l_1}\cdots\pi_{s_1}^{l_{s_1}}}.$$

Step 3 (On the way to the application of Lemma 1). Set $t = r + s_1 + 2$. Then we have

$$t \le n(s+1)+1 \le n(1+\log_2 m^+)+1 \le 3n\log m^+.$$

Now define

$$\lambda = \frac{\alpha_3-\alpha_1}{\alpha_3-\alpha_2}, \qquad \mu = \frac{\alpha_1-\alpha_2}{\alpha_3-\alpha_2}$$

and write $\eta_1 = (\sigma_2(\tau)/\tau)^{1/h_{\mathbb{K}}}$, $\eta_2 = (\sigma_2(\epsilon_1)/\epsilon_1)^{1/h_{\mathbb{K}}}$, …, $\eta_{r+1} = (\sigma_2(\epsilon_r)/\epsilon_r)^{1/h_{\mathbb{K}}}$; $\eta_{r+2} = (\sigma_2(\pi_1)/\pi_1)^{1/h_{\mathbb{K}}}$, …, $\eta_{r+s_1+1} = (\sigma_2(\pi_{s_1})/\pi_{s_1})^{1/h_{\mathbb{K}}}$ and $\psi_1 = (\sigma_3(\tau)/\tau)^{1/h_{\mathbb{K}}}$, $\psi_2 = (\sigma_3(\epsilon_1)/\epsilon_1)^{1/h_{\mathbb{K}}}$, …, $\psi_{r+1} = (\sigma_3(\epsilon_r)/\epsilon_r)^{1/h_{\mathbb{K}}}$, $\psi_{r+2} = (\sigma_3(\pi_1)/\pi_1)^{1/h_{\mathbb{K}}}$, …, $\psi_{r+s_1+1} = (\sigma_3(\pi_{s_1})/\pi_{s_1})^{1/h_{\mathbb{K}}}$, where the $h_{\mathbb{K}}$-th roots are fixed. Further, set $k_1 = q_0$, $k_2 = q_1$, …, $k_{r+1} = q_r$, $k_{r+2} = l_1$, …, $k_{r+s_1+1} = l_{s_1}$.

Eliminating x and y between the three linear forms $x-\alpha_1 y$, $x-\alpha_2 y$, and $x-\alpha_3 y$ yields (the so-called) *Siegel's identity*

$$(\alpha_1-\alpha_2)(x-\alpha_3 y)+(\alpha_2-\alpha_3)(x-\alpha_1 y)+(\alpha_3-\alpha_1)(x-\alpha_2 y)=0,$$

or

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

That is,

$$\lambda\,(\sigma_2(\rho)/\rho)^{k_0}\,\eta_1^{k_1}\cdots\eta_{t-1}^{k_{t-1}}+\mu\,(\sigma_3(\rho)/\rho)^{k_0}\,\psi_1^{k_1}\cdots\psi_{t-1}^{k_{t-1}}=1, \tag{7}$$

where ρ is a $w_{\mathbb{K}}h_{\mathbb{K}}$-th primitive root of unity, and $k_0 \le \omega_{\mathbb{K}}h_{\mathbb{K}}$.

Notice that none of λ, μ, ρ, η_1, …, η_{t-1}, ψ_1, …, ψ_{t-1}, nor σ_2, σ_3 depend on the selected solution of (1). Moreover, the mapping $(x,y)\to(k_0,k_1,\ldots,k_{t-1})$ is injective. Indeed, $(x-\alpha_1 y)^{h_{\mathbb{K}}} = (x'-\alpha_1 y')^{h_{\mathbb{K}}}$, with x, y, x', y in $\mathbb{Z}$, implies $x = x'$ and $y = y'$; notice that α_1 is real and that y, y' are positive. Therefore we obtain at least N_1 distinct solutions $(k_0,\ldots,k_{t-1})$ to (7).

Step 4 (Final step). We define the integer K as in Lemma 1. Hence

$$K \le 2\max_{0\le i\le t-1}\max\{2,|k_i|\} \le 2n^{2n^2+27n+44}M^{6n-2}(\log m^+)^3$$
$$\le n^{2n^2+27n+45}M^{6n-2}(\log m^+)^3.$$

With the notation of Lemma 1 and Lemma 7, we have

$$\eta^{k_j} = \frac{x_j - \alpha_2 y_j}{x_j - \alpha_1 y_j} \qquad \text{and} \qquad R_j = |\eta_{k_{j+1}}/\eta_{k_j}|.$$

However, in order to apply Lemma 1 we need to check the lower bounds

$$R_j \geq 9(t+1)^{t/2} K^t \qquad \text{and} \qquad |\lambda \eta^{k_1}| \geq 6.$$

The latter one follows from part (d) in Lemma 7. To prove the first, it is shown by part (c) of Lemma 7 that it suffices to notice that, for $j \geq t+10$, we have

$$2^{c_1} n^{c_2} M^{c_3} m^{c_4} \geq 9(3n \log m^+)^{t/2} (n^{2n^2+27n+45} M^{6n-2} (\log m^+)^3)^t,$$

where c_1, c_2, c_3 and c_4 (which depend on n and j) are defined in Lemma 7.

We assume $N_1 \geq 2t+11$, and apply Lemma 1 using the solutions (x_{t+10}, y_{t+10}), $\ldots$, (x_{2t+11}, y_{2t+11}). We obtain

$$\begin{aligned} |\lambda \eta^{k_{t+10}}| = \left| \frac{\alpha_3 - \alpha_1}{\alpha_3 - \alpha_2} \cdot \frac{x_{t+10} - \alpha_2 y_{t+10}}{x_{t+10} - \alpha_1 y_{t+10}} \right| &\leq \frac{1}{4}(t+1)^{t/2} K^t \\ &\leq \frac{1}{4}(3n \log m^+)^{t/2} (n^{2n^2+27n+45} M^{6n-2} (\log m^+)^3)^t. \end{aligned}$$

Finally, using part d) of Lemma 7 we get

$$\begin{aligned} \left| \frac{\alpha_3 - \alpha_1}{\alpha_3 - \alpha_2} \cdot \frac{x_{t+10} - \alpha_2 y_{t+10}}{x_{t+10} - \alpha_1 y_{t+10}} \right| &> \tfrac{1}{2} \left((2\sqrt{n} M^n m)^{(n-1)^{t+6} n} / 4nM^3 \right)^{n-1} \\ &= 2^{(n-1)^{t+7} n - 2n + 1} n^{\frac{1}{2}(n-1)^{t+7} n - (n-1)} M^{n^2 (n-1)^{t+7} - 3(n-1)} m^{n(n-1)^{t+7}}, \end{aligned}$$

which we see to be a contradiction on recalling that $t \geq 3$ and comparing the exponents of the absolute constant, and of n, M and m.

That means that N_1 is at most $2t+10$ and, as we saw at the beginning of the proof, this shows that the number of solutions of (1) satisfying (2) is at most $n(2t+11)$. This completes the proof of the Theorem.

Acknowledgements. The work of Béla Brindza was supported by grant D23992 from the Hungarian National Foundation for Scientific Research, and that of Ákos Pinter by grants 16975 and 19479 from the Hungarian National Foundation for Scientific Research and the Hungarian Academy of Sciences. Alf van der Poorten's research was supported in part by a grant from the Australian Research Council.

Added in proof. As kindly pointed out to us by Yann Bugeaud, one deduces from the proof of the first author's paper *On large values of binary forms*, Rocky Mountain J. Math. 26 (1996), 839–845, that the equation $|F(x,y)| = m$ has at most $6n$ solutions satisfying

$$H(x,y) \geq m^{1/(n-2)+1/(n-1)}.$$

References

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

[2] Brindza, B., On large values of binary forms. Rocky Mountain J. Math. 26 (1996), 839–845.

[3] Bugeaud, Y., Győry, K., Bounds for the solutions of unit equations. Acta Arith. 74 (1996), 67–80.

[4] — Bounds for the solutions of Thue-Mahler equations and norm form equations. Acta Arith. 74 (1996), 273–292.

[5] Győry, K., On the solutions of linear diophantine equations in algebraic integers in bounded norm. Ann. Univ. Sci. Budapest. Eötvös Sect. Math. 22/23 (1979–1980), 225–233.

[6] Mahler, K., An inequality for the discriminant of a polynomial. Michigan Math. J. 11 (1964), 257–262.

[7] Siegel, C.L., Abschätzung von Einheiten. Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II (1969), 71–86.

[8] Zimmert, R., Ideale kleiner Norm in Idealklassen und eine Regulatorabschätzung. Invent. Math. 62 (1981), 367–380.