[6] H. Niederreiter, *Distribution of Fibonacci numbers* mod 5^k, Fibonacci Quarterly 10 (1972), pp. 373–374.

[7] William A. Webb and Calvin T. Long, *Distribution modulo p^h of the general linear second order recurrence*, Atti. Accad. Naz. Lincei, Rend. Cl. Sci. fis. mat. nat., 58 (1975), pp. 92–100.

WASHINGTON STATE UNIVERSITY

Received on 22. 10. 1976
and in revised form on 24. 5. 1977 (884)

ACTA ARITHMETICA
XXXVI (1980)

On the greatest prime factor of (ax^m+by^n)

by

T. N. Shorey (Bombay, India)

1. Suppose that f is a polynomial with rational coefficients and has at least two distinct roots. Schinzel and Tijdeman [4] proved that the equation $y^m = f(x)$ (with $x, y, m \in \mathbf{Z}$, $|y| > 1$) implies that m is bounded. In [5], it is shown that the polynomial f can be replaced by a binary form $f(x, z)$ (where $f(1, 0) \neq 0$) with at least two distinct linear factors, with $(x, z) = 1$ and z composed solely of powers of primes from a fixed set. In this paper, we prove a generalization of this result. The purpose of this generalization is to strengthen Theorem 3 of [5] on the greatest prime factor of (ax^m+by^n). All these results depend on Gelfond–Baker theory of linear forms in logarithms.

2. For a real number c between 0 and 1 and for an integer m greater than 1, set

$$A = \max\left(2, \exp\left(c\left((\log m)(\log\log m)\right)^{1/2}\right)\right),$$
$$B = \max\left(2, c\left((\log m)(\log\log m)\right)^{1/2}\right).$$

Denote by S the set of all non zero integers composed of primes not exceeding B. Let $f(x, y) \in \mathbf{Q}[x, y]$ be a binary form of degree n with $f(1, 0) \neq 0$. Assume that $f(x, 1)$ has at least two distinct roots. We define the height of a rational number a/b, $(a, b) = 1$, as $\max(|a|, |b|)$. Assume that the maximum of the heights of the coefficients of f is not greater than A. Then we have:

THEOREM. *Let d be a positive integer. Then there exist effectively computable positive constants c, c_1 depending only on n and d such that the equation*

$$wz^m = f(x, y) \tag{1}$$

in integers m, w, x, y, z with $w \in S$, $y \in S$, $(x, y) = d$, $|z| > 1$ implies that

$$m < c_1.$$

The proof of the theorem depends on the results of Baker [2] and Van der Poorten [3] on linear forms in logarithms. As remarked earlier, the theorem generalizes the results of [4] and [5], Theorem 2. The results on the greatest prime factor of a polynomial or a binary form are used in [4] and [5]. We remark that the theorem does not depend on these results. This feature appears to be essential for the proof of the theorem on the lines of [4].

Denote by $P[x]$ the greatest prime factor of the integer x. An immediate consequence of the theorem is the following result that strengthens Theorem 3 of [5].

Corollary. *Let $n > 1$ be an integer. Let a and b be non zero integers. Then for all non zero integers x, y, m with $|x| > 1$, $(ax, by) = 1$ and $m > e^e$, we have*

$$P[ax^m + by^n] \gg_{a,b,n} \big((\log m)(\log\log m)\big)^{1/2},$$

where the constant implied by $\gg$ depends only on a, b, n and is effectively computable.

To prove the corollary from the theorem it suffices to write $ax^m + by^n = c'z^n$ for the smallest possible integer c' and to apply the theorem to the equation $ax^m = f(y, z) = -by^n + c'z^n$.

Proof of the theorem. We shall choose later suitably the constant c depending only on n and d. Here, and below, $c_2, c_3, \ldots$ denote effectively computable positive constants depending only on n and d. By straightforward simplifications, the equation (1) can be transformed to

$$vwz^m = g(x, y),$$

where v with $1 \leqslant v \leqslant A^{c_2}$ is an integer and

$$g(x, y) = (x - a_1 y)^{k_1} \ldots (x - a_q y)^{k_q}.$$

Here $k_1, \ldots, k_q$ are positive integers and $a_1, \ldots, a_q$ are distinct algebraic integers and $g(x, y)$ is a binary form with rational integer as coefficients which, in absolute value, do not exceed A^{c_3}. Observe that $\overline{|a_i|} \leqslant A^{c_4}$, $i = 1, \ldots, q$. Here $\overline{|a|}$ denotes the maximum of the absolute values of the conjugates of a.

Set $K = Q(a_1, \ldots, a_q)$ and $[K:Q] = N$. Then $N \leqslant n^n$. We suppose that there are r_1 real conjugate fields of K and $2r_2$ complex conjugate fields of K and that they are chosen in the usual manner. If a is in K, then $a^{(i)}$ is real, $1 \leqslant i \leqslant r_1$ and

$$a^{(i+r_2)} = \overline{a^{(i)}}, \quad r_1 + 1 \leqslant i \leqslant r_1 + r_2.$$

Set $r = r_1 + r_2 - 1$. We can choose r independent units $\eta_1, \ldots, \eta_r$ such that

$$\prod_{j=1}^{r} \log \overline{|\eta_j|} \leqslant c_5 R, \tag{2}$$

where R denotes the regulator of the field K. (For this choice, see Stark [7], p. 253.)

We can assume that m exceeds a sufficiently large integer depending only on n and d. Denote by D and h the discriminant and class number, respectively, of the field K. It is easy to check that $|D| \leqslant A^{c_6}$. From this inequality and from a result of Siegel [6], it follows that $R \leqslant A^{c_7}$. Further it follows that $h \leqslant A^{c_8}$.

Denote by $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ all the prime ideals of K which divide the integers in S or the ideal $[v] \prod_{1 \leqslant i < j \leqslant q} [a_i - a_j]$. Observe that the absolute value of the norm of the ideal $[v] \prod_{1 \leqslant i < j \leqslant q} [a_i - a_j]$ does not exceed A^{c_9}. Further the number of primes not greater than B does not exceed $2c(\log m)^{1/2}(\log\log m)^{-1/2}$. Thus

$$t \leqslant c_{10}\, c (\log m)^{1/2} (\log\log m)^{-1/2}. \tag{3}$$

Put $\beta_i = x - a_i y$ for $1 \leqslant i \leqslant q$ and $[\pi_k] = \mathfrak{p}_k^h$ for $1 \leqslant k \leqslant t$. Observe that $\log|\mathrm{Norm}(\pi_k)| \leqslant A^{c_{11}}$. Set $s = m/(m, \{k_1, \ldots, k_q\})$, where $\{k_1, \ldots, k_q\}$ denotes the least common multiple of $k_1, \ldots, k_q$. Refer to [5] for details and conclude that

$$\beta_i^h = \varrho_i \prod_{j=1}^{r} \eta_j^{b_{i,j}} \prod_{k=1}^{t} \pi_k'^{u_{i,k}} \gamma_i^s,$$

where ϱ_i is a root of unity of K, $b_{i,j} \in \mathbf{Z}$, $u_{i,j}$ are non-negative integers and γ_i is an integer of K. Further π_k' is an associate on π_k and

$$\log \overline{|\pi_k'|} \leqslant \log|\mathrm{Norm}(\pi_k)| + c_{12} R \leqslant A^{c_{13}}. \tag{4}$$

By incorporating every sth power in γ_i, we may assume that the integers $b_{i,j}$ and $u_{i,j}$ satisfy

$$0 \leqslant b_{i,j} < s, \quad 0 \leqslant u_{i,j} < s. \tag{5}$$

Set

$$\max(|\gamma_1^{(\tau)}|, |\gamma_2^{(\tau)}|) = \max_{\sigma} \max(|\gamma_1^{(\sigma)}|, |\gamma_2^{(\sigma)}|),$$

where the maximum is taken over all the embeddings of K. If $\beta_1^h = \beta_2^h$, then by the argument of [5], we conclude that $\log\max(|x|, |y|) \leqslant A^{c_{14}}$. Now it follows from (1) that $m < c_{15}$. Hence we can assume that $\beta_1^h \neq \beta_2^h$.

Let $\mathfrak{p}$ be any prime ideal of K dividing a rational prime $p \leqslant B$. We have

$$0 \neq |\beta_1^h - \beta_2^h|_{\mathfrak{p}} = |(x - a_1 y)^h - (x - a_2 y)^h|_{\mathfrak{p}} \leqslant |y|_{\mathfrak{p}}.$$

We can show that

$$\log\max(|\beta_1|_{\mathrm{p}}^{h}, |\beta_2|_{\mathrm{p}}^{h}) \geqslant -A^{c_{16}}.$$

Now it follows from a result of Van der Poorten ([3], Theorem 2) on p-adic linear forms in logarithms and from the inequalities $p \leqslant B$, (2), (3), (4), (5) that

$$|y| \leqslant \exp\big(m^{cc_{17}}\log\max(|\gamma_1^{(\tau)}|, |\gamma_2^{(\tau)}|)\big). \tag{6}$$

For this conclusion, we also require Lemma C of [5].

For convenience set $\alpha_1' = \alpha_1^{(\tau)}$, $\alpha_2' = \alpha_2^{(\tau)}$, $\beta_1' = \beta_1^{(\tau)}$, $\beta_2' = \beta_2^{(\tau)}$. We may assume that $|\beta_1'| \leqslant |\beta_2'|$. Then we have

$$|(\alpha_2' - \alpha_1')y| = |\beta_1' - \beta_2'| > \max(|\beta_1'|, |\beta_2'|)\left(\frac{1}{h}\right)\left|\frac{\beta_1'^h}{\beta_2'^h} - 1\right|. \tag{7}$$

It follows from the earlier estimates that

$$\max(|\beta_1'|, |\beta_2'|) > e^{-mA^{c_{18}}}\max(|\gamma_1^{(\tau)}|, |\gamma_2^{(\tau)}|)^{s/h}.$$

Now an application of Baker's result [2] on linear forms in logarithms gives

$$|(\alpha_2' - \alpha_1')y| > e^{-mA^{c_{18}}}\big(\max(|\gamma_1^{(\tau)}|, |\gamma_2^{(\tau)}|)\big)^{\frac{s}{h} - m^{cc_{19}}}.$$

Using (6), we get

$$|(\alpha_2' - \alpha_1')| > e^{-mA^{c_{18}}}\big(\max(|\gamma_1^{(\tau)}|, |\gamma_2^{(\tau)}|)\big)^{\frac{s}{h} - m^{cc_{20}}}. \tag{8}$$

Assume that

$$c < (2c_{20})^{-1}. \tag{9}$$

Now observe that $s/h > mA^{-c_{21}}$. Since the left-hand side of inequality (8) does not exceed $2A^{c_4}$, we obtain

$$\log\max(|\gamma_1^{(\tau)}|, |\gamma_2^{(\tau)}|) \leqslant A^{c_{22}}. \tag{10}$$

Combining (6) and (10), we get

$$\log|y| \leqslant m^{2cc_{17}}. \tag{11}$$

We can assume that

$$\log|x| > 2m^{2cc_{17}}, \tag{12}$$

otherwise $\log|f(x, y)| \leqslant 2nm^{2cc_{17}}$ and it follows from (1) that $m < c_{23}$ if we assume that

$$c < (4c_{17})^{-1}. \tag{13}$$

It follows from (11) and (12) that $\max(|\beta_1'|, |\beta_2'|) > \exp(\frac{3}{2}m^{2cc_{17}})$. Hence

by (7)

$$0 < |\beta_1'^h/\beta_2'^h - 1| < |x|^{-1/4}.$$

Applying again a result of Baker [2] on linear forms in logarithms, we claim that the left-hand side of the above inequality exceeds $\exp(-m^{cc_{24}})$. Thus we get $\log|x| \leqslant 4m^{cc_{24}}$.

If we take

$$c < (4c_{24})^{-1}, \tag{14}$$

we conclude, as earlier, from (1) that $m < c_{25}$. Now choose c with $0 < c < 1$ satisfying the inequalities (9), (13) and (14). This completes the proof of the theorem.

Remarks. (i) The theorem can be generalized further. For example, it is obvious from the proof that d can be taken to be less than A. The restriction on the greatest prime factor of the members of S can be considerably relaxed. We have not stated the theorem in this generality, as our main purpose is to prove the result on the greatest prime factor of $(ax^m + by^n)$.

(ii) It is not necessary to use the result of [6] for the proof of the theorem. We could have utilized the choice of units of [1].

References

[1] A. Baker, *Contributions to the theory of Diophantine equations: II The Diophantine equation $y^2 = x^3 + k$*, Phil. Trans. Roy. Soc. London, A 263 (1968), pp. 173–208.

[2] — *The theory of linear forms in logarithms, Advances in transcendence theory*, Academic Press, London and New York 1977.

[3] A. J. Van der Poorten, *Linear forms in logarithms in the p-adic case, Advances in transcendence theory*, Academic Press, London and New York 1977.

[4] A. Schinzel and R. Tijdeman, *On the equation $y^m = P(x)$*, Acta Arith. 31 (1976), pp. 199–204.

[5] T. N. Shorey, A. J. Van der Poorten, R. Tijdeman and A. Schinzel, *Applications of the Gelfond–Baker method to Diophantine equations, Advances in transcendence theory*, Academic Press, London and New York 1977.

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

[7] H. M. Stark, *Effective estimates of solutions of some Diophantine equations*, Acta Arith. 24 (1973), pp. 251–259.

SCHOOL OF MATHEMATICS
TATA INSTITUTE OF FUNDAMENTAL RESEARCH
Bombay, India

Received on 14. 12. 1976
and in revised form on 24. 5. 1977 (903)