Nieuw Archief voor Wiskunde (3) I, 113—122 (1953)

ON THE GREATEST PRIME FACTOR OF $ax^m + by^n$

BY

K. MAHLER

(Manchester)

A theorem by G. PÓLYA (Math. Z. 1, 1918, 143—148) and C. L. SIEGEL (Math. Z. 10, 1921, 173—213) states that if $f(x)$ is a polynomial with integral coefficients and at least two different zeros, then the greatest prime factor of $f(x)$ tends to infinity as the integer x increases indefinitely.

I proved (Math. Ann. 107, 1933, 691—730) the following more general result: „Let $F(x, y)$ be a binary form with integral coefficients which has at least three (real or complex) linear factors no two of which are proportional. Let the integers x and y be relatively prime. Then, as max $(|x|, |y|)$ tends to infinity, so does the greatest prime factor of $F(x, y)$".

Little is known about the greatest prime factors of the values of *non*-homogeneous polynomials in two variables. It has then perhaps some interest to study special polynomials. In this note, the following result will be established.

Theorem: *Let $m \geq 2$, $n \geq 3$, $a \neq 0$, and $b \neq 0$, be four integers, and let x and y be two integral variables which are relatively prime. Then, as max $(|x|, |y|)$ increases indefinitely, the greatest prime factor of $ax^m + by^n$ tends to infinity.*

The proof of this theorem is obtained essentially by generalizing that of Theorem 695 [1]) in E. LANDAU, Vorlesungen über Zahlentheorie 3, 61—64. However, it becomes necessary to make use not of the Thue-Siegel theorem, but of its $\mathfrak{p}$-adic generalization. In the

[1]) „Es sei $n \geq 3$ ganz rational; a, b, c, d ganz rational, $a \neq 0$, $b^2 - 4ac \neq 0$, $d \neq 0$. Dann hat die Diophantische Gleichung

$$ay^2 + by + c = dx^n$$

nur endlich viele Lösungen".

proof of the theorem the condition $(x, y) = 1$ will be replaced by the weaker one that (x, y) is bounded, and it will finally be shown that even less is required.

1. The proof is indirect; we assume the theorem is false and derive a contradiction.

Denote by $P_1, P_2, \ldots P_t$ an arbitrary finite set of primes, and by Π the set of all positive or negative integers of the form

$$\varepsilon P_1^{f_1} P_2^{f_2} \ldots P_t^{f_t}$$

where ε is $+1$ or -1 while $f_1, f_2, \ldots, f_t$ are arbitrary non-negative integers. We assume from now on:

„*There exists an infinite sequence S of different pairs of integers x, y with the following properties:*

$$(x, y) \text{ is bounded.} \tag{1}$$

$$\text{The integer } ax^m + by^n \text{ is either zero or contained in } \Pi.\text{''} \tag{2}$$

The theorem will be proved if it can be shown that these assumptions lead to a contradiction.

2. Since (x, y) is bounded and since $\max(|x|, |y|)$ tends to infinity as x, y run over S, there are in S only finitely many pairs x, y for which $y = 0$. For the same reasons, there are also at most finitely many pairs x, y in S satisfying $ax^m + by^n = 0$. For this equation requires that $\frac{x^m}{y^n} = -\frac{b}{a}$; but then (x, y) cannot be bounded unless both x and y are bounded.

We may therefore assume, without loss of generality, that the following further condition is satisfied:

$$y \neq 0 \text{ and } ax^m + by^n \neq 0 \text{ when } x, y \text{ is in } S. \tag{3}$$

3. The conditions (2) and (3) imply that for every pair x, y in S,

$$ax^m + by^n = \varepsilon P_1^{f_1} P_2^{f_2} \ldots P_t^{f_t},$$

where $\varepsilon = \mp 1$ and where $f_1, f_2, \ldots, f_t$ are non-negative integers. On dividing by m, these integers take the form

$$f_1 = g_1 m + h_1,\ f_2 = g_2 m + h_2,\ \ldots,\ f_t = g_t m + h_t;$$

here $g_1, g_2, \ldots, g_t$ are non-negative integers, and $h_1, h_2, \ldots, h_t$ are integers satisfying the inequalities

$$0 \leq h_1 < m,\ 0 \leq h_2 < m,\ \ldots,\ 0 \leq h_t < m.$$

Therefore, for all the pairs in S, the system of $t+1$ numbers

$$\varepsilon,\ h_1,\ h_2,\ \ldots,\ h_t$$

has not more than $2m^t$ possibilities. Since S may be replaced by any infinite subsequence, there is no loss of generality in assuming that

$$\varepsilon = \varepsilon^0,\ h_1 = h_1^0,\ h_2 = h_2^0,\ \ldots,\ h_t = h_t^0$$

assume fixed values for all pairs in S.

Put, for shortness,

$$c = \varepsilon^0 P_1^{h_1{}^0} P_2^{h_2{}^0} \ldots P_t^{h_t{}^0},\quad z = P_1^{g_1} P_2^{g_2} \ldots P_t^{g_t}.$$

By what has just been proved, c is a constant integer different from zero, and z is a variable element of Π. Furthermore, x, y, and z are connected by the relation

$$ax^m + by^n = cz^m. \tag{4}$$

4. Put

$$ax = x',\ a^{m-1}b = b',\ a^{m-1}c = c',$$

so that (4) takes the form,

$$x'^m + b'y^n = c'z^m.$$

Evidently $(x', y) = (ax, y)$ is a factor of (a, y) (x, y) and therefore, by (1), is bounded. The new coefficients b' and c' are constant integers different from zero. When x, y run over the pairs in S, the corresponding triplets of integers x', y, z form a new infinite sequence, the sequenze S' say.

For simplicity, we drop now again the accents in b', c', x', and S'. The results obtained so far may then be expressed as follows.

There are two fixed integers b and c, both different from zero, and an infinite sequence S of triplets of integers x, y, z, with the following properties:

All pairs of integers x, y are distinct, and therefore (5)

$$\lim \max(|x|, |y|) = \infty.$$

$$(x, y) \text{ is bounded.} \tag{6}$$

$$x^m + by^n = cz^m. \tag{7}$$

Both y and z are different from zero, and z belongs to Π. (8)

It is also true that

$$(x, z) \text{ is bounded.} \tag{9}$$

For, by (7), $(x, z)^m$ is a divisor of by^n, and it trivially is a factor of

bx^m. Hence, with $q = \max(m, n)$, $(x, z)^m$ divides $b(x, y)^q$, a number which is bounded.

5. To the last properties of the triplets in S one can add the further one that

$$\lim |z| = \infty. \tag{10}$$

For let this relation be false, i.e. let there exist infinitely many triplets x, y, z in S for which z is bounded. Since S may, if necessary, be replaced by a suitable infinite subsequence, it is permitted to assume that cz^m retains a constant value, c_0 say; evidently $c_0 \neq 0$. The Diophantine equation

$$x^m + by^n = c_0 \tag{11}$$

has thus infinitely many solutions in integers x, y. By a well-known theorem of C. L. SIEGEL (Abh. preuss. Akad. Wiss. 1929, No. 1), the curve (11) must then be rational. However, one easily shows that the curve is of genus

$$\tfrac{1}{2}\{(m-1)(n-2) + (m-d)\},$$

where $d = (m, n)$. This genus is positive because $m \geq 2$, $n \geq 3$, and $m \geq d$; hence a contradiction is obtained.

6. Since the integer c does not vanish, the m values of its m-th root, the numbers

$$\gamma_1, \gamma_2, \ldots, \gamma_m$$

say, are different algebraic integers. Let K be the algebraic field obtained by adjoining these m numbers to the rational field. The ideals occurring in the next sections are all ideals in K, and they are integral ideals unless the contrary is said. We exclude the zero ideal.

In K, the equation (7) can be factorized in the form,

$$\prod_{h=1}^{m} (x - \gamma_h z) = -by^n. \tag{12}$$

We shall replace this equation by m separate equations.

7. We introduce the ideals

$$\mathfrak{d}_{hk} = (x - \gamma_h z,\ x - \gamma_k z) \qquad (h, k = 1, 2, \ldots, m;\ h \neq k).$$

Evidently

$$\mathfrak{d}_{hk} \mid (\gamma_h - \gamma_k)x \text{ and } \mathfrak{d}_{hk} \mid (\gamma_h - \gamma_k)z$$

and therefore

$$\mathfrak{d}_{hk} \mid (\gamma_h - \gamma_k)(x, z).$$

On the right-hand side, the factor $\gamma_h - \gamma_k$ does not vanish, and (x, z) is by (9) a bounded integer. Hence $\mathfrak{d}_{hk}$ is of bounded norm and has only finitely many possibilities.

Hence, after possibly replacing S by a suitable infinite subsequence, we are allowed to assume that all ideals $\mathfrak{d}_{hk}$ remain constant when x, y, z run over the triplets in S.

8. Each of the m principal ideals $(x - \gamma_h z)$ admits of a factorization into ideal factors,

$$(x - \gamma_h z) = \mathfrak{a}_h \mathfrak{x}_h^n \qquad (h = 1, 2, \ldots, m),$$

where $\mathfrak{a}_h$ has no divisor which is the n-th power of a prime ideal. On the other hand, by the definition of $\mathfrak{d}_{hk}$,

$$(\mathfrak{a}_h \mathfrak{x}_h^n, \mathfrak{a}_k \mathfrak{x}_k^n) = \mathfrak{d}_{hk} \qquad (h \neq k),$$

whence

$$(\mathfrak{a}_h, \mathfrak{a}_k) \mid \mathfrak{d}_{hk} \qquad \text{if } h \neq k.$$

We assert that each ideal $\mathfrak{a}_h$ has only finitely many possibilities. If this assertion is false, then the norms of the prime ideal factors of at least one ideal $\mathfrak{a}_j$ are unbounded when x, y, z run over the triplets in S. Hence $\mathfrak{a}_j$ is infinitely often divisible by some prime ideal $\mathfrak{p}$ (not necessarily always the same) which does not divide the fixed ideal

$$(b) \prod_{\substack{h=1 \\ h \neq j}}^{m} \mathfrak{d}_{hj}.$$

Therefore $\mathfrak{p}$ is a factor of $\mathfrak{a}_j$, but not of the other ideals $\mathfrak{a}_h$ where $h \neq j$; moreover $\mathfrak{a}_j$ cannot be divisible by $\mathfrak{p}^n$.

Let now $\mathfrak{p}^s$ be the exact power of $\mathfrak{p}$ which divides

$$\prod_{h=1}^{m} (x - \gamma_h z) = \prod_{h=1}^{m} (\mathfrak{a}_h \mathfrak{x}_h^n).$$

Then s is not a multiple of n. On the other hand,

$$\prod_{h=1}^{m} (x - \gamma_h z) = (b y^n)$$

is divisible by an exact power of $\mathfrak{p}$ the exponent of which evidently is a multiple of n because $\mathfrak{p}$ is not a factor of (b). Therefore a contradiction arises, and the assertion about the ideals $\mathfrak{a}_h$ was in fact true.

It follows then that, after possibly replacing S by a suitable infinite subsequence, all m ideals $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_m$ remain constant when x, y, z run over the triplets in S.

9. If H is the class number of K, we can select H ideals

$$\mathfrak{b}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_H$$

in K so that, when $\mathfrak{z}$ is an arbitrary ideal, just one of the products

$$\mathfrak{b}_1\mathfrak{z}, \mathfrak{b}_2\mathfrak{z}, \ldots, \mathfrak{b}_H\mathfrak{z}$$

is principal. We denote by $\mathfrak{c}_h = \mathfrak{c}_h(\mathfrak{x}_h)$ that ideal $\mathfrak{b}_i$ for which the product $\mathfrak{c}_h\mathfrak{x}_h$ is a principal ideal; therefore each of

$$\mathfrak{c}_1, \mathfrak{c}_2, \ldots, \mathfrak{c}_m$$

has only finitely many possibilities when x, y, z run over the triplets in S. On replacing again S by an infinite subsequence, it may be assumed that these m ideals remain constant.

Since $\mathfrak{c}_h\mathfrak{x}_h$ is an integral principal ideal, there exist m integers

$$\xi_1, \xi_2, \ldots, \xi_m$$

in K such that

$$\mathfrak{c}_h\mathfrak{x}_h = (\xi_h) \qquad (h = 1, 2, \ldots, m);$$

the fractional ideals

$$\mathfrak{a}_h\mathfrak{c}_h^{-n} = (x - \gamma_h z)\,(\mathfrak{c}_h\mathfrak{x}_h)^{-n} = (x - \gamma_h z)\,(\xi_h)^{-n}$$

are therefore likewise principal, and they do not depend on the triplet x, y, z. Hence there exist m constant fractional numbers $\lambda_1, \lambda_2, \ldots, \lambda_m$ in K such that

$$\mathfrak{a}_h\mathfrak{c}_h^{-n} = (\lambda_h) \qquad (h = 1, 2, \ldots, m).$$

By $y \neq 0$,

$$\prod_{h=1}^{m} (\lambda_h\xi_h^n) = (by^n) \neq (0),$$

and therefore

$$\lambda_h \neq 0 \text{ and } \xi_h \neq 0.$$

10. It follows that there exist m units $\eta_1, \eta_2, \ldots, \eta_m$ in K for which

$$x - \gamma_h z = \lambda_h\xi_h^n\eta_h \qquad (h = 1, 2, \ldots, m).$$

By Dirichlet's theorem on the units in an algebraic field, each unit η_h can be written in the form

$$\eta_h = \varepsilon_h\theta_h^n \qquad (h = 1, 2, \ldots, m),$$

where ε_h and θ_h are again units, and where each ε_h has only finitely many possibilities.

Put now

$$\varkappa_h = \varepsilon_h \lambda_h \text{ and } \zeta_h = \theta_h \xi_h \qquad (h = 1, 2, \ldots, m),$$

so that

$$x - \gamma_h z = \varkappa_h \zeta_h^n \qquad (h = 1, 2, \ldots, m).$$

Then $\varkappa_1, \varkappa_2, \ldots, \varkappa_m$ are fractional elements of K, each one with only finitely many possible values; on the other hand, $\zeta_1, \zeta_2, \ldots, \zeta_m$ are integers in K that depend on the triplet x, y, z. Again

$$\varkappa_h \neq 0 \text{ and } \zeta_h \neq 0.$$

On replacing S by a suitable infinite subsequence, we may assume that $\varkappa_1, \varkappa_2, \ldots, \varkappa_m$ remain constant for all triplets in S.

In order to get rid of the fractions, choose a positive rational integer u such that

$$\sigma_1 = u\varkappa_1, \ \sigma_2 = u\varkappa_2, \ \ldots, \ \sigma_m = u\varkappa_m$$

are integers in K; $u, \sigma_1, \sigma_2, \ldots, \sigma_m$ are independent of the triplet x, y, z. The single equation (7) changes then finally into the system of m equations,

$$u(x - \gamma_h z) = \sigma_h \zeta_h^n \qquad (h = 1, 2, \ldots, m). \tag{13}$$

11. By hypothesis $m \geq 2$. There are thus always at least two equations (13), viz. those which belong to $h = 1$ and to $h = 2$. On forming their difference, we obtain the equation

$$\sigma_1 \zeta_1^n - \sigma_2 \zeta_2^n = u(\gamma_2 - \gamma_1) z. \tag{14}$$

By what has been proved, this equation possesses infinitely many solutions z, ζ_1, ζ_2 of the following kind. The variable z is a rational integer contained in Π, and $|z|$ tends to infinity when x, y, z run over the triplets in S. The two other variables ζ_1 and ζ_2 are integers in K; furthermore, their greatest common divisor (ζ_1, ζ_2) is a bounded ideal because the ideal

$$(\sigma_1 \zeta_1^n, \ \sigma_2 \zeta_2^n) = u\mathfrak{d}_{12}$$

is constant.

Two pairs of integers α_1, α_2 and β_1, β_2 in K are said to be associated if there exists a unit ε such that

$$\beta_1 = \alpha_1 \varepsilon, \ \beta_2 = \alpha_2 \varepsilon,$$

and they are otherwise called non-associated. It can easily be shown that at most finitely many pairs ζ_1, ζ_2 belonging to solutions z, ζ_1, ζ_2 of (14) can be associated. For assume that there exists one fixed pair of integers τ_1, τ_2 in K and an infinite sequence of units ε, also in K, such that

$$\zeta_1 = \varepsilon\tau_1,\ \zeta_2 = \varepsilon\tau_2$$

corresponding to an infinite sequence of solutions z, ζ_1, ζ_2 of (14). Then

$$u(\gamma_2 - \gamma_1)z = \varepsilon^n(\sigma_1\tau_1^n - \sigma_2\tau_2^n)$$

and so the rational integer z is of bounded norm, contrary to the limit relation $|z| \to \infty$.

12. We have thus proved that *there exists an infinite sequence of non-associated pairs of integers ζ_1, ζ_2 in K for which the form*

$$F(\zeta_1,\ \zeta_2) = \sigma_1\zeta_1^n - \sigma_2\zeta_2^n$$

is divisible exclusively by a fixed finite set of prime ideals, viz. only by those prime ideals that are divisors of the numbers

$$u,\ \gamma_2 - \gamma_1,\ P_1,\ P_2,\ \ldots,\ P_t.$$

This is, however, impossible. For by the $\mathfrak{p}$-adic generalization of the Thue-Siegel theorem (see C. J. PARRY, Acta math. 83, 1950, 1—100, in particular Theorem 2 and its Corollaries), the following theorem holds:

„*Let K be a field of finite degree over the rational field and of discriminant D. Let further F (ζ_1, ζ_2) be a binary form in ζ_1 and ζ_2 of degree not less than* 3, *with non-vanishing discriminant, and with integral coefficients in K. Then, for every given finite set $\mathfrak{P}$ of prime ideals in K, there exist at most finitely many non-associated pairs of integers ζ_1, ζ_2 in K such that,* (*i*) *the norm of the greatest common divisor of ζ_1 and ζ_2 does not exceed $|\sqrt{D}|$, and* (ii) *F (ζ_1, ζ_2) is divisible only by prime ideals in $\mathfrak{P}$*."

In the present case, the binary form

$$F(\zeta_1,\ \zeta_2) = \sigma_1\zeta_1^n - \sigma_2\zeta_2^n$$

is of the required kind. For its degree n is at least 3, and by $\sigma_1\sigma_2 \neq 0$ its discriminant does not vanish. On the other hand, it has *not* been proved that the norm of (ζ_1, ζ_2) is not greater than $|\sqrt{D}|$, but only that this norm is bounded. However, this difficulty can easily be surmounted.

13. For this purpose, put $(\zeta_1, \zeta_2) = \mathfrak{g}$; then $\mathfrak{g}$ is of bounded norm and therefore belongs to a finite set of ideals. By a well-known theorem in the theory of algebraic fields (see E. HECKE, Theorie

der algebraischen Zahlen, Leipzig 1923, Satz 96), the ideal class of $\mathfrak{g}$ contains an integral ideal $\mathfrak{k}$ of norm not greater than $|\sqrt{D}|$. This ideal has naturally only finitely many possibilities; the same is therefore true for the fractional ideal $\frac{\mathfrak{g}}{\mathfrak{k}}$. This fractional ideal is principal and of the form

$$\frac{\mathfrak{g}}{\mathfrak{k}} = (\chi)$$

where $\chi \neq 0$ is a fractional number in K which also has only finitely many possible values. From the definition of χ, the two numbers

$$Z_1 = \chi^{-1}\zeta_1 \text{ and } Z_2 = \chi^{-1}\zeta_2$$

are integers in K, and $\mathfrak{k}$ is their greatest common divisor.

The equation (14) implies now that

$$\sigma_1 Z_1^n - \sigma_2 Z_2^n = u(\gamma_2 - \gamma_1)\chi^{-n}z.$$

Since the expression on the left-hand side is an integer in K, the same is true for that on the right-hand side, and it is also obvious that the expression on the right-hand side admits only prime divisors of bounded norm. The theorem in 12. can now be applied because the norm of $(Z_1, Z_2) = \mathfrak{k}$ does not exceed $|\sqrt{D}|$, giving the assertion.

14. In the proof of our theorem we had replaced the original condition $(x, y) = 1$ by the weaker one that (x, y) is bounded. A natural and final condition can now be given without difficulty.

Theorem: *Let S be an infinite sequence of different pairs of integers x, y for which the greatest prime factor of $ax^m + by^n$ is bounded. Then the greatest prime factor of (x^m, y^n) is bounded, and so are the three quotients*

$$\frac{x^m}{(x^m,\ y^n)},\ \frac{y^n}{(x^m,\ y^n)},\ \frac{ax^m + by^n}{(x^m,\ y^n)}.$$

Proof: Put $(x^m, y^n) = \delta$ so that δ is a divisor of $ax^m + by^n$; the prime factors of δ are therefore bounded. Let $P_1, P_2, \ldots, P_t$ be all the different primes that are admissible as factors of δ, and then denote by Π, as in 1., the set of all integers different from zero that have $P_1, P_2, \ldots, P_t$ as their only prime factors. Thus, in particular, δ belongs to Π. By a construction similar to that in 3., δ can be shown to be of the form

$$\delta = \varphi\psi^{mn}$$

where φ is one of a finite set of integers not zero, and where ψ is contained in Π. Since ψ^{mn} is a divisor of δ and δ is a divisor of both x^m and y^n, the two quotients

$$v = \frac{x}{\psi^n} \text{ and } w = \frac{y}{\psi^m}$$

are integral. Further

$$(v^m, w^n) = \frac{\delta}{\psi^{mn}} = \varphi$$

is bounded, hence also (v, w). Finally, in

$$ax^m + by^n = \psi^{mn}(av^m + bw^n),$$

the left-hand side has by hypothesis only bounded prime factors; the same must therefore be true for $av^m + bw^n$.

We have thus derived from the sequence S of pairs x, y a new sequence T of pairs of integers v, w such that, (i) (v, w) is bounded, and (ii) the greatest prime factor of $av^m + bw^n$ is likewise bounded. Hence, by the theorem already proved, the sequence T cannot contain more than finitely many distinct pairs v, w. It follows then that v and w are bounded, and the assertion is now obvious from the equations

$$\frac{x^m}{(x^m, y^n)} = \frac{v^m}{\varphi}, \frac{y^n}{(x^m, y^n)} = \frac{w^n}{\varphi}, \frac{ax^m + by^n}{(x^m, y^n)} = \frac{av^m + bw^n}{\varphi}.$$

I conclude this note with a remark about the special case when $m = 2$ and $n = 3$. One can then give a rather shorter proof, using either my theorem on rational points on curves of genus 1 (Journ. reine u. angew. Math. 170, 1934, 168—178), or Parry's theorem in the special case of cubic forms. Conversely, the $\mathfrak{p}$-adic form of the Thue-Siegel theorem for cubic forms can be deduced from a slight generalization of our theorem on $ax^2 + by^3$, viz. to the case when both coefficients and variables are integers in an algebraic field of finite degree over the rational field.

(Received 23.2.1953)