COMPOSITIO MATHEMATICA

T. N. SHOREY
R. TIJDEMAN

On the greatest prime factors of polynomials at integer points

Compositio Mathematica, tome 33, n° 2 (1976), p. 187-195
<http://www.numdam.org/item?id=CM_1976__33_2_187_0>

COMPOSITIO MATHEMATICA, Vol. 33, Fasc. 2, 1976, pag. 187–195
Noordhoff International Publishing
Printed in the Netherlands

ON THE GREATEST PRIME FACTORS OF POLYNOMIALS AT INTEGER POINTS*

T. N. Shorey and R. Tijdeman

1

Let f be a polynomial with integer coefficients and at least two distinct roots. Denote by $P[n]$ the greatest prime factor of the integer n. Siegel [12] generalised earlier results of Størmer, Thue and Pólya by proving that $P[f(n)] \to \infty$ if $n \to \infty$. This result has been improved to

$$P[f(n)] \gg \log\log n. \tag{1}$$

Here the constant implied by $\gg$ depends only on f. Nagell, Mahler and Chowla proved (1) for certain polynomials of the form $Ax^2 + B$, $Ax^3 + B$. Schinzel [8] proved (1) for all polynomials f of degree 2 by using Gelfond's work on a p-adic measure of irrationality of the ratio of two logarithms of algebraic numbers. It follows from the results of Keates [4], proved with the help of Baker's estimate on solutions of the equation $y^2 = ax^3 + bx^2 + cx + d$, that (1) holds for all polynomials f of degree 3. Finally Sprindžuk [13] and Kotov [5] established (1) for all (irreducible) polynomials f of degree at least 4. Their method makes use of a p-adic analogue of the inequalities of Baker and Stark on linear forms in the logarithms of algebraic numbers. (In fact Sprindžuk proved such a result for binary forms $f(x, y)$). The inequality (1) has been applied by Schinzel and the second named author [9] in their investigations on the diophantine equation $y^m = f(x)$. In this paper, we give a proof of (1) for all polynomials f. Our proof does not make use of p-adic techniques. Moreover, we prove the following generalisation. (We write $\log_2 x$ for $\log\log x$ *and* $\log_3 x$ for $\log\log\log x$.)

* Dedicated to Professor Th. Schneider on his 65th birthday.

THEOREM 1: *Let $f(x)$ be a polynomial of degree n with rational integer coefficients and at least two distinct zeros. Let $B > 0$. Then for any natural numbers $X(> e^{e^e})$ and Y with*

$$Y \leq \exp((\log_2 X)^B), \tag{2}$$

there exists an effectively computable number $\epsilon > 0$ depending only on B and f such that

$$P\left[\prod_{i=1}^{Y} f(X+i)\right] > \epsilon Y \frac{\log_2 X}{\log_3 X}(\log Y + \log_3 X).$$

The type of this theorem seems to be new. Erdös [2] has given a lower bound for $P[\prod_{i=1}^{X} f(i)]$. See also Hooley [15]. Several authors gave lower bounds for $P[\prod_{i=1}^{Y}(X+i)]$. See [7, 11]. On applying Theorem 1 to $f(x) = 2x(2x \pm 1)$, we obtain the following

COROLLARY: *For all natural numbers $X > e^{e^e}$ and Y satisfying*

$$2 \leq Y \leq \exp((\log_2 X)^B),$$

we have

$$P\left[\prod_{i=1}^{Y}(X+i)\right] \geq \epsilon_1 Y \frac{\log_2 X}{\log_3 X}(\log Y + \log_3 X) \tag{3}$$

where $\epsilon_1 > 0$ is a constant depending only on B.

Recently Langevin [6] obtained (3) for fixed Y with $\epsilon_1 = (8+\delta)^{-1}$, $\delta > 0$. Erdös and Shorey [3] have proved (3) for $Y \ll (\log_2 X)^B$. For larger values of Y, this result is an improvement of earlier published results, see [10].

Theorem 1 is an immediate consequence of the following result.

THEOREM 2: *Let $f(x)$ be a polynomial with rational integer coefficients and at least two distinct roots. Let $A > 0$. Then there exists an effectively computable number $\epsilon_2 > 0$ depending only on A and f such that if*

$$P[f(X)] \leq \exp((\log_2 X)^A), \quad X \in \mathbb{Z}, \quad X > e^{e^e} \tag{4}$$

then

$$\omega(f(X)) \geq \epsilon_2 \frac{\log_2 X}{\log_3 X},$$

where $\omega(Y)$ denotes the number of distinct prime divisors of Y.

The proof of Theorem 2 depends on an inequality on linear forms in the logarithms of algebraic numbers. Let $n > 1$ be an integer. Let

$\alpha_1, \ldots, \alpha_n$ be non-zero algebraic numbers of heights at most $A_1, \ldots, A_n$, where each $A_i \geq e^e$. Let $\beta_1, \ldots, \beta_{n-1}$ denote algebraic numbers of heights at most $B (> e^e)$. Suppose that $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_{n-1}$ all lie in a field of degree D over rationals. Put

$$\Lambda = \log A_1 \cdots \log A_n, \qquad E = (\log \Lambda + \log\log B).$$

LEMMA: *For every $\epsilon > 0$, there exists an effectively computable number $C > 0$ depending only on ϵ such that*

$$|\beta_1 \log \alpha_1 + \cdots + \beta_{n-1} \log \alpha_{n-1} - \log \alpha_n|$$

either vanishes or exceeds

$$\exp(-(nD)^{C^n} \Lambda (\log \Lambda)^2 (\log (\Lambda B))^2 E^{2^{n+2+\epsilon}}).$$

This is the main theorem of [11]. We have assumed that the logarithms have their principal values. We remark that the arguments that we shall use for deriving Theorem 2 from the Lemma are well known. The crucial point in the Lemma is the explicit and good dependence of the lower bound on both n and D. The following simple consequence illustrates the usefulness of such a result. Let a and b be positive integers, $a < b$. Put $r = \omega(ab)$ and $p = P(ab)$. Then

$$b - a > a \exp(-r^{C' r} (\log p)^{3r} (\log_2 a)^2 (\log_3 a)^{4r}) \tag{5}$$

where $C' > 0$ is an absolute constant. This result can be compared with [14, Theorems 1, 3]. The inequality (5) appears to be better with respect to r.

2. Proof of Theorem 2

Denote the distinct roots of f by $\alpha_1, \ldots, \alpha_d$. By the hypothesis of the theorem, $d \geq 2$. It is no loss of generality to assume that f is monic. Indeed, if a_0 is the leading coefficient of f and N is the degree of f, then the polynomial g defined by $g(a_0 x) = a_0^{N-1} f(x)$ is monic and it suffices to prove the theorem for g. Also we may assume that $X \geq X_0$ where X_0 is some large positive constant depending only on A and f. Indeed, in doing so we omit at most X_0 values of X and, at the end of the proof, we can decrease ϵ_2 in such a way that the statement of Theorem 2 is also valid for these finitely many values of X. We suppose that the inequality (4) and the inequality

$$\omega(f(X)) \leq \left[\epsilon_2 \frac{\log_2 X}{\log_3 X}\right] =: m \tag{6}$$

for any ϵ_2 with $0 < \epsilon_2 < 1$ are satisfied. We shall arrive at a contradiction for a certain value of ϵ_2 depending only on A and f.

We first prove the special case that f has at least two distinct rational zeros, α_1 and α_2 say. Let

$$X - \alpha_1 = p_1^{k_1} \cdots p_s^{k_s}, \qquad X - \alpha_2 = q_1^{l_1} \cdots q_t^{l_t}.$$

Then

$$p_1^{k_1} \cdots p_s^{k_s} - q_1^{l_1} \cdots q_t^{l_t} = \alpha_2 - \alpha_1.$$

Hence

$$0 < |k_1 \log p_1 + \cdots + k_s \log p_s - l_1 \log q_1 - \cdots - l_t \log q_t|$$
$$= \frac{|\alpha_2 - \alpha_1|}{|X - \alpha_2|} < \frac{1}{\sqrt{X}}.$$

On the other hand, by the Lemma, applied with $B = 2 \log X$, $n = s + t \leq 2m$, $\Lambda \leq (\log_2 X)^{2Am}$ and $E \leq (\log_2 X)^2$, it follows that

$$|k_1 \log p_1 + \cdots + k_s \log p_s - l_1 \log q_1 - \cdots - l_t \log q_t|$$
$$> \exp(-(\log X)^{C\epsilon_2})$$

where $C > 1$ is a large constant depending only on A and f. Thus

$$\tfrac{1}{2} \log X < (\log X)^{C\epsilon_2}.$$

This is false for $\epsilon_2 = (2C)^{-1}$. This gives the proof in our special case.

We now turn to the proof of the general case. If $f(x)$ is reducible, then it has either two distinct rational roots or an irreducible factor of degree at least 2. It now suffices to prove the theorem for this irreducible factor. Hence we may assume, without loss of generality, that f is irreducible. Denote by K the field generated by $\alpha_1, \ldots, \alpha_d$ over the field of rationals. Let n be the degree of K over the field of rationals and h the class number of K. Let the prime decomposition of $f(X)$ be given by

$$f(X) = \pm p_1^{a_1} \cdots p_m^{a_m} \tag{7}$$

and the prime ideal decomposition of the ideal $[X - \alpha_1]$ in K by

$$[X - \alpha_1] = \mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_s^{b_s}. \tag{8}$$

We shall say that a prime ideal $\mathfrak{p}$ sits over a rational prime p if $\mathfrak{p} \cap \mathbb{Z} = (p)$. Here $\mathbb{Z}$ denotes the ring of rational integers. If we take the norm on both sides of equality (8), it follows from (7) that every prime ideal $\mathfrak{p}_j$ sits over some rational prime p_i. Further for every rational prime p_i, there are at most n prime ideals of K that can sit over p_i. Thus

$$s \leq mn. \tag{9}$$

It further follows that

$$b_i \leq c_1 \log X, \quad i = 1, \ldots, s, \tag{10}$$

where c_1 and the subsequent symbols c_2, $c_3, \ldots$ denote positive constants depending only on A and f. From (8), we get the ideal equation

$$[(X - \alpha_1)^h] = [u_1]^{b_1} \cdots [u_s]^{b_s},$$

where $u_1, \ldots, u_s$ are integers of K with $[u_i] = \mathfrak{p}_i^h$. Thus we have

$$(X - \alpha_1)^h = \epsilon u_1^{b_1} \cdots u_s^{b_s},$$

where ϵ is a unit of K. Since $[u_i] = \mathfrak{p}_i^h$ and $\mathfrak{p}_i$ sits over some p_j, it follows from (4) that

$$|\text{Norm}\,(u_i)| \leq \exp\,(nh(\log_2 X)^A), \quad i = 1, \ldots, s. \tag{11}$$

We suppose that there are r_1 real and $2r_2$ complex conjugate fields to K and that they are chosen in the usual manner: if α is in K then $\alpha^{(i)}$ is real for $1 \leq i \leq r_1$, and $\alpha^{(i+r_2)} = \overline{\alpha^{(i)}}$ for $r_1 + 1 \leq i \leq r_1 + r_2$. Put $r = r_1 + r_2 - 1$. Let $\eta_1, \ldots, \eta_r$ be a system of fundamental units for K. It is well known (see Baker [1, p. 39]) that there exist integers $v_1, \ldots, v_s$ of K which are associates of $u_1, \ldots, u_s$, respectively, and satisfy

$$|v_i^{(j)}| \leq |\text{Norm}\,(u_i)| \exp\left(n \sum_{k=1}^{r} |\log |\eta_k^{(j)}|\right),$$

for $i = 1, \ldots, s$ and $j = 1, \ldots, n$. Hence, by (11),

$$|v_i^{(j)}| \leq c_2 \exp\,(nh(\log_2 X)^A) \leq \exp\,(c_3(\log_2 X)^A).$$

We denote the height of v_i by $H(v_i)$. Since

$$H(v_i) \leq 2^n (\max |v_i^{(j)}|)^n,$$

we obtain

$$H(v_i) \leq \exp\,(c_4 (\log_2 X)^A), \quad i = 1, \ldots, s. \tag{12}$$

We have

$$(X - \alpha_1)^h = \epsilon_1 v_1^{b_1} \cdots v_s^{b_s},$$

where ϵ_1 is a unit of K. Put

$$\epsilon_1 = \rho \eta_1^{d_1} \cdots \eta_r^{d_r},$$

where $d_1, \ldots, d_r$ are integers and ρ is a root of unity of K. Putting

$$W = \rho v_1^{b_1} \cdots v_s^{b_s} \quad \text{and} \quad V = W^{-1},$$

we obtain

$$(X-\alpha_1)^h V = \eta_1^{d_1}\cdots\eta_r^{d_r}.$$

Hence, we have for $j=1,\ldots,r$,

$$d_1\log|\eta_1^{(j)}|+\cdots+d_r\log|\eta_r^{(j)}| = h\log|X-\alpha_1^{(j)}|+\log|V^{(j)}|. \tag{13}$$

Observe that

$$(nH(v_i))^{-1}\le|v_i^{(j)}|\le nH(v_i), \tag{14}$$

for $i=1,\ldots,s$ and $j=1,\ldots,r$. We have

$$|V| = |v_1^{-b_1}\cdots v_s^{-b_s}|.$$

Hence, in view of (14), (12), (10) and (9)

$$-(\log X)^2\le\log|V^{(j)}|\le(\log X)^2,\quad j=1,\ldots,r.$$

It follows that the right hand side of (13) does not exceed

$$c_5(\log X)^2.$$

On solving the coefficients d_k from the system of linear equations (13), the determinant of which is a non zero constant, we obtain

$$|d_k|\le c_6(\log X)^2,\quad k=1,\ldots,r. \tag{15}$$

Rewriting the expression for $(X-\alpha_1)^h$, we have

$$(X-\alpha_1)^h = \rho\eta_1^{d_1}\cdots\eta_r^{d_r}v_1^{b_1}\cdots v_s^{b_s}. \tag{16}$$

Similarly, we put

$$(X-\alpha_2)^h = \rho'\eta_1^{e_1}\cdots\eta_r^{e_r}w_1^{b_1'}\cdots w_t^{b_t'}, \tag{17}$$

where ρ' is a root of unity of K. Further $t, e_1,\ldots,e_r, b_1',\ldots,b_t'$ and $w_1,\ldots,w_t$ satisfy, respectively, the inequalities corresponding to those ((9), (15), (10), (12)) for $s, d_1,\ldots,d_r, b_1,\ldots,b_s$ and $v_1,\ldots,v_s$.

Suppose that $(X-\alpha_1)^h=(X-\alpha_2)^h$. Since $\alpha_1\ne\alpha_2$ $(d\ge2)$, we have $h>1$ and there exists an integer g with $0<g<h$ such that

$$X-\alpha_1 = e^{2\pi ig/h}(X-\alpha_2).$$

Thus

$$X\le\frac{|\alpha_1|+|\alpha_2|}{2\sin(\pi/h)} =: c_7,$$

which is not possible if we take $X_0>c_7$. Thus we can assume that

$(X-\alpha_1)^h \neq (X-\alpha_2)^h$. From (16) and (17), it follows that

$$0 \neq \left|\log\frac{\rho}{\rho'} + \sum_{i=1}^{r}(d_i - e_i)\log\eta_i + \sum_{i=1}^{s} b_i \log v_i - \sum_{i=1}^{t} b'_i \log w_i + M\log(-1)\right| < \frac{1}{\sqrt{X}},$$

where M with $|M| \leq c_8(\log X)^2$ is an integer. Here we have taken the principal branch of the logarithms. By the lemma, applied with $B = c_9(\log X)^2$, $n = r + s + t + 2 \leq 3m$, $\Lambda \leq (\log_2 X)^{3Am}$ and $E \leq (\log_2 X)^2$, it follows that the left hand side of the above inequality exceeds

$$\exp(-(\log X)^{C_1\epsilon_2}),$$

where $C_1 > 1$ is a large constant depending only on A and f. Thus

$$\tfrac{1}{2}\log X < (\log X)^{C_1\epsilon_2}.$$

This is false for $\epsilon_2 = (2C_1)^{-1}$. This completes the proof of Theorem 2.

3. Proof of Theorem 1

We can assume that $X \geq X_0$ where X_0 is a large positive constant depending only on B and f. Indeed, in doing so we omit a number of pairs (X, Y) which is bounded in terms of B and f. At the end of the proof we can decrease ϵ in such a way that the statement of Theorem 1 is also valid for these values of X and Y. Put

$$R = f(X+1)\cdots f(X+Y).$$

If $\log P[R] \geq (\log_2 X)^{2B}$, then the theorem follows immediately from (2). Thus we can assume that

$$\log P[R] \leq (\log_2 X)^{2B}.$$

Then

$$\log P[f(X+i)] \leq (\log_2 X)^{2B}, \quad i = 1, \ldots, Y.$$

It follows, from Theorem 2, that there exists a constant $\epsilon_3 > 0$ depending only on B and f such that

$$\omega(f(X+i)) \geq \epsilon_3 \frac{\log_2 X}{\log_3 X}, \quad i = 1, \ldots, Y.$$

Thus

$$\sum_{i=1}^{Y} \omega(f(X+i)) \geq \epsilon_3 Y \frac{\log_2 X}{\log_3 X}, \quad i = 1, \ldots, Y.$$

However, for any prime p, a congruence $f(x) \equiv 0 \pmod p$ has at

most n solutions which are incongruent mod p. Hence,

$$\begin{aligned}\sum_{i=1}^{Y} \omega(f(X+i)) &\leq \sum_{p/R} n\left(\left[\frac{Y}{p}\right]+1\right)\\ &\leq nY\sum_{p\leq Y}\frac{1}{p}+n\sum_{p/R}1\\ &\leq c_{10}Y\log_2 Y + n\omega(R),\end{aligned}$$

where $c_{10}>0$ is an absolute constant. Hence, by (2),

$$\begin{aligned}\omega(R) &\geq \frac{\epsilon_3 Y}{n}\frac{\log_2 X}{\log_3 X} - c_{10}Y\log_2 Y\\ &> \frac{\epsilon_3 Y}{2n}\frac{\log_2 X}{\log_3 X},\end{aligned}$$

if $X \geq X_0$. By prime number theory, it follows that

$$P[R] \geq \epsilon Y\frac{\log_2 X}{\log_3 X}(\log Y + \log_3 X)$$

for some positive $\epsilon = \epsilon(B, f)$. This completes the proof of Theorem 2.

REMARK: In the same way, one can obtain a slightly more general result. Let $0<a_1<\cdots<a_Y\leq Z$ be positive integers where $Z \ll Y\log_2 X/(\log_3 X)^3$. Then under the conditions of Theorem 1, we have

$$P\left[\prod_{i=1}^{Y} f(X+a_i)\right] \geq \epsilon_4 Y\frac{\log_2 X}{\log_3 X}(\log Y + \log_3 X)$$

where $\epsilon_4>0$ is a constant.

REFERENCES

[1] A. BAKER: *Transcendental Number Theory*, Cambridge University Press (1975).
[2] P. ERDÖS: On the greatest prime factor of $\Pi_{k=1}^{x} f(k)$. *J. London Math. Soc. 27* (1952) 379–384.
[3] P. ERDÖS and T. N. SHOREY: On the greatest prime factor of $2^p - 1$ for a prime p and other expressions. (To appear in Acta Arith.).
[4] M. KEATES: On the greatest prime factor of a polynomial. *Proc. Edinb. Math. Soc. (2) 16* (1969) 301–303.
[5] S. V. KOTOV: Greatest prime factor of a polynomial. *Mat. Zametki 13* (1973) 515–522; *Math. Notes 13* (1973) 313–317.
[6] M. LANGEVIN: Plus grand facteur premier d'entiers consecutifs. *C. R. Acad. Sc. Paris 280A* (1975) 1567–1570.
[7] K. RAMACHANDRA and T. N. SHOREY: On gaps between numbers with a large prime factor. *Acta Arith. 24* (1973) 99–111.
[8] A. SCHINZEL: On two theorems of Gelfond and some of their applications. *Acta Arith. 13* (1967) 177–236.

[9] A. SCHINZEL and R. TIJDEMAN: On the equation $y^m = P(x)$. (To appear in Acta Arith.).
[10] T. N. SHOREY: On gaps between numbers with a large prime factor II. *Acta Arith. 25* (1974) 365–373.
[11] T. N. SHOREY: On linear forms in the logarithms of algebraic numbers. (To appear in Acta Arith.).
[12] C. L. SIEGEL: Approximation algebraischer Zahlen. *Math. Z. 10* (1921) 173–213.
[13] V. G. SPRINDŽUK: The greatest prime divisor of a binary form. *Dokl. Akad. Nauk BSSR 15* (1971) 389–391.
[14] R. TIJDEMAN: On integers with many small prime factors. *Compositio Math. 26* (1973) 319–330.
[15] C. HOOLEY: On the greatest prime factor of quadratic polynomials, *Acta Math. 117* (1976) 281–299.

(Oblatum 1-VIII-1975)

T. N. Shorey
Tata Institute of Fundamental Research
Bombay-5, India

R. Tijdeman
Mathematical Institute,
R. U. Leiden, Netherlands