

# SÉMINAIRE DELANGE-PISOT-POITOU. THÉORIE DES NOMBRES

T. N. SHOREY

## **Some applications of linear forms in logarithms**

*Séminaire Delange-Pisot-Poitou. Théorie des nombres*, tome 17, n° 1 (1975-1976),  
exp. n° 3, p. 1-8

[http://www.numdam.org/item?id=SDPP\\_1975-1976\\_\\_17\\_1\\_A3\\_0](http://www.numdam.org/item?id=SDPP_1975-1976__17_1_A3_0)

© Séminaire Delange-Pisot-Poitou. Théorie des nombres  
(Secrétariat mathématique, Paris), 1975-1976, tous droits réservés.

L'accès aux archives de la collection « Séminaire Delange-Pisot-Poitou. Théorie des nombres » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme  
Numérisation de documents anciens mathématiques  
<http://www.numdam.org/>

SOME APPLICATIONS OF LINEAR FORMS IN LOGARITHMS

by T. N. SHOREY

1. Introduction.

I shall describe some applications of the following result on linear forms in logarithms of algebraic numbers.

Let  $n > 1$  be an integer. Let  $\alpha_1, \dots, \alpha_n$  be non-zero algebraic numbers of heights less than or equal to  $A_1, \dots, A_n$ , where each  $A_i \geq \exp e$ . Let  $\beta_1, \dots, \beta_{n-1}$  denote algebraic numbers of heights less than or equal to  $B$  ( $\geq \exp e$ ). Suppose that  $\alpha_1, \dots, \alpha_n$  and  $\beta_1, \dots, \beta_{n-1}$  all lie in a field of degree  $D$  over the rationals. Set

$$\Lambda = \log A_1 \dots \log A_n \quad \text{and} \quad E = (\log \Lambda + \log \log B) .$$

THEOREM 1. - Given  $\epsilon > 0$ , there exists an effectively computable number  $C > 0$  depending only on  $\epsilon$  such that either

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

vanishes or exceeds

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

This was proved by the author in [24]. It has been assumed that the logarithms have their principal values, but the result would hold for any choice of logarithms if  $C$  were allowed to depend on their determinations. The crucial point in the theorem is the explicit and good dependence of the lower bound on  $n$  and  $D$ . A result of this type (with every parameter explicit) was proved, for the first time, by BAKER [2], which was improved with respect to  $n$  by RAMACHANDRA [17].

2. Greatest prime factor of a polynomial.

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 [26] generalised earlier results of STÖRMER, THUE and POLYA by proving that  $P[f(n)]$  tends to infinity with  $n$ . However the result of SIEGEL was not effective. Effective versions of Siegel's result were given by CHOWLA, MAHLER and NAGELL for polynomials of the type  $Ax^2 + B$ ,  $Ax^3 + B$  where  $A$  and  $B$  are integers. By proving a  $p$ -adic analogue of Baker's effective estimate on the magnitude of the integral solutions of Thue's equation, COATES [4] gave an effective version of Siegel's result for all polynomials  $f$  of degree  $\geq 3$ . In fact COATES proved that

$$P[f(n)] \gg (\log \log n)^{1/4}, \quad n \geq \exp e, \quad n \in \mathbb{Z} .$$

This result has been improved to

$$(1) \quad P[f(n)] \gg \log \log n, \quad n \geq \exp e, \quad n \in \mathbb{Z}.$$

Here the constants implied by  $\gg$  are effectively computable and depend only on  $f$ . SCHINZEL [22] proved (1) for all polynomials  $f$  of degree 2 by using a  $p$ -adic measure of irrationality of the ratio of two logarithms of algebraic numbers. It follows from the results of KEATES [12], proved with the help of Baker's effective estimate on the magnitude of the integral solutions of  $y^2 = ax^3 + bx^2 + cx + d$ , that (1) holds for all polynomials  $f$  of degree 3. Finally, SPRINDŽUK [27] and KOTOV [13] proved (1) for all polynomials  $f$  of degree at least 4. Their method is  $p$ -adic. TLJDEMAN and the author [25] gave another proof of the inequality (1). The proof is different in the sense that it is not  $p$ -adic. It depends on theorem 1.

Further we proved the following generalization of (1).

THEOREM 2. - Let  $f$  be a polynomial with integer coefficients and at least two distinct roots. Let  $A > 0$ . Then for every natural numbers  $X (> \exp e)$  and  $Y$  with

$$Y \leq \exp((\log_2 X)^A),$$

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

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

We write  $\log_2 X$  for  $\log \log X$  and  $\log_3 X$  for  $\log \log \log X$ . ERDŐS [5] gave a lower bound for  $P\left[\prod_{i=1}^X f(i)\right]$ .

Let us consider the case when  $f$  is a linear polynomial. On applying theorem 2 to  $f(x) = 2x(2x \pm 1)$ , we obtain the following corollary.

COROLLARY. - For all natural numbers  $X (> \exp e)$  and  $Y$  satisfying

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

we have

$$(2) \quad P[X; Y] := P\left[\prod_{i=1}^Y (X+i)\right] \geq \varepsilon_1 Y \frac{\log_2 X}{\log_3 X} (\log Y + \log_3 X)$$

where  $\varepsilon_1 > 0$  is a constant depending only on  $A$ .

Recently, LANGEVIN [14] obtained (2) for fixed  $Y$  with  $\varepsilon_1 = (8 + \delta)^{-1}$ ,  $\delta > 0$  and  $X \geq X_0 = X_0(Y, \delta)$ .

ERDŐS and the author [9] proved (2) with  $Y \ll (\log_2 X)^B$ . For larger values of  $Y$ , the corollary gives an improvement on the earlier published results. In view of the work of RAMACHANDRA and the author [18], JUTILA [11] and the author [23], we have

$$(3) \quad P[X ; Y] \gg \max\left(Y \log Y \frac{\log_2 Y}{\log_3 Y}, Y \log_2 X\right)$$

for  $\exp e \leq Y \leq X^{2/3}$ . When  $Y > X^{2/3}$  and  $X \geq X_0$  where  $X_0$  is some absolute constant, it follows from well-known results on difference between consecutive primes that

$$P[X ; Y] \geq X + 1.$$

For earlier results in the direction of inequality (3), see RAMACHANDRA and the author [18].

### 3. The greatest prime factor of $a^n - b^n$ .

It was conjectured by ERDÖS ([6], p. 218) that  $P[2^n - 1]/n$  tends to infinity with  $n$ . The elementary result  $P[a^n - b^n] > n$  when  $n > 2$  and  $a > b > 0$  was proved by ZSIGMONDY [30] and the result was rediscovered by BIRKHOFF and VANDIVER [3]. It was improved by SCHINZEL [21]; he showed that  $P[a^n - b^n] > 2n$  if  $ab$  is a square or twice a square provided that one excludes the cases  $n = 4, 6, 12$  when  $a = 2, b = 1$ .

For any positive integer  $n$  and relatively prime integers  $a > b > 0$ , we denote by  $\varphi_n(a, b)$  the  $n$ -th cyclotomic polynomial; that is

$$\varphi_n(a, b) = \prod_{i=1, (i,n)=1}^n (a - \zeta^i b),$$

where  $\zeta$  is a primitive  $n$ -th root of unity. We shall write, for brevity,

$$P_n = P[\varphi_n(a, b)].$$

STEWART [28] proved the following theorem.

THEOREM 3. - For any  $\chi$  with  $0 < \chi < (\log 2)^{-1}$  and any integer  $n (> 2)$  with at most  $\chi \log \log n$  distinct prime factors, we have

$$P_n/n > f(n)$$

where  $f$  is a function, strictly increasing and unbounded, which can be specified explicitly in terms of  $a, b$  and  $\chi$ .

The proof of theorem 3 depends on a result of Baker on linear forms in logarithms of algebraic numbers. If that is replaced by theorem 1 in the proof of Stewart for theorem 3, then one can prove the theorem with

$$(4) \quad f(n) = c_1 (\log n)^\lambda / \log \log n$$

where  $\lambda = 1 - \chi \log 2$  and  $c_1 = c_1(a, b, \chi)$  is an effectively computable constant.

Let us consider the case when  $a = 2, b = 1$  and  $n = p$  a prime. Then (4) gives

$$(5) \quad P[2^p - 1] \gg_\varepsilon p(\log p)^{1-\varepsilon}$$

for every  $\varepsilon > 0$ . STEWART [28] proved (5) with the lower bound  $p(\log p)^{1/4}$ . ERDÖS and the author [9] improved the lower bound of (5) to constant times  $p \log p$ . Further ERDÖS and the author [9] strengthened the conclusion of inequality (5) for almost all primes  $p$ .

THEOREM 4. - For almost all primes  $p$

$$P[2^p - 1] \geq p \frac{(\log p)^2}{(\log \log p)^3}.$$

For a slightly stronger version of theorem 4, see [9]. The proof depends on theorem 1 and Brun's Sieve method.

4. The number of distinct prime factors of a block of consecutive integers.

Denote by  $\omega(n)$  the number of distinct prime factors of the integer  $n$ . A weaker form of a conjecture of GRIMM [10] is as follows: Let  $n$  and  $g$  be natural numbers. If all the numbers  $(n+1), \dots, (n+g)$  are composite, then  $\omega((n+1) \dots (n+g)) \geq g$ . A consequence of this conjecture is that

$$p_{n+1} - p_n < \sqrt{p_n / \log p_n}$$

for large  $n$ . See ERDÖS and SELFRIDGE [8]. Here  $p_n$  denotes the  $n$ -th prime. RAMACHANDRA, TIJDEMAN and the author [19] proved the following result.

THEOREM 5. - There exists an effectively computable constant  $c_2 > 0$  such that for all positive integers  $n$  and  $g$  with

$$1 \leq g \leq \exp(c_2 (\log n)^{1/2}),$$

$$\omega((n+1) \dots (n+g)) \geq g.$$

Theorem 5 follows immediately from the following.

THEOREM 6. - Let  $u$  and  $k$  ( $\geq 2$ ) be positive integers. Then there exists an effectively computable constant  $c_3 > 0$  such that if

$$u \geq \exp(c_3 (\log k)^2),$$

then the number  $N$  of numbers among  $(u+1), \dots, (u+k)$  whose all prime factors are less than or equal to  $k$  does not exceed  $\pi(k)$ .

Let  $\varepsilon > 0$ . If  $u > \exp k^\varepsilon$ , then theorem 1 can be used to improve the bound of theorem 6 for  $N$  as follows:

$$(6) \quad P = O_\varepsilon \left( k \frac{\log \log k}{(\log k)^2} \right).$$

See the author [24]. For a weaker version of this result, see RAMACHANDRA [17]. Let  $B > 0$ . It follows immediately from (6) that for  $1 \leq g \leq (\log n)^B$ ,

$$(7) \quad \omega((n+1) \dots (n+g)) \geq g + \pi(g) - c_4 g \frac{\log \log g}{(\log g)^2}$$

where  $c_4 = c_4(B) > 0$  is a constant. ERDÖS and SELFRIDGE [7] defined

$$f(n) = \max_{0 \leq k < \infty} \frac{1}{k+1} \sum_{i=0}^k v(n, i),$$

where

$$v(n, i) = \sum_{p|n+i, p>i} 1.$$

ERDÖS and SELFRIDGE [7] conjectured that  $f(n) \rightarrow \infty$  as  $n \rightarrow \infty$ . This seems very hard to prove. The inequality (7) shows that  $f(n) > 1$  for  $n \geq n_0$  where  $n_0$  is a large constant. Indeed this can be obtained from a weaker version of inequality (6) which is due to RAMACHANDRA [17].

5. Gap between numbers which have the same greatest prime factor or have the same prime factors.

Let  $\exp e < a < b$  be integers. Suppose that  $P[a] = P[b]$ . Then TIJDEMAN [29] proved that

$$(8) \quad b - a \geq 10^{-6} \log \log a.$$

The proof of Tijdeman depends on Baker's estimate on the magnitude of integral solutions of Mordell's equation  $y^2 = x^3 + k$ . We remark that the inequality (8), apart from the constant, also follows from theorem 1. See ERDÖS and the author [9]. Suppose that for every prime  $p$ ,  $p|a$  if, and only if,  $p|b$ . Then, using theorem 1, ERDÖS and the author [9] proved that there exists a constant  $\delta > 0$  such that

$$b - a \gg (\log a)^\delta.$$

By using the work of STARK on  $y^2 = x^3 + k$ , LANGEVIN [15] proved the above inequality with  $\delta = \frac{1}{6} + \varepsilon$  for every  $\varepsilon > 0$ .

6. Greatest prime factor of a convergent of a continued fraction of a real algebraic number.

Let  $\alpha \notin \mathbb{Q}$  be a real algebraic number. Denote by  $p_n/q_n$ ,  $q_n > 0$ , the  $n$ -th convergent of the continued fraction of  $\alpha$ . It follows from a result of MAHLER [16] that  $P[p_n q_n]$  tends to infinity with  $n$ . Further it follows from a result of RIDOUT [20] that both  $P[p_n]$  and  $P[q_n]$  tend to infinity with  $n$ . However these results were not effective. Baker's first result [1] on linear forms in logarithms of algebraic numbers gives an effective version of Mahler's result. It follows from theorem 1 that for  $n \geq 2$

$$(9) \quad P[p_n q_n] \geq c_5 \log \log q_n$$

where  $c_5 > 0$  is an effectively computable constant depending only on  $\alpha$ .

Proof of inequality (9). - It is no loss of generality to assume that  $n \geq n_0$  where  $n_0$  is a large positive constant depending only on  $\alpha$ . Since  $q_n \geq n$ , we have  $q_n \geq n_0$ . We shall assume that the inequality

$$P[p_n q_n] \leq \delta \log_2 q_n$$

is satisfied for any  $\delta$  with  $0 < \delta < 1$  and arrive at a contradiction for a certain value of  $\delta$  depending only on  $\alpha$ . By prime number theory, it follows that

$$\max(\omega(p_n), \omega(q_n)) \leq 2\delta \frac{\log_2 q_n}{\log_3 q_n} := m.$$

First assume that  $\alpha > 0$ .

Write

$$p_n = s_1^{a_1} \dots s_m^{a_m}, \quad q_n = t_1^{b_1} \dots t_m^{b_m},$$

where  $s_1, \dots, s_m, t_1, \dots, t_m$  are primes and  $a_1, \dots, a_m, b_1, \dots, b_m$  are non negative integers. Further the integers  $s_i$  and  $t_j$  do not exceed  $\delta \log_2 q_n$  and  $a_i$ 's and  $b_i$ 's do not exceed  $c_6 \log q_n$  where  $c_6$  and the subsequent symbols  $c_7, c_8, \dots$  are positive constants depending only on  $\alpha$ . It is well known that

$$0 < \left| \alpha - \frac{p_n}{q_n} \right| < 1/q_n^2$$

i. e.

$$0 < |\alpha q_n p_n^{-1} - 1| < c_7 q_n^{-2}.$$

Since  $c_7 q_n^{-2} < 1/2$  for  $n \geq n_0$ , we have

$$0 < |\log \alpha + \log q_n - \log p_n| < 2c_7 q_n^{-2}$$

i. e.

$$(10) \quad 0 < \left| \log \alpha - \sum_{i=1}^m a_i \log s_i + \sum_{i=1}^m b_i \log t_i \right| < 2c_7 q_n^{-2}.$$

Here the logarithms have their principal values. Now apply theorem 1 with  $n = 2m + 1$ ,  $D = 1$ ,  $A \leq (c_8 \log_3 q_n)^{2m}$ ,  $B \leq c_6 \log q_n$  and  $E \leq c_q \log_2 q_n$ . We get

$$(11) \quad \left| \log \alpha + \sum_{i=1}^m a_i \log s_i - \sum_{i=1}^m b_i \log t_i \right| > \exp(-(\log q_n)^{c_{10} \delta}).$$

Combining (10) and (11), we get

$$(\log q_n)^{c_{10} \delta} \geq c_{11} \log q_n.$$

This is not possible if  $\delta = (2c_{10})^{-1}$  and  $n \geq n_0$ . This completes the proof of inequality (9) when  $\alpha > 0$ . If  $\alpha < 0$ , set  $\alpha = -\beta$  with  $\beta > 0$ . Now  $p_n < 0$ . We have  $0 < |-\beta - (p_n/q_n)| < 1/q_n^2$ , i. e.  $0 < |\beta - ((-p_n)/q_n)| < 1/q_n^2$ . Now proceed similarly as above. This completes the proof of inequality (9).

#### REFERENCES

- [1] BAKER (A.). - Linear forms in the logarithms of algebraic numbers, I, *Mathematika*, London, t. 13, 1966, p. 204-216.
- [2] BAKER (A.). - Linear forms in the logarithms of algebraic numbers, IV, *Mathematika*, London, t. 15, 1968, p. 204-216.

- [3] BIRKHOFF (G. D.) and VANDIVER (H. S.). - On the integral divisors of  $a^n - b^n$ , *Annals of Math.*, Series 2, t. 5, 1904, p. 173-180.
- [4] COATES (J.). - An effective  $p$ -adic analogue of a theorem of Thue, *Acta Arithm.*, Warszawa, t. 15, 1969, p. 279-305.
- [5] ERDÖS (P.). - On the greatest prime factor of  $\prod_{k=1}^x f(k)$ , *J. London math. Soc.*, t. 27, 1952, p. 379-384.
- [6] ERDÖS (P.). - Some recent advances and current problems in number theory, "Lectures on modern mathematics", Vol. III, p. 196-244. - New York, J. Wiley and Sons, 1965.
- [7] ERDÖS (P.) and SELFRIDGE (J. L.). - Some problems on the prime factors of consecutive integers, *Illinois J. Math.*, t. 11, 1967, p. 428-430.
- [8] ERDÖS (P.) and SELFRIDGE (J. L.). - Some problems on the prime factors of consecutive integers, II., "Proceedings of the Washington State University conference on number theory", p. 13-21. - Pullman, Washington State University, 1971.
- [9] ERDÖS (P.) and SHOREY (T. N.). - On the greatest prime factor of  $2^p - 1$  for a prime  $p$  and other expressions, *Acta Arithm.*, t. 30, 1976, p. 257-265.
- [10] GRIMM (C. A.). - A conjecture on consecutive composite numbers, *Amer. math. Monthly*, t. 76, 1969, p. 1126-1128.
- [11] JUTILA (M.). - On numbers with a large prime factor, II., *J. Indian math. Soc.*, t. 38, 1974, p. 125-130.
- [12] KEATES (M.). - On the greatest prime factor of a polynomial, *Proc. Edinburgh math. Soc.*, Series 2, t. 16, 1969, p. 301-308.
- [13] KOTOV (S. V.). - Greatest prime factor of a polynomial, *Math. Notes*, t. 13, 1973, p. 313-317 ; and [in Russian] *Mat. Zametki*, t. 13, 1973, p. 515-522.
- [14] LANGEVIN (M.). - Plus grand facteur premier d'entiers consécutifs, *C. R. Acad. Sc. Paris*, t. 280, 1975, Serie A, p. 1567-1570.
- [15] LANGEVIN (M.). - Plus grand facteur premier d'entiers voisins, *C. R. Acad. Sc. Paris*, t. 281, 1975, Série A, p. 491-493.
- [16] MAHLER (K.). - Ein Analogon zu einem Schneiderschen Satz, *Koninkl. Nederl. Akad. Wetensch., Proc.*, t. 39, 1936, p. 633-640 and p. 729-737.
- [17] RAMACHANDRA (K.). - Application of Baker's theory to two problems considered by Erdős and Selfridge, *J. Indian math. Soc.*, t. 37, 1973, p. 25-34.
- [18] RAMACHANDRA (K.) and SHOREY (T. N.). - On gaps between numbers with a large prime factor, *Acta Arithm.*, Warszawa, t. 24, 1973, p. 99-111.
- [19] RAMACHANDRA (K.), SHOREY (T. N.) and TLJDEMAN (R.). - On Grimm's problem relating to factorisation of a block of consecutive integers, II., *J. reine angew. Math.* (to appear).
- [20] RIDOUT (D.). - Rational approximations to algebraic numbers, *Mathematika*, London, t. 4, 1957, p. 125-131.
- [21] SCHINZEL (A.). - On primitive prime factors of  $a^n - b^n$ , *Proc. Cambridge philos. Soc.*, t. 58, 1962, p. 555-562.
- [22] SCHINZEL (A.). - On two theorems of Gel'fond and some of their applications, *Acta Arithm.*, Warszawa, t. 13, 1967, p. 177-236.
- [23] SHOREY (T. N.). - On gaps between numbers with a large prime factor, II., *Acta Arithm.*, Warszawa, t. 25, 1974, p. 365 - 373.
- [24] SHOREY (T. N.). - On linear forms in the logarithms of algebraic numbers, *Acta Arithm.*, Warszawa, t. 30, 1976, p. 37-42.
- [25] SHOREY (T. N.) and TLJDEMAN (R.). - On the greatest prime factor of polynomials at integer points (to appear).

- [26] SIEGEL (C. L.). - Approximation algebraischer Zahlen, Math. Z., t. 10, 1921, p. 173-213.
- [27] SPRINDŽUK (V. G.). - The greatest prime factor of a binary form, Dokl. Akad. Nauk BSSR, t. 15, 1971, p. 389-391.
- [28] STEWART (C. L.). - The greatest prime factor of  $a^n - b^n$ , Acta Arithm., Warszawa, t. 26, 1975, p. 427-433.
- [29] TIJDEMAN (R.). - On integers with many small prime factors, Compositio Math., Groningen, t. 26, 1973, p. 319-330.
- [30] ZSIGMONDY (K.). - Zur Theorie der Potenzreste, Monatsh. für Math., t. 3, 1892, p. 265-289.

(Texte reçu le 19 janvier 1976)

T. N. SHOREY  
Mathematisch Instituut  
Post Box 2160  
LEIDEN (Pays-Bas)

and

Tata Institute of Fundamental Research  
BOMBAY 5 (Inde)

---