

- [8] А. В. Малышев и У. М. Пачев, *Об арифметике матриц второго порядка*, В сб.: *Исследования по теории чисел*. 6, Зап. научн. семинаров ЛОМИ, т. 93, 1980, 41–86.
- [9] Ю. Г. Тетерин, *Действие группы классов на представлениях чисел тернарной квадратичной формой. Формулы Зигеля и Кнезера-Сии-Петерса*, В сб.: *Исследования по теории чисел*. 9, Зап. научн. семинаров ЛОМИ, т. 151, 1986, 141–158.
- [10] Н. Г. Чеботарев, *Основы теории Галуа*, ч. 2, Ленинград–Москва 1937, 159 с.
- [11] *Algebraic Number Theory* (ed. by J. W. S. Cassels and A. Fröhlich), London–New York 1967 [русск. пер. *Алгебраическая теория чисел* (под ред. Дж. Касселса и А. Фрелиха), Москва 1969, 483 с.]
- [12] J. W. S. Cassels, *Rational quadratic forms*, London 1978, xvi, 413 p. [русск. пер.: Дж. Касселс, *Рациональные квадратичные формы*, Москва 1982, 436 с.]
- [13] Cl. Chevalley, *Sur certains idéaux d'un algèbre simple*, Abh. Math. Seminar Hamburg. Univ. 10 (1934), 83–105.
- [14] M. Deuring, *Algebren*, Berlin 1935 (1968), viii, 143 p.
- [15] M. Eichler, *The basis problem for modular form and the traces of the Hecke operators*, in: *Modular functions of one variable*, I, Lect. Notes in Math., 320, Berlin 1973, 75–151.
- [16] H. Hasse, *Über gewisse Ideale in einer einfachen Algebra*, Act. Sci. Ind. 109, Paris 1934, 16 p.
- [17] H. Hijikata, *Explicit formula of the traces of Hecke operators for  $\Gamma_0(N)$* , J. Math. Soc. Japan 26 (1974), 56–82.
- [18] W. Kořinek, *Maximale kommutative Körper in einfachen Systemen hyperkomplexer Zahlen*, Mém. Soc. Sci. Bohême 1932, 1 (1933), 1–24.
- [19] A. V. Malyshev, *Yu. V. Linnik's ergodic method in number theory*, Acta Arith. 27 (1975), 555–598.
- [20] O. T. O'Meara, *Introduction to quadratic forms*, Berlin 1963 (1971, 1973), xi, 342 p.
- [21] E. Noether, *Zerfallende verschränkte Produkte und ihre Maximalordnungen*, Act. Sci. Ind. 111, Paris 1934.
- [22] H. P. Rehm, *On a theorem of Gauss concerning the number of integral solutions of the equation  $x^2 + y^2 + z^2 = m$* , In: *Ternary quadratic forms and norms*, New York–Basel 1982, 31–38.
- [23] I. Reiner, *Maximal orders*, London 1975, xii, 395 p.
- [24] B. Rice, *Quaternions and binary quadratic forms*, Proc. Amer. Math. Soc. 27 (1971), 1–7.
- [25] T. R. Shemanske, *Representations of ternary quadratic forms and the class number of imaginary quadratic fields*, Pacific J. Math. 122 (1986), 223–250.
- [26] M.-F. Vignéras, *Arithmétique des algèbres de quaternions*, Lect. Notes in Math. 800, Berlin 1980, vii, 169 p.
- [27] A. Weil, *Basic number theory*, Berlin 1967 [русск. пер.: А. Вейль, *Основы теории чисел*, Москва 1972, 408 с.]

Поступило 22.11.1988

(1883)

## On the greatest prime factor of an arithmetical progression (II)

by

T. N. SHOREY (Bombay) and R. TIJDEMAN (Leiden)

*To the memory of Professor V. G. Sprindžuk*

1. For an integer  $v > 1$ , we denote by  $P(v)$  the greatest prime factor of  $v$  and we write  $\omega(v)$  for the number of distinct prime factors of  $v$ . We put  $P(1) = 1$  and  $\omega(1) = 0$ . Let  $a$ ,  $d$  and  $k$  be positive integers satisfying  $\gcd(a, d) = 1$  and  $k \geq 3$ . We put

$$\chi = a + (k-1)d, \quad \chi_1 = \chi/k, \quad \chi_2 = \max(\chi_1, 3),$$

$$\Delta(a; d) = a(a+d) \dots (a+(k-1)d)$$

and

$$P = P(\Delta(a; d)), \quad \omega = \omega(\Delta(a; d)).$$

A classical theorem of Sylvester [5] states that

$$(1) \quad P > k \quad \text{if } a \geq d+k.$$

Langevin [2] improved (1) to

$$P > k \quad \text{if } a > k.$$

Further, Shorey and Tijdeman [4] showed that

$$(2) \quad P > k \quad \text{if } d \geq 2 \quad \text{and} \quad (a, k, d) \neq (2, 3, 7).$$

Also, Langevin [3] obtained results which imply that, under suitable conditions, there exists some number  $r > 1$  such that

$$P > C_1 k \log \log a \quad \text{if } a > k^r$$

where  $C_1 > 0$  is an effectively computable number depending only on  $r$ . This is an immediate consequence of the following result.

**THEOREM 1.** *Let  $\varepsilon > 0$  and*

$$(3) \quad \chi > k^{1+\varepsilon}.$$

There exists an effectively computable number  $C_2 > 0$  depending only on  $\varepsilon$  such that

$$(4) \quad P > C_2 k \log \log \chi.$$

By taking  $a = 1$  and  $d = [(\log \log \chi)^{1/2}]$ , we observe that the restriction (3) cannot be relaxed to  $\chi > k$ . On the other hand, the assumption (3) is no more necessary if we are contented with  $\log \log \chi_2$  instead of  $\log \log \chi$  in estimate (4). See Corollary 1.

More precisely, we prove:

**THEOREM 2.** *Let  $\varepsilon > 0$ . There exist effectively computable numbers  $C_3$  and  $C_4 > 0$  depending only on  $\varepsilon$  such that for  $\chi_1 \geq C_3$ , either*

$$(5) \quad \omega \geq (1 - \varepsilon)k \frac{\log \chi_1}{\log k}$$

or

$$(6) \quad P \geq C_4 k \log \log \chi.$$

The following result follows immediately from Theorem 2 and (2).

**COROLLARY 1.** *There exists an effectively computable absolute constant  $C_5 > 0$  such that*

$$(7) \quad P \geq C_5 k \log \log \chi_2.$$

For deriving Corollary 1, we observe that (7) is a consequence of (2) if  $\chi_1$  is bounded. In fact, in this case, it follows immediately from the Prime Number Theorem for arithmetical progressions that for  $\varepsilon > 0$  and  $\psi > 0$  with  $\chi_1 \leq \psi$ , there exists an effectively computable number  $C_6$  depending only on  $\varepsilon$  and  $\psi$  such that for  $k \geq C_6$ , we have

$$\omega \geq (1 - \varepsilon)k / \log k \quad \text{and} \quad P \geq (1 - \varepsilon)\chi.$$

2. In this section, we state results that we shall use from other sources for the proof of our theorems. Let  $F(X, Y) \in \mathbb{Z}[X, Y]$  be a binary form with at least three distinct linear factors in its factorisation over  $\mathbb{C}$ . Denote by  $L$  the splitting field of  $F$  and we write  $l$ ,  $R_L$  and  $h_L$ , respectively, for the degree, regulator and class number of  $L$ . Let  $H(F)$  be the maximum of the absolute values of the coefficients of  $F$ . Let  $p_1, \dots, p_s$  be distinct prime numbers and  $A$  some non-zero rational integer. We start with the following theorem of Györy [1] on an estimate for integer solutions of Thue–Mahler equations.

**LEMMA 1.** *All solutions of the Thue–Mahler equation*

$$F(x, y) = Ap_1^{z_1} \dots p_s^{z_s}$$

in  $x, y, z_1, \dots, z_s$  with  $\gcd(x, y) = 1, z_1 \geq 0, \dots, z_s \geq 0$  satisfy

$$\log(\max(|x|, |y|)) \leq C_7(s+1)^{C_8(s+1)} P^{2l} (1 + \log(|A|H(F)))$$

where  $C_7$  and  $C_8$  are effectively computable numbers such that  $C_7$  depends only on  $l, R_L, h_L$  and  $C_8$  only on  $l$ .

The next lemma contains an elementary fundamental argument of Erdős.

**LEMMA 2.** *Let*

$$S \subseteq \{a, a+d, \dots, a+(k-1)d\}, \quad s_0 = \min_{s \in S} s.$$

Denote by  $T$  the set of all elements  $s \in S$  such that  $P(s) \leq k$ . Then

$$(8) \quad |T| \leq \frac{k \log k}{\log s_0} + \pi(k).$$

**Proof.** For every  $p \leq k$ , we choose an  $f(p) \in T$  such that  $p$  does not appear to a higher power in the factorisation of any other element of  $T$ . Denote by  $T_1$  the set obtained from  $T$  by deleting all  $f(p)$  with  $p \leq k$ . Then

$$|T_1| \geq |T| - \pi(k)$$

and

$$s_0^{|T| - \pi(k)} \leq \prod_{t \in T_1} t \leq \prod_{p \leq k} p^{\lfloor \frac{k}{p} \rfloor + \lfloor \frac{k}{p^2} \rfloor + \dots} = k!$$

which implies (8).

3. We apply Lemma 2 to obtain the following result.

**LEMMA 3.** *Let  $\varepsilon > 0, V \geq 2$  and  $\chi > e^e$ . If*

$$(9) \quad \log k \leq (\log \log \chi)^V, \quad P \leq (\log \chi)^{1/2 - \varepsilon}$$

then

$$(10) \quad \omega \geq C_9 k \frac{\log \log \chi}{\log \log \log \chi}$$

and

$$(11) \quad P \geq C_{10} k \frac{\log \log \chi}{\log \log \log \chi} (\log k + \log \log \log \chi)$$

where  $C_9 > 0$  and  $C_{10} > 0$  are effectively computable numbers depending only on  $\varepsilon$  and  $V$ .

**Proof.** We denote by  $C_{11}, \dots, C_{16}$  effectively computable positive numbers depending only on  $\varepsilon$  and  $V$ . If  $k \leq C_{11}$ , we apply Lemma 1 with

$$(12) \quad F(X, Y) = X(X+Y)(X+2Y)$$

to conclude (10). Thus, we may assume that  $k \geq C_{12}$  with  $C_{12}$  sufficiently large.

Now, we apply Lemma 1 to the binary form (12) to derive from (9) that

$$\omega((a + \mu d)(a + \mu d + d)(a + \mu d + 2d)) \geq C_{13} \frac{\log \log \chi}{\log \log \log \chi}$$

for  $k/2 \leq \mu < k$ . Consequently, we obtain

$$\begin{aligned} \omega &\geq C_{14} k \frac{\log \log \chi}{\log \log \log \chi} - \sum_{p \leq k} \left( \left\lfloor \frac{k}{p} \right\rfloor + 1 \right) \\ &\geq C_{15} k \left( \frac{\log \log \chi}{\log \log \log \chi} - \log \log k \right) \geq C_{16} k \frac{\log \log \chi}{\log \log \log \chi}, \end{aligned}$$

the last inequality follows from (9). Then, the assertion (11) follows immediately from Prime Number Theory.

Lemma 3 admits the following consequence.

COROLLARY 2. Let  $\varepsilon > 0$  and  $\chi > e^e$ . If

$$(13) \quad k < (\log \chi)^{1/2 - \varepsilon}$$

then

$$P \geq C_{17} k \frac{\log \log \chi}{\log \log \log \chi} (\log k + \log \log \log \chi)$$

where  $C_{17}$  is an effectively computable number depending only on  $\varepsilon$ .

Proof. In view of Lemma 3 with  $V = 2$  and  $\varepsilon$  replaced by  $\varepsilon/2$ , we may assume that

$$P \geq (\log \chi)^{(1 - \varepsilon)/2}$$

which, together with (13), proves Corollary 2.

LEMMA 4. Let  $\varepsilon > 0$ . There exist effectively computable numbers  $C_{18}$  and  $C_{19} > 0$  depending only on  $\varepsilon$  such that for  $k \geq C_{18}$  and  $\chi_1 \geq C_{18}$  we have

$$(14) \quad \omega \geq k \min \left( (1 - \varepsilon) \frac{\log \chi_1}{\log k}, C_{19} \right).$$

Proof. We may assume that  $0 < \varepsilon < 1$  and that  $C_{18}$  is sufficiently large. We put  $\varepsilon_1 = \varepsilon/4$ . Suppose  $a < \varepsilon_1 \chi$ . Then, we write  $\mu$  for the least positive integer such that  $A := a + \mu d \geq \varepsilon_1 \chi$ . Thus  $A - d < \varepsilon_1 \chi$  and

$$(k - 1 - \mu)d = \chi - A > (1 - \varepsilon_1)\chi - d$$

which implies that

$$k - \mu > (1 - \varepsilon_1)(k - 1) \geq (1 - 2\varepsilon_1)k.$$

Therefore, we conclude that there exists some  $\mu$  with  $0 \leq \mu \leq 2\varepsilon_1 k$  such that  $a + \mu d \geq \varepsilon_1 \chi$ .

We put  $K = k - \mu$  and we denote by  $S$  the set of all integers  $A, A + d, \dots, A + (K - 1)d$ . Let  $T$  be the set of all elements  $s \in S$  with  $P(s) \leq K$ . Then

$$\omega \geq |S| - |T| = K - |T|.$$

Further, we apply Lemma 2 with  $s_0 \geq \varepsilon_1 \chi$  to derive that

$$|T| \leq \frac{K \log K}{\log s_0} + \pi(K) = \left( \frac{\log K}{\log k} \right) \frac{K}{1 + \nu} + \pi(K) \leq \frac{K}{1 + \nu} + \pi(K)$$

where

$$\nu = \frac{\log(\varepsilon_1 \chi_1)}{\log k} \geq (1 - \varepsilon_1) \frac{\log \chi_1}{\log k}$$

if  $C_{18}$  is sufficiently large.

First, we suppose that

$$(15) \quad \chi < k^{1/(1 - \varepsilon_1)}.$$

Then  $\nu < \varepsilon_1/(1 - \varepsilon_1)$  and  $|T| \leq K(1 - (1 - \varepsilon_1)\nu) + \pi(K)$ . Therefore

$$\omega \geq K(1 - \varepsilon_1)\nu - \pi(K) \geq (1 - 2\varepsilon_1)K \frac{\log \chi_1}{\log k} \geq (1 - \varepsilon)k \frac{\log \chi_1}{\log k},$$

since  $K \geq (1 - 2\varepsilon_1)k$ . Thus, we may assume that (15) is not valid. Then  $\nu \geq \varepsilon_1$  and

$$|T| \leq C_{20}K$$

where  $0 < C_{20} < 1$  is an effectively computable number depending only on  $\varepsilon$ . Thus

$$\omega \geq (1 - C_{20})(1 - 2\varepsilon_1)k.$$

This completes the proof of Lemma 4.

4. Proof of Theorem 1. We may assume that  $0 < \varepsilon < 1$ . By Corollary 2 and (3), we may suppose that  $k \geq C_{18}^{1/\varepsilon} > C_{18}$  and  $\chi_1 > k^\varepsilon \geq C_{18}$ . Now, we apply Lemma 4 and Prime Number Theory to derive that

$$(16) \quad P > C_{21}k \log k$$

where  $C_{21} > 0$  is an effectively computable number depending only on  $\varepsilon$ . Furthermore, in view of Corollary 2, we may suppose that

$$(17) \quad k \geq (\log \chi)^{1/2 - \varepsilon}.$$

Finally, we combine (16) and (17) to obtain (4).

Proof of Theorem 2. We refer to Corollary 2 to assume that  $k \geq C_{18}$  and (17). Let  $C_3 > C_{18}$ . Then, if (5) is not valid, we refer to Lemma 4 to derive that  $\omega \geq C_{19}k$  which implies (16). Hence, the assertion (6) follows from (16) and (17).

## References

- [1] K. Györy, *Explicit upper bounds for the solutions of some diophantine equations*, Ann. Acad. Sci. Fenn. Ser. AI 5 (1980), 3–12.
- [2] M. Langevin, *Plus grand facteur premier d'entiers en progression arithmétique*, Séminaire Delange–Pisot–Poitou, 18e année, 1976/77, no 3, 6 p.
- [3] — *Facteurs premiers d'entiers en progression arithmétique*, Acta Arith. 39 (1981), 241–249.
- [4] T. N. Shorey and R. Tijdeman, *On the greatest prime factor of an arithmetical progression*, to appear.
- [5] J. J. Sylvester, *On arithmetic series*, Messenger Math. 21 (1892), 1–19 and 87–120.

SCHOOL OF MATHEMATICS  
TATA INSTITUTE OF FUNDAMENTAL RESEARCH  
Homi Bhabha Road  
Bombay 400005  
India

MATHEMATICAL INSTITUTE  
R.U. LEIDEN  
Postbus 9512  
2300 RA Leiden  
The Netherlands

Received on 22.11.1988

(1884)

Abonnements  
Échange  
Numéros antérieurs

Subscriptions  
Library exchange  
Back numbers

Abonnement  
Austausch  
Ankauf

Подписка  
Книгообмен  
Продажа

Institut Matematyczny Polskiej Akademii Nauk  
skr. poczt. 137, 00-950 Warszawa, telex PL 816112

BOOKS PUBLISHED BY THE POLISH ACADEMY OF SCIENCES  
INSTITUTE OF MATHEMATICS

- S. Banach, *Oeuvres*, vol. II, 1979, 470 pp.
- S. Mazurkiewicz, *Travaux de topologie et ses applications*, 1969, 380 pp.
- W. Sierpiński, *Oeuvres choisies*, vol. I, 1974, 300 pp.; vol. II, 1975, 780 pp.; vol. III, 1976, 688 pp.
- J. P. Schauder, *Oeuvres*, 1978, 487 pp.
- K. Borsuk, *Collected papers*, Parts I, II, 1983, xxiv+1357 pp.
- H. Steinhaus, *Selected papers*, 1985, 899 pp.
- K. Kuratowski, *Selected papers*, 1988, Lii+610 pp.
- W. Orlicz, *Collected papers*, Parts I, II, 1988, Liv+viii+1688 pp.
- T. Ważewski, *Selected papers*, 1990, xx+572 pp.

MONOGRAFIE MATEMATYCZNE

43. J. Szarski, *Differential inequalities*, 2nd ed., 1967, 256 pp.
50. K. Borsuk, *Multidimensional analytic geometry*, 1969, 443 pp.
51. R. Sikorski, *Advanced calculus. Functions of several variables*, 1969, 460 pp.
58. C. Bessaga and A. Pełczyński, *Selected topics in infinite-dimensional topology*, 1975, 353 pp.
59. K. Borsuk, *Theory of shape*, 1975, 379 pp.
62. W. Narkiewicz, *Classical problems in number theory*, 1986, 363 pp.

BANACH CENTER PUBLICATIONS

- Vol. 10. *Partial differential equations*, 1983, 422 pp.
- Vol. 11. *Complex analysis*, 1983, 362 pp.
- Vol. 12. *Differential geometry*, 1984, 288 pp.
- Vol. 13. *Computational mathematics*, 1984, 792 pp.
- Vol. 14. *Mathematical control theory*, 1985, 643 pp.
- Vol. 15. *Mathematical models and methods in mechanics*, 1985, 725 pp.
- Vol. 16. *Sequential methods in statistics*, 1985, 554 pp.
- Vol. 17. *Elementary and analytic theory of numbers*, 1985, 498 pp.
- Vol. 19. *Partial differential equations*, 1987, 397 pp.
- Vol. 20. *Singularities*, 1988, 498 pp.
- Vol. 21. *Mathematical problems in computation theory*, 1988, 597 pp.
- Vol. 22. *Approximation and function spaces*, 1989, 486 pp.
- Vol. 23. *Dynamical systems and ergodic theory*, 1989, 479 pp.
- Vol. 24. *Numerical analysis and mathematical modelling*, 1990, 566 pp.
- Vol. 25. *Combinatorics and graph theory*, 1989, 251 pp.
- Vol. 26. *Topics in algebra*, Part 1 and 2, in the press.

Władysław Narkiewicz

15000.zł

## CLASSICAL PROBLEMS IN NUMBER THEORY

363 pp., cloth bound

The development of the theory of numbers centres around certain old problems and this book is devoted to some of them. The author's aim was to give a survey of the history of selected problems, presenting proofs of the major results concerning them and indicating the current state of research. Necessarily a choice of problems had to be made, and it was influenced by the wish to demonstrate various techniques. Two major omissions are to be noted: Fermat's Last Theorem and problems of distribution of primes.

*Contents:* Elementary problems (perfect numbers, Mersenne numbers, Euler's function, Egyptian fractions); Primitive roots (character sums, least primitive roots, Artin's conjecture); Problems on consecutive integers (Catalan's conjecture, Erdős-Selfridge theorem, Grimm's conjecture); Waring's theorem; Binary quadratic forms.

Wacław Sierpiński

## OEUVRES CHOISIES

Tome I: BIBLIOGRAPHIE, THÉORIE DES NOMBRES,  
ANALYSE MATHÉMATIQUE

Tome II: THÉORIE DES ENSEMBLES ET SES APPLICATIONS  
TRAVAUX DES ANNÉES 1908-1929

Tome III: THÉORIE DES ENSEMBLES ET SES APPLICATIONS  
TRAVAUX DES ANNÉES 1930-1966

Les oeuvres choisies de Wacław Sierpiński sont réunies en trois volumes dont le premier contient les travaux sur la Théorie des Nombres et l'Analyse Mathématique et les deux autres — ceux de la Théorie des Ensembles et ses applications.

La liste complète des travaux scientifiques de Wacław Sierpiński en comporte 724. Les travaux choisis pour être publiés se distinguent soit par leur actualité, soit par leur importance pour le développement des mathématiques, soit encore par la beauté intrinsèque des résultats obtenus et des méthodes employées.

Stefan Banach

## OEUVRES

Volume II

TRAVAUX SUR L'ANALYSE FONCTIONNELLE

470 p., relié

Ce volume contient tous les travaux d'analyse fonctionnelle de Stefan Banach, ainsi que son fondamental traité "Théorie des opérations linéaires" et une bibliographie de ses écrits. Une ample étude de Aleksander Pełczyński présente une revue des recherches relatives aux parties de l'analyse fonctionnelle qui ont eu pour point de départ le traité de Banach et les résultats qui y sont exposés.

---

To be ordered at your bookseller or directly at

Institute of Mathematics, Polish Academy of Sciences

P.O. Box 137, 00-950 Warszawa, Poland, telex PL 816112

Sprzedaż numerów bieżących i archiwalnych w księgarni Ośrodka  
Rozpowszechniania Wydawnictw Naukowych PAN, ORPAN, Pałac Kultury  
i Nauki, 00-901 Warszawa

---

ISBN 83-01-09787-6

ISSN 0065-1036