[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. Kořínek, *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)

ACTA ARITHMETICA
LIII (1990)

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

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

and

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

A classical theorem of Sylvester [5] states that

$$P > k \quad \text{if } a \geqslant d+k. \tag{1}$$

Langevin [2] improved (1) to

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

Further, Shorey and Tijdeman [4] showed that

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

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*

$$\chi > k^{1+\varepsilon}. \tag{3}$$

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

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

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 ε such that for $\chi_1 \geqslant C_3$, either*

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

or

(6) $$P \geqslant C_4 k \log\log \chi.$$

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) $$P \geqslant C_5 k \log\log \chi_2.$$

For deriving Corollary 1, we observe that (7) is a consequence of (2) if χ_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 $\chi_1 \leqslant \psi$, there exists an effectively computable number C_6 depending only on ε and ψ such that for $k \geqslant C_6$, we have

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

2. In this section, we state results that we shall use from other sources for the proof of our theorems. Let $F(X, Y) \in \mathbf{Z}[X, Y]$ be a binary form with at least three distinct linear factors in its factorisation over $\mathbf{C}$. 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 $p_1, \ldots, p_s$ be distinct prime numbers and A some non-zero rational integer. We start with the following theorem of Győry [1] on an estimate for integer solutions of Thue–Mahler equations.

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

$$F(x, y) = A p_1^{z_1} \ldots p_s^{z_s}$$

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

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

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*

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

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

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

Proof. For every $p \leqslant k$, 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 $p \leqslant k$. Then

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

and

$$s_0^{|T|-\pi(k)} \leqslant \prod_{t \in T_1} t \leqslant \prod_{p \leqslant k} p^{[\frac{k}{p}]+[\frac{k}{p^2}]+\cdots} = k!$$

which implies (8).

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

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

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

then

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

and

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

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

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

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

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

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

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

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

$$\omega \geqslant C_{14}k\frac{\log\log\chi}{\log\log\log\chi} - \sum_{p\leqslant k}\left(\left[\frac{k}{p}\right]+1\right)$$

$$\geqslant C_{15}k\left(\frac{\log\log\chi}{\log\log\log\chi} - \log\log k\right) \geqslant C_{16}k\frac{\log\log\chi}{\log\log\log\chi},$$

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*

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

then

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

where C_{17} *is an effectively computable number depending only on* ε.

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

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

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* ε *such that for* $k \geqslant C_{18}$ *and* $\chi_1 \geqslant C_{18}$ *we have*

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

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 μ for the least positive integer such that $A := a+\mu d \geqslant \varepsilon_1\chi$. Thus $A - d < \varepsilon_1\chi$ and

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

which implies that

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

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

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

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

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

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

where

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

if C_{18} is sufficiently large.

First, we suppose that

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

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

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

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

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

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

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

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 $k \geqslant C_{18}^{1/\varepsilon} > C_{18}$ and $\chi_1 > k^\varepsilon \geqslant C_{18}$. Now, we apply Lemma 4 and Prime Number Theory to derive that

$$P > C_{21}k\log k \tag{16}$$

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

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

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

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

References

[1] K. Győry, *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)

ISBN 83-01-09787-6 ISSN 0065-1036