ACTA ARITHMETICA
LXI.4 (1992)

On the number of prime factors of a finite arithmetical progression

by

T. N. Shorey (Bombay) and R. Tijdeman (Leiden)

1. Introduction. Let a, d and k be positive integers with $d > 1$, $k > 2$, $\gcd(a, d) = 1$. Put $\Delta = a(a+d)\dots(a+(k-1)d)$. Denote by $P(x)$ and $\omega(x)$ the greatest prime factor and the number of distinct prime divisors of x, respectively. Put $\omega = \omega(a, d, k) = \omega(\Delta)$ and $\chi = a + (k-1)d$. In this paper we derive lower bounds for ω as a function of χ and k. In [8] we proved that $\omega \geq \pi(k)$ where $\pi(x)$ denotes the number of prime numbers $\leq x$. This bound is not bad for small a and d as we obviously have $\omega \leq \pi(\chi)$. For a further study of cases with ω near to $\pi(k)$, see Moree [5]. Since it has not yet been disproved (and it is even conjectured to be true!) that there are arbitrarily long arithmetical progressions $d+1, 2d+1, \dots, (k-1)d+1$ consisting of primes, we cannot expect to be able to prove anything better than $\omega \geq k-1$ for χ large.

In Section 2 we consider values of χ up to e^k. By using combinatorial methods we prove in Theorem 1 that $\omega \geq \lfloor k\log(\chi/k)/\log\chi\rfloor$ where $\lfloor\ \rfloor$ denotes the integer part function. In Theorem 2 we show that the bound is not far from the best possible in certain ranges. In Theorem 3 we obtain a sharpening of Theorem 1 for values of χ larger than a constant power of k.

In Section 3 we apply estimates for linear forms in (p-adic) logarithms of algebraic numbers. Corollary 4.2 states that $\omega \geq k-1$ if $\log\chi \gg_\varepsilon k^{4/3+\varepsilon}$ and provides a characterization of the cases with $\omega = k-1$. This is derived from Corollary 4.1. In Corollary 4.1 and Theorem 5 we obtain bounds of the form $\omega \geq k + (1-\varepsilon)\pi_d(k)$ and $\omega \geq k + \pi_d(k) - 2$ where $\pi_d(k)$ denotes the number of primes $\leq k$ coprime to d. In Theorem 5 the condition even becomes $\log\log\chi \gg k$.

Finally, in Section 4, we assume that $P(d)$ or $P(a)$ is bounded from above by a suitable power of $\log\chi$. In Theorem 6 we derive the inequality $\omega \geq k + (1-\varepsilon)\pi_d(k)$ under the rather weak assumption that $\log\chi$ exceeds a constant power of $\log k$ (in place of k). The used method is similar to the one applied in Section 3. For the place of the obtained results with respect to the existing literature we refer to the survey papers [9] or [10].

2. Bounds for ω if χ is small. We use the notation of the first paragraph of the Introduction. Let G be the set of primes p with $p \le k$ and $\gcd(p,d)=1$. Then $\pi_d(k)=|G|$ where $|A|$ denotes the cardinality of a set A. For every $p \in G$ we choose an $f(p) \in \{0,1,\ldots,k-1\}$ such that

$$\mathrm{ord}_p(a+f(p)d) = \max_{0\le j<k} \mathrm{ord}_p(a+jd).$$

We write H for the set of all i with $0 \le i < k$ such that $P(a+id) \le k$. We denote by H_0 the set of all elements of H which do not appear in the range of f. Note that

$$\omega \ge k+\pi_d(k)-|H| \ge k-|H_0|. \tag{2.1}$$

It will turn out that the following simple and known estimations are very useful.

Lemma 1. (a) $\prod_{j\in H_0}(a+jd) \le (k-1)!$,

(b) $\mathrm{lcm}_{j\in H_0}(a+jd) < k^{\pi_d(k)}$.

Proof. (a) By counting the multiplicities of primes on both sides we have

$$\prod_{j\in H_0}(a+jd) \le \prod_{p<k} p^{\lfloor \frac{k-1}{p}\rfloor + \lfloor \frac{k-1}{p^2}\rfloor + \cdots} = (k-1)!.$$

(b) For every $p \in G$ and $j \in H_0$ we have $\gcd(a+jd, a+f(p)d) < k$. ∎

Theorem 1.

$$\omega \ge \left\lfloor k\frac{\log(\chi/k)}{\log\chi}\right\rfloor.$$

Proof. Put $t = \lfloor k\log(\chi/k)/\log\chi\rfloor$. We assume that $t>0$. Suppose $\omega \le t-1$. Then $|H_0| \ge k-t+1$ in view of (2.1). Hence, by Lemma 1(a),

$$\prod_{j=0}^{k-t}(a+jd) \le (k-1)!\,,$$

from which it follows that

$$\left(\frac{\chi}{k-1}\right)^{k-t}(k-t)! \le \prod_{j=1}^{k-t} j\left(\frac{a}{k-1}+d\right) \le (k-1)!.$$

We infer from the above inequality that $(\chi/k)^{k-t} \le k^{t-1}$, whence $\chi^{k-t} \le k^{k-1}$ and

$$t \ge k-(k-1)\frac{\log k}{\log\chi} > k\left(1-\frac{\log k}{\log\chi}\right).$$

This contradicts the definition of t. ∎

The following result shows that Theorem 1 is not far from best possible if $\chi < k^c$ for some constant c.

THEOREM 2. *For every prime number d and every positive integer $k > 2$ there exists a positive integer $a < d$ such that*

$$\omega \le k \log \frac{\log \chi}{\log k} + c_1 \frac{k}{\log k}$$

where c_1 is some absolute constant.

Proof. We shall use

$$\sum_{p \le x} \frac{1}{p} = \log\log x + C + O\left(\frac{1}{\log x}\right), \qquad x \to \infty,$$

where C is some absolute constant (see [4], pp. 350–351). Hence

$$\sum_{k<p\le kd} \left\lfloor \frac{kd}{p} \right\rfloor \le kd \sum_{k<p\le kd} \frac{1}{p} = kd \log \frac{\log(kd)}{\log k} + O\left(\frac{kd}{\log k}\right).$$

The left side equals the number of positive integers $\le kd$ which are divisible by a prime number $> k$ counted according to their multiplicities. We split the integers from 1 to kd coprime to d into $d-1$ arithmetical progressions of length k with difference d. Hence there exists an integer a with $0 < a < d$ such that $\omega = \omega(a,d,k)$ satisfies

$$\omega \le \pi(k) + \frac{kd}{d-1} \log \frac{\log(kd)}{\log k} + O\left(\frac{k}{\log k}\right)$$

where the first term on the right side counts the prime factors $\le k$ and the others majorize the remaining prime factors. Note that $(k-1)d < \chi < kd$. Hence

$$\begin{aligned}\frac{kd}{d-1} \log \frac{\log(kd)}{\log k} \\ &= k \log \frac{\log \chi}{\log k} + O\left(\frac{k}{d} \log \frac{\log(kd)}{\log k}\right) + O\left(k \log \frac{\log(kd)}{\log((k-1)d)}\right) \\ &= k \log \frac{\log \chi}{\log k} + O\left(\frac{k \log d}{d \log k}\right) + O\left(\frac{1}{\log(kd)}\right). \ \blacksquare\end{aligned}$$

Remark. If $\log \chi = (1+o(1)) \log k$ and $\chi/k \to \infty$, then according to Theorem 1

$$\omega \ge (1+o(1)) k \frac{\log(\chi/k)}{\log k}, \qquad k \to \infty, \tag{2.2}$$

and by Theorem 2 there are instances with

$$\omega \le (1+o(1)) k \frac{\log(\chi/k)}{\log k}. \tag{2.3}$$

This implies that Theorem 1 cannot be improved on by any constant factor > 1. The situation occurs when $\chi = (1+o(1))k(\log k)^c$ $(c > 1)$ whence

$$\omega \ge (1+o(1))ck\frac{\log\log k}{\log k}$$

and if $\chi = (1+o(1))ke^{(\log k)^\delta}$ $(0 < \delta < 1)$, whence

$$\omega \ge (1+o(1))k(\log k)^{\delta-1}.$$

If $\chi = (1+o(1))k^c$ for some $c > 1$, then Theorem 1 implies $\omega \gg_c k$ and Theorem 2 the existence of cases with $\omega \ll_c k$, so that the ratio of upper and lower bound is bounded.

If $\chi > \exp(k^\delta)$ for some $\delta > 0$, then the next theorem provides a better lower bound than Theorem 1 does.

THEOREM 3. *Let t be any positive integer. If*

$$\frac{\log\chi}{\log k} > \frac{\pi_d(k)}{t} + \frac{t+1}{2}, \tag{2.4}$$

then $\omega \ge k - t$.

In the proof we use the following version of Lemma 4 of [7].

LEMMA 2. *If $a_1, a_2, \ldots, a_n$ are any positive integers, then*

$$\prod_{j=1}^{n} a_j \le \operatorname{lcm}(a_1, a_2, \ldots, a_n) \prod_{1\le i<j\le n} \gcd(a_i, a_j).$$

Proof. For any prime p choose a_{i_p} such that p does not appear to a higher power in the factorisation of any other number $a_1, a_2, \ldots, a_n$. Then the number of factors p dividing the left side is equal to the number of factors p dividing

$$a_{i_p}\prod_{i\ne i_p}\gcd(a_i, a_{i_p}). \ ■$$

Proof of Theorem 3. Suppose that $t < k$ and $\omega < k-t$. Hence, by (2.1), $t < |H_0|$. Choose a subset J of positive elements of H_0 with $|J| = t$. By Lemma 2 we have

$$\prod_{j\in J}(a+jd) \le \operatorname{lcm}_{j\in J}(a+jd) \prod_{\substack{i,j\in J\\ i<j}} \gcd(a+id, a+jd).$$

Observe that $a + jd \ge \chi/k$ for $j \in J$ and that $\gcd(a+id, a+jd) \le k$ for $0 < i < j < k$. Hence, by Lemma 1(b),

$$(\chi/k)^t \le k^{\pi_d(k)}k^{\binom{t}{2}}.$$

This implies

$$\frac{\log \chi}{\log k} \le \frac{\pi_d(k)}{t} + \frac{t+1}{2},$$

contradicting (2.4). ∎

Since $\pi_d(k) \le \pi(k) < (1+\varepsilon)k/\log k$ for $k \ge k_0(\varepsilon)$ according to the prime number theorem, we have the following consequences:

If $\chi \ge \exp(k^{\delta})$ $(\frac{1}{2} < \delta < 1)$ then $\omega \ge k - (1+\varepsilon)k^{1-\delta}$ for $k \ge k_0(\delta, \varepsilon)$.

If $\chi \ge \exp(\delta k)$ $(\delta > 0)$ then $\omega \ge k - \lfloor \delta^{-1} \rfloor - 1$ for $k \ge k_1(\delta)$.

In particular, if $\chi \ge \exp((1+\varepsilon)k)$ $(\varepsilon > 0)$, then $\omega \ge k-1$ for $k \ge k_2(\varepsilon)$. (If 1 and the primes $p_1, p_2, \ldots, p_{k-1}$ are in arithmetical progression, we take $a = 1$ and $d = p_1 - 1$ to observe that $\omega = k - 1$.)

3. Bounds for ω if χ is large. The proofs in Sections 3 and 4 depend on the theory of linear forms in logarithms. Let $\alpha_1, \ldots, \alpha_n$ be non-zero algebraic numbers of heights not exceeding $A_1, \ldots, A_n$, respectively, where $A_j \ge 3$ for $1 \le j \le n$. We put

$$\Omega = \prod_{j=1}^{n} \log A_j, \qquad \Omega' = \Omega/\log A_n$$

and

$$K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n), \qquad [K : \mathbb{Q}] = D.$$

We start with the following estimate of Baker [1] on linear forms in logarithms.

Lemma 3. *There exist effectively computable absolute constants c_2 and c_3 such that the inequalities*

$$0 < |\alpha_1^{b_1} \ldots \alpha_n^{b_n} - 1| < \exp(-(c_2 n D)^{c_3 n} \Omega \log \Omega' \log B)$$

have no solution in rational integers $b_1, \ldots, b_n$ of absolute values not exceeding B with $B \ge 2$.

Next, we state an estimate of Yu [11, Corollary of Theorem 2] on p-adic linear forms in logarithms.

Lemma 4. *Let p and q be positive prime numbers. Let $\mathfrak{p}$ be a prime ideal of K satisfying $\mathfrak{p} \mid p$ and*

$$\operatorname{ord}_{\mathfrak{p}}(\alpha_j) = 0 \quad \textit{for } 1 \le j \le n \tag{3.1}$$

and

$$p(p^{f_{\mathfrak{p}}} - 1) \not\equiv 0 \pmod{q}$$

where $f_{\mathfrak{p}}$ is given by

$$N_{K/\mathbb{Q}}\mathfrak{p} = p^{f_{\mathfrak{p}}}.$$

Assume that

$$[K(\alpha_1^{1/q},\ldots,\alpha_n^{1/q}):K]=q^n. \tag{3.2}$$

There exists an effectively computable absolute constant c_4 *such that*

$$\operatorname{ord}_{\mathfrak{p}}(\alpha_1^{b_1}\ldots\alpha_n^{b_n}-1)\le(qnD)^{c_4n}p^D\Omega(\log B)^2$$

for all rational integers $b_1,\ldots,b_n$ *with absolute values at most* B (≥ 2) *such that* $\alpha_1^{b_1}\ldots\alpha_n^{b_n}\ne 1$.

Finally, we state an application of the theory of linear forms in logarithms for the proofs of Theorems 5, 7 and 7′. Let $F(X,Y)\in\mathbb{Z}[X,Y]$ be a binary form with at least three distinct linear factors in its factorisation over $\mathbb{C}$. We 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. Then Győry [3] proved

Lemma 5. *All solutions of the Thue–Mahler equation*

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

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

$$\log(\max(|x|,|y|))\le c_5(s+1)^{c_6(s+1)}P^{2l}(1+\log(|A|H(F)))$$

where c_5 *and* c_6 *are effectively computable numbers such that* c_5 *depends only on* l,R_L,h_L *and* c_6 *only on* l.

We recall that H is the set of all i with $0\le i<k$ such that $P(a+id)\le k$. We write H' for the set of all $a+id$ with $i\in H$. Let

$$\mathcal{K}=\min(k(\pi_d(k))^{-1},\,(\pi_d(k))^{1/2}). \tag{3.3}$$

We observe that $\mathcal{K}=0$ whenever $\pi_d(k)=0$ and

$$\mathcal{K}\le k^{1/3}. \tag{3.4}$$

We prove

Lemma 6. *Let* $\varepsilon>0$. *There exist effectively computable numbers* C_1,C_2 *and* C_3 *depending only on* ε *such that for*

$$k\ge C_1,\qquad \pi_d(k)\ge C_2\qquad \textit{and}\qquad \log\chi\ge\mathcal{K}k(\log k)^{C_3},$$

we have

$$|H'|\le\varepsilon\pi_d(k).$$

Proof. We assume that $0<\varepsilon<1$. We write $C_4,C_5,\ldots,C_{13}$ for effectively computable positive numbers depending only on ε. We may assume that $k\ge C_4$ and $\pi_d(k)\ge C_4$ with C_4 sufficiently large. For every $p\in G$, we choose an $F(p)\in H'$ such that p does not appear to a higher power in the factorisation of any other element of H'. Let H_1 be the set of all the elements of H' which do not appear in the image of F more than $\lfloor \varepsilon^{-1} \rfloor =: \tau$ times. We write H_2 for the complement of H_1 in H'. We suppose that

$$|H'| > 2\varepsilon\pi_d(k). \tag{3.5}$$

We observe that

$$|H'| = |H_1| + |H_2| \tag{3.6}$$

and

$$\varepsilon^{-1}|H_2| < (\tau+1)|H_2| \le \pi_d(k). \tag{3.7}$$

By (3.6), (3.5) and (3.7), we derive that

$$|H_1| > \varepsilon\pi_d(k). \tag{3.8}$$

For $a + jd \in H_1$, we write

$$a + jd = m_j p_{j,1}^{a_{j,1}} \dots p_{j,\tau_j}^{a_{j,\tau_j}} =: m_j s_j \tag{3.9}$$

where $\tau_j \le \tau,\ p_{j,i} \in G,\ F(p_{j,i}) = a + jd,\ a_{j,i}$ and m_j are positive integers such that the primes $p_{j,1}, \dots, p_{j,\tau_j}$ do not appear in the factorisation of m_j. The factorisation in (3.9) is such that, if $p^b \mid m_j$ for some prime p and some positive integer b, then $p^b \mid a + id$ for some $i \ne j$, whence $p^b < k$. We put $|v_1| = |H_1|$ and $v = \lfloor v_1/2 \rfloor$. We order m_j with $a+jd \in H_1$ in the decreasing order

$$m_{j_1} \ge m_{j_2} \ge \dots \ge m_{j_v} \ge \dots \ge m_{j_{v_1}}. \tag{3.10}$$

We write

$$M_\nu = m_{j_\nu}, \qquad S_\nu = s_{j_\nu} \quad \text{for } 1 \le \nu \le v_1. \tag{3.11}$$

We observe from the definition of H_1 that

$$\operatorname{lcm}(M_1, \dots, M_{v_1}) \le k^{\pi_d(k)}. \tag{3.12}$$

Further, we see from the proof of Lemma 1(a) that

$$\prod_{\nu=1}^{v_1} M_\nu \le k^k. \tag{3.13}$$

Now, we apply Lemma 2 with $n = \lfloor \sqrt{\pi_d(k)} \rfloor$ and $a_\nu = M_\nu$ for $1 \le \nu \le n$ to conclude from (3.10) and (3.12) that

$$M_n^n \le k^{\pi_d(k)} k^{\binom{n}{2}}. \tag{3.14}$$

Then, we observe from (3.10) and (3.14) that

$$\log M_v \le \log M_n \le C_5(\pi_d(k))^{1/2} \log k. \tag{3.15}$$

Writing

$$j_{\nu_i} = J_i \quad \text{for } i = 1, 2, 3, \tag{3.16}$$

we see from (3.8) and (3.13) that there are three distinct integers ν_1, ν_2, ν_3 between v and v_1 such that $a + J_1 d$, $a + J_2 d$, $a + J_3 d$ are elements of H_1 satisfying

$$\log\max(M_{\nu_1}, M_{\nu_2}, M_{\nu_3}) \le C_6 k(\pi_d(k))^{-1}\log k. \tag{3.17}$$

By (3.17), (3.10), (3.15) and (3.3), we conclude that

$$\log\max(M_{\nu_1}, M_{\nu_2}, M_{\nu_3}) \le C_7 \mathcal{K}\log k. \tag{3.18}$$

We denote by U the maximum of exponents of primes $p_{j,i}$ in (3.9) with $j = J_1, J_2, J_3$. Without loss of generality, we may assume that $U = a_{J_3,1}$. Further, we write $p = p_{J_3,1}$. We have

$$(J_1 - J_2)(a + J_3 d) + (J_2 - J_3)(a + J_1 d) + (J_3 - J_1)(a + J_2 d) = 0. \tag{3.19}$$

By (3.19), (3.9), (3.16) and (3.11),

$$-(J_1 - J_2)M_{\nu_3}S_{\nu_3} = (J_2 - J_3)M_{\nu_1}S_{\nu_1} - (J_1 - J_3)M_{\nu_2}S_{\nu_2}. \tag{3.20}$$

We write

$$M'_{\nu_1} = M_{\nu_1}/\gcd(M_{\nu_1}, S_{\nu_2}), \qquad M'_{\nu_2} = M_{\nu_2}/\gcd(M_{\nu_2}, S_{\nu_1}), \tag{3.21}$$

$$S'_{\nu_1} = S_{\nu_1}/\gcd(M_{\nu_2}, S_{\nu_1}), \qquad S'_{\nu_2} = S_{\nu_2}/\gcd(M_{\nu_1}, S_{\nu_2}). \tag{3.22}$$

We notice that

$$\gcd(M'_{\nu_1}M'_{\nu_2}, S'_{\nu_1}S'_{\nu_2}) = 1. \tag{3.23}$$

Now, we derive from (3.20), (3.21), (3.22) and (3.18) that

$$U = \mathrm{ord}_p(S_{\nu_3}) \le \mathrm{ord}_p(\Omega) + C_8\mathcal{K}\log k \tag{3.24}$$

where

$$\Omega = \frac{S'_{\nu_1}}{S'_{\nu_2}} \cdot \frac{(J_2 - J_3)M'_{\nu_1}}{(J_1 - J_3)M'_{\nu_2}} - 1. \tag{3.25}$$

By (3.11), (3.16) and (3.9), we write S'_{ν_1}/S'_{ν_2} as a power product of primes

$$p_{J_i,\mu} \quad \text{with } i = 1, 2, \quad 1 \le \mu \le \tau_{J_i}, \ \mathrm{ord}_{p_{J_i,\mu}}(S'_{\nu_1}S'_{\nu_2}) \ne 0 \tag{3.26}$$

whose exponents, in absolute values, do not exceed $a_{J_i,\mu}$, respectively. We denote by $\mathcal{S}_{J_1,J_2}$ the set of non-zero integers composed of primes (3.26).

Now, we show that

$$U \le \mathcal{K}k(\log k)^{C_9}(\log\log\chi)^2. \tag{3.27}$$

For this, we shall derive from Lemma 4 that

$$\mathrm{ord}_p(\Omega) \le \mathcal{K}k(\log k)^{C_{10}}(\log\log\chi)^2. \tag{3.28}$$

Then we combine (3.24) and (3.28) to conclude (3.27). For showing (3.28), we may assume that

$$\mathrm{ord}_p(\Omega + 1) = 0. \tag{3.29}$$

Further, we notice that p is different from the primes (3.26). Consequently, we derive from (3.29) and (3.25) that

$$\mathrm{ord}_p\biggl(\frac{(J_2-J_3)M'_{\nu_1}}{(J_1-J_3)M'_{\nu_2}}\biggr)=0.$$

Therefore, the assumption (3.1) in Lemma 4 is satisfied.

Let q be a prime between $(\log k)^2$ and $2(\log k)^2$ such that $q\nmid p(p-1)$. This choice is possible, since

$$\prod_{(\log k)^2<q<2(\log k)^2} q>2^{(\log k)^2}>k(k-1)\ge p(p-1).$$

We first assume that

$$\frac{(J_2-J_3)M'_{\nu_1}}{(J_1-J_3)M'_{\nu_2}}\mu \quad \text{with } \mu\in\mathcal{S}_{J_1,J_2} \tag{3.30}$$

is a qth power of a rational number. Then we derive from (3.23), $q\ge(\log k)^2$ and the fact that every prime power factor of some M_ν is less than k that the numerator and the denominator of the reduced fraction of $(J_2-J_3)M'_{\nu_1}/(J_1-J_3)M'_{\nu_2}$ are elements of $\mathcal{S}_{J_1,J_2}$. Now, we take $\alpha_1,\dots,\alpha_n$ in Lemma 4 as distinct primes from (3.26) and we observe that the assumption (3.2) is satisfied. Finally, we apply Lemma 4 with $n=\omega(S'_{\nu_1}S'_{\nu_2})\le 2\tau$, $D=1$, $p\le k$, $q\le 2(\log k)^2$, $A_1=A_2=\ldots=A_n=k$ and $B=2\log\chi$ to conclude that

$$\mathrm{ord}_p(\Omega)\le k(\log k)^{C_{11}}(\log\log\chi)^2$$

which implies (3.28).

Next, we assume that (3.30) is not a qth power of a rational number. Now we apply Lemma 4 with $\alpha_1,\dots,\alpha_{n-1}$ as primes from (3.26) and $\alpha_n=(J_2-J_3)M'_{\nu_1}/(J_1-J_3)M'_{\nu_2}$. By a result of Baker and Stark (see [2, Lemma 3]), the assumption (3.2) is satisfied. We take in Lemma 4

$$\begin{gathered}n=\omega(S'_{\nu_1}S'_{\nu_2})+1\le 2\tau+1,\quad D=1,\quad p\le k,\quad q\le 2(\log k)^2,\\ B=2\log\chi,\quad A_1=A_2=\ldots=A_{n-1}=k,\quad \log A_n=C_7\mathcal{K}\log k,\end{gathered}$$

as we can by (3.18), (3.21), (3.22) and we conclude (3.28) in this case too.

Finally, we combine (3.9) with $j=\max(J_1,J_2,J_3)$, (3.18) and (3.27) to obtain

$$\log\chi<\log k+\log(a+jd)\le\mathcal{K}k(\log k)^{C_{12}}(\log\log\chi)^2\,,$$

which implies that $\log\chi<\mathcal{K}k(\log k)^{C_{13}}$. ∎

If $\pi_d(k)<C_2$, we have

LEMMA 7. *Let $\theta>0$. There exist effectively computable numbers C_{14} and C_{15} depending only on θ such that for*

$$k\ge C_{14},\quad \pi_d(k)\le\theta\quad \textit{and}\quad \log\chi\ge k(\log k)^{C_{15}},$$

we have

$$|H'| \le 2.$$

Proof. Let J_1, J_2 and J_3 be distinct integers between 0 and $k-1$ such that $a + J_i d \in H'$ for $i = 1, 2, 3$. Then

$$P(a + J_i d) \le k, \quad \omega(a + J_i d) \le \theta \quad \text{for } i = 1, 2, 3.$$

Now, we apply Lemma 4 as in the proof of Lemma 6 to conclude that $\log \chi < k(\log k)^{C_{16}}$. ■

We combine Lemmas 6 and 7 to derive the following result:

THEOREM 4. *Let $\varepsilon > 0$. There exist effectively computable numbers C_{17} and C_{18} depending only on ε such that for*

$$k \ge C_{17} \quad \textit{and} \quad \log \chi \ge \mathcal{K} k(\log k)^{C_{18}},$$

we have

$$\omega \ge k + \min((1-\varepsilon)\pi_d(k),\ \pi_d(k) - 2). \tag{3.31}$$

Proof. Let $\varepsilon > 0$. We may assume that $\pi_d(k) > 0$ and k exceeds a sufficiently large effectively computable number depending only on ε. Then we combine Lemmas 6 and 7 to conclude that

$$|H'| \le \max(\varepsilon \pi_d(k), 2).$$

Observe that $|H| = |H'|$. Thus (3.31) follows from (2.1). ■

We combine Theorem 4 and (3.4) to obtain

COROLLARY 4.1. *Let $\varepsilon > 0$. There exist effectively computable numbers C_{19} and C_{20} depending only on ε such that for*

$$k \ge C_{19} \quad \textit{and} \quad \log \chi \ge k^{4/3}(\log k)^{C_{20}},$$

we have

$$\omega \ge k + \min((1-\varepsilon)\pi_d(k), \pi_d(k) - 2).$$

COROLLARY 4.2. *There exist effectively computable absolute constants C_{21} and C_{22} such that*

$$k \ge C_{21}, \quad \log \chi \ge k^{4/3}(\log k)^{C_{22}}, \quad \omega < k$$

imply that

$$\omega = k - 1$$

and at least one of the following possibilities holds:

(i) *$a = 1$ and $a + d, a + 2d, \ldots, a + (k-1)d$ are all powers of primes $\ge k$,*

(ii) *$a < k$ and there exists j with $0 < j < k$ such that a and $a + jd$ are powers of the same prime $p < k$ and the p-free part of any other term in the* *arithmetical progression* $\{a, a+d, \ldots, a+(k-1)d\}$ *is a power of a prime* $\geq k$.

Proof. In view of Corollary 4.1, we may assume that $\pi_d(k) \in \{0,1\}$. First, we turn to the case that $\pi_d(k) = 0$. Then, since $\gcd(a,d) = 1$, we observe that $a+d, a+2d, \ldots, a+(k-1)d$ are composed of primes $\geq k$ and these prime factors have to be distinct. Hence $\omega = k-1$, $a = 1$ and every other term of the AP (Arithmetical Progression) is the power of a prime $\geq k$.

Thus, we may assume that $\pi_d(k) = 1$. Then we observe that there are at least two terms of the AP which are powers of the same prime $p < k$ with $\gcd(p,d) = 1$. Suppose that $a+id$ and $a+jd$ are powers of p with $i < j$. Then $a+id \mid a+jd$, whence $a+id \mid (j-i)$ by $\gcd(a,d) = 1$. It follows that $a+id < k$. Thus $a < k$, which, together with $\log\chi \geq k^{4/3}(\log k)^{C_{22}}$, implies that $d > k$. Consequently, we notice from $a+id < k$ that $i = 0$. Thus, we conclude that there exists precisely one j with $0 < j < k$ such that a and $a+jd$ are powers of p. Furthermore, since $\pi_d(k) = 1$, the remaining $k-2$ terms of the AP contribute their own primes $\geq k$. Therefore $\omega \geq k-1$. Further, since $\omega < k$ and $\pi_d(k) = 1$, we derive that $\omega = k-1$, each of the $k-2$ terms of the AP contributes precisely one prime $\geq k$ and there is no contribution other than p from primes $< k$. ■

As an immediate consequence of Corollary 4.2, we derive that $\omega \geq k$ whenever $k \geq C_{21}$, $\log\chi \geq k^{4/3}(\log k)^{C_{22}}$ and $a \geq k$. We close this section by improving the estimate (3.31) of Theorem 4 if χ is much larger as compared with k.

Theorem 5. *There exist effectively computable absolute constants* C_{23} *and* C_{24} *such that for*

$$k \geq C_{23} \qquad \textit{and} \qquad \log\log\chi \geq C_{24}k,$$

we have

$$\omega \geq k + \pi_d(k) - 2.$$

Proof. It is enough to prove that $|H'| \leq 2$. Let J_1, J_2 and J_3 be distinct integers between 0 and $k-1$ such that

$$P(a+J_id) \leq k \quad \text{ for } i = 1,2,3\,.$$

Then we apply Lemma 5 to the binary form

$$(a+J_1d)(a+J_2d)(a+J_3d).$$

We conclude that

$$\log\chi < \log k + \log(a+d) \leq C_{25}^k$$

for some effectively computable absolute constant C_{25}. ■

4. Bounds for ω if $P(d)$ or $P(a)$ is small. We write $\omega_k(d)$ for the number of prime divisors of d not exceeding k. We start this section with the following result.

LEMMA 8. (a) *Let $\varepsilon > 0$. There exist effectively computable numbers C_{25}, C_{26} and C_{27} depending only on ε such that for*

$$k \ge C_{25}, \quad \pi_d(k) \ge C_{26}, \quad \log\chi \ge (\log k)^{C_{27}}$$

and

$$P(d) < (\log\chi)^{1/2-\varepsilon}, \tag{4.1}$$

we have

$$\omega \ge k + (1-\varepsilon)\pi_d(k).$$

(b) *The assertion of Lemma* 8(a) *is also valid if* (4.1) *is replaced by*

$$P(a) < (\log\chi)^{1/2-\varepsilon}, \quad \omega_k(d) \le (1-\varepsilon)\pi(k). \tag{4.2}$$

Proof. We denote by $C_{28}, C_{29}, \ldots, C_{34}$ effectively computable positive numbers depending only on ε. We may assume that $k \ge C_{28}$ and $\pi_d(k) \ge C_{28}$ where C_{28} is sufficiently large. Further, we may suppose that

$$\omega < k + (1-\varepsilon)\pi_d(k). \tag{4.3}$$

By taking C_{28} sufficiently large, we have

$$(1-\varepsilon)\pi_d(k) < \pi_d(k) - 2. \tag{4.4}$$

Now, we apply Corollary 4.1 to derive from (4.3) and (4.4) that (4.1) implies

$$\omega_k(d) \le P(d) \le (1-\varepsilon)\pi(k).$$

Therefore, both under (4.1) and under (4.2),

$$\pi_d(k) \ge \pi(k) - \omega_k(d) \ge \varepsilon\pi(k)\,,$$

which, together with (3.3), implies that

$$\mathcal{K} \le (2\log k)/\varepsilon. \tag{4.5}$$

By (4.3), we have

$$|H'| > \varepsilon\pi_d(k). \tag{4.6}$$

Instead of (3.19), the proofs of Lemma 8(a) and (b) depend on the following relations: For distinct integers J_1 and J_2 between 0 and $k-1$,

$$(J_1 - J_2)d = (a + J_1 d) - (a + J_2 d)\,, \tag{4.7}$$

$$-(J_1 - J_2)a = J_2(a + J_1 d) - J_1(a + J_2 d)\,. \tag{4.8}$$

(a) As in the proof of Lemma 6, we apply Lemma 4 to (4.7) for deriving from (4.6) and (4.5) that

$$\operatorname{ord}_p(d) \le p(\log k)^{C_{29}}(\log\log\chi)^2. \tag{4.9}$$

Now, we combine (4.9) and (4.1) for obtaining

$$\log d \le (\log \chi)^{1-\varepsilon}(\log k)^{C_{29}}(\log\log \chi)^2. \tag{4.10}$$

On the other hand, we apply Lemma 3 via (4.7) for deriving that

$$\log d \ge \log \chi - (\log k)^{C_{30}}. \tag{4.11}$$

By (4.10) and (4.11), we find that $\log \chi \le (\log k)^{C_{31}}$.

(b) Instead of (3.19), we apply Lemmas 3 and 4 to (4.8) as in the proof of Lemma 8(a). We obtain

$$\log a \le (\log \chi)^{1-\varepsilon}(\log k)^{C_{32}}(\log\log \chi)^2$$

and

$$\log a \ge \log \chi - (\log k)^{C_{33}}.$$

We combine these estimates to obtain $\log \chi \le (\log k)^{C_{34}}$. ■

Lemma 9. (a) *Let $\varepsilon > 0$ and $\theta > 0$. There exist effectively computable numbers C_{35} and C_{36} depending only on ε and θ such that for*

$$k \ge C_{35}, \qquad \pi_d(k) \le \theta, \qquad \log \chi \ge (\log k)^{C_{36}}$$

and (4.1), *we have*

$$|H'| \le 1.$$

(b) *The assertion of Lemma* 9(a) *is also valid if* (4.1) *is replaced by*

$$P(a) < (\log \chi)^{1/2-\varepsilon}. \tag{4.12}$$

Proof. Let J_1 and J_2 be distinct integers between 0 and $k-1$ such that $a + J_i d \in H'$ for $i = 1, 2$. Then $P(a + J_i d) \le k$ and $\omega(a + J_i d) \le \theta$ for $i = 1, 2$, since $\pi_d(k) \le \theta$. Now, we apply Lemmas 3 and 4 via (4.7) and (4.8) to conclude the proof of Lemma 9. ■

We combine Lemmas 8 and 9 to obtain the following result.

Theorem 6. (a) *Let $\varepsilon > 0$. There exist effectively computable numbers C_{37} and C_{38} depending only on ε such that for*

$$k \ge C_{37}, \qquad \log \chi \ge (\log k)^{C_{38}}$$

and (4.1), *we have*

$$\omega \ge k + \min((1-\varepsilon)\pi_d(k), \pi_d(k) - 1). \tag{4.13}$$

(b) *The assertion of* (a) *is also valid if* (4.1) *is replaced by* (4.2).

If $P(d)$ or $P(a)$ is small, we apply Theorem 6 to obtain the following refinement of Corollary 4.2.

Corollary 6.1. (a) *There exist effectively computable absolute constants C_{39} and C_{40} such that*

$$k \ge C_{39}, \qquad \log \chi \ge (\log k)^{C_{40}}, \qquad \omega < k \tag{4.14}$$

and (4.1) *imply that $\omega = k-1, a = 1$ and $a+d, a+2d, \ldots, a+(k-1)d$ are all powers of primes $\ge k$.*

(b) *The assertion of* (a) *is also valid if* (4.1) *is replaced by* (4.2).

Proof. By Theorem 6, we observe from (4.13) and (4.14) that $\omega = k-1$ and $\pi_d(k) = 0$. Then, as in the proof of Corollary 4.2, we derive that $a = 1$ and $a+d, a+2d, \ldots, a+(k-1)d$ are all powers of primes $\ge k$. ■

If $d = 1$ and χ is large with respect to k, Pólya [6] derived from the Thue–Siegel theorem that $\omega \ge k + \pi(k) - 1$. We extend this result by sharpening (4.13) whenever χ is much larger than k and $P(d)$.

For this, we prove

Theorem 7. *Let $\varepsilon > 0$. There exist effectively computable numbers C_{41} and C_{42} depending only on ε such that for*

$$k \ge C_{41}, \qquad \omega \le k + \pi_d(k) - 2$$

and (4.1), *we have*

$$\log\log \chi \le C_{42}(\omega(d)\log \omega(d) + k). \tag{4.15}$$

Proof. Since $\omega \le k + \pi_d(k) - 2$, we observe that $|H'| \ge 2$. Let J_1 and J_2 be distinct integers between 0 and $k-1$ such that $P(a+J_1 d) \le k$ and $P(a+J_2 d) \le k$. Now, we apply Lemma 5 to the binary form

$$Y(X+J_1Y)(X+J_2Y) \qquad \text{with } X = a, Y = d \tag{4.16}$$

to conclude (4.15). ■

As an immediate consequence of Theorem 7, we obtain the following extension of a result of Pólya already mentioned.

Corollary 7.1. *There exist effectively computable absolute constants C_{43} and C_{44} such that for*

$$k \ge C_{43}, \qquad \log\log\chi \ge C_{44}(k + P(d)),$$

we have

$$\omega \ge k + \pi_d(k) - 1.$$

We write

$$\omega' = \omega((a+d)\ldots(a+(k-1)d)).$$

We obtain an analogue of Theorem 7 with (4.1) replaced by (4.12).

THEOREM 7′. *Let $\varepsilon > 0$. There exist effectively computable numbers C_{45} and C_{46} depending only on ε such that for*

$$k \geq C_{45}, \quad \omega' \leq k + \pi_d(k-1) - 3$$

and (4.12), *we have*

$$\log\log\chi \leq C_{46}(\omega(a)\log(\omega(a)+1) + k).$$

Proof. The proof is similar to the proof of Theorem 7; instead of (4.16), we apply Lemma 5 to the binary form

$$X(X + J_1Y)(X + J_2Y) \quad \text{with } X = a,\ Y = d. \ \blacksquare$$

It is clear that Theorem 7′ implies the following result.

COROLLARY 7.1′. *There exist effectively computable absolute constants C_{47} and C_{48} such that for*

$$k \geq C_{47}, \quad \log\log\chi \geq C_{48}(k + P(a)),$$

we have

$$\omega' \geq k + \pi_d(k-1) - 2.$$

References

[1] A. Baker, *The theory of linear forms in logarithms*, in: Transcendence Theory: Advances and Applications, A. Baker and D. W. Masser (eds.), Academic Press, 1977, 1–27.

[2] A. Baker and H. M. Stark, *On a fundamental inequality in number theory*, Ann. of Math. 94 (1971), 190–199.

[3] K. Győry, *Explicit upper bounds for the solutions of some diophantine equations*, Ann. Acad. Sci. Fenn. Ser. AI 5 (1980), 3–12.

[4] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Oxford University Press, 1988.

[5] P. Moree, *On arithmetical progressions having few different prime factors in comparison with their lengths*, to appear.

[6] G. Pólya, *Zur arithmetischen Untersuchung der Polynome*, Math. Z. 1 (1918), 143–148.

[7] K. Ramachandra, T. N. Shorey and R. Tijdeman, *On Grimm's problem relating to factorisation of a block of consecutive integers*, J. Reine Angew. Math. 273 (1975), 109–124.

[8] T. N. Shorey and R. Tijdeman, *On the number of prime factors of an arithmetical progression*, J. Sichuan Univ. 26 (1990), 72–74.

[9] —, —, *On the greatest prime factor of an arithmetical progression III*, in: Diophantine Approximation and Transcendental Numbers, Luminy 1990, Ph. Philippon (ed.), to appear.

[10] R. Tijdeman, *On the product of the terms of a finite arithmetic progression*, in: Proc. Conf. Diophantine Approximations and Transcendence Theory, RIMS Kokyuroku 708, Kyoto Univ., Kyoto 1989, 51–62.

[11] K. Yu, *Linear forms in the p-adic logarithms*, Acta Arith. 53 (1989), 107–186.

SCHOOL OF MATHEMATICS
TATA INSTITUTE OF FUNDAMENTAL RESEARCH
HOMI BHABHA ROAD
BOMBAY 400005, INDIA

MATHEMATICAL INSTITUTE
R. U. LEIDEN
P.O. BOX 9512
2300 RA LEIDEN, THE NETHERLANDS

Received on 8.10.1991 (2178)