ACTA ARITHMETICA
IX (1964)

On prime numbers in an arithmetic progression with a prime-power difference

by

M. B. Barban, Yu. V. Linnik and N. G. Tshudakov (Leningrad)

To Professor L. J. Mordell on his 75-th anniversary

§ 1. The distribution of primes in the segments of an arithmetic progression has attracted the attention of many authors since the proof of Dirichlet's celebrated theorem (1837).

The extended Riemann hypothesis, not proved up to now, would lead to the following asymptotic law:

Let $D>1$ be a natural number; $(l,D)=1$, $\varepsilon>0$ being an arbitrarily small number and x and arbitrarily large number. Then

$$\pi(x,D,l)=h^{-1}\mathrm{li}\,x\big(1+O(\lg x)^{-M}\big) \tag{1.1}$$

for

$$x\geqslant D^{2+\varepsilon},\quad h=\varphi(D),\quad \pi(x,D,l)=\sum 1,\quad p\equiv l(\mathrm{mod}\,D),\quad p\leqslant x.$$

In particular, the minimal prime $P_{\min}(D,l)$ in the progression $n\equiv l\ (\mathrm{mod}\,D)$ must satisfy the inequality

$$P_{\min}(D,l)<c(\varepsilon)D^{2+\varepsilon}. \tag{1.2}$$

We have no means of proving (1.1) at present; the same can be said about (1.2). In article [1], the simpler variant of which was given in [2], it was shown that there exists a constant $c>1$ such that

$$P_{\min}(D,l)<D^{c}. \tag{1.3}$$

Pang Cheng Tung [3] showed in 1957, using papers [1] and [2], that $c\leqslant 5448$. The result of this author is the best up to date.

However, for some subsequences $\vartheta=\{D\}$ of the moduli D one can hope for a considerable improvement of the estimate of the constant c. Obviously for this purpose one must have more information on the zeros of the series $L(s,\chi)$ than in the general case.

In particular, for the moduli of the type $D = p^n$, where $p \geqslant 3$ is a fixed prime, $n = 1, 2, \ldots$, new and important data were obtained by A. G. Postnikov [4] in 1954 (see also [5]). The work of A. G. Postnikov was continued by S. M. Rosin [6].

The authors of this article have studied the asymptotic law acting on the short segments of the arithmetic progressions with the difference $D = p^n$. We have obtained the following result:

THEOREM. *Let $p \geqslant 3$ be a prime, $D = p^n$ $(n = 1, 2, 3, \ldots)$, $\varepsilon > 0$ being an arbitrarily small number. Then the following asymptotic law:*

$$\pi(x, D, l) = h^{-1}\operatorname{li} x\big(1+O(\lg x)^{-M}\big) \tag{1.4}$$

holds for $x \geqslant D^{\frac{8}{3}+\varepsilon}$, M being arbitrarily large.

It is clear that (1.4) implies the inequality:

$$P_{\min}(D, l) < c_1(\varepsilon) D^{\frac{8}{3}+\varepsilon} \tag{1.5}$$

for the moduli of the type defined above. We see that (1.4) is near to (1.1).

The sign O can depend only on ε. One can find a constant c such that $\pi(x, D, l) > 0$ for $n \geqslant c_2 \exp p^2$ for any prime $p \geqslant 3$.

Notations:

$v = h^{-1}x$;

$$a_n = \begin{cases} 1, & \text{if} \quad n \equiv l \pmod{D}, \\ 0, & \text{if} \quad n \not\equiv l \pmod{D}, \end{cases} \qquad n = 1, 2, 3, \ldots;$$

$\Lambda(n)$ — Mangoldt's function;

$$S_m(x) = S_m(x, D, l) = \frac{1}{m!}\sum_{m \leqslant x} a_n \Lambda(n)\left(\lg\frac{x}{n}\right)^m, \qquad m = 0, 1, 2, \ldots$$

In particular:

$S_0(x) = \psi(x, D, l) = \sum_{n \leqslant x} a_n \Lambda(n)$;

$\delta_m(x) = v^{-1}\big(S_m(x) - v\big) = \delta_m(x, D, l)$;

$d_m(x) = \sup|\delta_m(u, D, l)|$ for $u \geqslant x$; $(l, D) = 1$;

$\varrho = \beta + i\gamma$ — the zeros of the function $L(s, \chi)$ in the stripe $0 < \beta < 1$;

$\mathfrak{a}(D)$ — the set of ϱ for all $L(s, \chi) \bmod D$;

$N(\sigma, T)$ — the number of the elements of $\mathfrak{a}(D)$ situated in the rectangle $\sigma \leqslant \gamma \leqslant 1$, $|\gamma| \leqslant T$;

$\mathfrak{a}_\nu(D)$ — the set of the elements of $\mathfrak{a}_\nu(D)$ situated in the rectangles:

$$0 < \beta < 1, \quad \nu \leqslant |\gamma| < \nu+1 \quad (\nu = 0, 1, 2, \ldots);$$

$\varrho(\chi)$ — the set of all ϱ for a given $L(s, \chi)$;

$\beta(t) = \max\beta$ for all β with the ordinate $\gamma = t$; if there are no such zeros, $\beta(t) = \frac{1}{2}$;

$\beta_\nu(t) = \max\beta(t)$ for $\nu \leqslant |t| \leqslant \nu+1$ $(\nu = 0, 1, 2, \ldots)$;

$$f(s) = \sum_{n=1}^{\infty} a_n n^{-s} = -h^{-1}\sum_{\chi}\bar{\chi}(l)\frac{L'}{L}(s, \chi);$$

Later on we shall consider certain subsets $\vartheta = \{D\}$ of the moduli D.

The latter c denotes the constants independent of ϑ, x, D, l; the same meaning we shall attach to the symbols "O" and "$\ll$". The letter b denotes the constants depending upon ϑ but not upon x, D, l.

It is well known (cf. [8], theorem 44 on p. 28) that there exists an absolute constant such that for all $\varrho \in \mathfrak{a}(D)$, except perhaps one real $\varrho = \beta_1$, the following inequality holds: $|\varrho| \geqslant \mu(\lg D)^{-1}$ ($\mu > 0$ being a constant). The zero β_1 if it exists for a given $\mathfrak{a}(D)$, is called the *exclusive zero* $\bmod D$.

We know about this zero (Siegel's theorem, cf. [8], p. 60) that

$$\beta_1 \geqslant \mu'' D^{-\varepsilon}$$

for any $\varepsilon > 0$; $\mu'' = \mu''(\varepsilon)$. We have no means at present of calculating it algorithmically. The classical theorems connecting the functions $\pi(x, D, l)$ and $\psi(x, D, l)$ (cf. [8], p. 70) enable us to reduce the proof of our fundamental theorem to the estimation of the value of $\delta_0(x)$ for $x \geqslant D^{\frac{8}{3}+\varepsilon}$; we must only show that for such values of x the estimate $d_0(x, D) \leqslant b_1(\lg x)^{-M}$ holds. Here $x \geqslant D^{\frac{8}{3}+\varepsilon}$, $D = p^n$, M is an arbitrary positive number.

§ 2. LEMMA 1. *Let $x > h$; then for any $\varepsilon > 0$ and $m = 1, 2, 3, \ldots$ the following estimate holds:*

$$|\delta_m(x)| \leqslant c_1 \lg x \sum_{\nu=0}^{\infty} I_\nu + O(hx^{-1+\varepsilon}),$$

where

$$I_0 = \int_0^{\beta_0} N(\sigma, 0)x^{\sigma-1}d\sigma,$$

$$I_\nu = \nu^{-m-1}\int_0^{\beta_\nu}\big(N(\sigma, \nu+1) - N(\sigma, \nu)\big)x^{\sigma-1}d\sigma, \qquad \textit{for} \quad \nu = 1, 2, 3, \ldots$$

The constant c_1 and the O-sign of the second summand on the right-hand side depend upon ε and m; if for a given D there is no β_1 the O-sign can be given effectively.

Proof. It is well known that

$$\frac{1}{2\pi i}\int_{(2)}\frac{y^s}{s^{m+1}}\,ds = \begin{cases}\frac{1}{m!}\lg^m y & \text{if} \quad y\geqslant 1,\\ 0 & \text{if} \quad 0<y<1.\end{cases}$$

We have therefore for $x>0$

$$S_m(x) = \frac{1}{2\pi i}\int_{(2)}\frac{x^s}{s^{m+1}}f(s)\,ds$$

as the series $f(s)$ converges absolutely in the half-plane $\sigma>1$.

The integration contour can be transferred to the line $\sigma = -\frac{1}{2}$ for there is a sequence of straight lines $t = T_n$ $(n = 1, 2, 3, \ldots)$, $T_n\to\infty$ for $n\to\infty$ such that $f(s)\ll \lg^2(DT_n)$ on these lines (cf. [9], p. 226). Taking into account all the singular points of the integrand, we obtain by the residue theorem for the analytical functions:

(2.1)
$$\delta_m(x) = \delta_{m_1}(x)+\delta_{m_2}(x)+\delta_{m_3}(x),$$

$$\delta_{m_1}(x) = -\sum_{\chi}\bar\chi(l)\sum_{\varrho(\chi)}\frac{x^{\varrho-1}}{\varrho^{m+1}},$$

$$\delta_{m_2}(x) = -x^{-1}\sum_{\chi}\bar\chi(l)\operatorname*{Res}_{s=0}\frac{x^s}{s^{m+1}}\cdot\frac{L'}{L}(s,\chi),$$

$$\delta_{m_3}(x) = \frac{v^{-1}}{2\pi i}\int_{(-\frac12)}\frac{x^s}{s^{m+1}}f(s)\,ds.$$

To begin with, we remark that

$$|\delta_{m1}(x)|\leqslant\sum_{\nu=0}^{\infty}Q_\nu, \qquad Q_\nu = \sum_{\varrho\in\mathfrak{a}_\nu}x^{\beta-1}|\varrho|^{-m-1},$$

for $\nu\geqslant 1$ we have

(2.2)
$$Q_\nu\ll \nu^{-m-1}\sum_{\nu\leqslant|\gamma|\leqslant\nu+1}x^{\beta-1}.$$

To estimate the value of Q_0, we break up all the zeros of $\mathfrak{a}_0(D)$ into 3 groups:

$$|\varrho|\geqslant\varepsilon/2, \qquad \varepsilon/2\geqslant|\varrho|\geqslant(\lg D)^{-1}, \qquad \mu(\lg D)^{-1}\geqslant|\varrho|$$

(the second and the third group may be void for a given $\varepsilon>0$; β_1 can belong to the first group).

Recalling the estimate for β_1 (§ 1) and taking into account the well-known estimation $N(0,1)\ll h\lg D$ which is a particular case of the estimations:

(2.3)
$$N(0,1)\ll h\lg D, \qquad N(0,\nu+1)-N(0,\nu)\ll h\lg D\nu$$

(cf. [9], pp. 220-221) we get after some simple computations

(2.4)
$$Q_0\ll\sum_{0\leqslant|\gamma|\leqslant 1}x^{\beta-1}+hx^{-1+\frac{\varepsilon}{2}}(\lg D)^{m+2}+\frac{x^{\beta_1-1}}{\beta_1^{m+1}}\ll\sum_{0\leqslant|\gamma|\leqslant 1}x^{\beta-1}+hx^{-1+\varepsilon}.$$

On the other hand, the elements of the theory of Stieltjes integral enable us to obtain the equality

(2.5)
$$\sum_{\nu\leqslant|\gamma|\leqslant\nu+1}x^{\beta-1} = \lg x\int_0^{\beta_\nu}\big(N(\sigma,\nu+1)-N(\sigma,\nu)\big)x^{\sigma-1}d\sigma+ +\big(N(0,\nu+1)-N(0,\nu)\big)x^{-1} \quad \text{for} \quad \nu\geqslant 1,$$

$$\sum_{0\leqslant|\gamma|\leqslant 1}x^{\beta-1} = \lg x\int_0^{\beta_0}N(\sigma,1)x^{\sigma-1}d\sigma+N(0,1)x^{-1} \quad \text{for} \quad \nu = 0.$$

The estimations (2.3) give further

(2.6)
$$x^{-1}N(0,1)+x^{-1}\sum_{\nu=1}^{\infty}\nu^{-m-1}\big(N(0,\nu+1)-N(0,\nu)\big)\ll x^{-1}h\lg D.$$

The relations (2.2), (2.4), (2.5) and (2.6) lead to the relation

(2.7)
$$|\delta_{m_1}(x)|\ll\lg x\sum_{\nu=0}^{\infty}I_\nu+hx^{-1+\varepsilon}.$$

To estimate $\delta_{m_2}(x)$ we use again the above mentioned partition of $\mathfrak{a}_0(D)$. Moreover, we use the information on $\frac{L'}{L}(s,\chi)$ which is expounded in [9], p. 218 and p. 228. In the neighbourhood of $s = 0$ we put

$$\frac{L'}{L}(s,\chi) = \frac{\nu_0}{s}+\sum_{k=1}^{\infty}d_k s^k.$$

Then

(2.8)
$$\operatorname*{Res}_{s=0}\frac{x^s}{s^{m+1}}\cdot\frac{L'}{L}(s,\chi) = \sum_{\mu=0}^{m}\frac{1}{\mu!(m-\mu)!}(\lg x)^\mu d_{m-\mu}+\frac{\nu_0}{(m+1)!}(\lg x)^{m+1}.$$

The differentiation by terms of the equality (2.10) in [9], p. 218 leads to the relation

$$d_k = -\frac{1}{2k!}\left[\frac{d^k}{dx^k}\cdot\frac{\Gamma'}{\Gamma}\left(\frac{1}{2}(s+a)\right)-\frac{\nu_0}{s}\right]-\sum_{\varrho}\varrho^{-k-1} \ll O(\lg D)^{k+2}+\beta_1^{-k-1};$$

we have, moreover,

$$(2.9)\qquad \nu_0 = O(\lg D).$$

The relations (2.1), (2.8) and (2.9) give

$$(2.10)\qquad |\delta_{m_2}(x)| \leqslant x^{-1}h\max_{\chi}\left|\operatorname*{Res}_{s=0}\frac{x^{s}}{s^{m+1}}\cdot\frac{L'}{L}(s,\chi)\right| \leqslant hx^{-1+\varepsilon}.$$

Using the estimate

$$\frac{L'}{L}(s,\chi) \ll \lg D(|s|+2)$$

for $\sigma < 0$ (cf. [9], p. 227), we finally get

$$(2.11)\qquad |\delta_{m_3}(x)| \ll x^{-\frac{3}{2}}h\lg D \ll hx^{-1+\varepsilon}.$$

The relations (2.7), (2.10) and (2.11) prove the lemma.

Lemma 2. *Let the sequence ϑ be such that*

$$(\alpha)\qquad N(\sigma, T) \leqslant b_2T^A D^{B(1-\sigma)}\lg^C D,$$

$$(\beta)\qquad \beta(\gamma) \leqslant 1-\eta(D) \quad \textit{for} \quad |\gamma| \leqslant \tau.$$

(*The quantities $A, B, C, \tau, \eta(D)$ are determined by ϑ*).

Then for a natural $m \geqslant A+1$ and a fixed $\varepsilon > 0$ arbitrarily small, and $\lambda = (\lg D)^{-1}(\lg xD^{-B}) \geqslant \varepsilon$ the following estimate holds:

$$|\delta_m(x)| \leqslant b_3(\varepsilon)\lg^C D\left[D^{-\eta(D)\lambda}+\sum_{\nu=\tau}^{\infty}\nu^{-2}\exp\left(-c_3\lambda\frac{\lg D}{\lg D+\lg\nu}\right)\right]+O(hx^{-1+\varepsilon}).$$

Proof. First of all, we note that on account of the property (β), there is no zero β_1 in our case. Using now the property (α) we get the estimate for the quantity I_ν by Lemma 1: for $\nu \leqslant \tau$:

$$I_\nu \ll \nu^{-m-1}\int_0^{\beta_\nu} N(\sigma, \nu+1)x^{\sigma-1}d\sigma \ll b_2(\nu+1)^{A-m-1}\lg^C D\left(\lg\frac{x}{D^B}\right)^{-1}D^{\lambda(\beta_\nu-1)}$$
$$\ll b_2\nu^{-2}\lg^C D(\lambda\lg D)^{-1}D^{-\lambda\eta(D)};$$

analogously,

$$I_0 \ll b_2D^{-\lambda\eta(D)}\lg^C D(\lambda\lg D)^{-1}.$$

Therefore

$$(2.12)\qquad \lg x\sum_{\nu=0}^{\tau}I_\nu \ll b_2D^{-\lambda\eta(D)}(\lg D)^C\sum_{\nu=1}^{\infty}\nu^{-2} \ll b_2D^{-\lambda\eta(D)}(\lg D)^C.$$

For $\nu > \tau$, we shall use the first theorem of Page (cf. [8], p. 115, theorem 40):

$$1-\beta_\nu \geqslant c_3(\lg D\nu)^{-1} \qquad (\nu = 1, 2, 3, \ldots).$$

This theorem gives for I_ν, the estimate

$$(2.13)\qquad \lg xI_\nu \ll b_2\nu^2\lg^C D\exp\left(-c_3\lambda\frac{\lg D}{\lg D+\lg\nu}\right).$$

(2.12) and (2.13) give the proof of the lemma.

Corollary. *If the sequence ϑ is such that the property (β) is of the form*

$$\eta(D) = b_4(\lg D)^{-a}, \qquad 0 < a < 1$$

$$\tau = (\lg D)^M, \qquad M > 0, \qquad \textit{and moreover } B \geqslant 2,$$

then

$$d_m(x, D) \ll b_5(\varepsilon)\lg x^{-\frac{1}{2}M} \qquad \textit{for} \qquad x > D^{B+\varepsilon}.$$

Proof. In fact, in this case

$$hx^{-1+\varepsilon} = O((\lg x)^{-M}),$$

$$|\delta_m(x)| \leqslant b_3(\varepsilon)\lg^C D\left[\exp(-b_4\lambda(\lg D)^{1-a})+\sum_{\nu=\tau}^{\infty}\nu^{-2}\exp\left(-c_3\lambda\frac{\lg D}{\lg D+\lg\nu}\right)\right]+$$
$$+O(hx^{-1+\varepsilon}).$$

Hence, writing

$$Q_1 = (\lg x)^{M/2}\lg^C D\exp(-b_4\lambda(\lg D)^{1-a}),$$

$$\delta_\nu = (\lg x)^{M/2}\nu^{-2}\exp\left(-c_3\lambda\frac{\lg D}{\lg D+\lg\nu}\right),$$

$$\nu_0 = (\lg x)^M,$$

we get

$$\lg Q_1 \leqslant (M+C)\lg\lg D+M\lg(\lambda+B)-b_4\lambda(\lg D)^{1-a} \leqslant -\tfrac{1}{2}b_4\lambda(\lg D)^{1-a}$$

for $\lambda \geqslant \lambda_0(m)$ uniformly with respect to D. Hence for all $\lambda \geqslant \varepsilon$, $D \epsilon \vartheta$ we have

(2.14) $$Q_1 \leqslant b_6.$$

Analogously, for $\tau \leqslant \nu \leqslant \nu_0$ we get the estimate

$$\lg(\nu^{3/2}\delta_\nu) \leqslant -c_3\lambda\frac{\lg D}{\lg D+\lg\nu_0}+\frac{M}{2}\lg(\lambda+B).$$

But $\lg\nu_0 = O(\lambda\lg D)$ and $\lg(\lambda+B) = O(\lambda)$ for $\lambda\to\infty$; these relations hold uniformly with respect to D; hence we have for a sufficiently large λ (uniformly with respect to D)

$$\lg\nu^{3/2}\delta_\nu \leqslant 0 \quad \text{or} \quad \nu^{3/2}\delta_\nu \leqslant b_7;$$

hence

(2.15) $$\sum_{\nu=\tau}^{\nu_0}\delta_\nu \leqslant b_7\sum_{\nu=1}^{\infty}\nu^{-3/2} \leqslant b_7'.$$

Finally, we have

(2.16) $$\sum_{\nu=\nu_0}^{\infty}\delta_\nu \leqslant (\lg x)^{M/2}\sum_{\nu=\nu_0}^{\infty}\nu^{-2} \ll (\lg x)^{M/2}\nu_0^{-1} \ll 1.$$

The relations (2.14), (2.15) and (2.16) show that

$$(\lg x)^{M/2}|\delta_m(x)| \leqslant b_5(\varepsilon)$$

under the conditions of the lemma. This proves our corollary.

We note now that the functions $S_\nu(x)$ ($\nu = 0, 1, 2, \ldots$) increase monotonously with x; they are all continuous for $\nu \geqslant 1$; finally

$$\frac{\partial}{\partial u}S_\nu(xe^u) = S_{\nu-1}(xe^u)$$

for $\nu \geqslant 2$ and $xe^u \geqslant 1$ for given D.

From the asymptotic law for primes in progressions it follows immediately that there exists for every natural ν at least one function $x_\nu(D)$ such that

$$d_\nu\big(x_\nu(D), D\big) \to 0$$

if D runs over all natural numbers. The class of such functions for a given ν will be denoted by the letter P_ν.

If we are given a sequence ϑ, we can consider the problem of the construction of the functions of the above-mentioned type for the sequence ϑ, such that they increase as slowly as possible if $D\to\infty$. Moreover, we shall be interested in the estimate of $d_\nu\big(x_\nu(D), D\big)$.

LEMMA 3. *Let $x_\nu \epsilon P_\nu$ for a certain ν and a given sequence ϑ; then*

1. $x_\mu = e^{\nu-\mu}x_\nu \epsilon P_\mu$ $(\mu = 0, 1, 2, \ldots, \nu)$,
2. $d_0\big(x_0(D), D\big) \leqslant b_8 d_\nu^{1/2^\nu}$.

Proof. Choose D_ν so large that $d_\nu\big(x_\nu(D), D\big) \leqslant 1$ for all $D \geqslant D_\nu$. The mean value theorem gives

$$S_\nu(xe^\eta)-S_\nu(x) = \eta S_{\nu-1}(xe^{\eta\theta}),$$
$$S_\nu(x)-S_\nu(xe^{-\eta}) = \eta S_{\nu-1}(xe^{-\theta'\eta}),$$

where $0 \leqslant \theta, \theta' \leqslant 1$, $\eta > 0$. Since $S_{\nu-1}(xe^u)$ is monotonic the following inequalities hold:

$$S_{\nu-1}(xe^{-\theta'\eta}) \leqslant S_{\nu-1}(x) \leqslant S_{\nu-1}(xe^{\theta\eta}).$$

On the other hand, for $\eta \leqslant 1$ and $x \geqslant x_\nu e$ we have the estimate

$$S_\nu(x)-S_\nu(xe^{-\eta}) = \nu\eta+O(\nu\eta^2)+O(\nu d_\nu),$$

where $d_\nu = d_\nu\big(x_\nu(D), D\big)$. An analogous estimate holds also for $S_\nu(xe^\eta)-$ $-S_\nu(x)$. Now put $\eta = \sqrt{d_\nu} \leqslant 1$. Comparing the relations mentioned above we get

$$|\delta_{\nu-1}(x)| \leqslant b_9\sqrt{d_\nu} \quad \text{for} \quad x \geqslant x_\nu l,$$

i.e.

(2.17) $$d_{\nu-1} = d_{\nu-1}(x_\nu l, D) \leqslant b_9\sqrt{d_\nu}.$$

Hence, $d_{\nu-1}\to 0$ for $D\to\infty$. Therefore

$$x_\nu l \epsilon P_{\nu-1}.$$

Applying this process of induction for all the values of x_ν from a given ν up to $\nu = 2$, we recognize the validity of the first assertion of our lemma up to the value $\nu = 1$. The transition from $\nu = 1$ to $\nu = 0$ is effected as in paper [10], p. 216. The second assertion of the lemma results from a ν-feld iteration of the relation (2.17).

LEMMA 4. *Let $T \geqslant 1$ and suppose that for all the characters χ* mod$D$ *with $D\epsilon\vartheta$ the following estimate holds:*

$$\max_\chi |L(\tfrac{1}{2}+it, \chi)| \leqslant M(D)(T+2)^{c_0} \quad \textit{for all } |t| \leqslant T.$$

Then

$$N(\sigma, T) \leqslant b_{10}T^{1+2c_0}\big(DM^2(D)\big)^{2(1-\sigma)}\lg^7 D.$$

The proof is given in [7], p. 422.

In what follows we suppose that the sequence ϑ is the sequence $\vartheta_p = \{p^n\}$, where $p > 2$ is a fixed prime; $n = 1, 2, 3, \ldots$

We consider the properties of the characters $\chi(\nu) \bmod D$ where $D \epsilon \vartheta_p$. Let $p > 2$; for each prime of this type we fix a primitive root $g \bmod p^2$ (say, the least one). Then, as we know, the multiplicative group $(\bmod p^n)$ will be a cyclic one with the generator g. Therefore we can put

$$\chi(\nu) = \zeta^{\mathrm{ind}\,\nu},$$

where ζ is a root of unity of degree $h = \varphi(p^n)$. Denote by $\deg\chi$ ($\deg\zeta$) the degree of the character (the degree of the number ζ); in the case of a character it is the least power h such that $\chi^h = \chi_0$ — the principal character. In our case, $h = \deg\chi = \deg\zeta = \deg\chi(g)$. We have obviously $h' \mid p^{n-1}(p-1)$. Let $h' = p^\beta\delta$, $\delta \mid p-1$. We shall show that $p^{\beta+1}$ is the principal (i.e. least) modulus of the character $\chi(\nu)$.

In fact, first of all it is clear that if $p \nmid n$ and $n \equiv n' \pmod{p^{\beta+1}}$, then $\mathrm{ind}\, n \equiv \mathrm{ind}\, n' \left(\bmod \varphi(p^{\beta+1})\right)$; therefore

$$\zeta^{\mathrm{ind} n} = \zeta^{\mathrm{ind} n'}, \quad \text{i.e.} \quad \chi(n) = \chi(n')$$

for $(n, p) \neq 1$. Hence $p^{\beta+1}$ is a modulus for $\chi(\nu)$.

Now let $p^{\beta'}$ be the principal modulus of $\chi(\nu)$; as $g^{\varphi(p^{\beta'})} \equiv 1 \pmod{\beta'}$, we have $\zeta^{\varphi(p^{\beta'})} = \chi(g^{\varphi(p^{\beta'})})$; but then $h\left(\varphi(p^{\beta'})\right)$, i.e. $p^\beta \mid p^{\beta'-1}$ and so $\beta+1 \leqslant \beta'$. This proves our assertion: $\beta+1 = \beta'$.

In particular, if $h = 2$, the principal modulus of χ equals p as $\beta = 0$. In this case the only real character $\bmod p^n$ is $\left(\frac{\nu}{p}\right)$ — the Legendre symbol.

LEMMA 5. *For each positive number M and $\varepsilon > 0$, arbitrarily small, there exists such a constant $b_{11}(M, \varepsilon)$ that*

$$\beta(\gamma) \leqslant 1 - b_{11}(\lg D)^{-\frac{3}{4}}(\lg\lg D)^{-(\frac{3}{4}+\varepsilon)} \tag{2.18}$$

if $\varrho \epsilon \mathfrak{a}(D)$ and $|\gamma| \leqslant (\lg D)^M$.

First of all, we remark that, the second summand of the right-hand side of (2.18) being monotonic, it is sufficient to prove our lemma only for those χ for which $D = p^n$ is the principal modulus. Therefore, taking into account what we said above about real characters, we shall expound the proof only for complex characters with the principal modulus $D = p^n$.

The investigation of the quantity $\beta(\gamma)$ will be conducted by the classical method, i.e. will be guided by the estimate of the absolute value $|L(s, \chi)|$ in the half-plane $\sigma \geqslant \frac{1}{2}$. First of all, let $1-\sigma \leqslant (\lg D)^{-1}$; $|t| \leqslant 2(\lg D)^{M+1}$. It is well known that we then have

$$\lg|L(s, \chi)| \leqslant b_{12}\lg\lg D. \tag{2.19}$$

(For instance, we can put $N = h[|t|+1]$ in the inequality (35.6) of the book [8], p. 101.) Therefore, suppose $1-\sigma > (\lg D)^{-1}$. In the half-plane $\sigma \geqslant \frac{1}{2}+\varepsilon$ we have the estimate

$$|L(s,\chi)| \ll |s|\Big(\int_0^D |S(x)|x^{-\sigma-1}dx + D^{-1-\sigma}\int_0^D |S(x)|\,dx\Big), \tag{2.20}$$

where $S(x) = \sum_{\nu\leqslant x}\chi(\nu)$ (this extimate is an immediate consequence of the application of the Abelian summation method and the periodicity of $S(x)$; cf. [8], p. 99).

In our case

$$D^{-1-\sigma}|s|\int_0^D |S(x)|\,dx \ll D^{-\varepsilon}(\lg D)^{M+1} \ll 1. \tag{2.21}$$

(Here the well-known Vinogradov-Polya estimate for the characters $|S(x)| \ll \sqrt{D}\lg D$ for any $x > 0$ is applied.)

The estimate of the first summand on the right-hand side of (2.20) requires the investigation of the behaviour of $S(x)$ for ϑ_p, as was done in paper [6].

Lemma 1 of paper [6] proves that

$$\sum_{N}^{N+x-1}\chi(\nu)| \leqslant x\Delta^{-1} \quad \text{if} \quad x \geqslant l,$$

N being an arbitrary integer. Here $l = p^{2(n\lg n)^{\frac{3}{4}}}$, $\Delta = p^{n(\lg n)^{\frac{1}{4}}}$; $n \geqslant 2$.

Using this estimate we get

$$\int_0^{D-1} |S(x)|x^{-\sigma-1}dx = \sum_{\nu=0}^{\nu_0}\int_{\nu l}^{(\nu+1)l} |S(x)|x^{-\sigma-1}dx \tag{2.22}$$

$$\ll \frac{l^{1-\sigma}}{1-\sigma} + \Delta^{-1}\frac{l^{1-\sigma}\nu_0^{1-\sigma}}{1-\sigma} + \frac{1}{2}l^{1-\sigma} \ll \frac{l^{1-\sigma}}{1-\sigma} + \Delta^{-1}\frac{D^{1-\sigma}}{1-\sigma},$$

where $\nu_0 l \leqslant D-1 < (\nu_0+1)l$. The estimates (2.20), (2.21) and (2.22) in our case give

$$|L(s, \chi)| \ll (\lg D)^{M+1}\max[\Delta^{-1}D^{1-\sigma}, l^{1-\sigma}]. \tag{2.23}$$

We now choose σ_1 so that $\Delta^{-1}D^{1-\sigma_1} = 1$; then for any $\sigma \geqslant \sigma_1$ the estimate (2.23) is improved to

$$|L(s, \chi)| \ll (\lg D)^{M+1}l^{1-\sigma}$$

or

$$\lg|L(s, \chi)| \leqslant b_{12}\lg\lg D, \tag{2.23'}$$

because $(1-\sigma_1)\lg l \leqslant 4\lg p\cdot \lg\lg D$. Comparing (2.19) and (2.23') we see that the estimate (2.19) holds in the half-stripe S: $\sigma \geqslant \sigma_1$, $|t| \leqslant 2(\lg D)^{M+1}$. We now construct the circles C and C' with centres at the points $s_0 = 1+\eta+it$ and $s_1 = 1+\eta+2ti$ and radii $R = \sigma_1 - 1$; here $\eta > 0$. Both circles are situated inside S; therefore the values of $|L(s, \chi)|$ and $|L(s, \chi^2)|$ are estimated by the formula (2.19). As $L(s, \chi)$ and $L(s, \chi^2)$ are regular inside S, the classical method of the estimation of the value of $\beta(\gamma)$ is applicable to them (cf. [8], p. 116-117). This method shows that if η is so small that

$$\eta c_4(b_{12}\lg\lg D - \lg \eta) \leqslant 0{,}5R,$$

then

$$1-\beta(t) \geqslant \tfrac{1}{7}\eta. \tag{2.24}$$

Simple computation shows that in the capacity of η one can take the value η, satisfying the equation

$$\eta(1-\sigma_1)^{-1}(\lg\lg D)^{1+\varepsilon} = 1. \tag{2.25}$$

Then for sufficiently large values of $D \geqslant D_0(M, \varepsilon)$ our requirements with respect to η will be satisfied and the inequality (2.24) will hold. Finding the value of η from the equation (2.25) and putting this value into (2.24), we prove (2.18).

LEMMA 6. *If $D \epsilon \vartheta_p$, the following estimate holds:*

$$S(x) = \sum_{\nu\leqslant x}\chi(\nu) \ll D^{\frac{1}{6}}(\lg D)^{\frac{1}{2}}\sqrt{Q}, \quad \textit{where} \quad Q = \min(x, D^{\frac{2}{3}}). \tag{2.26}$$

Proof. First of all, we remark that it is sufficient to prove our lemma for the characters with the principal modulus $D = p^n$ because the right-hand side of (2.26) is monotonic with respect to D. Further, it is sufficient to prove our lemma for $x \leqslant D^{\frac{2}{3}}$; for larger values of x it is an immediate consequence of the well-known estimate of Vinogradov-Polya mentioned above. Thus, let $x \leqslant D^{\frac{2}{3}}$. We define a natural number s as the least of all numbers that are larger than or equal to $(n+2)/3$; if $x \leqslant p^s$, our lemma follows immediately from the trivial estimate $|S(x)| \leqslant x$. Therefore, we shall suppose that $p^s \leqslant x \leqslant D^{\frac{2}{3}}$. We obviously have

$$|S(x)| \leqslant \sum_{\mu=0}^{\mu_0} S_\mu, \tag{2.27}$$

where

$$S_\mu = \sum_{N\leqslant\nu\leqslant N'}\chi(\nu), \quad N = 2^\mu p^s, \quad N' \leqslant 2N \quad (\mu = 0, 1, 2, \ldots, \mu_0)$$
$$2^{\mu_0}p^s \leqslant x < 2^{\mu_0+1}p^s.$$

Thus the problem is reduced to the estimates of the sums of the type

$$S_N = \sum_{N\leqslant\nu\leqslant N'}\chi(\nu)$$

under the conditions $p^s \leqslant N \leqslant D^{\frac{2}{3}}$; $N' \leqslant 2N$.

We now put $\nu = l+up^s$; $(l, p) = 1$. Then, by the Buniakowski-Schwartz inequality

$$|S_N| \leqslant \sum_{(l)}{}' \Big|\sum_{u=N_1}^{N_2}\chi(l+up^s)\Big| \leqslant p_1^{\frac{s}{2}}S^{\frac{1}{2}}, \tag{2.28}$$

where $\sum_{(l)}'$ denotes the summation over all l running over the reduced system of residues $\bmod p^s$, $N_1 = p^{-s}(N-l)$, $N_2 = p^{-s}(N'-l)$, we have

$$S_1 = \sum_{(l)}{}' \Big|\sum_{u=N_1}^{N_2}\chi(l+up^s)\Big|^2.$$

Now let l^* be such that $ll^* \equiv (\bmod p^{m-1})$; then

$$S_1 = \sum_{(l)}{}' \Big|\sum_{u=N_1}^{N_2}\chi(1+l^*p^s u)\Big|^2.$$

On the other hand, if $p \geqslant 2$, we can write for any natural v

$$\chi(1+pv) = \exp\left(\frac{2\pi i}{\varphi(p^n)}\right)\mathrm{ind}_g\,(1+pv).$$

In paper [5], p. 21, it is shown that

$$\mathrm{ind}_g(1+pv) \equiv A(p-1)f(v)\big(\mathrm{mod}(p-1)p^{n-1}\big),$$

where $p\nmid A$, A does not depend upon v,

$$f(v) = v+a_2v^2+\ldots+a_Nv^N.$$

The coefficients $a_2, \ldots, a_N$ are integers, $a_2 \equiv \frac{1}{2}p\,(\bmod p^{n-1})$, so that $a_2 = pa_2'$, $p\nmid a_2'$. In our case $v = l^*p^{s-1}u$, so that $v^m \equiv 0\,(\bmod p^{n-1})$ for $m \geqslant 3$. Hence

$$\chi(1+l^*p^s u) = \exp\big(2\pi i(\alpha u^2+\beta u)\big),$$

where $\alpha = \Lambda l^{*2}a_2'p^{-r}$, $\beta = \Lambda l^{*}p^{s-n}$, $r = n-2s$,

(2.29) $$S_1 = \sum_{(l)}{}' \Big|\sum_{u=N_1}^{N_2} \exp\big(2\pi i(\alpha u^2+\beta u)\big)\Big|^2.$$

The interior sum on the right-hand side of (2.29) is a trigonometric sum for a quadratic polynomial; the estimates of such sums are well known; in particular, it is known that

(2.30) $$\Big|\sum_{u=N_1}^{N_a} \exp\big(2\pi i(\alpha u^2+\beta u)\big)\Big|^2 \ll \sum_{|u|\leqslant N_2-N_1} \min\Big(N_2-N_1, \frac{1}{\{\alpha u\}}\Big),$$

where $\{x\}$ denotes the distance to the nearest prime. In our case, putting (2.30) into (2.29) and changing the order of summation over u and l, we get

(2.31) $$S_1 \ll \sum_{\tau=0}^{\tau_0} \sum_{|u'|\leqslant Np^{-s-\tau}} \sum_{(l)}{}' \min\Big(Np^{-s}, \frac{1}{\{\Lambda a_2' u' p^{-\mu} l^{*2}\}}\Big),$$

where $p^T \| u$, i.e. $u = u'p^T$, $p\nmid u'$, $\mu = r-\tau$, $\tau_0 \leqslant \lg Np^{-s}/\lg p$.

Consider now the changing of the value in the brackets on the right-hand side of (2.31) if l changes; the variable l runs over all reduced residue classes mod p^μ with the multiplicity $p^{s-\mu}$. The variable l^{*2} also runs over these classes but with the multiplicity $\leqslant 2p^{s-\mu}$ on account of l^* being squared. As $p\nmid \Lambda a_2' u'$, the variable $\Lambda a_2' u' l^{*2}$ also runs over the above-mentioned classes with the same multiplicity as l^{*2}. Therefore, taking into account that $s-\mu \leqslant \tau+5$, we get

$$\sum_{(l)}{}' \min\Big(Np^{-s}, \frac{1}{\{\Lambda a_2' u' p^{-\mu} l^{*2}\}}\Big) \leqslant 2p^5 p^{s-\mu} \sum_{l=1}^{p^\mu} \min\Big(Np^{-5}, \frac{1}{\{lp^{-\mu}\}}\Big)$$
$$\ll p^T \sum_{l=1}^{p^\mu}\Big(Np^{-s}, \frac{1}{\{lp^{-n}\}}\Big) \ll p^\tau(Np^{-s}+p^\mu \lg D) \leqslant p^\tau Np^{-s}+p^r\lg D.$$

Using this estimate and the inequality (2.31), we get

$$S_1 \ll \sum_{T=0}^{\tau_0} Np^{-s-T}(p^\tau Np^{-s}+p^r\lg D) \ll N^2p^{-2s}\tau_0+Np^{-s+2}\lg D\sum_{\tau=0}^{\infty}p^{-\tau}$$
$$\ll (N^2p^{-2s}+N)\lg D \ll N\lg D,$$

because

(2.32) $$N^2p^{-2s} \leqslant N.$$

The relations (2.28) and (2.32) give

$$|S_N| \ll p^{s/2}\sqrt{N\lg D}.$$

Comparing this inequality with (2.27) we get

$$|S(x)| \leqslant p^s(\lg D)^{\frac{1}{2}} \sum_{\mu=0}^{\mu_0} 2^{\mu/2} \ll p^s(\lg D)^{\frac{1}{2}}(xp^{-s})^{\frac{1}{2}}$$
$$\ll p^{s/2}\sqrt{x\lg D} \ll D^{\frac{1}{6}}\sqrt{x\lg D}.$$

This relation proves the lemma.

Lemma 7. *If $D\in\vartheta_p$, then for any t*

$$|L(\tfrac{1}{2}+it, \chi)| \ll (|t|+1)D^{\frac{1}{6}}(\lg D)^{\frac{3}{2}}.$$

Proof. The Abel summation method gives (cf. [8], p. 99):

(2.34) $$|L(\tfrac{1}{2}+it, \chi)| \leqslant |s|\int_1^\infty |S(x)|x^{-\frac{3}{2}}dx.$$

But for $x \leqslant D^{1/3}$ we have $|S(x)| \leqslant x$; hence:

$$|s|\int_1^{D^{1/3}} |S(x)|x^{-\frac{3}{2}}dx \ll (|t|+1)\int_1^{D^{1/3}} x^{-\frac{1}{2}}dx \ll D^{\frac{1}{6}}(|t|+1).$$

The remaining part of the integral (2.34) can be estimated with help of Lemma 6:

$$\int_{D^{1/3}}^{\infty} |S(x)|x^{-\frac{3}{2}}dx \ll \int_{D^{1/3}}^{D^{2/3}} D^{\frac{1}{6}}(\lg D)^{\frac{1}{2}}x^{-1}dx + \int_{D^{2/3}}^{\infty} D^{\frac{1}{6}}(\lg D)^{\frac{1}{2}}D^{\frac{2}{3}}x^{-\frac{3}{2}}dx$$
$$\ll D^{\frac{1}{6}}(\lg D)^{\frac{3}{2}}.$$

Combining these estimates we prove Lemma 7.

We now pass on to the proof of our theorem. Comparing the Lemmas 4 and 6 shows us that in our case

$$N(\sigma, T) \leqslant b_{13}T^3D^{\frac{8}{3}(1-\sigma)}(\lg D)^{13}.$$

Lemma 5 shows that we can take

$$\eta(D) = b_{14}(\lg D)^{-\frac{4}{5}}, \qquad \tau = (\lg D)^M,$$

M being an arbitrary positive number: $b_{14} = b_{14}(M)$. Then all the conditions of the Corollary to Lemma 2 are fulfilled; we can take $a = \frac{4}{5}$, $m = 4$ in that corollary. Hence, using the estimates of the corollary, we get

$$d_4(x, D) \ll b_{15}(\lg x)^{-\frac{1}{32}M} \quad \text{for} \quad x \geqslant D^{\frac{8}{3}+\varepsilon}.$$

Now the application of Lemma 3 gives

$$|d_0(x, D)| \ll b_{16}(\lg x)^{-\frac{1}{32}M} \quad \text{for} \quad x \geqslant D^{\frac{8}{3}+\varepsilon}.$$

Since M can be chosen as an arbitrary positive number, we have thus proved our theorem.

References

[1] Yu. V. Linnik, *On the least prime in an arithmetic progression*, I: Matem. Sbornik 15 (57) (1944), pp. 139-178; II: 15 (57) (1944), pp. 347-368.

[2] K. A. Rodosski, *On the least prime in an arithmetic progression*, Matem. Sbornik 34 (76) (1955), pp. 331-356 (Russian).

[3] Pang Cheng-Tung, *Least prime in an arithmetic progression*, Science Records (China) 1 (1957), pp. 311-313.

[4] A. G. Postnikov, *On the sum of the characters for a prime power modulus*, Izvestia AN SSSR, ser. matem., 19 (1955), pp. 11-16 (Russian).

[5] — *On Dirichlet's L-series with character modulus equal to a power of a prime number*, J. Indian Math., Ser. 20, 1-3 (1956), pp. 217-226.

[6] S. M. Rosin, *On the zeros of Dirichlet's L-series*, Izvestia AN SSSR, ser. matem., 23 (1959), pp. 503-508 (Russian).

[7] M. B. Barban, *The density of the zeros of Dirichlet's L-series and the problem on the addition of prime and "almost prime" numbers*, Matem. Sbornik 61 (4) (1963), pp. 418-425.

[8] N. G. Tschudakov, *Introduction to the theory of L-functions*, Moskow 1947 (Russian).

[9] Karl Prachar, *Primzahlverteilung*, Berlin 1957.

[10] A. Walfisz, *Weylsche Exponentialsummen in der neueren Zahlentheorie*, Berlin 1963.

Reçu par la Rédaction le 21. 1. 1964

ACTA ARITHMETICA
IX (1964)

On n-dimensional additive moduli and Diophantine approximations

by

A. M. Ostrowski (Basel)

Introduction. By the famous Kronecker's Theorem, if $\alpha_1, \ldots, \alpha_n$ are linearly independent, any point in the n-dimensional unity cube

$$C \quad (0 \leqslant x_\nu < 1) \qquad (\nu = 1, \ldots, n)$$

can be approximated by a point

$$(p\alpha_\nu - p_\nu) \qquad (\nu = 1, \ldots, n)$$

for a positive integer p and integers p_ν. The question arises, how large p must be taken if we want to be able to approximate any point of C with the precision δ. The answer depends on the "degree of independence" of the α_ν, defined as the function $\eta(\varepsilon)$ given for any ε, $0 < \varepsilon < 1$, by

$$\eta(\varepsilon) = \operatorname{Inf} |m_1\alpha_1 + \ldots + m_n\alpha_n + m|,$$

where the integers $m_0, m_1, \ldots, m_n$ satisfy the inequality

$$0 < \sqrt{m_1^2 + \ldots + m_n^2} < 1/\varepsilon.$$

The first estimate of a bound for p was given by Landau [3]. A much better estimate was announced (1925) by Thomas [4], whose bound has the order of $\delta^{-n}/\eta(\delta)$; he gave also explicit numerical constants.

However, Thomas' paper written up with unusual carelessness is practically unreadable, as in particular its geometric part contains not only considerable gaps in the argumentation but also evidently erroneous statements(1).

As I needed a corresponding result in another investigation I lost some time trying to prove Thomas' statements in his way and finally decided to take up the geometric investigation of n-dimensional lattices ab

(1) In particular the formula on page 892: $OP_{s-1}^2 = O_sP_s^2 + {}_s\alpha_{s-1}^2 O_{s-1}P_{s-1}^2$ which appears out of the blue and is used in an essential way to obtain the final estimates, is certainly only true in exceptional cases.