On the density of some sets of primes, IV

by

K. Wnukiewicz (Poznań)

1. If $a$ denotes an integer and $p$ a prime number not dividing $a$ then there exists a positive $y$ such that $a^y \equiv 1 \pmod{p}$. The least of those $y$'s we shall denote by $\text{ord}_p a$.

If $a$ is fixed and $p$ is allowed to vary, then surprisingly little is known about the set of values of $\text{ord}_p a$. In 1927, Emil Artin enunciated the celebrated hypothesis, now usually known as Artin's conjecture, that for any given non-zero integer $a$ other than 1, $-1$ or a perfect square there exist infinitely many primes $p$ for which $\text{ord}_p a = p - 1$. In [7] C. Hooley proved Artin's conjecture subject to the assumption that the natural extension of the Riemann hypothesis to the Dedekind zeta-function over certain Galois fields is true. For some other results connected with this problem we refer to the papers by J. Goldstein [4], P. J. Stephens [13], [14] and R. Warlimont [15].

The problem of the density of the sets of primes for which $\text{ord}_p a$ is divisible or not divisible by a fixed prime $q$ was investigated for an arbitrary integer $a \neq 0$ by H. Hasse [5], [6], who determined the Dirichlet density of such sets.

We proved in [16] some asymptotic formulae for the number of primes $p$ for which $q^r \mid \text{ord}_p a$, where $q$ is a fixed prime and $r = 0, 1, 2, \ldots$

In [18] we improved the results of [16] by getting smaller remainders of the order $1/\log^2 x$ — however, for odd $q$ only.

In the present paper we solve fully the above problem by determining the asymptotic formulae for the number of primes $p$ for which $\text{ord}_p a$ is divisible by an arbitrary integer $n \geq 2$. We also derive an asymptotic formula for the number of primes $p$ for which the congruence $a^x \equiv a \pmod{p}$ has a solution. This is the special case of the problem concerning the existence of the positive density of a set of primes for which the congruence $a^x \equiv c \pmod{p}$ has no solution if $c$ is not a power of $a$ (see [11]).
Let us observe that the solvability of the congruence \( a^m \equiv a \pmod{p} \) is equivalent to the condition that \( \text{ord}_p a \) is not divisible by any prime divisor of \( m \) (see Lemma 4.1).

The remainders in the asymptotic formulae are of the size \( 1/\log^2 x \). and the dependence on the numbers \( a \) and \( n \) in the remainders explicitly counted. Our basic results are obtained by the use of the estimates of the sum of characters over prime ideals of the ring of algebraic integers of the field \( \mathbb{Q}^{\sqrt{M}} \), given in Lemma 3.6 (compare Lemmas 3 and 4 in [18]). The estimate obtained is more precise than the estimate following from the effective version of the Chebotarev density theorem, proved by J. Lagarias and A. Odlyzko in [5].

2. In the following we denote by \( a \) and \( n \) integers greater than 1. Let us write

\[
\begin{align*}
  n &= q_1^{a_1} q_2^{a_2} \cdots q_r^{a_r}, \\
  a(q_i) &\geq 1 \quad \text{for} \quad i = 1, 2, \ldots, r, \\
  q_1 < q_2 < \cdots < q_r,
\end{align*}
\]

where \( q_i \) are primes, and let

\[
\prod_{q \mid a} q = k, \quad \prod_{q \mid a} q = M,
\]

where \( q \) runs over different prime divisors of \( a \) and \( n \) respectively.

Let \( t \geq 1 \) be the largest natural number such that \( a \) is the \( t \)th power in \( Z \).

Denote further

\[
H = \prod_{q \mid a} q^{a(q_i)}.
\]

We shall denote by \( b \) a positive integer satisfying the condition

\[
a = b^M.
\]

In our investigation two more parameters will be used, namely \( \delta \) and \( s \) determined as follows:

\[
b = 2^s \delta^2,
\]

where \( \delta \) is equal to 0 or 1, \( s \) denotes the product of different odd primes and \( v \) is a positive integer.

In the following \( x > 3 \), \( c \) denotes an integer, \( c \neq 0, \pm 1 \), and \( m \) denotes a natural number.

Write further

\[
\begin{align*}
  N_1(x, m, c) &= \sum_{p^m \mid a, (p, c) = 1} \1, \\
  N(x, m, c) &= \sum_{p^m \mid a, (p, m) = 1} \1
\end{align*}
\]

and

\[
\pi(x) = \sum_{p \leq x} 1.
\]

The symbols \( \mu(l) \), \( \psi(l) \) and \( (a, \beta) \) denote as usual the Möbius function, the Euler function and the greatest common divisor of \( a, \beta \) respectively. We denote by \( C_i, i = 1, 2, \ldots \), the numerical constants and by \( |A| \) the number of element of the finite set \( A \).

3. In the present paper we prove the following theorems:

**Theorem 1.** If

\[
x \geq \exp M, \quad \frac{\log x}{(\log \log x)^2} \geq C_i k^2,
\]

where \( C_i \) is a sufficiently large numerical constant, then

\[
(3.1) \quad \frac{1}{\pi(x)} N_1(x, n, a) = a(k, \delta, s, H) + O \left( \frac{Hy^2}{\psi(k) \log^{-1} q_i} \left( \log \log x \right)^{+3} \right),
\]

where

\[
(3.2) \quad a(k, \delta, s, H) = \beta(k, \delta, s, 2) \Delta(k, 2s, H) + \Delta(k, l, H),
\]

\[
(3.3) \quad \Delta(k, l, H) = \left( \frac{\mu(l)}{\psi(l)} \prod_{q \mid d} \frac{1}{q^{\nu(q)}} \prod_{q \mid d} \frac{1 - q^{-\nu(q)}}{(q - 1)} \prod_{q \mid d} \left( \frac{1 - q^{-\nu(q)}}{q - 1} \right) \right)
\]

for \( l | k \),

and for integer \( \gamma \)

\[
(3.4) \quad \beta(k, \delta, s, \gamma) = \begin{cases} 
  \frac{1}{2} & \text{for } \delta = 0, s > 1, 2s | k, \ s = 1 \pmod{4}, \\
  \frac{2 - 4^\gamma}{4} & \text{for } \delta = 0, s > 1, 2s | k, \ s \neq 1 \pmod{4}, \\
  \frac{2(4^\gamma - 4^\gamma)}{16} & \text{for } \delta = 1, s \geq 1, 2s | k, \\
  0 & \text{otherwise.}
\end{cases}
\]

The parameters \( \gamma(d) \) are determined as in (2.3), the parameters \( \delta \) and \( s \) as in (2.5).

The constant implied by the symbol \( O \) is numerical; however, in the case of an even \( k \), the constant under consideration is not effective.
Theorem 1'. If
\[ x \gg \exp \exp^4 M, \quad \frac{\log x}{(\log \log x)^2} \gg C_1 k^2, \]
then
\[ (3.5) \quad \frac{1}{\pi(x)} N_1(x, n, a) = a(k, \delta, s, \Pi) + O \left( \frac{\log \log x}{\log x} \right), \]
where the constant in $O$ is numerical and effective and $a(k, \delta, s, \Pi)$ is determined by (3.2)–(3.4) and $C_1$ is the same as in Theorem 1.

Remark 1. From Theorems 1 and 1' we can immediately deduce similar theorems for $a < 0$. This follows from the fact that for $k$ odd we have $N_1(x, k, a) = N_1(x, k, -a)$; on the other hand, for $k$ even, $N_1(x, k, -a) = N_1(x, k, a^2) - N_1(x, k, a)$. Moreover, we have the equality $N_1(x, n, a) = N_1(x, k, a)$. (See Lemma 1 and Corollary 4.1.)

Theorem 2. If
\[ x \gg \exp M, \quad \frac{\log x}{(\log \log x)^2} \gg C_1 k^2, \]
then
\[ (3.6) \quad \frac{1}{\pi(x)} N(x, n, b) \]
\[ = 1 + \beta(k, \delta, s, a(2)-1) + O \left( \frac{\log \log x}{\psi(k) \log^{-1} q_1} \right), \]
where $a(2)$ is determined by (2.1) and the constant in $O$ is numerical but not effective in the case of an even $k$.

The parameters $\delta$ and $s$ are determined in (2.5), $b(k, \delta, s, a(2)-1)$ is determined in (3.4) and $C_1$ is as in Theorem 1.

Theorem 2'. If
\[ x \gg \exp \exp^4 M, \quad \frac{\log x}{(\log \log x)^2} \gg C_1 k^2, \]
then
\[ (3.7) \quad \frac{1}{\pi(x)} N(x, n, b) \]
\[ = 1 + \beta(k, \delta, s, a(2)-1) + O \left( \frac{\log \log x}{\psi(k) \log^{-1} q_1} \right), \]
where the constant implied by the symbol $O$ is numerical and effective and $b(k, \delta, s, a(2)-1)$ is determined in (3.4).

Remark 2. From Theorems 2 and 2' we can immediately derive the respective theorems for an arbitrary integer $a, a \neq 0, \pm 1$. This follows from the fact that
(a) $N(x, n, a) = N(x, nH, b)$,
(b) if $n = 2^t, \ (2, t) = 1, \ a \neq \pm 1$, then
\[ N(x, n, a) = N(x, n, a), \]
(c) if $n = 2t, \ (2, t) = 1$, then
\[ N(x, n, a) = N(x, n/2, a) + N(x, 2n, a) - N(x, n, a) \]
(see Corollary 4.2).

4. The proofs of the theorems will rest on the following lemmas.

Lemma 4.1. If $p \nmid c$, then the congruence $c^n \equiv c \pmod{p}$ is solvable if and only if $(n, \varphi_c) = 1$.

Corollary 4.1. If $p \nmid c$, then the congruence $c^n \equiv c \pmod{p}$ is solvable if and only if the congruence $c^p \equiv c \pmod{p}$ is solvable.

Corollary 4.2. If $p \nmid c$, $q$ denotes a prime, $a$ a natural number, then $c^{a^2} \equiv c^{a-1} \pmod{p}$ is solvable iff $q^t \mid \varphi_c$.

Lemma 4.2. If $p \nmid c$, then the congruence $c^n \equiv c \pmod{p}$ is solvable if and only if $c$ is the $N$th power residue $\pmod{p}$, $N$ being the maximal divisor of $p - 1$ whose prime factors all divide $n$.

The lemma follows from the definition of the power residue.

Lemma 4.3. Suppose $1 < \xi < (x-1)/q$. If $M_0(\xi)$ denotes the set
\[ \{ N_0 : N_0 = q_1^{l_1} q_2^{l_2} \ldots q_r^{l_r}, \ l_i > 0, \ \xi < N_0 < x-1, \ N_0 \leq q_i \} \]
for each $q_i | N_0$,
then
\[ |M_0(\xi)| \leq r \left( \frac{\log x}{\log q_1} + 1 \right)^{r-1}. \]

If $N$ is an arbitrary natural number of the form $N = q_1^{l_1} q_2^{l_2} \ldots q_r^{l_r}$, $\xi < N$, then there exist a number $N_0 \in M_0(\xi)$ and a number $m = q_1^{\beta_1} q_2^{\beta_2} \ldots q_r^{\beta_r}$, $\beta_i > 0$, $i = 1, 2, \ldots, r$ such that $N = m N_0$.

The first part of the lemma follows by induction. The proof of the second part is obvious.

Let $m$ be a natural number. We denote
\[ M(x, m, c) = \sum_{p \equiv c (\text{mod} m) \text{ is a prime residue mod} p} 1. \]
The equality (4.3) follows from Corollary 4.2 and the principle of Legendre.

5. In this section we state some lemmas from the theory of the Hecke–Landau $\zeta$-functions.

Denote by $K$ a field of algebraic numbers, by $v$ and $\lambda$, respectively, the degree and the discriminant of $K$, by $E$ the ring of algebraic integers of $K$, by $\mathfrak{p}$ a given ideal of $E$, by $N_E$ the norm of an ideal $\alpha$ of $E$, and by $p$ a prime ideal of $K$. Let $\chi$ be a character of the group of ideal-classes mod $\mathfrak{p}$; $\zeta(s, \chi)$ the Hecke–Landau Zeta-function (see [9]), and $\zeta_K(z)$ the Dedekind Zeta-function.

The character of the prime of ideal-classes mod $\mathfrak{p}$ will be denoted by $\chi_{\mathfrak{p}}$, the exceptional real character by $\chi_{\mathfrak{p}}$ (see [18] and [18]) and the hypothetical real simple zero of $\zeta(z, \chi)$ by $\beta_1$. We denote the product $|\Delta|N_E$ by $D$.

Denote further

$$E_0 = E_0(\chi) = \begin{cases} 1 & \text{for } \chi = \chi_{\mathfrak{p}}, \\ 0 & \text{for } \chi \neq \chi_{\mathfrak{p}} \end{cases}; \quad E_1 = E_1(\chi) = \begin{cases} 1 & \text{for } \chi = \chi_{\mathfrak{p}}, \\ 0 & \text{for } \chi \neq \chi_{\mathfrak{p}} \end{cases}$$

**Lemma 5.1.** There exists a numerical constant $C_1$ such that

$$\sum_{N \leq x} \chi(p) p = E_0 \log x - E_1 \log x + 0 \left( \frac{\log^2 D}{\log x} \right) 
+ \begin{cases} O\left( \frac{\log^2 D}{\log x} \right) & \text{for } \chi = \chi_{\mathfrak{p}}, \\ O\left( \frac{\log^2 D}{\log x} \right) & \text{for } \chi \neq \chi_{\mathfrak{p}} \end{cases}$$

where

$$\omega(z, p, v) = \frac{\log \sigma(z, p, v)}{\max\left(\log^2 D, \log x\right)}$$

and the constant implied by the symbol $O$ is numerical.

This lemma follows from Lemma 1 of [18]. The proof is similar to the proof of Lemma 9 in [17].

**Lemma 5.2.** Let us denote by $K$ a normal extension of the field $Q$. Then for any $v > 0$ there exists a numerical constant $O(e)$ such that

$$\beta_1 = \max\left(1 - (32\log |\Delta|N_E)^{-1}, 1 - (U(v)(|\Delta|N_E)^{v}e)^{-1}\right).$$

For $e \gg 1$ the constant $O(e)$ is effective and for $e < 1$ it is not.

The lemma follows from Theorem 1' of paper [12] and the theorem of Siegel on the exceptional zero.

In the following we denote by $m$ a natural number of the form

$$n = \prod_{q \leq q_0} q^{[k]}$$

where $1(q) > 0$ for every prime divisor $q$ of $k$. We will denote by $K$ the field $Q(\sqrt{D})$ and by $B$ its ring of integers.
For \(a \in R\) and a prime ideal \(p\) of \(R\), \(p \nmid [ma]\), we denote by \(\left( \frac{a}{p} \right)\) the
\(m\)th power residue symbol.

For the ideal \(a\) of \(R_{\text{f}}(a, [ma]) = 1\) we put
\[
\left( \frac{a}{p} \right)_m = \prod_{p \mid m} \left( \frac{a}{p} \right)_m.
\]

Let \(a_1, a_2, \ldots, a_m\) denote arbitrary rational integers and \(M\) the product
of different prime divisors of the product \(a_1 a_2 \ldots a_m\). For given integers
\(j_1, j_2, \ldots, j_\tau\), \(1 \leq j_i \leq m\), \(i = 1, 2, \ldots, \tau\) we define
\[
\chi_{j_1, \ldots, j_\tau}(a) = \begin{cases}
\left( \frac{a_{j_1}^{\tau_1} \cdots a_{j_\tau}^{\tau_\tau}}{a} \right)_m & \text{for } (a, [m^2M]) = 1, \\
0 & \text{otherwise}.
\end{cases}
\]

From Lemma 27 of [3] it follows that \(\chi_{j_1, \ldots, j_\tau}\) is a character of the
group of ideal-classes mod \([m^2M]\) of the ring \(R\).

For \(\tau\) mth roots of unity \(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_\tau\) we put
\[
S(m, a_1, a_2, \ldots, a_\tau) = \sum_{j_1 = 1}^m \cdots \sum_{j_\tau = 1}^m (\varepsilon_1^{j_1} \cdots \varepsilon_\tau^{j_\tau})^{-1},
\]

where \(\beta \in R\).

If there exist integers \(j_1^0, 1 \leq j_1^0 \leq m, 1 \leq i \leq \tau\) such that \(\chi_{j_1, \ldots, j_\tau}^{j_1^0} = \chi_1\),
where \(\chi_1\) is the exceptional character of the group of ideal-classes mod \([m^2M]\)
of the ring \(R\), \(X \neq 0\), then we define
\[
\overline{N}_1(m, a_1, a_2, \ldots, a_\tau) = \sum_{j_1 = 1}^m \cdots \sum_{j_\tau = 1}^m (\varepsilon_1^{j_1} \cdots \varepsilon_\tau^{j_\tau})^{-1},
\]

where \(\beta' \in R\).

If such a \(j_1^0\) do not exist then we put \(\overline{N}_1(m, a_1, a_2, \ldots, a_\tau) = 0\).

Remark 3. If \(m\) is odd then \(\chi_{j_1, \ldots, j_\tau}\) cannot be a real non-principal character. This results from the following lemma of [2]:

**Lemma 8.3.** Let \(m\) be a positive rational integer, and let \(o\) be a further rational integer which is a \(m\)-th power residue (mod \(p\)) for all but finitely many rational primes \(p = 1 \pmod{m}\); then \(o\) is of the form \(\beta^m\), \(\beta \in R\).

Note that, if \(a^2 = \beta^m\), \(a, \beta \in R\) and \(m\) is odd, then
\[
a = (\beta^{(m-1)/2})^m.
\]

We define further
\[
S(x, m, a_1, \ldots, a_\tau, \varepsilon_1, \ldots, \varepsilon_\tau) = \sum_{n \equiv x \pmod{m} \atop (n^m, a_1 \cdots a_\tau) = 1} 1,
\]

where \(p\) are prime-ideals of the ring \(R\).

**Lemma 8.4.** If \(x \geq \exp m\), \(a \geq \log^2 M\) then there exists a numerical constant \(C_4\) such that
\[
S(x, m, a_1, \ldots, a_\tau, \varepsilon_1, \ldots, \varepsilon_\tau) = m^{-r} \overline{N}(m, a_1, \ldots, a_\tau) \pi(x) - \overline{N}(m, a_1, \ldots, a_\tau) \log^2 D \exp(-C_4 \omega(x, D, \varepsilon)),
\]

and the constant implied by the symbol \(O\) is numerical. (We recall that according to the notation introduced above, in this lemma the letter \(D\) denotes the product of the norm of the ideal \([m^2M]\) of the ring \(R\) and the absolute value of the discriminant of the field \(Q(\sqrt[2]{m})\). Moreover, \(\beta\) denotes the exceptional zero of \(L(s, \chi_1, \tau)\)).

**Proof.** From the definition of \(S(x, m, a_1, \ldots, a_\tau, \varepsilon_1, \ldots, \varepsilon_\tau)\) and \(\overline{N}(m, a_1, \ldots, a_\tau)\) it follows that
\[
S(x, m, a_1, \ldots, a_\tau, \varepsilon_1, \ldots, \varepsilon_\tau) - m^{-r} \overline{N}(m, a_1, \ldots, a_\tau) \sum_{N \leq x} 1
\]

\[
= m^{-r} \sum_{j_1 = 1}^m \cdots \sum_{j_\tau = 1}^m (\varepsilon_1^{j_1} \cdots \varepsilon_\tau^{j_\tau})^{-1} \sum_{N \leq x} \chi_{j_1, \ldots, j_\tau}(n),
\]

where \(\sum\) denotes that the summation runs over such prime-ideals \(p\) of the
ring \(R\) which are not divisors of the product \(ma_1 a_2 \ldots a_\tau\). Since in the
sum \(\sum\), the ideals \(p\) are not ramified, it follows under the assumption of
the lemma
\[
\sum' 1 = \varphi(m) \sum_{p \equiv 1 \pmod{m}} 1 + O(a^{1/2} \log x),
\]

Applying the Siegel–Walfisz theorem on primes in arithmetical progressions (see [10], Satz 8.3, p. 144) we have
\[
\sum' 1 = \pi(x) + O(x \exp(-C_4 \nu \log x)).
\]
The characters $\chi_{k_{1j_1}, \ldots, k_{j_j}}$ in (5.6) are not principal because of the condition $a_j^2 \cdots a_1^2 \neq \beta^m$ (see Lemma 5.3). Hence applying Lemma 5.3 to the sum $\sum_{N_{x, y}} \chi_{x_{1j_1}, \ldots, x_{j_j}}(y)$ and using the estimate (5.7), we get (5.5).

In the following we consider the sum $S(x, m, a_1, \ldots, a_j, e_1, \ldots, e_j)$ in the particular case $j = 1$, $a_1 = a$, $e_1 = 1$. We shall denote this sum by $S(x, m, a)$. The sum (5.4) will be denoted in this case by $N(m, a)$.

**Lemma 5.5.** Suppose $m = \prod_p q^m(p), l(q) \geq 0$. Under (2.4) and (2.5) we have

$$N(m, a) = 2(H, m)$$

in the following three cases:

(i) $N(m, a) = 2(H, m)$.
(ii) $N(m, a) = 2(\mathbb{Z}/m\mathbb{Z}, m)$.
(iii) $N(m, a) = 2(\mathbb{Z}/m\mathbb{Z}, m)$.

In the remaining cases

$$N(m, a) = (H, m).$$

The proof of the lemma follows from Lemma 2 of [1].

**Lemma 5.6.** With the notation of Section 2, let $m = \prod_p q^m(p), l(q) \geq 0$, $2 \mid m = 2^r$, $2 \notmid m = 2^r H(H, m)$,

$$E(l, \gamma) = \begin{cases} 0 & \text{for } l \leq \gamma, \\ 1 & \text{for } l > \gamma, \end{cases}$$

where $H$ is determined by (2.3).

Suppose further that $t \geq 1, 0 < a \leq 1$ and $C_6 \geq 0$ is an arbitrary numerical constant.

If

$$m \leq \exp \left( \frac{C_4}{C_6 + 1} \log m \right)$$

and $\beta$ is the exceptional zero of the function $\zeta(\zeta, \chi_2)$, where $\chi_2$ is the exceptional character of the group of ideal classes $\operatorname{mod}[m^3 M]$ of the ring $\mathbb{Z}$, then

$$E(l, \gamma) = \begin{cases} 0 & \text{for } l \leq \gamma, \\ 1 & \text{for } l > \gamma, \end{cases}$$

where $H$ is determined by (2.3).

Suppose further that $l \geq 1, 0 < a \leq 1$ and $C_6 \geq 0$ is an arbitrary numerical constant.

If

$$S(x, m, a) = m^{-1} N(m, a) \pi(x) + E(l, \gamma) O_1 \left( \frac{H^2 m}{l} \right) \log l + O_2 \left( \log l \right)$$

where the constant in $O_2$ depends only on $C_4$, $C_6$, $a$, $t$ and the constant in $O_1$ is absolute $\leq 2$. In this lemma, the constant $C_6$ is from Lemma 5.4.

Proof. From Lemmas 5.3 and 5.5 it follows that there exist at most $2(H, m)$ values for $j$ in the interval $1 \leq j \leq m$ for which the character $\chi_j = \left( \frac{a_j}{a} \right)$ is real and non-principal. Moreover, in the case $l \leq \gamma$

each character $\chi_j(1 \leq j \leq m)$ is principal or non-real. Hence, owing to (5.8) and using the formula for the degree and the discriminant of the field $\mathbb{K}$ and the norm of the ideal $[m^3 M]$, we get in view of Lemma 5.4 the estimate (5.9).

**Corollary 5.1.** If the conditions of Lemma 5.6 are fulfilled then for any $q > 0$ there exist constants $C_7 \geq 0$ such that

$$\frac{N(m, a)}{\varphi(m)} \pi(x) \leq C_7 \epsilon \left( \frac{H^2 m}{l} \right) \left( \frac{1}{\log l} \right)^{\gamma} + C_8 \left( \frac{1}{\log l} \right)^{\gamma} \log l \log x.$$
However, with the value for $\xi$ chosen above, condition (6.2) is fulfilled if we suppose $\sigma$ to be greater than a numerical constant and $C_\sigma$ to be sufficiently large. Hence, if the conditions of Theorem 1 are fulfilled, we have from (6.1)

$$
\max_{N \leq N_0, \alpha} M_w(N, \alpha) \leq O_{\alpha \eta}(\log \log x)^{1+\log_2 \log \log x},
$$

where the constant $C_{\alpha \eta}$ is effective for $\eta$ odd. From this estimate and Lemma 4.4 we get

$$
N_1(x, k, a) = \sum_{N \leq x} \sum_{k \equiv 1} \frac{\mu(l) M(x, lN, a')}{N \phi(lN)} \pi(x) + O \left( \frac{Hk^2 \log \log x}{\phi(k)} \frac{\log \log x}{\log \log \log x} \right),
$$

where the constant in $O$ is numerical but not effective in the case of an even $k$.

In case $m = lN, l | k, a = 1, t = 1, C_s = 2$ we apply Corollary 5.1. Moreover, in this corollary we replace the number $a$ by $a'$. If the conditions of Theorem 1 are fulfilled, for $N \leq x$ and sufficiently large $C_s$, we have

$$
M(x, lN, a') = \frac{N(lN, a')}{N \phi(lN)} \pi(x) + O \left( \frac{Hk^2 \log \log x}{\phi(k)} \frac{\log \log x}{\log \log \log x} \right),
$$

where for odd $k$ the constant in $O$ is effective.

From (6.4) and (6.3) we get

$$
\frac{1}{\pi(x)} N_1(x, k, a) = \sum_{N \leq x} \sum_{k \equiv 1} \frac{\mu(l) \frac{N(lN, a')}{N \phi(lN)} \pi(x)}{N \phi(lN)} + O \left( \frac{Hk^2 \log \log x}{\phi(k)} \frac{\log \log x}{\log \log \log x} \right) = S_1 + S_2 + S_3 + S_4 + B(x, H, r, k, g_1).
$$

On the other hand, from Lemma 5.5, for $\eta \geq 0$ it follows that

$$
\sum_{N \leq x} \sum_{k \equiv 1} \frac{\mu(l) \frac{N(lN, a')}{N \phi(lN)}}{N \phi(lN)} = \sum_{N \leq x} \sum_{k \equiv 1} \frac{\mu(l) \phi(N, H)}{N} \sum_{l \equiv 1} \frac{\phi(lN)}{N},
$$

where $\eta = 2$ if one of the three conditions (i), (ii), (iii) of Lemma 5.5 is satisfied and $\eta = 1$ otherwise.

If $d$ is fixed, for such $N$ that $d | N$, $(N, k/d) = 1$ we have the equality

$$
\sum_{l \equiv 1} \frac{\mu(l)}{N \phi(lN)} = N^{-1} \prod_{d | l \phi} \left( 1 - \frac{1}{d} \right).
$$

Hence

$$
\sum_{N > x} \sum_{l \equiv 1} \frac{\mu(l) \frac{N(lN, a')}{N \phi(lN)}}{N \phi(lN)} = \sum_{d | l \phi} \sum_{d' \equiv 1, d \phi} \frac{\phi(N, H)}{N} \prod_{d | l \phi} \left( 1 - \frac{1}{d} \right).
$$

From (6.6), for $\eta = \xi$ we get

$$
S_2 \leq \sum_{N \leq x} \sum_{l \equiv 1} \frac{2Hk^2}{N \phi(lN)} \sum_{d | l \phi} \frac{2H}{(N_0 m)^2} \leq C_\xi H \xi^{-2} \sum_{N \leq N_0 m} 1
$$

$$
\leq C_\xi \frac{Hr k^2}{(\log \log x)^{1+\gamma}} \frac{\log \log x}{\log \log \log x}.
$$

On the other hand, owing to (6.5) and (6.6) for $\eta = 0$, and owing to the last estimate, we have

$$
\frac{1}{\pi(x)} N_1(x, k, a) = \sum_{N \leq x} \sum_{k \equiv 1} \frac{\mu(l) \phi(N, H)}{N} \prod_{d | l \phi} \left( 1 - \frac{1}{d} \right) + B(x, H, r, k, g_1).
$$

Considering in turn

(a) $\delta = 0, s > 1, 2s | k, \delta = 1 \pmod{4}$,
(b) $\delta = 0, s > 1, 2s | k, \delta = 1 \pmod{4}$,
(c) $\delta = 1, s \geq 1, 2s | k$

and the remaining cases, we can reduce the estimate (6.7) to the form (3.1).

Similarly, applying Lemma 5.3 for $\sigma = 1$ we get Theorem 1'.

Theorem 2 follows from Theorem 1 and Lemma 4.5.

References


1 Acta Arithmetica XLIII, 1
Multidimensional covering systems of congruences

by

J. Fabrykowski (Warszawa)

1. Introduction. Covering systems of congruences in one variable have been studied for many years. The aim of the present paper is to extend the results obtained for such systems to multidimensional systems introduced recently by A. Schinzel [8]. We begin by defining the principal notions.

DEFINITION 1. A system of congruences

(1) \[ b_{1i} + \sum_{j=1}^{k} b_{ij} x_j \equiv 0 \mod m_i \quad (1 \leq i \leq n) \]

covers a set \( S \subseteq \mathbb{Z}^k \) if every vector \([x_1, \ldots, x_k] \in S\) satisfies one of the congruences of the system.

DEFINITION 2. A congruence of the system (1) is called essential if there exists an integral vector \([x_1, \ldots, x_k] \in \mathbb{Z}^k\) which satisfies this and only this congruence.

DEFINITION 3. A system of the form (1) is called regular if all congruences are essential.

DEFINITION 4. A system of the form (1) is called covering if it covers the set \( \mathbb{Z}^k \) and disjoint covering if it is regular and every vector in \( \mathbb{Z}^k \) satisfies one and only one congruence of this system.

For one dimensional systems \((k=1)\) it is usual to take \( b_{1i} = 1 \) which can be relaxed to \((b_{1i}, m_i) = 1\). Here are principal results concerning such systems.

Theorem A (see [7], Theorems 2–4). For a disjoint covering system

\[ x \equiv a_i \mod m_i \quad (1 \leq i \leq n), \]

where \( 1 < m_1 \leq m_2 \leq \ldots \leq m_n \) we have

\[ \sum_{i=1}^{n} \frac{1}{m_i} = 1, \quad m_{n-1} = m_n, \]

for every \( i = 1, 2, \ldots, n \) there exists a \( t \neq i \) such that \( m_t \mid m_i \), if \( p \) is the least prime factor of \( m_n \) then \( m_n = m_{n-1} = \ldots = m_{n-p+1} \).