ACTA ARITHMETICA
XLIII (1984)

On the density of some sets of primes, IV

by

K. Wiertelak (Poznań)

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

If a is fixed and p is allowed to vary, then surprisingly little is known about the set of values of $\operatorname{ord}_p a$. 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 $\operatorname{ord}_p a = p-1$. 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 $\operatorname{ord}_p a$ 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 $q^r \| \operatorname{ord}_p a$, 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 $\operatorname{ord}_p a$ is divisible by an arbitrary integer $n \geqslant 2$. We also derive an asymptotic formula for the number of primes p for which the congruence $a^{ny} \equiv a \pmod{p}$ 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 $a^y \equiv c \pmod{p}$ has no solution if c is not a power of a (see [11]).

Let us observe that the solvability of the congruence $a^{nv} \equiv a \pmod p$ is equivalent to the condition that $\operatorname{ord}_p a$ is not divisible by any prime divisor of n (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 is 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 $Q(\sqrt[m]{1})$, 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 [8].

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

(2.1) $$n = q_1^{\alpha(q_1)} q_2^{\alpha(q_2)} \dots q_r^{\alpha(q_r)}, \quad \alpha(q_i) \geqslant 1 \quad \text{for} \quad i = 1, 2, \dots, r, \quad q_1 < q_2 < \dots < q_r,$$

where q_i are primes, and let

(2.2) $$\prod_{q|n} q = k, \quad \prod_{q|a} q = M,$$

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

Let $t \geqslant 1$ be the largest natural number such that a is the tth power in Z.

Denote further

(2.3) $$H = \prod_{\substack{q|n \\ q^{\gamma(q)} \| t}} q^{\gamma(q)}.$$

We shall denote by b a positive integer satisfying the condition

(2.4) $$a = b^H.$$

In our investigation two more parameters will be used, namely δ and s determined as follows:

(2.5) $$b = 2^\delta s v^2,$$

where δ 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

$$N_1(x, m, c) = \sum_{\substack{p \leqslant x, (p,c)=1 \\ c^{my} \equiv c \pmod p \\ \text{is solvable}}} 1, \quad N(x, m, c) = \sum_{\substack{p \leqslant x, (p,c)=1 \\ m | \operatorname{ord}_p c}} 1$$

and

$$\pi(x) = \sum_{p \leqslant x} 1.$$

The symbols $\mu(l)$, $\varphi(l)$ and (α, β) denote as usual the Möbius function, the Euler function and the greatest common divisor of α, β respectively.

We denote by C_i, $i = 1, 2, \dots$, 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*

$$x \geqslant \exp M, \quad \frac{\log x}{(\log\log x)^2} \geqslant C_1 k^2,$$

where C_1 is a sufficiently large numerical constant, then

(3.1) $$\frac{1}{\pi(x)} N_1(x, n, a) = \alpha(k, \delta, s, H) + O\left(\frac{Hrk^3}{\varphi(k)\log^{r-1} q_1} \cdot \frac{(\log\log x)^{r+3}}{\log^2 x}\right),$$

where

(3.2) $$\alpha(k, \delta, s, H) = \beta(k, \delta, s, \gamma(2)) A(k, 2s, H) + A(k, l, H),$$

(3.3) $$A(k, l, H) = \begin{cases} \dfrac{\mu(l)}{\varphi(l)} \prod_{q|l} \dfrac{1}{q^{\gamma(q)}(q+1)} \sum_{d|\frac{k}{l}} \left(\left(\prod_{q|\frac{k}{ld}} \dfrac{q-2}{q-1}\right) \prod_{q|d} \left(\dfrac{1-q^{-\gamma(q)}}{q-1} + \dfrac{q^{-\gamma(q)}}{q^2-1}\right)\right) & \textit{for} \quad l|k, \\ 0 \quad \textit{for} \quad l \nmid k \end{cases}$$

and for integer γ

(3.4) $$\beta(k, \delta, s, \gamma) = \begin{cases} -\dfrac{1}{2} & \textit{for} \quad \delta = 0,\ s > 1,\ 2s|k,\ s \equiv 1 \pmod 4, \\ \dfrac{2-(4^\gamma, 4)}{4} & \textit{for} \quad \delta = 0,\ s > 1,\ 2s|k,\ s \not\equiv 1 \pmod 4, \\ \dfrac{2(4^\gamma, 4)-(4^\gamma, 16)}{16} & \textit{for} \quad \delta = 1,\ s \geqslant 1,\ 2s|k, \\ 0 & \textit{otherwise}. \end{cases}$$

The parameters $\gamma(q)$ are determined as in (2.3), the parameters δ 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*

$$x \geqslant \exp\exp\sqrt[4]{M}, \qquad \frac{\log x}{(\log\log x)^2} \geqslant C_1 k^2,$$

then

$$(3.5)\qquad \frac{1}{\pi(x)} N_1(x, n, a) = a(k, \delta, s, H) + O\left(\frac{H2^r k^2}{\varphi(k)\log^{r-1} q_1} \cdot \frac{(\log\log x)^{r+2}}{\log x}\right),$$

where the constant in O is numerical and effective and $a(k, \delta, s, H)$ 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 4.1 and Corollary 4.1).

THEOREM 2. *If*

$$x \geqslant \exp M, \qquad \frac{\log x}{(\log\log x)^2} \geqslant C_1 k^2,$$

then

$$(3.6)\qquad \frac{1}{\pi(x)} N(x, n, b) = \frac{1+\beta\big(k, \delta, s, a(2)-1\big)}{n\prod_{q|k}(1-1/q^2)} + O\left(\frac{nr2^r k^2}{\varphi(k)\log^{r-1} q_1} \cdot \frac{(\log\log x)^{r+3}}{\log^2 x}\right),$$

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 δ and s are determined in (2.5), $\beta\big(k, \delta, s, a(2)-1\big)$ *is determined in* (3.4) *and C_1 is as in Theorem* 1.

THEOREM 2'. *If*

$$x \geqslant \exp\exp\sqrt[4]{M}, \qquad \frac{\log x}{(\log\log x)^2} \geqslant C_1 k^2,$$

then

$$(3.7)\qquad \frac{1}{\pi(x)} N(x, n, b) = \frac{1+\beta\big(k, \delta, s, a(2)-1\big)}{n\prod_{q|k}(1-1/q^2)} + O\left(\frac{n4^r k}{\varphi(k)\log^{r-1} q_1} \cdot \frac{(\log\log x)^{r+2}}{\log x}\right),$$

where the constant implied by the symbol O is numerical and effective and $\beta\big(k, \delta, s, a(2)-1\big)$ *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 $n = 2^a t$, $(2, t) = 1$, $a \neq 1$, 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 $c^{ny} \equiv c \pmod p$ is solvable if and only if $(n, \operatorname{ord}_p c) = 1$.*

Clear.

COROLLARY 4.1. *If $p \nmid c$, then the congruence $c^{ny} \equiv c \pmod p$ is solvable if and only if the congruence $c^{ky} \equiv c \pmod p$ is solvable.*

COROLLARY 4.2. *If $p \nmid c$, q denotes a prime, a a natural number, then $c^{q^a y} \equiv c^{q^{a-1}} \pmod p$ is solvable iff $q^a \nmid \operatorname{ord}_p c$.*

LEMMA 4.2. *If $p \nmid c$, then the congruence $c^{ky} \equiv c \pmod p$ is solvable if and only if c is the N-th power residue* (mod 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 $1 \leqslant \xi \leqslant (x-1)/q_r$. If $M_0(\xi)$ denotes the set*

$$M_0(\xi) = \{N_0\colon N_0 = q_1^{l_1} q_2^{l_2} \ldots q_r^{l_r},\ l_i \geqslant 0,\ \xi < N_0 \leqslant x-1,\ N_0 \leqslant \xi q_i \text{ for each } q_i | N_0\},$$

then

$$|M_0(\xi)| \leqslant r\left(\frac{\log \xi}{\log q_1} + 1\right)^{r-1}.$$

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 $m = q_1^{\beta_1} q_2^{\beta_2} \ldots q_r^{\beta_r}$, $\beta_i \geqslant 0$, $i = 1, 2, \ldots, r$ such that $N = mN_0$.

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

$$M(x, m, c) = \sum_{\substack{p \leqslant x,\, p\nmid c \\ p \equiv 1 \pmod m \\ c \text{ is a } m\text{th residue} \bmod p}} 1.$$

LEMMA 4.4. *Suppose $k \leqslant \xi \leqslant (x-1)/q_r$. Then there exists a numerica constant C_2 such that*

$$(4.1)\qquad \Big|N_1(x,k,c) - \sum_{\substack{N\leqslant\xi\\ N=q_1^{l_1}q_2^{l_2}\ldots q_r^{l_r}\\ l_1\geqslant 0,\ldots,l_r\geqslant 0}} \sum_{\substack{l\mid k\\ l\leqslant\frac{x-1}{N}}} \mu(l)M(x,lN,c^l)\Big| \leqslant C_2 r\left(\frac{\log\xi}{\log q_1}\right)^{r-1} \max_{N_0\in M_0(\xi)} M(x,N_0,c),$$

where $M_0(\xi)$ denotes the set of Lemma 4.3 and $q_1, q_2, \ldots, q_r$ are determined in (2.1).

Proof. We denote for the number $N = q_1^{l_1}q_2^{l_2}\ldots q_r^{l_r}$, $l_i \geqslant 0$, $i = 1, 2, \ldots, r$,

$$A_N = \{p \leqslant x\colon p\nmid c,\ p-1 = Nt,\ (k,t) = 1,\ c \text{ is a } N\text{th residue} \bmod p\}.$$

Since $A_N \cap A_{N'} = \emptyset$ for $N \neq N'$, owing to Lemma 4.2, we have

$$(4.2)\qquad N_1(x,k,a) = \sum_{\substack{N\leqslant\xi\\ N=q_1^{l_1}q_2^{l_2}\ldots q_r^{l_r}\\ l_1\geqslant 0,\ldots,l_r\geqslant 0}} |A_N| + \sum_{\substack{\xi<N\leqslant x-1\\ N=q_1^{l_1}q_2^{l_2}\ldots q_r^{l_r}\\ l_1\geqslant 0,\ldots,l_r\geqslant 0}} |A_N| = S_1+S_2.$$

From the second part of Lemma 4.3 we get

$$S_2 \leqslant \sum_{N_0\in M_0(\xi)} M(x,N_0,c).$$

Hence from the first part of Lemma 4.3 and owing to the inequality $k \leqslant \xi$ we have

$$(4.3)\qquad S_2 \leqslant C_2 r\left(\frac{\log\xi}{\log q_1}\right)^{r-1} \max_{N_0\in M_0(\xi)} M(x,N_0,c).$$

On the other hand, using the well-known Legendre principle we get

$$(4.4)\qquad S_1 = \sum_{\substack{N\leqslant\xi\\ N=q_1^{l_1}q_2^{l_2}\ldots q_r^{l_r}\\ l_1\geqslant 0,\ldots,l_r\geqslant 0}} \sum_{\substack{l\mid k\\ 1\leqslant l\leqslant\frac{x-1}{N}}} \mu(l)M(x,lN,c^l).$$

Finally from (4.2)–(4.4) Lemma 4.4 follows.

LEMMA 4.5. *We have the equality*

$$(4.5)\qquad N(x,n,c) = \sum_{k'\mid k} \mu(k')N_1(x,k',c^{n/k'}),$$

where k is defined by (2.2).

The equality (4.5) 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 ζ-functions.

Denote by K a field of algebraic numbers, by ν and Δ, respectively, the degree and the discriminant of K, by $\overline{K}$ the ring of algebraic integers of K, by $\mathfrak{f}$ a given ideal of $\overline{K}$, by $N\mathfrak{a}$ the norm of an ideal $\mathfrak{a}$ of $\overline{K}$, and by $\mathfrak{p}$ a prime ideal of $\overline{K}$. Let χ be a character of the group of ideal-classes mod $\mathfrak{f}$, $\zeta(s,\chi)$ the Hecke–Landau Zeta-function (see [9]), and $\zeta_K(s)$ the Dedekind Zeta-function.

The principal character of the group of ideal-classes mod $\mathfrak{f}$ will be denoted by χ_0, the exceptional real character by χ_1 (see [8] and [18]) and the hypothetical real simple zero of $\zeta(s,\chi_1)$ by β_1. We denote the product $|\Delta|N\mathfrak{f}$ by D.

Denote further

$$(5.1)\qquad E_0 = E_0(\chi) = \begin{cases}1 & \text{for } \chi = \chi_0,\\ 0 & \text{for } \chi \neq \chi_0,\end{cases} \qquad E_1 = E_1(\chi) = \begin{cases}1 & \text{for } \chi = \chi_1,\\ 0 & \text{for } \chi \neq \chi_1.\end{cases}$$

LEMMA 5.1. *There exists a numerical constant C_3 such that*

$$(5.2)\qquad \sum_{N\mathfrak{p}\leqslant x} \chi(\mathfrak{p}) = E_0 \operatorname{li} x - E_1 \operatorname{li} x^{\beta_1} + O\left(\frac{x\log 2D}{\sqrt{\log x}} \exp\big(-C_3\omega(x,D,\nu)\big)\right),$$

where

$$\omega(x,D,\nu) = \frac{\log x}{\max\big((\nu\log x)^{1/2}, \log D\big)}$$

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 $\varepsilon > 0$ there exists a numerical constant $C(\varepsilon)$ such that*

$$(5.3)\qquad \beta_1 < \max\Big(1-(32\log|\Delta|\sqrt{N\mathfrak{f}})^{-1},\ 1-\big(C(\varepsilon)(|\Delta|\sqrt{N\mathfrak{f}})^{\varepsilon/\nu}\big)^{-1}\Big).$$

For $\varepsilon \geqslant 1$ the constant $C(\varepsilon)$ is effective and for $\varepsilon < 1$ 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

$$m = \prod_{q\mid k} q^{l(q)},$$

where $l(q) \geqslant 0$ for every prime divisor q of k. We will denote by K the field $Q(\sqrt[m]{1})$ and by R its ring of integers.

For $a \in R$ and a prime ideal $\mathfrak{p}$ of R, $\mathfrak{p} \nmid [ma]$, we denote by $\left(\frac{a}{\mathfrak{p}}\right)_m$ the mth power residue symbol.

For the ideal $\mathfrak{a}$ of R, $(\mathfrak{a}, [ma]) = 1$ we put

$$\left(\frac{a}{\mathfrak{a}}\right)_m = \prod_{\mathfrak{p}^w \| \mathfrak{a}} \left(\frac{a}{\mathfrak{p}}\right)_m^w.$$

Let $a_1, a_2, \ldots, a_\tau$ denote arbitrary rational integers and M the product of different prime divisors of the product $a_1 a_2 \ldots a_\tau$. For given integers $j_1, j_2, \ldots, j_\tau$, $1 \leqslant j_i \leqslant m$, $i = 1, 2, \ldots, \tau$ we define

$$\chi_{j_1,\ldots,j_\tau}(\mathfrak{a}) = \begin{cases} \left(\dfrac{a_1^{j_1} a_2^{j_2} \ldots a_\tau^{j_\tau}}{\mathfrak{a}}\right)_m & \text{for} \quad (\mathfrak{a}, [m^2 M]) = 1, \\ 0 & \text{otherwise}. \end{cases}$$

From Lemma 27 of [3] it follows that $\chi_{j_1,j_2,\ldots,j_\tau}$ is a character of the group of ideal-classes mod $[m^2 M]$ of the ring R.

For τ mth roots of unity $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_\tau$ we put

$$\overline{N}(m, a_1, a_2, \ldots, a_\tau) = \sum_{\substack{j_1=1 \\ a_1^{j_1} a_2^{j_2} \ldots a_\tau^{j_\tau} = \beta^m}}^{m} \ldots \sum_{j_\tau=1}^{m} (\varepsilon_1^{j_1} \ldots \varepsilon_\tau^{j_\tau})^{-1}, \tag{5.4}$$

where $\beta \in R$.

If there exist integers j_i^0, $1 \leqslant j_i^0 \leqslant m$, $1 \leqslant i \leqslant \tau$ such that $\chi_{j_1^0,\ldots,j_\tau^0} = \chi_1$, where χ_1 is the exceptional character of the group of ideal-classes mod $[m^2 M]$ of the ring R, $\chi_1 \neq \chi_0$, then we define

$$\overline{N}_1(m, a_1, a_2, \ldots, a_\tau) = \sum_{\substack{j_1=1 \\ a_1^{j_1^0+j_1} \ldots a_\tau^{j_\tau^0+j_\tau} = \beta'^m}}^{m} \ldots \sum_{j_\tau=1}^{m} (\varepsilon_1^{j_1} \ldots \varepsilon_\tau^{j_\tau})^{-1},$$

where $\beta' \in R$.

If such a j_i^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 $\chi_{j_1,j_2,\ldots,j_\tau}$ cannot be a real non-principal character. This results from the following lemma of [2]:

LEMMA 5.3. *Let m be a positive rational integer, and let c be a further rational integer which is a m-th-power residue* (mod p) *for all but finitely many rational primes $p \equiv 1 (\bmod m)$; then c is of the form β^m, $\beta \in R$.*

Note that, if $a^2 = \beta^m$, $a, \beta \in R$ and m is odd, then

$$a = (\beta^{(1-m)/2} a)^m.$$

We define further

$$S(x, m, a_1, \ldots, a_\tau, \varepsilon_1, \ldots, \varepsilon_\tau) = \sum_{\substack{N\mathfrak{p} \leqslant x, \mathfrak{p} \nmid [ma_1 \ldots a_\tau] \\ \left(\frac{a_j}{\mathfrak{p}}\right)_m = \varepsilon_j}} 1,$$

where $\mathfrak{p}$ are prime-ideals of the ring R.

LEMMA 5.4. *If $x \geqslant \exp m$, $x \geqslant \log^2 M$ then there exists a numerical constant C_4 such that*

$$S(x, m, a_1, \ldots, a_\tau, \varepsilon_1, \ldots, \varepsilon_\tau) = m^{-\tau} \overline{N}(m, a_1, \ldots, a_\tau) \pi(x) - m^{-\tau} N_1(m, a_1, \ldots, a_\tau) \operatorname{li} x^{\beta_1} + O\left(\frac{x \log 2D}{\sqrt{\log x}} \exp\left(-C_4 \omega(x, D, \nu)\right)\right), \tag{5.5}$$

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 $[m^2 M]$ of the ring R and the absolute value of the discriminant of the field $Q(\sqrt[m]{1})$. Moreover, β_1 denotes the exceptional zero of $\zeta(s, \chi_{j_1^0,\ldots,j_\tau^0})$.)

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

$$S(x, m, a_1, \ldots, a_\tau, \varepsilon_1, \ldots, \varepsilon_\tau) - m^{-\tau} \overline{N}(m, a_1, \ldots, a_\tau) \sum_{N\mathfrak{p} \leqslant x}{}' 1 = m^{-\tau} \sum_{\substack{j_1=1 \\ a_1^{j_1} \ldots a_\tau^{j_\tau} \neq \beta^m}}^{m} \ldots \sum_{j_\tau=1}^{m} (\varepsilon_1^{j_1} \ldots \varepsilon_\tau^{j_\tau})^{-1} \sum_{N\mathfrak{p} \leqslant x}{}' \chi_{j_1,\ldots,j_\tau}(\mathfrak{p}), \tag{5.6}$$

where $\sum'$ denotes that the summation runs over such prime-ideals $\mathfrak{p}$ of the ring R which are not divisors of the product $m a_1 a_2 \ldots a_\tau$. Since in the sum $\sum_{N\mathfrak{p} \leqslant x}' 1$, the ideals $\mathfrak{p}$ are not ramified, it follows under the assumption of the lemma

$$\sum_{N\mathfrak{p} \leqslant x}{}' 1 = \varphi(m) \sum_{\substack{p \leqslant x \\ p \equiv 1 (\bmod m)}} 1 + O(x^{1/2} \log x).$$

Applying the Siegel–Walfisz theorem on primes in arithmetical progressions (see [10], Satz 8.3, p. 144) we have

$$\sum_{N\mathfrak{p} \leqslant x}{}' 1 = \pi(x) + O\left(x \exp(-C_5 \sqrt{\log x})\right). \tag{5.7}$$

The characters $\chi_{j_1,\ldots,j_\tau}$ in (5.6) are not principal because of the condition $a_1^{j_1}\ldots a_\tau^{j_\tau}\neq\beta^m$ (see Lemma 5.3). Hence applying Lemma 5.1 to the sum $\sum'_{N\mathfrak{p}\leqslant x}\chi_{j_1,j_2,\ldots,j_\tau}(\mathfrak{p})$ and using the estimate (5.7), we get (5.5).

In the following we consider the sum $S(x,m,a_1,\ldots,a_\tau,\varepsilon_1,\ldots,\varepsilon_\tau)$ in the particular case $\tau=1$, $a_1=a$, $\varepsilon_1=1$. We shall denote this sum by $S(x,m,a)$. The sum (5.4) will be denoted in this case by $\bar{N}(m,a)$.

LEMMA 5.5. *Suppose* $m=\prod_{q|n}q^{l(q)}$, $l(q)\geqslant 0$. *Under* (2.4) *and* (2.5) *we have*

$$\bar{N}(m,a)=2(H,m)$$

in the following three cases:

(i) $\delta=0$, $s|m$, $s>1$, $2(H,m)|m$, $2\|m$, $s\equiv 1\ (\mathrm{mod}\ 4)$,

(ii) $\delta=0$, $4s|m$, $s>1$, $2(H,m)|m$,

(iii) $\delta=1$, $8s|m$, $2(H,m)|m$.

In the remaining cases

$$\bar{N}(m,a)=(H,m).$$

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

LEMMA 5.6. *With the notation of Section* 2, *let* $m=\prod_{q|n}q^{l(q)}$, $l(q)\geqslant 0$, $2^l\|m$, $a=b^H$, $2^\gamma\|H$,

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

where H *is determined by* (2.3).

Suppose further that $t\geqslant 1$, $0<\alpha\leqslant 1$ *and* $C_6\geqslant 0$ *is an arbitrary numerical constant.*

If

$$(5.8)\qquad (m^3M)^{\varphi(m)}\leqslant\exp\left(\left(\frac{C_4}{C_6+1}\right)^2\frac{\log^\alpha x}{\log^t\log x}\right)$$

and β_1 *is the exceptional zero of the function* $\zeta(s,\chi_1)$, *where* χ_1 *is the exceptional character of the group of ideal-classes* mod$[m^2M]$ *of the ring* R, *then*

$$(5.9)\qquad S(x,m,a)=m^{-1}\bar{N}(m,a)\pi(x)+E(l,\gamma)O_1\big(m^{-1}(H,m)\mathrm{li}\,x^{\beta_1}\big)+\\ +O_2\Big(x\exp\big(-(1.7C_6+1.2)\sqrt{\alpha}\log^{(1-\alpha)/2}x\log^{(1+t)/2}\log x\big)\Big)$$

where the constant in O_2 *depends only on* C_4, C_6, α, t *and the constant in* O_1 *is absolute* $\leqslant 2$. *In this lemma, the constant* C_4 *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 $1\leqslant j\leqslant m$ for which the character $\chi_j(\mathfrak{a})=\left(\frac{a^j}{\mathfrak{a}}\right)_m$ is real and non-principal. Moreover, in the case $l\leqslant\gamma$, each character χ_j $(1\leqslant j\leqslant m)$ is principal or non-real. Hence, owing to (5.8) and using the formula for the degree and the discriminant of the field K and the norm of the ideal $[m^2M]$, 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* $\varepsilon>0$ *there exist constants* $C_7(\varepsilon)$ *and* C_8 *such that*

(5.10)
$$\left|M(x,m,a)-\frac{\bar{N}(m,a)}{m\varphi(m)}\pi(x)\right|\leqslant C_7(\varepsilon)E(l,\gamma)\frac{(H,m)\sqrt{M}}{\prod_{p|m}(1-1/p)}\cdot\frac{x}{(\log x)^{1+1/\varepsilon}}+\\ +C_8x\exp\big(-(1.7C_6+1.2)\sqrt{\alpha}\log^{(1-\alpha)/2}x\log^{(1+t)/2}\log x\big).$$

For $\varepsilon\geqslant 1$ *the constant* C_7 *is explicitly calculable and for* $\varepsilon<1$, *it is not. The constant* C_8 *can be counted explicitly depending on* C_4, C_6, α, t.

The corollary follows from the formula

$$M(x,m,a)=\frac{1}{\varphi(m)}S(x,m,a)+O(\sqrt{x})$$

and Lemma 5.2.

6. Proof of Theorem 1. We use Lemma 4.4 with

$$\xi=\frac{\log x}{C_9k\log^2\log x}.$$

For the sake of brevity we shall denote by N any number of the form $q_1^{l(q_1)}q_2^{l(q_2)}\ldots q_r^{l(q_r)}$, where $l(q_1)\geqslant 0,\ldots,l(q_r)\geqslant 0$.

For $N_0\in M_0(\xi)$ we have

$$\varphi(N_0)\geqslant N_0\frac{\varphi(k)}{k}>\xi\frac{\varphi(k)}{k}.$$

From Corollary 5.1 for $C_6=2$, $t=1$, $\alpha=1$ and from Lemma 5.5, we get

$$(6.1)\qquad \max_{N_0\in M_0(\xi)}M(x,N_0,a)\\ \leqslant\frac{Hk}{\varphi(k)}\cdot\frac{\pi(x)}{\xi^2}+C_7E(l_0,\gamma)\frac{H\sqrt{M}k}{\varphi(k)}\cdot\frac{x}{(\log x)^{1+1/\varepsilon}}+C_8\frac{x}{\log^3x},$$

provided

$$(6.2)\qquad \varphi(N_0)\log(N_0^3M)\leqslant\left(\frac{C_4}{3}\right)^2\frac{\log x}{\log\log x},$$

where, in (6.1), $l_0=\max_{\substack{2^l\|N_0\\ N_0\in M_0(\xi)}}l$.

However, with the value for ξ chosen above, condition (6.2) is fulfilled if we suppose x to be greater than a numerical constant and C_9 to be sufficiently large. Hence, if the conditions of Theorem 1 are fulfilled, we have from (6.1)

$$\max_{N_0\in M_0(\xi)} M(x, N_0, a) \leqslant C_{10}\frac{k^3H}{\varphi(k)}\cdot\frac{\pi(x)\log^4\log x}{\log^2 x},$$

where the constant C_{10} is effective for n odd. From this estimate and Lemma 4.4 we get

$$(6.3)\quad N_1(x, k, a) = \sum_{N\leqslant\xi}\sum_{\substack{l|k\\ l\leqslant\frac{x-1}{N}}}\mu(l)M(x, lN, a^l)+O\left(\frac{Hk^3r}{\varphi(k)}\cdot\frac{\log^{r+3}\log x}{\log^{r-1}q_1}\cdot\frac{\pi(x)}{\log^2 x}\right),$$

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

In the case $m = lN$, $l|k$, $a = 1$, $t = 1$, $C_6 = 2$ we apply Corollary 5.1. Moreover, in this corollary we replace the number a by a^l.

If the conditions of Theorem 1 are fulfilled, for $N\leqslant\xi$ and sufficiently large C_9 we have

$$(6.4)\qquad M(x, lN, a^l) = \frac{\bar{N}(lN, a^l)}{lN\varphi(lN)}\pi(x)+O\left(\frac{Hk^2}{\varphi(k)}\cdot\frac{\pi(x)}{\log^2 x}\right),$$

where for odd k the constant in O is effective.

From (6.4) and (6.3) we get

$$(6.5)\quad \frac{1}{\pi(x)}N_1(x, k, a) = \sum_{N}\sum_{l|k}\mu(l)\frac{\bar{N}(lN, a^l)}{lN\varphi(lN)}+\sum_{N>\xi}\sum_{l|k}\mu(l)\frac{\bar{N}(lN, a^l)}{lN\varphi(lN)}+ +O\left(\frac{Hrk^3}{\varphi(k)\log^{r-1}q_1}\cdot\frac{\log^{r+3}\log x}{\log^2 x}\right) = S_1+S_2+R(x, H, r, k, q_1).$$

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

$$\sum_{N>\eta}\sum_{l|k}\mu(l)\frac{\bar{N}(lN, a^l)}{lN\varphi(lN)} = \sum_{d|k}\sum_{\substack{N>\eta\\ (N,k/d)=1\\ d|N}}\frac{\varrho\cdot(N, H)}{N}\sum_{l|k}\frac{\mu(l)}{\varphi(lN)},$$

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

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

$$\sum_{l|k}\frac{\mu(l)}{N\varphi(lN)} = N^{-1}\prod_{q|\frac{k}{d}}\left(\frac{q-2}{q-1}\right).$$

Hence

$$(6.6)\quad \sum_{N>\eta}\sum_{l|k}\mu(l)\frac{\bar{N}(lN, a^l)}{lN\varphi(lN)} = \sum_{d|k}\sum_{\substack{N>\eta\\ (N,k/d)=1\\ d|N}}\frac{\varrho\cdot(N, H)}{N^2}\prod_{q|\frac{k}{d}}\left(\frac{q-2}{q-1}\right).$$

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

$$S_2\leqslant\sum_{N>\xi}\frac{2H}{N^2}\leqslant\sum_{N_0\in M_0(\xi)}\sum_{\substack{m=q_1^{\delta_1}\ldots q_r^{\delta_r}\\ \delta_i\geqslant 0}}\frac{2H}{(N_0m)^2}\leqslant C_{12}H\xi^{-2}\sum_{N_0\in M_0(\xi)}1 \leqslant C_{13}\frac{Hrk^2}{(\log q_1)^{r-1}}\frac{(\log\log x)^{r+3}}{\log^2 x}.$$

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

$$(6.7)\quad \frac{1}{\pi(x)}N_1(x, k, a) = \sum_{d|k}\sum_{\substack{N\\ (N,k/d)=1\\ d|N}}\frac{\varrho\cdot(N, H)}{N^2}\prod_{q|\frac{k}{d}}\left(\frac{q-2}{q-1}\right)+R(x, H, r, k, q_1).$$

Considering in turn

(a) $\delta = 0$, $s>1$, $2s|k$, $s\equiv 1 \pmod 4$,
(b) $\delta = 0$, $s>1$, $2s|k$, $s\not\equiv 1 \pmod 4$,
(c) $\delta = 1$, $s\geqslant 1$, $2s|k$

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

Similarly, applying Lemma 5.2 for $\varepsilon = 1$ we get Theorem 1'.

Theorem 2 follows from Theorem 1 and Lemma 4.5.

References

[1] P. D. T. A. Elliott, *A problem of Erdős concerning power residue sums*, Acta Arith. 13 (1967), pp. 131–149.

[2] — *The distribution of power residues and certain related results*, ibid. 17 (1970), pp. 141–159.

[3] — *On the mean value of f(p)*, Proc. London Math. Soc. (3) 21 (1970), pp. 28–96.

[4] L. J. Goldstein, *Analogues of Artin's conjecture*, Trans. Amer. Math. Soc. 149 (1970), pp. 431–442.
[5] H. Hasse, *Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von gerader bzw. ungerader Ordnung* mod*p ist*, Math. Ann. 166 (1966), pp. 19–23.
[6] — *Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von durch eine vorgegebene Primzahl $l \neq 2$ teilbarer bzw. unteilbarer Ordnung* mod*p ist*, ibid. 162 (1965), pp. 74–76.
[7] C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. 225 (1967), pp. 209–220.
[8] J. Lagarias and A. Odlyzko, *Effective versions of the Chebotarev density theorem*, *Algebraic number fields* (ed. Fröhlich), Academic Press, London–New York 1977, pp. 409–464.
[9] E. Landau, *Über Ideale und Primideale in Idealklassen*, Math. Zeitschr. 2 (1918), pp. 52–154.
[10] K. Prachar, *Primzahlverteilung*, Berlin 1957.
[11] A. Schinzel, *A refinement of a theorem of Gerst on power residues*, Acta Arith. 17 (1970), pp. 161–168.
[12] H. M. Stark, *Some effective cases of the Brauer–Siegel theorem*, Inventiones Math. 23 (1974), pp. 135–152.
[13] P. J. Stephens, *Prime divisors of second-order linear recurrences*, J. Number Theory 8 (1976), pp. 313–345.
[14] — *An average result for Artin's conjecture*, Mathematika 16 (1969), pp. 178–188.
[15] R. Warlimont, *On Artin's conjecture*, J. London Math. Soc. (2), 5 (1972), pp. 91–94.
[16] K. Wiertelak, *On the density of some sets of primes, I*, Acta Arith. 34 (1978), pp. 183–196.
[17] — *On the density of some sets of primes, II*, ibid. 34 (1978), pp. 197–210.
[18] — *On the density of some sets of primes, III*, Studies in Pure Mathematics, To the Memory of Paul Turán, pp. 761–773.

INSTITUTE OF MATHEMATICS
OF THE ADAM MICKIEWICZ UNIVERSITY
Poznań

Received on 12. 3. 1982
and in revised form on 30. 8. 1982 (1295)

ACTA ARITHMETICA
XLIII (1984)

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

$$b_{i0}+\sum_{j=1}^{k} b_{ij}x_j \equiv 0 \bmod m_i \quad (1 \leqslant i \leqslant n) \tag{1}$$

covers a set $S \subset \boldsymbol{Z}^k$ 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 $[x_1, \ldots, x_k] \in \boldsymbol{Z}^k$ 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 $\boldsymbol{Z}^k$, and *disjoint covering* if it is regular and every vector in $\boldsymbol{Z}^k$ satisfies one and only one congruence of this system.

For one dimensional systems ($k = 1$) it is usual to take $b_{i1} = 1$ which can be relaxed to $(b_{i1}, m_i) = 1$. Here are principal results concerning such systems.

Theorem A (see [7], Theorems 2–4). *For a disjoint covering system $x \equiv a_i \bmod m_i$ $(1 \leqslant i \leqslant n)$, where $1 < m_1 \leqslant m_2 \leqslant \ldots \leqslant m_n$ we have*

$$\sum_{i=1}^{n} 1/m_i = 1, \quad m_{n-1} = m_n,$$

for every $i = 1, 2, \ldots, n$ there exists a $t \neq i$ such that $m_i | m_t$,

if p is the least prime factor of m_n then $m_n = m_{n-1} = \ldots = m_{n-p+1}$.