ACTA ARITHMETICA
XXXIV (1978)

On the density of some sets of primes, I

by

K. Wiertelak (Poznań)

1. If $(a, m) = 1$, there exists a positive γ such that $a^\gamma \equiv 1 \pmod m$ For example (Euler's theorem) $\gamma = \varphi(m)$. The least of these γ's is called the exponent to which a belongs modulo m.

The sets A and B of primes p for which a given integer $a \neq 0$ belongs to an even and an odd exponent mod p, respectively, were investigated in the case of $a = 2$ by W. Sierpiński [7], A. Brauer [2] and A. Aigner [1].

W. Sierpiński proved that A contains all primes $p \equiv \mp 5 \pmod{2^3}$ and an infinity of primes $p \equiv 1 \pmod{2^3}$.

A. Brauer and A. Aigner proved that also B contains an infinity of primes $p \equiv 1 \pmod{2^3}$.

H. Hasse (see [4]) developed and generalized those investigations and determined the Dirichlet density of A and B for an arbitrary integer $a \neq 0$.

In [5] H. Hasse introduced the condition that the exponent under consideration should be divisible and non-divisible respectively by a prime $q > 2$.

The aim of this note is to prove some asymptotic formulae for the number of primes p for which a given integer $a \neq 0, \mp 1$ belongs mod p to an exponent δ divisible exactly by q^r, $r \geqslant 0$ ($q^r \| \delta$). We obtain also some stronger estimates under the hypothesis that real zeros of certain Dedekind Zeta-functions are situated not too close to the point $s = 1$ of the complex plane.

In the following the finite sets of primes p for which $(p, a) > 1$ will be dropped.

2. The letter a is a given non-zero integer, p, q are prime numbers. Consider the following sets of primes p:

$$B(a, q, r, l) = \{p\colon q^l \| p-1,\ q^r \| \delta,\ \delta - \text{order of } a \bmod p\},$$

where $r = 0, 1, 2, \ldots, l$, $l = 0, 1, 2, \ldots$,

$$B(a, q, r) = \{p\colon q^r \| \delta\} = \bigcup_{l=r}^{\infty} B(a, q, r, l)$$

$r = 0, 1, 2, \ldots$

Write further

$$N(x, a, q, r, l) \stackrel{\text{def}}{=} \sum_{\substack{p \leqslant x \\ p \in B(a,q,r,l)}} 1, \tag{2.1}$$

$$N(x, a, q, r) \stackrel{\text{def}}{=} \sum_{\substack{p \leqslant x \\ p \in B(a,q,r)}} 1,$$

and

$$\Pi(x, m, t) = \sum_{\substack{p \leqslant x, (l, m)=1 \\ p \equiv t \pmod m}} 1.$$

Let k be the maximal integer for which $|a|$ can be written in the form $|a| = b^{2^k}$, b being a positive integer.

We shall prove the following theorems:

THEOREM 1. *If* $|a| = b^{2^k}$, *then for*

$$2^{k+r+2} \leqslant \frac{\log_2 x}{\log_3 x} \tag{2.2}$$

we have the estimate

$$N(x, a, 2, r) = a(a, r)\frac{x}{\log x} + O\left(\left(\frac{1}{2}\right)^{(r+k)/2}\left(\frac{\log_3 x}{\log_2 x}\right)^{1/2}\frac{x}{\log x}\right), \tag{2.3}$$

where for $b = 2b_1^2$

$$\begin{aligned} &a(\mp b, 0) = a(\mp b, 1) = \tfrac{7}{24}, \\ &a(b^{2^k}, 0) = a(-b^{2^k}, 1) = \begin{cases} \frac{7}{12}, & k = 1, \\ 1 - \frac{1}{3}(\frac{1}{2})^k, & k \geqslant 2, \end{cases} \\ &a(b^{2^k}, 1) = a(-b^{2^k}, 0) = \begin{cases} \frac{1}{3}, & k = 1, \\ \frac{1}{3}(\frac{1}{2})^{k+1}, & k \geqslant 2, \end{cases} \\ &a(\mp b^{2^k}, r) = \begin{cases} \frac{1}{3}, & k = 0,\ r = 2, \\ \frac{1}{3}(\frac{1}{2})^{k+r}, & k + r > 2,\ r \geqslant 2 \end{cases} \end{aligned} \tag{2.4}$$

and for $b \neq 2b_1^2$

$$\begin{aligned} &a(b^{2^k}, 0) = a(-b^{2^k}, 1) = 1 - \tfrac{2}{3}(\tfrac{1}{2})^k, \\ &a(b^{2^k}, 1) = a(-b^{2^k}, 0) = \tfrac{1}{3}(\tfrac{1}{2})^k, \\ &a(b^{2^k}, r) = a(-b^{2^k}, r) = \tfrac{1}{3}(\tfrac{1}{2})^{r+k-1}, \quad r \geqslant 2. \end{aligned} \tag{2.5}$$

The constant implied by the O-notation depends only on b.

THEOREM 2. *If* q *is an odd prime and if* $|a| = b^{q^k}$, *then for*

$$q^{k+r+2} \leqslant \frac{\log_2 x}{\log_3 x} \tag{2.6}$$

we have the estimate

$$N(x, a, q, r) = a(a, q, r)\frac{x}{\log x} + O\left(\left(\frac{1}{q}\right)^{(k+r-2)/2}\left(\frac{\log_3 x}{\log_2 x}\right)^{1/2}\frac{x}{\log x}\right), \tag{2.7}$$

where

$$a(a, q, r) = \begin{cases} 1 - \dfrac{1}{q^{k-1}(q^2-1)}, & r = 0, \\ \dfrac{1}{q^{k+r-1}(q+1)}, & r \geqslant 1. \end{cases} \tag{2.8}$$

The constant implied by the O-notation depends only on b.

THEOREM 3. *Under the hypothesis that for the fields*

$$K_{l,l'} \stackrel{\text{def}}{=} Q\left(\sqrt[q^l]{a}, \sqrt[q^{l'}]{1}\right),$$

$l' = l$ *or* $l' = l+1$, $l = k+r$, $k+r+1, \ldots$, *the Dedekind Zeta-functions* $\zeta_{K_{l,l'}}(s) \neq 0$ *for* $s > 1 - \dfrac{C_1}{\log(2|\Delta|)}$, *where* Δ *denotes the discriminant of the fields* $K_{l,l'}$ *and* C_1 *is a positive numerical constant, we have, for*

$$q^{k+r+2} \leqslant \frac{\log x}{\log_2^4 x}, \tag{2.9}$$

the estimate

$$N(x, a, q, r) = a(a, q, r)\frac{x}{\log x} + O\left(\left(\frac{1}{q}\right)^{(k+r-2)/2}\frac{x}{\log^{3/2} x}\log_2^2 x\right), \tag{2.10}$$

where $a(a, 2, r) = a(a, r)$ *are determined by* (2.4) *or* (2.5) *and* $a(a, q, r)$ $(q > 2)$ *by* (2.8). *The constant implied by the O-notation depends only on* b.

The case $k = 0$ seems particularly interesting. Therefore we state the results obtained in this special case in the following corollaries:

COROLLARY 1. *If* $b > 1$ *is not a square of an integer, then for* $2^{r+2} \leqslant \dfrac{\log_2 x}{\log_3 x}$ *we have the estimate*

$$N(x, \mp b, 2, r) = a(\mp b, r)\frac{x}{\log x} + O\left(\left(\frac{1}{2}\right)^{r/2}\left(\frac{\log_3 x}{\log_2 x}\right)^{1/2}\frac{x}{\log x}\right), \tag{2.11}$$

where for $b = 2b_1^2$

$$\begin{aligned} &a(\mp b, 0) = a(\mp b, 1) = \tfrac{7}{24}, \\ &a(\mp b, r) = \begin{cases} \frac{1}{3}, & r = 2, \\ \frac{1}{3}(\frac{1}{2})^r, & r > 2, \end{cases} \end{aligned} \tag{2.12}$$

and for $b \neq 2b_1^2$

$$a(\mp b, r) = \begin{cases} \frac{1}{3}, & r = 0, \\ \frac{1}{3}(\frac{1}{2})^{r-1}, & r \geqslant 1. \end{cases} \tag{2.13}$$

COROLLARY 2. *If* $b > 1$ *is not a* q*-th power of an integer,* q *being an odd prime, then for* $q^{r+2} \leqslant \dfrac{\log_2 x}{\log_3 x}$ *we have*

$$N(x, \mp b, q, r) = a(\mp b, q, r)\frac{x}{\log x} + O\left(\left(\frac{1}{q}\right)^{(r-2)/2}\left(\frac{{}^1\log_3 x}{\log_2 x}\right)^{1/2}\frac{x}{\log x}\right), \tag{2.14}$$

where

$$a(\mp b, q, r) = \begin{cases} 1 - \dfrac{q}{q^2-1}, & r = 0, \\ \dfrac{1}{q^{r-1}(q+1)}, & r \geqslant 1. \end{cases} \tag{2.15}$$

The constant implied by the O-notation in (2.11) *and* (2.14) *depends only on* b.

Remark. From (2.12), (2.13) it follows that

$$a(\mp b, 2, 0) = a(\mp b, 2, 1)$$

and we are faced with the problem of investigating the oscillatory properties of the difference

$$N(x, \mp b, 2, 1) - N(x, \mp b, 2, 0).$$

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

LEMMA 1. *Let us denote by* K *a normal extension of the field* Q *of rational numbers, by* n *and* Δ *the degree and the discriminant of* K*, respectively, and by* C_3 *and* C_4 *any positive constants.*

Write further

$$\Pi(x, K) = \sum_{N\mathfrak{p} \leqslant x} 1, \quad \mathfrak{p} - \textit{prime ideals}.$$

Then there exists a numerical constant C_2 *such that*

$$\Pi(x, K) = \operatorname{li} x + O\left(x\exp\left(-C_2\frac{\log^{1/2} x}{n^{1/2}}\right)\right) \tag{3.1}$$

provided

$$1 \leqslant |\Delta| \leqslant \log^{C_3} x, \quad 1 \leqslant n \leqslant C_4\frac{\log_2 x}{\log_3 x} \tag{3.2}$$

and the constant implied by the O-notation depends only on C_3 *and* C_4.

LEMMA 2. *Under the hypothesis that, for some special normal extensions* K *of the field* Q *of rational numbers, we have* $\zeta_K(s) \neq 0$ *for* $s > 1 - \dfrac{C_5}{\log(2|\Delta|)}$

(C_5 *— a numerical constant,* $C_5 > 0$) *where* Δ *denotes the discriminant of* K*, there exist numerical constants* C_6 *and* C_7 *such that*

$$\Pi(x, K) = \operatorname{li} x + O\left(x\exp\left(-C_6\omega(x, \Delta, n)\right)\right) \tag{3.3}$$

for

$$1 \leqslant |\Delta| \leqslant \exp\left(C_7\frac{\log x}{\log_2^2 x}\right), \quad x \geqslant e^e,$$

where

$$\omega(x, \Delta, n) = \frac{\log x}{\max(n^{1/2}\log^{1/2} x, \log|\Delta|)} \tag{3.4}$$

and the constant in the O-symbol is numerical.

The proofs of Lemmas 1 and 2 are postponed until the second paper of this series (see [9], Lemma A and B).

We mention only that the proofs follow the classical Landau pattern, taking into account, also the dependence on the parameters of the field.

It is remarkable that application of analogous lemmas, worked out for the much stronger Sokolovskiĭ zero-free domain for Dedekind Zeta-functions (see [8]) would only produce weaker error terms in Theorems 1–3 of the present paper. The difficulty lies in the fact that in Sokolovskiĭ zero-free domain, the dependence on n and Δ is not so simple as in the classical case (see [10]). Moreover the errors are influenced essentially by the hypothetical real zeros of Dedekind Zeta-functions (see (3.2)).

LEMMA 3. *Suppose* $l \geqslant 0$. *The condition* $p \in B(a, q, 0, l)$ *is equivalent to the solvability of the congruence* $v^{q^l} \equiv a \pmod p$ *with* $q^l \| p-1$.

LEMMA 4. *Suppose* $0 \leqslant k \leqslant l$, $q^l \| p-1$. *Then the solvability of the congruence* $v^{q^l} \equiv b^{q^k} \pmod p$ *is equivalent to the solvability of the congruence* $v^{q^{l-k}} \equiv b \pmod p$.

LEMMA 5. *Suppose* $s \geqslant 0$. *The congruence* $v^{q^s} \equiv b \pmod p$ *with* $q^s | p-1$ *has solutions if and only if this congruence has* q^s *different solutions.*

The proofs of Lemmas 3–5 are obvious and we omit them.

For any algebraic extension M of a field L, we denote the degree of M over L by $[M:L]$.

Put $u = 2^\tau$, $v = 2^{\tau'}$, $\tau' \geqslant \tau \geqslant 1$, where τ, τ' are natural numbers. Write further

$$G(u, v, b) = Q(\sqrt[u]{b}, \sqrt[v]{1}). \tag{3.5}$$

LEMMA 6. *If the integer* $b > 0$ *is not a square of an integer, then*

$$n(u, v, b) = [G(u, v, b):Q] = C(v, b)u\varphi(v), \tag{3.6}$$

where

$$C(v,b)=\begin{cases}\frac{1}{2} & \text{for } b=2b_1^2,\ v\geqslant 8\ (b_1 - \text{integer}\geqslant 1),\\ 1 & \text{otherwise.}\end{cases} \tag{3.7}$$

Proof. Write

$$L=L(u,v,b)=Q(\sqrt[u]{b})\cap Q(\sqrt[v]{1}).$$

If $L\neq Q$, then L is a normal extension of Q and the polynomial x^u-b splits into m conjugate irreducible polynomials over L and $m|u$.

Hence, denoting by r the degree of the conjugate polynomials, we have $u=rm$ and the constant terms of these polynomials are of the form $(\sqrt[u]{b})^r\varepsilon^j$, where ε is the uth primitive root of unity and j is a natural number.

Therefore $\sqrt[m]{b}\in Q(\sqrt[v]{1})$ and this is possible only if $m=2$ (see [3], Lemma 2). It follows that x^u-b factorizes into two polynomials over L and both are of degree $u/2$. Hence $[L:Q]=2$. Since $\sqrt{b}\in Q(\sqrt[v]{1})$ and $\sqrt{b}\in Q(\sqrt[u]{b})$, we have $\sqrt{b}\in L$ and $L=Q(\sqrt{b})$.

But $L=Q(\sqrt{b})$ if and only if $b=2b_1^2$, $v\geqslant 8$.

Indeed, if $L=Q(\sqrt{b})$ then $\sqrt{b}\in Q(\sqrt[v]{1})$, and therefore $b=2b_1^2$, $v\geqslant 8$ (see [3], Lemma 2). If $b=2b_1^2$, $v\geqslant 8$, then $\sqrt{2}\in Q(\sqrt[v]{1})$. Hence $Q(\sqrt{b})\cap Q(\sqrt[v]{1})\neq 0$ and further $Q(\sqrt[u]{b})\cap Q(\sqrt[v]{1})\neq Q$. Therefore $L=Q(\sqrt{b})$.

Finally we conclude that in the case of $b=2b_1^2$, $v\geqslant 8$, the fields $Q(\sqrt[u]{b})$, $Q(\sqrt[v]{1})$ are linearly disjoint over $Q(\sqrt{b})$ and in the remaining cases they are linearly disjoint over Q (see [3], Lemma 1).

In the first case

$$n(u,v,b)=\tfrac{1}{2}u\varphi(v) \quad \text{for} \quad b=2b_1^2,\ v\geqslant 8$$

and in the remaining cases

$$n(u,v,b)=u\varphi(v).$$

Corollary 3. *If an integer $b>0$ is not a square of an integer, then*

$$G(u,v,b)=G(u,2v,b)\Leftrightarrow b=2b_1^2,\quad v=2^{\tau}=4. \tag{3.8}$$

Corollary 4. *If $u=2$, $v\geqslant 8$, $b=2b_1^2$, then*

$$G(u,v,b)=Q(\sqrt[v]{1}).$$

Lemma 7. *Let q be an odd prime, τ, τ' natural numbers, $\tau'\geqslant\tau\geqslant 1$, $u=q^{\tau}$, $v=q^{\tau'}$ and $G(u,v,q,b)=Q(\sqrt[u]{b},\sqrt[v]{1})$.*

If an integer b is not the q-th power of an integer, then

$$n(u,v,q,b)=[G(u,v,q,b):Q]=u\varphi(v). \tag{3.9}$$

Proof. Write

$$L=L(u,v,q,b)=Q(\sqrt[u]{b})\cap Q(\sqrt[v]{1}).$$

If $L\neq Q$ then L is a normal extension of Q and the polynomial x^u-b splits into m conjugate irreducible polynomials over L, where $m|u$. Hence $\sqrt[m]{b}\in Q(\sqrt[v]{1})$ and $m=2$ (see [3], Lemma 2) and this contradicts the condition $m|u$. Finally $L=Q$ and the fields $Q(\sqrt[u]{b})$, $Q(\sqrt[v]{1})$ are linearly disjoint over Q. Hence (3.9) follows.

Let the condition that the prime p splits completely in the field G be indicated by $R(p,G)$.

Lemma 8. *If $a>0$, $a=b^{q^k}$, $0\leqslant k\leqslant l$, $l\geqslant 0$, then*

$$N(x,a,q,0,l)=M(x,q,l-k,l)-M(x,q,l-k,l+1), \tag{3.10}$$

where

$$M(x,q,l-k,\tau')=\sum_{\substack{p\leqslant x\\ R(p,G(q^{l-k},q^{\tau'},a,b))}} 1 \quad (\tau'=l \text{ or } l+1). \tag{3.11}$$

Proof. From Lemma 3 it immediately follows that

$$N(x,a,q,0,l)=\sum_{\substack{p\leqslant x,\ q^l\|p-1\\ \sqrt[q^l]{a}\equiv a(\mathrm{mod}\,p)}} 1.$$

Hence, owing to Lemma 4,

$$N(x,a,q,0,l)=\sum_{\substack{p\leqslant x,\ q^l\|p-1\\ \sqrt[q^{l-k}]{a}\equiv b(\mathrm{mod}\,p)}} 1=\sum_{\substack{p\leqslant x,\ q^{l}|p-1\\ \sqrt[q^{l-k}]{a}\equiv b(\mathrm{mod}\,p)}} 1-\sum_{\substack{p\leqslant x,\ q^{l+1}|p-1\\ \sqrt[q^{l-k}]{a}\equiv b(\mathrm{mod}\,p)}} 1. \tag{3.12}$$

From Lemma 5 it follows that for $\tau'=l$ or $\tau'=l+1$ the simultaneous conditions that $q^{\tau'}|p-1$ and that the congruence $\sqrt[q^{l-k}]{a}\equiv b\,(\mathrm{mod}\,p)$ is solvable are equivalent to the simultaneous conditions that $q^{\tau'}|p-1$ and that the congruence $\sqrt[q^{l-k}]{a}\equiv b\,(\mathrm{mod}\,p)$ has q^{l-k} different solutions.

Next these conditions are equivalent to the fact that p splits completely in the field $Q(\sqrt[v]{1})$ (see [6], th. 4.14, p. 167) and in the field $Q(\sqrt[u]{b})$ (see [6], th. 4.11, p. 163), where $u=q^{l-k}$, $v=q^{\tau'}$.

Therefore primes p satisfying the conditions that $p\leqslant x$, $q^{\tau'}|p-1$ and that the congruence $\sqrt[q^{l-k}]{a}\equiv b\,(\mathrm{mod}\,p)$ has q^{l-k} different solutions are the primes $p\leqslant x$ that split completely in the field $G(u,v,b)=Q(\sqrt[u]{b},\sqrt[v]{1})$. Hence owing to (3.12) Lemma 8 follows.

LEMMA 9. *Write*

$$\delta(x)=\begin{cases}0, & \text{for} \quad x\leqslant 0,\\ x, & \text{for} \quad x>0.\end{cases}$$

If $|a|=b^{2^k}$, *then for*

$$2^{l+1+\delta(l-k-r)}\leqslant\frac{\log_2 x}{\log_3 x}$$

we have the estimate

$$N(x,a,2,r,l)=a(a,l,r)\operatorname{li}x+O\left(x\exp\left(-C_8\left(\frac{\log x\log_3 x}{\log_2 x}\right)^{1/2}\right)\right), \tag{3.13}$$

where for $b=2b_1^2$

$$a(\mp b,l,0)=a(\mp b,l,1)=\begin{cases}\dfrac{1}{2^{2l}}, & l=1,\\ 0, & l=2,\\ \dfrac{1}{2^{2l-1}}, & l\geqslant 3,\end{cases}$$

$$a(b^{2^k},l,0)=a(-b^{2^k},l,1)=\begin{cases}\dfrac{1}{2^{2l}}, & 1\leqslant l\leqslant k,\\ 0, & l=k+1,\ k=1,\\ \dfrac{1}{2^{l}}, & l=k+1,\ k\geqslant 2,\\ \dfrac{1}{2^{2l-k-1}}, & l\geqslant k+2,\end{cases}$$

(3.14)

$$a(b^{2^k},l,1)=a(-b^{2^k},l,0)=\begin{cases}0, & 1\leqslant l\leqslant k,\\ \dfrac{1}{2^{2l-k-1}}, & l=k+1,\ k=1,\\ 0, & l=k+1,\ k\geqslant 2,\\ \dfrac{1}{2^{2l-k-1}}, & l\geqslant k+2,\end{cases}$$

$$a(b^{2^k},l,r)=a(-b^{2^k},l,r)=\begin{cases}0, & r\leqslant l\leqslant k+r-1,\ r\geqslant 2,\\ \dfrac{1}{2^{2l-k-r}}, & l=k+r=2,\ r\geqslant 2,\\ 0, & l=k+r>2,\ r\geqslant 2,\\ \dfrac{1}{2^{2l-k-r}}, & l\geqslant k+r+1,\ r\geqslant 2\end{cases}$$

and for $b\neq 2b_1^2$

$$a(b^{2^k},l,0)=a(-b^{2^k},l,1)=\begin{cases}\dfrac{1}{2^{l}}, & 1\leqslant l\leqslant k,\\ \dfrac{1}{2^{2l-k}}, & l\geqslant k+1,\end{cases}$$

$$a(b^{2^k},l,1)=a(-b^{2^k},l,0)=\begin{cases}0, & 1\leqslant l\leqslant k,\\ \dfrac{1}{2^{2l-k}}, & l\geqslant k+1,\end{cases} \tag{3.15}$$

$$a(b^{2^k},l,r)=a(-b^{2^k},l,r)=\begin{cases}0, & r\leqslant l\leqslant r+k-1,\ r\geqslant 2,\\ \dfrac{1}{2^{2l-k-r+1}}, & l\geqslant r+k,\ r\geqslant 2.\end{cases}$$

The constant implied by the O-notation depends only on b, and in the case $a(a,l,r)=0$ *this constant is equal to zero.*

Proof. It is easy to notice that

$$N(x,b^{2^k},2,r,l)=N(x,b^{2^k+r},2,0,l)-N(x,b^{2^k+r-1},2,0,l), \qquad 1\leqslant r\leqslant l,$$

$$\begin{aligned}&N(x,-b^{2^k},2,r,l)=N(x,b^{2^k},2,r,l), \quad 2\leqslant r\leqslant l,\\ &N(x,-b^{2^k},2,1,l)=N(x,b^{2^k},2,0,l),\\ &N(x,-b^{2^k},2,0,l)=N(x,b^{2^k},2,1,l).\end{aligned} \tag{3.16}$$

Therefore we have to investigate only the case $a>0$.

(a) Let $l\leqslant k$. Then the congruence $\nu^{2^l}\equiv b^{2^k}\pmod p$ is solvable for any p such that $2^l\| p-1$. Hence, owing to Lemma 3, we have

$$N(x,a,2,0,l)=\Pi(x,2^l,1)-\Pi(x,2^{l+1},1) \quad \text{for} \quad l\leqslant k. \tag{3.17}$$

(b) Let $l>k$, $l=2$, $b=2b_1^2$ $(k=0,1)$. Owing to Lemma 8, we get

$$N(x,a,2,0,l)=M(x,2,l-k,l)-M(x,2,l-k,l+1). \tag{3.18}$$

Since $b>0$ is not a square of an integer, it follows from (3.11), (3.19) and Corollary 3 that

$$N(x,a,2,0,l)=0 \quad \text{for} \quad k<l,\ l=2,\ b=2b_1^2\ (k=0,1). \tag{3.19}$$

(c) Consider the case $l=k+1$, $k\geqslant 2$, $b=2b_1^2$. From Corollary 4 (see [6], Lemma 4.14, p. 167) we have

$$M(x,2,l-k,\tau')=\sum_{\substack{p\leqslant x\\ R(p,Q(\sqrt{1}))=2^{\tau'}}}1=\sum_{\substack{p\leqslant x\\ 2^{\tau'}\| p-1}}1.$$

Hence, owing to (3.18),

$$N(x, a, 2, 0, l) = \Pi(x, 2^l, 1) - \Pi(x, 2^{l+1}, 1) \quad \text{for} \quad l = k+1, \quad k \geqslant 2, \ b = 2b_1^2. \tag{3.20}$$

(d) Consider the remaining cases. Since $G = G(2^{l-k}, 2^{\tau'}, b)$ is a normal extension of Q, we have

$$\Pi(x, G) = n(2^{l-k}, 2^{\tau'}, b) M(x, 2, l-k, \tau') + O\{n(2^{l-k}, 2^{\tau'}, b)\omega(b)\} + O\Big\{n(2^{l-k}, 2^{\tau'}, b) \sum_{p^2 \leqslant x} 1\Big\},$$

where $\omega(b) = \sum_{p|b} 1$.

Therefore

$$M(x, 2, l-k, \tau') = \frac{\Pi(x, G)}{n(2^{l-k}, 2^{\tau'}, b)} + O(\sqrt{x}), \tag{3.21}$$

where the constant in O depends only on b.

Denote by $\Delta = \Delta(G)$ the discriminant of the field $G(2^{l-k}, 2^{\tau'}, b)$. Then (see [6], Corollary 4, p. 262)

$$|\Delta| \leqslant (2b)^{2^{2l-k}(2l-k)}, \qquad n(2^{l-k}, 2^{\tau'}, b) \leqslant 2^{l-k} 2^{\tau'-1} \leqslant 2^{2l-k}. \tag{3.22}$$

Hence in this case, owing to Lemma 1, we have for $2^{2l-k} \leqslant 2\dfrac{\log_2 x}{\log_3 x}$ the estimate

$$\Pi(x, G) = \operatorname{li} x + O\left(x \exp\left(-C_9\left(\frac{\log x \log_3 x}{\log_2 x}\right)^{1/2}\right)\right) = \operatorname{li} x + O\{R(x)\}$$

and the constant in O depends only on b.

Further, owing to (3.21) and Lemma 8, we have

$$N(x, a, 2, 0, l) = \frac{1}{n(2^{l-k}, 2^l, b)} - \frac{1}{n(2^{l-k}, 2^{l+1}, b)} + O\{R(x)\}.$$

Owing to Lemma 6, we have

$$N(x, a, 2, 0, l) = \frac{1}{C(2^l, b) 2^{2l-k}} \operatorname{li} x + O\{R(x)\} \tag{3.23}$$

for $2^{2l-k} \leqslant 2\dfrac{\log_2 x}{\log_3 x}$.

Finally from (3.16), (3.6), (3.17), (1.19), (3.20) and (3.23) Lemma 9 follows.

LEMMA 10. *If* $|a| = b^{q^k}$ (q – *odd prime*), *then for*

$$q^{l+2+\delta(l-k-r)} \leqslant \frac{\log_2 x}{\log_3 x}$$

(*the function* $\delta(x)$ *is defined in Lemma* 9) *we have the estimate*

$$N(x, a, q, r, l) = a(a, q, r, l) \operatorname{li} x + O\left(x \exp\left(-C_{10}\left(\frac{\log x \log_3 x}{\log_2 x}\right)^{1/2}\right)\right), \tag{3.24}$$

where

$$a(a, q, 0, l) = \begin{cases} 1 - \dfrac{1}{q-1}, & l = 0, \\ \dfrac{1}{q^{l+\delta(l-k)}}, & l > 0, \end{cases} \tag{3.25}$$

$$a(a, q, r, l) = \begin{cases} 0, & 0 \leqslant l \leqslant k+r-1, \ r \geqslant 1, \\ \dfrac{1}{2^{2l-k-r+1}}(q-1), & l \geqslant k+r, \ r \geqslant 1. \end{cases}$$

The constant in O *depends only on* b *and in the case* $a(a, q, r, l) = 0$ *this constant is equal to zero.*

Proof. Note that for $q \neq 2$

$$N(x, b^{q^k}, q, r, l) = N(x, b^{q^{k+r}}, q, 0, l) - N(x, b^{q^{k+r-1}}, q, 0, l) \quad \text{for } 1 \leqslant r \leqslant l,$$
$$N(x, -b^{q^k}, q, r, l) = N(x, b^{q^k}, q, r, l) \quad \text{for} \quad 0 \leqslant r \leqslant l. \tag{3.26}$$

Hence we have to consider only the case $a > 0$. From Lemma 3 we get

$$N(x, a, q, 0, l) = \Pi(x, q^l, 1) - \Pi(x, q^{l+1}, 1) \quad \text{for} \quad 0 \leqslant l \leqslant k. \tag{3.27}$$

Let $l > k$. Since for the discriminant Δ and the degree n of the field $G(q^{l-k}, q^r, b)$ we have the inequalities

$$|\Delta| \leqslant (qb)^{q^{2l-k+1}(2l-k+1)}, \quad n < q^{2l-k+1}, \tag{3.28}$$

therefore, as in the proof of Lemma 9, we get, owing to Lemmas 6, 7, 8, the estimate

$$N(x, a, q, 0, l) = \frac{1}{q^{2l-k}} \operatorname{li} x + O\left(x \exp\left(-C_{10}\left(\frac{\log x \log_3 x}{\log_2 x}\right)^{1/2}\right)\right) \tag{3.29}$$

for

$$q^{2l-k+1} \leqslant \frac{\log_2 x}{\log_3 x}, \quad l > k.$$

From (3.26)–(3.29) Lemma 10 follows.

LEMMA 11. *If for the fields* $K_{l,\tau'} = Q(\sqrt[q^l]{|a_i|}, \sqrt[q^{\tau'}]{1})$, $\tau' = l$ *or* $\tau' = l+1$, $l = k+r, k+r+1, \ldots$ $\zeta_{K_{l,\tau'}}(s) \neq 0$ *for* $s > 1 - \dfrac{C_{11}}{\log(2|\Delta|)}$, *where* Δ *denotes the discriminant of the fields* $K_{l,\tau'}$ *and* C_{11} *is a positive numerical constant, then for*

$$q^{l+2+5(l-k-r)} \leqslant \frac{\log x}{\log_2^4 x} \tag{3.30}$$

we have the estimate

$$N(x, a, q, r, l) = a(a, q, r, l)\operatorname{li} x + O\left(x\exp\left(-C_{12}\log_2^2 x\right)\right), \tag{3.31}$$

where the constant implied by the O-notation depends only on b and the coefficients $a(a, q, r, l)$ *are defined by the formulae* (3.14), (3.15) *or* (3.25).

Proof. Put $q = 2$. It suffices to consider the case (d) from the proof of Lemma 9. From (3.21) and the estimates (3.22) and owing to Lemma 2 we get for

$$2^{2l-k} \leqslant \frac{\log x}{\log_2^4 x}$$

the estimate

$$M(x, 2, l-k, \tau') = \frac{\operatorname{li} x}{n(2^{l-k}, 2^{\tau'}, b)} + O\left(x\exp\left(-C_{13}\log_2^2 x\right)\right),$$

where the constant in O depends only on b. The further part of the proof is similar to the proof of Lemma 9.

For $q \geqslant 3$ the proof is similar.

4. Proofs of Theorems 1, 2 and 3. From the definition of $N(x, a, q, r)$ we have

$$N(x, a, q, r) = \sum_{l=r}^{\infty} N(x, a, q, r, l) = \sum_{q^r \leqslant q^l \leqslant x-1} N(x, a, q, r, l).$$

Choose

$$\xi = q^{(k+r-2)/2}\sqrt{\frac{\log_2 x}{\log_3 x}}$$

and write $N(x, a, q, r)$ in the form

$$N(x, a, q, r) = \sum_{q^r \leqslant q^l < \xi} N(x, a, q, r, l) + \sum_{\xi \leqslant q^l \leqslant x-1} N(x, a, q, r, l) = I_1 + I_2. \tag{4.1}$$

Since owing to (2.2) and (2.6) for l satisfying the inequality $q^r \leqslant q^l < \xi$ the conditions

$$q^{l+2+5(l-k-r)} \leqslant \frac{\log_2 x}{\log_3 x}, \quad q^{k+r} \leqslant \xi$$

are satisfied, therefore owing to Lemmas 9 and 10, we get

$$\begin{aligned} I_1 &= \sum_{q^r \leqslant q^l < \xi} a(a, q, r, l)\operatorname{li} x + O\left(x\exp\left(-C_{14}\frac{\log^{1/2} x}{\log_2^{1/2} x}\right)\right) \\ &= a(a, q, r)\operatorname{li} x + O\left(\frac{q^{k+r}}{\xi^2}\right) \\ &= a(a, q, r)\operatorname{li} x + O\left(\left(\frac{1}{q}\right)^{(k+r-2)/2}\sqrt{\frac{\log_3 x}{\log_2 x}}\,\frac{x}{\log x}\right). \end{aligned} \tag{4.2}$$

Next

$$\begin{aligned} I_2 &= \sum_{\xi \leqslant q^l \leqslant x-1} N(x, a, q, r, l) \leqslant \sum_{\xi \leqslant q^l \leqslant x-1} \left(\Pi(x, q^l, 1) - \Pi(x, q^{l+1}, 1)\right) \\ &= O\left(\frac{x}{\xi\log x}\right) = O\left(\left(\frac{1}{q}\right)^{(k+r-2)/2}\sqrt{\frac{\log_3 x}{\log_2 x}}\,\frac{x}{\log x}\right). \end{aligned} \tag{4.3}$$

From (4.1)–(4.3) Theorems 1 and 2 follow.

We prove Theorem 3 similarly by the use of Lemma 11, choosing

$$\xi = q^{(k+r-2)/2}\cdot\frac{\log^{1/2} x}{\log_2^2 x}.$$

References

[1] A. Aigner, *Bemerkung und Lösung zum Problem* 29, Elem. d. Math. 15 (1960), pp. 66–67.

[2] A. Brauer, *A note on a number-theoretical paper of Sierpiński*, Proc. Amer. Math. Soc. 11 (1960), pp. 406–409.

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

[4] H. Hasse, *Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl a ≠ 0 von gerader bzw. ungerader Ordnung* mod *p ist*, Math. Ann. 166 (1966), pp. 19–23.

[5] — *Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl a ≠ 0 von durch eine vorgegebene Primzahl l ≠ 2 teilbarer bzw. unteilbarer Ordnung* mod *p ist*, ibid. 162 (1965), pp. 74–76.

[6] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Polish Scientific Publishers, Warszawa 1974.

[7] W. Sierpiński, *Sur une décomposition des nombres premiers en deux classes*, Collect. Math. 10 (1958), pp. 81–83; — siehe auch Problem 29, Elem. d. Math. 14 (1959), p. 60.

[8] А. В. Соколовский, *Теорема о нулях дзета-функции Дедекинда и расстояние между „соседними" простыми идеалами*, Acta Arith. 23 (1968), pp. 321–334.

[9] K. Wiertelak, *On the density of some sets of primes, II*, ibid., this volume, pp. 197–210.

[10] K. M. Bartz, *On a theorem of A. V. Sokolovskiĭ*, ibid., this volume, pp. 113–126.

INSTITUTE OF MATHEMATICS OF THE ADAM MICKIEWICZ UNIVERSITY
Poznań

Received on 13. 2. 1976
and in revised form on 18. 6. 1976 (812)

ACTA ARITHMETICA
XXXIV (1978)

On the density of some sets of primes, II

by

K. Wiertelak (Poznań)

1. Denote by K an algebraic number field generated by an algebraic number ϑ. Denote further by n the degree of K and by Δ the discriminant of K.

The Dedekind zeta function $\zeta_K(s)$, $s = \sigma + it$ is defined for $\sigma > 1$ by the absolutely convergent series

$$\zeta_K(s) = \sum_{m=1}^{\infty} F(m) m^{-s},$$

where $F(m)$ denotes the number of ideals of the field K, having the norm equal to m.

The function $\zeta_K(s)$ can be continued over the whole complex plane as a regular function, except $s = 1$, where there is a simple pole.

In the region $\sigma > 1$ we have

$$-\frac{\zeta_K'}{\zeta_K}(s) = \sum_{m=1}^{\infty} G(m) m^{-s}, \tag{1.1}$$

where

$$G(m) = \sum_{(N\mathfrak{p})^l = m} \log N\mathfrak{p}$$

and series in (1.1) is absolutely convergent in this region (see [1], p. 89).

It was proved by E. Landau that $\zeta_K(s) \neq 0$ in the region

$$\sigma \geqslant 1 - \frac{1}{nC_1 \log t}, \quad t \geqslant C_2, \tag{1.2}$$

where C_1 is a positive numerical constant and the constant C_2 depends on the field K (see [1], p. 105). E. Landau did not express C_2 in terms of the degree n and the discriminant Δ of the field K. The purpose of this paper is to express C_2 of (1.2) in terms of the degree n and the discriminant Δ of the field K, to extend (1.2) to $-\infty < t < +\infty$ and also