

ON THE DENSITY OF SOME SETS OF PRIMES p , FOR WHICH

$n \mid \text{ord}_p a$

KAZIMIERZ WIERTEŁAK

Abstract: In the present paper we derive an asymptotic formula for prime numbers p for which n exactly divides the order $a \pmod{p}$.

Keywords: primitive root mod p , field of the type $Q(\sqrt[k]{a}, \sqrt[k]{1})$

1.

Let n, a denote natural numbers, $n > 1$, $a > 1$ and p a prime number not dividing a . The least positive γ such that $a^\gamma \equiv 1 \pmod{p}$ we denote by $\text{ord}_p a$.

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

In the present paper we derive an asymptotic formula for prime numbers p for which $n \parallel \text{ord}_p a$ ($n \parallel \text{ord}_p a$ means that for each $q^\alpha \parallel n$ there is $q^\alpha \parallel \text{ord}_p a$, where q is a prime).

2.

Let us write

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

where q_i are primes, and let

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

where q runs over different prime divisors of n . In the following we denote by q a prime number.

1991 Mathematics Subject Classification: Math. Subject Classification N 76

Acknowledgment. Partially supported by KBN Grant nr 2 P03A 024 17.

Let $t \geq 1$ be the largest natural number such that a is the t -th power in \mathbb{Z} . Denote further

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

We shall denote by b a positive integer satisfying the condition

$$a = b^H. \tag{2.4}$$

We introduce two parameters δ and s (see [3]) determined as follows

$$b = 2^\delta s v^2, \tag{2.5}$$

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 and m denote natural numbers.

Write further

$$\begin{aligned} N_1(x, m, c) &= \sum_{\substack{p \leq x, (p,c)=1 \\ (\text{ord}_p c, n)=1}} 1, & N(x, m, c) &= \sum_{\substack{p \leq x, (p,c)=1 \\ m | \text{ord}_p c}} 1, \\ N_2(x, m, c) &= \sum_{\substack{p \leq x, (p,c)=1 \\ n \parallel \text{ord}_p c}} 1, & \pi(x) &= \sum_{p \leq x} 1. \end{aligned}$$

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.

Theorem 1. *If*

$$x \geq \exp M, \quad \frac{\log x}{(\log \log x)^2} \geq c_1 k^2,$$

where c_1 is a sufficiently large numerical constant, then

$$\frac{1}{\pi(x)} N_1(x, n, a) = \alpha(k, \delta, s, H) + O\left(\frac{H r k^3}{\varphi(k) \log^{r-1} q_1} \cdot \frac{(\log \log x)^{r+3}}{\log^2 x}\right), \tag{2.6}$$

where

$$\alpha(k, \delta, s, H) = \beta(k, \delta, s, \gamma(2)) A(k, 2s, H) + A(k, 1, H). \tag{2.7}$$

$$A(k, l, H)$$

$$= \begin{cases} \mu(l) l / \varphi(l) \prod_{q|l} 1/q^{\gamma(q)} (q+1) \prod_{q|k/l} (1 - q^{1-\gamma(q)}) / (q^2 - 1) & \text{for } l \nmid k \\ 0 & \text{for } l \nmid k \end{cases} \tag{2.8}$$

and for an integer γ

$$\beta(k, \delta, s, \gamma) = \begin{cases} -\frac{1}{2} & \text{for } \delta = 0, s > 1, 2s \mid k, s \equiv 1 \pmod{4} \\ (2 - (4^\gamma, 4))/4 & \text{for } \delta = 0, s > 1, 2s \mid k, s \equiv 3 \pmod{4} \\ (2(4^\gamma, 4) - (4^\gamma, 16))/16 & \text{for } \delta = 1, s \geq 1, 2s \mid k \\ 0 & \text{otherwise} \end{cases} \tag{2.9}$$

The parameters $\gamma(q)$ are determined as in (2.3), the parameters δ and s as in (2.5).

For the proof see [3]. Let us observe that our formula (2.8) differs from the corresponding formula in [3] (cf. (3.3) there). The new expression gives of course the same value of $A(k, l, H)$, but in a more compact form.

Theorem 2. *If*

$$x \geq \exp M, \quad \frac{\log x}{(\log \log x)^2} \geq c_1 k^2,$$

then

$$\frac{1}{\pi(x)} N(x, n, a) = \frac{1 + \beta(k, \delta, s, \alpha(2) + \gamma(2) - 1)}{nH \prod_{q \mid k} (1 - 1/q^2)} + O\left(\frac{nHr2^r k^2 (\log \log x)^{r+3}}{\varphi(k) \log^{r-1} q_1 \log^2 x}\right). \tag{2.10}$$

where $\alpha(2)$ is determined by (2.1) and H as in (2.3).

Proof follows from Theorem 2 and Remark 2 of [3].

Theorem 3. *If*

$$x \geq \exp M, \quad \frac{\log x}{(\log \log x)^2} \geq c_1 k^2,$$

then

$$\frac{1}{\pi(x)} N_2(x, n, a) = \frac{1 + \beta'(k, \delta, s, \alpha(2) + \gamma(2))}{nH \prod_{q \mid k} (1 + 1/q)} + O\left(\frac{Hnr3^r k^3 (\log \log x)^{r+3}}{\varphi(k) \log^{r-1} q_1 \log^2 x}\right), \tag{2.11}$$

and for an integer γ

$$\beta'(k, \delta, s, \gamma) = \begin{cases} -1/2 & \text{for } \delta = 0, s > 1, 2s \mid k, s \equiv 1 \pmod{4}, \\ 1 & \text{for } \delta = 0, s > 1, 2s \mid k, s \equiv 3 \pmod{4}, \gamma = 1 \\ -1/2 & \text{for } \delta = 0, s > 1, 2s \mid k, s \equiv 3 \pmod{4}, \gamma \geq 2, \\ -1/8 & \text{for } \delta = 1, s \geq 1, 2s \mid k, \gamma = 1 \\ 1 & \text{for } \delta = 1, s \geq 1, 2s \mid k, \gamma = 2, \\ -1/2 & \text{for } \delta = 1, s \geq 1, 2s \mid k, \gamma \geq 3 \\ 0 & \text{otherwise.} \end{cases} \tag{2.12}$$

Proof. For an even k , we have

$$\begin{aligned} \frac{1}{\pi(x)}N_2(x, n, a) &= \frac{1}{\pi(x)} \sum_{d|k} \mu(d) \sum_{\substack{p \leq x \\ nd | \text{ord}_p a}} 1 = \frac{1}{\pi(x)} \sum_{d|k} \mu(d)N(x, nd, a) \\ &= \frac{1}{\pi(x)} \sum_{d|k/2} \mu(d)N(x, nd, a) + \frac{1}{\pi(x)} \sum_{2d|k} \mu(2d)N(x, 2dn, a). \end{aligned}$$

Hence, from the Theorem 2 we get

$$\begin{aligned} \frac{1}{\pi(x)}N_2(x, n, a) &= \sum_{d|\frac{k}{2}} \mu(d) \frac{1 + \beta(k, \delta, s, \alpha(2) + \gamma(2) - 1)}{ndH \prod_{q|k} (1 - 1/q^2)} \\ &\quad - \sum_{d|k/2} \mu(d) \frac{1 + \beta(k, \delta, s, \alpha(2) + \gamma(2))}{2dnH \prod_{q|k} (1 - 1/q^2)} + O\left(\frac{Hnr3^r k^3}{\varphi(k) \log^{r-1} q_1} \frac{(\log \log x)^{r+3}}{\log^2 x}\right) \\ &= \frac{1}{Hn \prod_{q|k} (1 + 1/q)} (1 + 2\beta(k, \delta, s, \alpha(2) + \gamma(2) - 1) \\ &\quad - \beta(k, \delta, s, \alpha(2) + \gamma(2)) + O\left(\frac{Hnr3^r k^3}{\varphi(k) \log^{r-1} q_1} \frac{(\log \log x)^{r+3}}{\log^2 x}\right)). \end{aligned} \tag{2.13}$$

Hence, from (2.9) we obtain

$$\begin{aligned} &2\beta(k, \delta, s, \alpha(2) + \gamma(2) - 1) - \beta(k, \delta, s, \alpha(2) + \gamma(2)) \\ &= \begin{cases} -1/2 & \text{for } \delta = 0, s > 1, 2s | k, s \equiv 1 \pmod{4} \\ 1 & \text{for } \delta = 0, s > 1, 2s | k, s \equiv 3 \pmod{4}, \alpha(2) + \gamma(2) = 1 \\ -1/2 & \text{for } \delta = 0, s > 1, 2s | k, s \equiv 3 \pmod{4}, \alpha(2) + \gamma(2) \geq 2 \\ -1/8 & \text{for } \delta = 1, s \geq 1, 2s | k, \alpha(2) + \gamma(2) = 1 \\ 1 & \text{for } \delta = 1, s \geq 1, 2s | k, \alpha(2) + \gamma(2) = 2 \\ -1/2 & \text{for } \delta = 1, s \geq 1, 2s | k, \alpha(2) + \gamma(2) \geq 3 \\ 0 & \text{otherwise.} \end{cases} \end{aligned} \tag{2.14}$$

Owing to (2.13) and (2.14) we get (2.11) for even k .

For an odd k , we have

$$\begin{aligned} \frac{1}{\pi(x)}N_2(x, n, a) &= \frac{1}{\pi(x)} \sum_{d|k} \mu(d)N(x, nd, a) \\ &= \sum_{d|k} \mu(d) \frac{1}{ndH \prod_{q|k} (1 - 1/q^2)} + O\left(\frac{Hnr3^r k^3}{\varphi(k) \log^{r-1} q_1} \frac{(\log \log x)^{r+3}}{\log^2 x}\right) \\ &= \frac{1}{Hn \prod_{q|k} (1 + \frac{1}{q})} + O\left(\frac{Hnr3^r k^3}{\varphi(k) \log^{r-1} q_1} \frac{(\log \log x)^{r+3}}{\log^2 x}\right). \end{aligned}$$

hence, it follows (2.11) for odd k . ■

References

- [1] J. Lagarias and A. Odlyzko, *Effective versions of the Chebotarev density theorem*, Algebraic number fields (ed. Frühlich), Academic Press, London-New York, 1977, pp. 409–464.
- [2] K. Wiertelak, *On the density of some sets of primes, I*, Acta Arith., **34** (1978), 183–196.
- [3] K. Wiertelak, *On the density of some sets of primes, IV*, Acta Arith., **43** (1984), 177–190.

Address: Faculty of Mathematics and Computer Science, Adam Mickiewicz University, Matejki 48/49, 60-769 Poznań, Poland.

Received: 20 May 2000