Functiones et Approximatio
XXXIII (2005), 121–127

ON THE DENSITY OF SOME SETS OF PRIMES, V

KAZIMIERZ WIERTELAK*

Abstract: In the present paper we derive an asymptotic formula for $\sum\limits_{p\leqslant x,\, r_k(p)=q_\tau} 1$, where k is a product of different odd primes, q_τ is the τ-th consecutive prime and $r_k(p)$ the least prime q such that $(\mathrm{ord}_p\, q, k) = 1$.
Keywords: primitive roots mod p, cyclotomic fields

1. Let k be a product of different odd primes. For a prime p, we denote by $r_k(p)$ the least prime q such that $(\mathrm{ord}_p\, q, k) = 1$.

In the following, the symbols $\mu(l)$, $\varphi(l)$, $\omega(l)$ and (α, β) denote as usual the Möbius function, the Euler function, the number of different prime divisors of l and the greatest common divisor of α, β respectively. By N and N_0 we denote positive integers whose all prime factors divide k; l denotes a generic divisor of k, p_0 is the least prime factor dividing k and $r = \omega(k)$, q_τ denotes the τ-th consecutive prime, p and q denote generic prime numbers.

We denote by c_i, $i = 1, 2, \ldots$ numerical constants and by $|A|$ the number of elements of a finite set A. If $p - 1 = Nt$, where $(t, k) = 1$, we write $N \parallel p - 1$.

Moreover, let

$$N(x, k, q_\tau) = \sum_{\substack{p\leqslant x\\ r_k(p)=q_\tau}} 1, \qquad \pi(x) = \sum_{p\leqslant x} 1.$$

2. The purpose of the present paper is to prove an asymptotic formula for $N(x, k, q_\tau)$.

Theorem. *If k is odd and $x \geqslant \exp\exp q_\tau$, $k^2 \leqslant \frac{\log x}{\log_2^3 x}$, then*

$$\frac{1}{\pi(x)} N(x, k, q_\tau) = \beta_\tau(k) + O\left(\frac{2^\tau r k^3}{\varphi(k)\, \log^{r-1} p_0} \cdot \frac{(\log_2 x)^{r+5}}{\log^2 x}\right), \tag{1}$$

2001 Mathematics Subject Classification: N 76

* Partially supported by KBN Grant nr 1P03A00826

where

$$\beta_\tau(k)=\sum_{s=0}^{\tau-1}(-1)^s\binom{\tau-1}{s}\prod_{q|k}\left(\frac{q-2}{q-1}+\frac{1}{q^{2+s}-1}\right) \tag{2}$$

and $\beta_\tau(k)>0$.

3. The proof of the Theorem will rest on the following lemmas.

Lemma 3.1. *If $p\nmid c$, then $(\operatorname{ord}_p c,k)=1$ if and only if c is an N-th power residue (mod p), where $N\parallel p-1$.*

The lemma follows from the definition of the power residue.

Lemma 3.2. *Suppose $\xi>1$. If $\mathcal{M}_r(\xi)$ denotes the set*

$$\mathcal{M}_r(\xi)=\{N_0:\xi<N_0\leqslant\xi q\ \text{ for each }\ q|N_0\}$$

then

$$|\mathcal{M}_r(\xi)|\leqslant r\left(\frac{\log\xi}{\log p_0}+1\right)^{r-1}. \tag{3}$$

If N is an arbitrary natural number whose all prime factors divide k and $N>\xi$ then there exist a number $N_0\in\mathcal{M}_r(\xi)$ and a positive integer number m such that $N=mN_0$.

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

Let $m,a_1,\ldots,a_{s+1}$ $(s=0,1,\ldots,\tau-1)$ denote arbitrary natural numbers. Moreover, let

$$\begin{aligned}B&=B(m,a_1,\ldots,a_{s+1})\\&=\{p:p\equiv1(\operatorname{mod}m),a_1,\ldots,a_{s+1}\text{: are: }m\text{-th power: residue: }(\operatorname{mod}p)\},\end{aligned}$$

$$M(x,m,a_1,\ldots,a_{s+1})=\sum_{\substack{p\leqslant x\\p\in B}}1.$$

Lemma 3.3. *With the notation of section 1, there exists a numerical constant c_1 such that for $\xi\geqslant k$ we have*

$$\begin{aligned}&\left|N(x,k,q_\tau)-\sum_{N\leqslant\xi}\sum_{l\leqslant\frac{x-1}{N}}\mu(l)\sum_{\{i_1,\ldots,i_s\}\subset\{1,2,\ldots,\tau-1\}}M(x,Nl,q_{i_1}^l,\ldots,q_{i_s}^l,q_r^l)\right|\\&\qquad\leqslant c_1 2^\tau r\left(\frac{\log\xi}{\log p_0}\right)^{r-1}\max_{N_0\in\mathcal{M}_r(\xi)}M(x,N_0,q_\tau),\end{aligned} \tag{4}$$

where $\mathcal{M}_r(\xi)$ has the same meaning as in Lemma 3.2.

Proof. Let

$$B_i=B_i(x)=\{p\leqslant x:(\operatorname{ord}_p q_i,k)=1\}$$

then

$$N(x,k,q_\tau)=\sum_{s=0}^{\tau-1}(-1)^s\sum_{\{i_1,\dots,i_s\}\subset\{1,2,\dots,\tau-1\}}|B_{i_1}\cap B_{i_2}\cap\ldots\cap B_{i_s}\cap B_\tau|. \tag{5}$$

For fixed N and $s\geqslant 0$ we write

$$\begin{aligned}A_N&=A_N(x,q_{i_1},\dots,q_{i_s},q_\tau)\\&=\{p\leqslant x: N\,\|\,p-1,\ q_{i_1},\dots,q_{i_s},q_\tau \text{ are: } N\text{-th power residue } (\operatorname{mod} p)\}.\end{aligned}$$

Since $A_N\cap A_{N'}=\emptyset$ for $N\neq N'$, we have using Lemma 3.1

$$\begin{aligned}|B_{i_1}\cap B_{i_2}\cap\ldots\cap B_{i_s}\cap B_\tau|&=\sum_{N\leqslant x-1}|A_N|\\&=\sum_{N\leqslant\xi}|A_N|+\sum_{\xi<N\leqslant x-1}|A_N| = S_1+S_2.\end{aligned} \tag{6}$$

From the second part of Lemma 3.2 we get

$$S_2\leqslant\sum_{N_0\in\mathcal{M}_r(\xi)}M(x,N_0,q_\tau).$$

Hence from the first part of Lemma 3.2 and owing to the inequality $k\leqslant\xi$ we have

$$S_2\leqslant c_1 r\left(\frac{\log\xi}{\log p_0}\right)^{r-1}\max_{N_0\in\mathcal{M}_r(\xi)}M(x,N_0,q_\tau). \tag{7}$$

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

$$S_1=\sum_{N\leqslant\xi}\sum_{l\leqslant\frac{x-1}{N}}\mu(l)\,M(x,Nl,q_{i_1}^l,\dots,q_{i_s}^l,q_\tau^l). \tag{8}$$

From (5) – (8) the result follows.

4. In the following we denote by $K=K_m$ the cyclotomic field generated by the m-th root of unity $\sqrt[m]{1}$, and by R_m its ring of integers.

For $\alpha\in R_m$ and a prime ideal $\mathfrak{p}$ of R_m, $\mathfrak{p}\nmid[m\alpha]$, we denote by $\left(\frac{\alpha}{\mathfrak{p}}\right)_m$ the m-th power residue symbol.

For an ideal $\mathfrak{a}$ of R_m, $(\mathfrak{a},[m\alpha])=1$ we put

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

Let $a_1, a_2, \ldots, a_{s+1}$ denote arbitrary natural integers and M the product of different prime divisors of the product $a_1 a_2 \cdot \ldots \cdot a_{s+1}$. For given integers $j_1, j_2, \ldots, j_{s+1}$, $1 \leqslant j_i \leqslant m$, $i = 1, \ldots, s+1$ we define

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

From Lemma 27 of [3] it follows that $\chi_{j_1,j_2,\ldots,j_{s+1}}$ is a character of the group of ideal classes mod $m^2 M$ of the ring R_m. If m is odd then $\chi_{j_1,j_2,\ldots,j_{s+1}}$ cannot be a real non-principal character (see [2] Lemma 6).

For a fixed $\beta \in R_m$ we put

$$\overline{N}(m, a_1, \ldots, a_{s+1}) = \sum_{\substack{j_1=1 \\ }}^{m} \cdots \sum_{\substack{j_{s+1}=1 \\ a_1^{j_1}\cdot\ldots\cdot a_{s+1}^{j_{s+1}} = \beta^m}}^{m} 1 \tag{9}$$

and

$$S(x, m, a_1, \ldots, a_{s+1}) = \sum_{\substack{N\mathfrak{p} \leqslant x \\ \mathfrak{p} \nmid [m a_1 \ldots a_{s+1}] \\ \left(\frac{a_j}{\mathfrak{p}}\right)_m = 1,\ j=1,\ldots,s+1}} 1 \tag{10}$$

where $\mathfrak{p}$ runs over the set of prime ideals of the ring R_m.

Lemma 4.1. *Suppose that* $t \geqslant 1$, $0 < \alpha \leqslant 1$, $M = q_1 \ldots q_r$, $c_2 \geqslant 0$ *is an arbitrary numerical constant and let* c_3 *is sufficiently small numerical constant.*

If

$$((Nl)^3 M)^{\varphi(Nl)} \leqslant \exp\left(\left(\frac{c_3}{c_2+1}\right)^2 \frac{\log^\alpha x}{\log_2^t x}\right), \tag{11}$$

then

$$\begin{aligned} &S(x, Nl, q_{i_1}^l, \ldots, q_{i_s}^l, q_r^l) \\ &= \frac{\pi(x)}{N^{s+1}} + O\left(x \exp\left(-(1{,}7c_2 + 1{,}2)\sqrt{\alpha} \log^{\frac{1-\alpha}{2}} x \, \log_2^{\frac{1+t}{2}} x\right)\right), \end{aligned} \tag{12}$$

where the constant in O *depends only on* c_2, c_3, α, t.

The proof of the lemma follows from Lemma 5.4 of [5]. It is enough to note that if k is odd, then $\overline{N}(Nl, q_{i_1}^l, \ldots, q_{i_s}^l, q_r^l) = l^{s+1}$ and $\chi_{j_1,\ldots,j_{s+1}}$ for $a_j = q_{i_j}$, $j = 1, \ldots, s$, $a_{s+1} = q_r^l$ cannot be a real non-principal character (cf. Lemma 5.6 of [5] and Lemma 4.6 of [6]).

Lemma 4.2. *If the conditions of Lemma 4.1 are satisfied, then there exists a numerical constant c_4 depending only on c_2, c_3, α, t such that*

$$\begin{aligned}&\left| M(x, Nl, q_{i_1}^l, \dots, q_{i_s}^l, q_\tau^l) - \frac{\pi(x)}{N^{s+1}\varphi(Nl)}\right| \\ &< c_4 x \exp\left(-(1,7c_2+1,2)\sqrt{\alpha}\log^{\frac{1-\alpha}{2}} x \log_2^{\frac{1+t}{4}} x\right). \end{aligned} \tag{13}$$

The Lemma follows from the formula

$$M(x, Nl, q_{i_1}^l, \dots, q_{i_s}^l, q_\tau^l) = \frac{1}{\varphi(Nl)} S(x, Nl, q_{i_1}^l, \dots, q_{i_s}^l, q_\tau^l) + O(\sqrt{x})$$

and Lemma 4.1 (cf. Lemma 4.7 of [6]).

5. Proof of Theorem. We use Lemma 3.3 with $\xi = \frac{\log x}{k \log_2^3 x}$.

If the conditions of the Theorem are fulfilled, for $N_0 \in \mathcal{M}_r(\xi)$ and sufficiently large x we have

$$\varphi(N_0)\log(N_0^3 q_\tau) \leqslant \xi k \log[(\xi k)^3 q_\tau] \leqslant \left(\frac{c_3}{c_2+1}\right)^2 \frac{\log x}{\log_2 x}.$$

Moreover

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

Hence owing to Lemma 4.2 for $t = 1$, $\alpha = 1$, $c_2 = 2$ we obtain

$$\begin{aligned}\max_{N_0 \in \mathcal{M}_r(\xi)} M(x, N_0, q_\tau) &\leqslant \frac{1}{\xi^2}\frac{k}{\varphi(k)}\pi(x) + c_4 \frac{x}{\log^4 x} \\ &\leqslant c_5 \frac{k^3}{\varphi(k)} \frac{x \log_2^6 x}{\log^3 x}. \end{aligned} \tag{14}$$

From this estimate and Lemma 3.3 we have

$$\begin{aligned}&N(x, k, q_\tau) \\ &= \sum_{N \leqslant \xi} \sum_{l \leqslant \frac{x-1}{N}} \mu(l) \sum_{s=0}^{\tau-1} (-1)^s \sum_{\{i_1,\dots,i_s\} \subset \{1,2,\dots,\tau-1\}} M(x, Nl, q_{i_1}^l, \dots, q_{i_s}^l, q_\tau^l) \\ &\quad + O(\pi(x) R(x, k, q_\tau)), \end{aligned} \tag{15}$$

where

$$R(x, k, q_\tau) = \frac{2^\tau r k^3}{\varphi(k) \log^{r-1} p_0} \frac{(\log_2 x)^{r+5}}{\log^2 x}.$$

If the conditions of the Theorem are fulfilled, for $N \leqslant \xi$ and sufficiently large x we obtain

$$\varphi(Nl)\log\left((Nl)^3 M\right) \leqslant \left(\frac{c_3}{3}\right)^2 \frac{\log x}{\log_2 x},$$

hence owing to Lemma 4.2 applied for $N \leqslant \xi$, $t = 1$, $\alpha = 1$, $c_2 = 2$ we have

$$M(x, Nl, q_{i_1}^l, \ldots, q_{i_s}^l, q_\tau^l) = \frac{\pi(x)}{N^{s+1}\varphi(Nl)} + O\left(\frac{x}{\log^4 x}\right).$$

Hence, using (15) we obtain

$$\begin{aligned} \frac{1}{\pi(x)} N(x, k, q_\tau) &= \sum_N \sum_{l|k} \frac{\mu(l)}{N\varphi(Nl)}\left(1 - \frac{1}{N}\right)^{\tau-1} \\ &\quad + \sum_{N>\xi} \sum_{l|k} \frac{\mu(l)}{N\varphi(Nl)}\left(1 - \frac{1}{N}\right)^{\tau-1} + O(R(x, k, q_\tau)) \qquad (16) \\ &= S_1 + S_2 + O(R(x, k, q_\tau)). \end{aligned}$$

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

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

Hence, for $\eta \geqslant 0$

$$\begin{aligned} &\sum_{N>\eta} \sum_{l|k} \frac{\mu(l)}{N\varphi(Nl)}\left(1 - \frac{1}{N}\right)^{\tau-1} \\ &= \sum_{d|k} \sum_{\substack{N>\eta \\ (N,k/d)=1 \\ d|N}} \frac{\left(1 - \frac{1}{N}\right)^{\tau-1}}{N} \prod_{l|k} \frac{\mu(l)}{\varphi(Nl)} \qquad (17) \\ &= \sum_{d|k} \sum_{\substack{N>\eta \\ (N,k/d)=1 \\ d|N}} \frac{\left(1 - \frac{1}{N}\right)^{\tau-1}}{N^2} \prod_{q|\frac{k}{d}} \frac{q-2}{q-1}. \end{aligned}$$

Therefore, for $\eta = \xi$ we have

$$S_2 \leqslant c_6 \xi^{-2} |\mathcal{M}_0(\xi)| = O(R(x, k, q_\tau)).$$

On the other hand, owing to (16) and (17) for $\eta = 0$, and owing to the last estimate, we obtain

$$\frac{1}{\pi(x)} N(x, k, q_\tau) = \beta_\tau(k) + O(R(x, k, q_\tau)).$$

Finaly, from (17) applied for $\eta = 0$ we conclude that $\beta_\tau(k) > 0$.

References

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

[2] P.D.T.A. Elliott, *The distribution of power residues and certain related results*, ibid. **17** (1970), 141–159.

[3] P.D.T.A. Elliott, *On the mean value of $f(p)$*, Proc. London Math. Soc. **21** (1970), 28–96.

[4] K. Wiertelak, *On the density of some sets of primes, III*, Studies in Pure Mathematics, To the Memory of Paul Turàn, 761–773.

[5] K. Wiertelak, *On the density of some sets of primes, IV*, Acta Arith. **43** (1984), 177–190.

[6] K. Wiertelak, *On the distribution of the smallest natural numbers having order modp not coprime with a given integer*, Acta Math. Hungar. **80(4)** (1998), 271–284.

Address: Adam Mickiewicz University, Faculty of Mathematics and Computer Science 61-614 Poznań, Poland

E-mail: wiertela@amu.edu.pl

Received: 15 March 2005