DE GRUYTER
OPEN

Ann. Univ. Paedagog. Crac. Stud. Math. 13 (2014), 7-14
DOI: 10.2478/aupcsm-2014-0001

FOLIA 149

Annales Universitatis Paedagogicae Cracoviensis
Studia Mathematica XIII (2014)

Jan Górowski, Adam Łomnicki

Simple proofs of some generalizations of the Wilson's theorem

Abstract. In this paper a remarkable simple proof of the Gauss's generalization of the Wilson's theorem is given. The proof is based on properties of a subgroup generated by element of order 2 of a finite abelian group. Some conditions equivalent to the cyclicity of $(\Phi(n), \cdot_n)$, where $n > 2$ is an integer are presented, in particular, a condition for the existence of the unique element of order 2 in such a group.

1. Introduction

The famous Wilson's theorem, giving the necessary condition for the primality, has many generalizations. One of them was proposed and proved by Gauss. However his proof was quite long and complicated. Short proof of the Gauss's result was given by G.A. Miller in [4]. Other generalizations of the Wilson's theorem may be found in [1] and [2].

The most far-reaching generalization of the Wilson's theorem is Theorem 2.4, cited in this paper. It can be proved using the notions of abelian groups. The known proofs (to authors) of Theorem 2.4 are based on the strong result from the group theory, which states that each finite abelian group is isomorphic to the product group $(\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \ldots \times \mathbb{Z}_{p_k^{\alpha_k}}, \otimes)$, where p_j for $j \in \{1, \ldots, k\}$ are prime numbers such that $p_j \neq p_l$ for $j, l \in \{1, \ldots, k\}$, $l \neq j$ and $\alpha_1, \ldots, \alpha_k$ are positive integers.

In this paper we give a simple proof of Theorem 2.4 which does not require the use of the mentioned theorem on the form of the finite abelian group. We also prove the Gauss's generalization of the Wilson's theorem. Finally, we present four conditions equivalent to the cyclicity of the group $(\Phi(n), \cdot_n)$, where

$$\Phi(n) = \{m \in \mathbb{Z} : \ 0 < m < n, \gcd(m, n) = 1\}.$$

AMS (2010) Subject Classification: 20K01, 11A07.

In the sequel $(G,\cdot)$ stands for a finite abelian group with 1 as the neutral element. By the order of G we understand the number of elements of G and we denote it by $\operatorname{ord} G$. In particular, $\operatorname{ord}\Phi(n) =: \varphi(n)$, $n \geq 2$. For any $g \in G$ we define $\operatorname{ord} g := \operatorname{ord}\langle g\rangle$, where $\langle g\rangle$ is the cyclic group generated by g. Of course, $\operatorname{ord} 1 = 1$. Moreover, let $G_{\operatorname{ord} 2} := \{g \in G :\ \operatorname{ord} g \leq 2\}$. Notice that $1 \in G_{\operatorname{ord} 2}$ and $G_{\operatorname{ord} 2}$ is a subgroup of $(G,\cdot)$.

By $2\mathbb{N}$ we denote the set of all positive even integers, $\mathbb{P}$ stands for the set of primes and the symbol $(a)_n$ will be used to denote the reminder of the division of integer a by integer $n \geq 2$. Finally, let $\mathbb{N}_k := \mathbb{N} \setminus \{0, 1, \ldots, k-1\}$, where $k \geq 1$ is an integer and let $[x]$ be the integer part of $x \in \mathbb{R}$.

2. Towards the Wilson's theorem

We start by proving the following results.

Lemma 2.1
If a finite abelian group $(G,\cdot)$ has an element of order 2, then $G_{\operatorname{ord} 2}$ is of even order.

Proof. Suppose that there is $a \in G$ such that $a \neq 1$, $a^2 = 1$. Then $\{1, a\}$ is a subgroup of $(G,\cdot)$ and in view of the Lagrange's theorem, 2 divides the order of $(G_{\operatorname{ord} 2},\cdot)$, so the assertion follows. Notice that $(G,\cdot)$ must be also of even order in this case.

Lemma 2.2
Let $(G,\cdot)$ be a finite abelian group such that $\operatorname{ord} G_{\operatorname{ord} 2} \geq 4$ and let $a \in G_{\operatorname{ord} 2} \setminus \{1\}$. Then for every $b \in G_{\operatorname{ord} 2} \setminus \{1, a\}$ there exists $\overline{b} \in G_{\operatorname{ord} 2} \setminus \{1, a, b\}$ such that $b \cdot \overline{b} = a$. Moreover, if $b, c \in G_{\operatorname{ord} 2} \setminus \{1, a\}$ are such that $b \neq c$ and $\overline{b}, \overline{c} \in G_{\operatorname{ord} 2} \setminus \{1, a, b, c\}$ satisfy $b \cdot \overline{b} = c \cdot \overline{c} = a$, then $\overline{b} \neq \overline{c}$.

Proof. Assume $b \in G_{\operatorname{ord} 2} \setminus \{1, a\}$. Since $G_{\operatorname{ord} 2} = \{b \cdot x :\ x \in G_{\operatorname{ord} 2}\}$ and $b \cdot 1 \neq a$, $b \cdot a \neq a$ and $b \cdot b \neq a$ we get that there is $\overline{b} \in G_{\operatorname{ord} 2} \setminus \{1, a, b\}$ such that $b \cdot \overline{b} = a$. Hence $\overline{b} = a \cdot b$.

The second assertion follows from the cancellation law in a group.

Now we consider the order of the subgroup $G_{\operatorname{ord} 2}$ of any finite and abelian group $(G,\cdot)$. Notice that if $G_{\operatorname{ord} 2} = \{1\}$, then the order of $G_{\operatorname{ord} 2}$ equals 2^0. Otherwise there is $m_1 \neq 1$ such that $m_1 \in G_{\operatorname{ord} 2}$. If $\{1, m_1\} =: G^1_{\operatorname{ord} 2} = G_{\operatorname{ord} 2}$, then $G_{\operatorname{ord} 2}$ is of order 2. If $G^1_{\operatorname{ord} 2} \neq G_{\operatorname{ord} 2}$, then there exists $m_2 \in G_{\operatorname{ord} 2} \setminus G^1_{\operatorname{ord} 2}$. Let $G^2_{\operatorname{ord} 2} := \{1, m_1, m_2, m_1 \cdot m_2\}$. If $G_{\operatorname{ord} 2} = G^2_{\operatorname{ord} 2}$ we get that the order of $G_{\operatorname{ord} 2}$ is equal to 4. If $G_{\operatorname{ord} 2} \neq G^2_{\operatorname{ord} 2}$ we obtain the existence of $m_3 \in G_{\operatorname{ord} 2} \setminus G^2_{\operatorname{ord} 2}$. Put $G^3_{\operatorname{ord} 2} := G^2_{\operatorname{ord} 2} \cup \{m_3, m_1 \cdot m_3, m_2 \cdot m_3, m_1 \cdot m_2 \cdot m_3\}$, then $G^3_{\operatorname{ord} 2}$ is a subgroup of $(G_{\operatorname{ord} 2},\cdot)$ of order 8. Continuing in this fashion we obtain the following result.

Lemma 2.3
If $(G,\cdot)$ is a and $G_{\operatorname{ord} 2}$ is an abelian subgroup of $(G,\cdot)$, then $\operatorname{ord} G_{\operatorname{ord} 2} = 2^n$ for some nonnegative integer n or $\operatorname{ord} G_{\operatorname{ord} 2} = \infty$.

Now we can prove

THEOREM 2.4
If a finite abelian group $(G,\cdot)$ has an element of order 2, then

(i) $\prod_{x\in G} x = a$ *if* $G_{\operatorname{ord} 2} = \{1,a\}$,

(ii) $\prod_{x\in G} x = 1$ *if* $\operatorname{ord} G_{\operatorname{ord} 2} > 2$.

Proof. To prove (i) suppose that $G_{\operatorname{ord} 2} = \{1,a\}$. If $G = G_{\operatorname{ord} 2}$ the assertion obviously follows, therefore assume that $G\setminus G_{\operatorname{ord} 2} \neq \emptyset$. It follows that the elements of $G \setminus G_{\operatorname{ord} 2}$ can be arranged in pairs (x,y) such that $x\cdot y = 1$ and $x \neq y$. This and the fact that

$$\prod_{x\in G} x = \prod_{x\in G\setminus\{1,a\}} x \cdot \prod_{x\in\{1,a\}} x$$

yield (i).

Now suppose that $\operatorname{ord} G_{\operatorname{ord} 2} > 2$. From Lemma 2.1 we infer that $\operatorname{ord} G_{\operatorname{ord} 2} \geq 4$. Fix $a \in G_{\operatorname{ord} 2} \setminus \{1\}$. By Lemma 2.2 the elements of $G_{\operatorname{ord} 2} \setminus \{1,a\}$ can be arranged in pairs (x,y) such that $x\cdot y = a$ and $x \neq y$. Moreover, similarly as in the proof of (i) we get

$$\prod_{x\in G\setminus G_{\operatorname{ord} 2}} x = 1.$$

Thus

$$\prod_{x\in G} x = \prod_{x\in G\setminus G_{\operatorname{ord} 2}} x \cdot \prod_{x\in G_{\operatorname{ord} 2}} x = \prod_{x\in G_{\operatorname{ord} 2}} x = a^{\frac{s+1}{2}},$$

where $s+1 = \operatorname{ord} G_{\operatorname{ord} 2}$. What is left is to show that $\frac{s+1}{2}$ is an even integer. Let $a,b \in G_{\operatorname{ord} 2} \setminus \{1\}$ be such that $a \neq b$, by Lemma 2.2 we obtain that $b\cdot \overline{b} = a$ for some $\overline{b} \in G_{\operatorname{ord} 2} \setminus \{1,a,b\}$. Furthermore, $\{1,a,b,\overline{b}\}$ is a subgroup of $(G_{\operatorname{ord} 2},\cdot)$. The Lagrange's theorem now implies that 4 divides the order of $(G_{\operatorname{ord} 2},\cdot)$, i.e. $s+1$, and this completes the proof. Let us notice that the divisibility by 4 follows also from Lemma 2.3.

From Theorem 2.4 we obtain the following results.

COROLLARY 2.5
If there are no elements of order 2 in a finite abelian group $(G,\cdot)$, then $\prod_{x\in G} x = 1$.

COROLLARY 2.6
If $(G,\cdot)$ is a finite abelian group with elements of order 2, then for every element $a \in G$ of order 2 we have

$$\prod_{x\in G} x = a^{\frac{s+1}{2}},$$

where $s+1 = \operatorname{ord} G_{\operatorname{ord} 2}$.

Now we turn to the group $(\Phi(n),\cdot_n)$, where $n \geq 2$ is a fixed integer. Corollary 2.6 yields

THEOREM 2.7
If $n \in \mathbb{N}_3$ *and* $s+1 = \operatorname{ord}\Phi(n)_{\operatorname{ord}2}$, *then*

$$\prod_{k\in\Phi(n)} k \equiv (-1)^{\frac{s+1}{2}} \bmod n.$$

Proof. Notice that since $n-1 \in \Phi(n)$ and $n-1 \in \Phi(n)_{\operatorname{ord}2}$ by Corollary 2.6 we have

$$\left(\prod_{k\in\Phi(n)} k\right)_n = \left((n-1)^{\frac{s+1}{2}}\right)_n = \left((-1)^{\frac{s+1}{2}}\right)_n.$$

Hence

$$\prod_{k\in\Phi(n)} k \equiv (-1)^{\frac{s+1}{2}} \bmod n.$$

Observe that Theorem 2.7 implies the famous Wilson's theorem.

THEOREM 2.8 (WILSON'S THEOREM)
If $p \in \mathbb{P}$, *then* $p|(p-1)!+1$.

Proof. For $p=2$ Theorem 2.8 holds true. Therefore assume $p \in \mathbb{P}\setminus\{2\}$. Then $\Phi(p) = \{1,2,\ldots,p-1\}$ and by Theorem 2.7 we get

$$(p-1)! \equiv (-1)^{\frac{s+1}{2}} \bmod p,$$

where $s+1 = \operatorname{ord}\Phi(p)_{\operatorname{ord}2}$. If $p>2$, then $p-1$ is the only element of order 2 in the group $(\Phi(p),\cdot_p)$. Indeed, if $k \in \Phi(p)$ such that $1<k<p-1$ were an element of order 2 we would have $k^2 \equiv 1 \bmod p$, thus $(k-1)(k+1) \equiv 0 \bmod p$ and in consequence $k-1 \equiv 0 \bmod p$ or $k+1 \equiv 0 \bmod p$. which is impossible as p is a prime.

Let us remark that our Theorem 2.7 improves the condition

$$\prod_{k\in\Phi(n)} k \equiv (-1)^{\varphi(n)+1} \bmod n, \qquad n \in \mathbb{N}_2$$

given in [3]. This condition does not hold as for $n=8$ we have $\Phi(8) = \{1,3,5,7\}$ but $1\cdot 3\cdot 5\cdot 7 \not\equiv (-1)^5 \bmod 8$.

3. Elements of order 2 in groups $\Phi(n)$

Recall that every $n \in \mathbb{N}_2$ can be represented as a product of prime powers, i.e.

$$n = \prod_{j=0}^{k} p_j^{\alpha_j}, \tag{1}$$

where $\alpha_j \in \mathbb{N}_1$ and $p_j \in \mathbb{P}$ for $j \in \{0,1,\ldots,k\}$ are such that $p_j \neq p_l$ for $j,l \in \{0,1,\ldots,k\}$, $j \neq l$. The form (1) will be called the *canonical representation* or the *standard form* of n.

THEOREM 3.1
If $n \in \mathbb{N}_3$, *then* $\operatorname{ord}\Phi(n)_{\operatorname{ord}2} = 2$ *if and only if* $n = 4$ *or* $n = p^\alpha$ *or* $n = 2p^\alpha$, *where* $p \in \mathbb{P} \setminus \{2\}$ *and* $\alpha \in \mathbb{N}_1$.

Proof. Observe that if $n = 4$, then $\operatorname{ord}\Phi(4)_{\operatorname{ord}2} = 2$. Let $n = p^\alpha$, where $p \in \mathbb{P} \setminus \{2\}$ and $\alpha \in \mathbb{N}_1$ and let $x \in \Phi(p^\alpha)_{\operatorname{ord}2}$. Then $x^2 \equiv 1 \bmod p^\alpha$ hence $(x-1)(x+1) \equiv 0 \bmod p^\alpha$ and hence

$$(x - 1 \equiv 0 \bmod p^\alpha \quad \text{and} \quad x + 1 \not\equiv 0 \bmod p^\alpha)$$

or

$$(x - 1 \not\equiv 0 \bmod p^\alpha \quad \text{and} \quad x + 1 \equiv 0 \bmod p^\alpha).$$

Indeed, if $x-1 \equiv 0 \bmod p^\alpha$ and $x+1 \equiv 0 \bmod p^\alpha$, then $(x+1)-(x-1) \equiv 0 \bmod p^\alpha$, which is impossible. As $0 \le x - 1 \le p^\alpha - 2$ we get $2 \le x + 1 \le p^\alpha$ and the only elements of $\{0, 1, \ldots, p^\alpha\}$ divisible by p^α are 0 and p^α we infer that $x = 1$ or $x = p^\alpha - 1$. Therefore, $\Phi(p^\alpha)_{\operatorname{ord}2} = \{1, p^\alpha - 1\}$. Similar arguments apply to the case $n = 2p^\alpha$.

Now we prove the reverse implication. To obtain a contradiction suppose that there is an $n \in \mathbb{N}_5$ such that for every $p \in \mathbb{P} \setminus \{2\}$ and $\alpha \in \mathbb{N}_1$ we have $n \ne p^\alpha$ and $n \ne 2p^\alpha$ and for which $\operatorname{ord}\Phi(n)_{\operatorname{ord}2} = 2$. Such n is of one of the following forms:

a) $n = 2^\alpha$, where $\alpha \ge 3$,

b) $n = \prod_{j=1}^k p_j^{\alpha_j}$, where $k > 1$ and $p_j \in \mathbb{P} \setminus \{2\}$, $\alpha_j \in \mathbb{N}_1$ for $j \in \{1, 2, \ldots, k\}$,

c) $n = 2^\alpha \prod_{j=1}^k p_j^{\alpha_j}$, where $k \ge 1$, $\alpha \ge 2$ and $p_j \in \mathbb{P} \setminus \{2\}$, $\alpha_j \in \mathbb{N}_1$ for $j \in \{1, 2, \ldots, k\}$,

d) $n = 2^\alpha \prod_{j=1}^k p_j^{\alpha_j}$, where $k \ge 2$, $\alpha \ge 1$ and $p_j \in \mathbb{P} \setminus \{2\}$, $\alpha_j \in \mathbb{N}_1$ for $j \in \{1, 2, \ldots, k\}$.

Notice that forms b), c) and d) are the canonical representations of n.

In the case a) we have $2^{\alpha-1}-1, 2^{\alpha-1}+1 \in \Phi(2^\alpha)_{\operatorname{ord}2}$, hence $\operatorname{ord}\Phi(2^\alpha)_{\operatorname{ord}2} > 2$, a contradiction.

In the case b) in the view of the Chinese Reminder Theorem (abbreviated here as CRT) the following system of congruences

$$\begin{cases} x \equiv 1 \bmod p_1^{\alpha_1}, \\ x \equiv -1 \bmod \prod_{j=2}^k p_j^{\alpha_j} \end{cases} \tag{2}$$

has a unique solution $\overline{x} \in \{0, 1, \ldots, n-1\}$. It is clear that $\overline{x} \notin \{0, 1, n-1\}$ thus $\overline{x} \in \{2, \ldots, n-2\}$. Moreover, we see that $\overline{x} \in \Phi(n)$ and $\overline{x}^2 \equiv 1 \bmod n$ as $\gcd(p_1^{\alpha_1}, \prod_{j=2}^k p_j^{\alpha_j}) = 1$. Thus $1, \overline{x}, n-1 \in \Phi(n)_{\operatorname{ord}2}$, which gives $\operatorname{ord}\Phi(n)_{\operatorname{ord}2} > 2$.

Now turn to the case c). By CRT there is a unique solution $\overline{x} \in \{0, 1, \ldots, n-1\}$ of the system

$$\begin{cases} x \equiv 1 \bmod 2^\alpha, \\ x \equiv -1 \bmod \prod_{j=1}^k p_j^{\alpha_j}. \end{cases}$$

It is easy to check that $\overline{x} \in \{2, \ldots, n-2\}$. Furthermore, we have $\overline{x} \in \Phi(n)$ and $\overline{x}^2 \equiv 1 \bmod n$ as $\gcd(2^\alpha, \prod_{j=1}^{k} p_j^{\alpha_j}) = 1$. Therefore $1, \overline{x}, n-1 \in \Phi(n)_{\operatorname{ord} 2}$ which contradicts the fact that $\operatorname{ord} \Phi(n)_{\operatorname{ord} 2} = 2$.

Finally, considering the system

$$\begin{cases} x \equiv 1 \bmod 2^\alpha p_1^{\alpha_1}, \\ x \equiv -1 \bmod \prod_{j=2}^{k} p_j^{\alpha_j}, \end{cases}$$

similarly as above we obtain $\operatorname{ord} \Phi(n)_{\operatorname{ord} 2} > 2$ in the case d). This is the last required contradiction and the proof is completed.

THEOREM 3.2
If $n \in \mathbb{N}_3$, then

$$\operatorname{ord} \Phi(n)_{\operatorname{ord} 2} \equiv 0 \bmod 4 \tag{3}$$

if and only if $n \neq 4$ and $n \neq p^\alpha$ and $n \neq 2p^\alpha$, where $p \in \mathbb{P} \setminus \{2\}$ and $\alpha \in \mathbb{N}_1$.

Proof. Fix $n \in \mathbb{N}_3$. In view of Theorem 3.1 and its proof it suffices to show that if n satisfies one of the conditions a), b), c) or d) (considered in the proof of Theorem 3.1), then (3) holds true.

Assuming a) to hold we obtain that $\{1, 2^{\alpha-1}-1, 2^{\alpha-1}+1, 2^\alpha-1\}$ is a subgroup of $(\Phi(n)_{\operatorname{ord} 2}, \cdot_n)$. Thus by the Lagrange's theorem we get (3).

Now let b) hold true, then $\{1, \overline{x}, n-\overline{x}, n-1\}$, where $\overline{x} \in \{2, 3, \ldots, n-2\}$ is a solution of (2), is a subgroup of $(\Phi(n)_{\operatorname{ord} 2}, \cdot_n)$ which in virtue of the Lagrange's theorem yields (3)

The same reasoning applies to the cases c) and d).

From Theorems 2.7, 3.1 and 3.2 we get the following generalization of the Wilson's theorem.

THEOREM 3.3 (GAUSS)
If $n \in \mathbb{N}_3$, then

$$\prod_{k \in \Phi(n)} k = \begin{cases} -1, & \text{if } n = 4 \text{ or } n = p^\alpha \text{ or } n = 2p^\alpha, \text{ where } p \in \mathbb{P} \setminus \{2\} \text{ and } \alpha \in \mathbb{N}_1, \\ 1, & \text{otherwise.} \end{cases}$$

Finally we prove

THEOREM 3.4
If $n \in \mathbb{N}_3$ and $s+1 = \operatorname{ord} \Phi(n)_{\operatorname{ord} 2}$, then

$$\prod_{\substack{k \in \Phi(n) \\ k \leq [\frac{n}{2}]}} k^2 \equiv (-1)^{\frac{s+1+\varphi(n)}{2}} \bmod n. \tag{4}$$

Proof. Since $k \in \Phi(n)$ if and only if $n - k \in \Phi(n)$ we have

$$\prod_{k\in\Phi(n)} k = \prod_{\substack{k\in\Phi(n)\\ k\le[\frac{n}{2}]}} k \cdot \prod_{\substack{k\in\Phi(n)\\ k>[\frac{n}{2}]}} k = \prod_{\substack{k\in\Phi(n)\\ k\le[\frac{n}{2}]}} k \cdot \prod_{\substack{k\in\Phi(n)\\ k\le[\frac{n}{2}]}} (n-k)$$
$$\equiv (-1)^{\frac{\varphi(n)}{2}} \prod_{\substack{k\in\Phi(n)\\ k\le[\frac{n}{2}]}} k^2 \bmod n,$$

which by Theorem 2.7 yields (4).

Notice that from Theorems 3.4 and 3.1 we immediately obtain the result from [2], namely

$$\prod_{\substack{k\in\Phi(n)\\ k\le\frac{n-1}{2}}} k^2 \equiv (-1)^{\frac{1}{2}\varphi(n)+\varepsilon} \bmod n, \qquad n \in \mathbb{N}_3 \setminus 2\mathbb{N},$$

where $\varepsilon = 1$ for $n = p^\alpha$, $p \in \mathbb{P} \setminus \{2\}$, $\alpha \in \mathbb{N}_1$ and $\varepsilon = 0$ otherwise.

By Theorems 3.1, 3.2 and 3.4 we have

THEOREM 3.5
If $n \in \mathbb{N}_3$, then

$$\prod_{\substack{k\in\Phi(n)\\ k\le[\frac{n}{2}]}} k^2 \equiv (-1)^{\frac{1}{2}\varphi(n)+1} \bmod n \iff n = 4 \text{ or } n = p^\alpha \text{ or } n = 2p^\alpha,$$
$$\prod_{\substack{k\in\Phi(n)\\ k\le[\frac{n}{2}]}} k^2 \equiv (-1)^{\frac{1}{2}\varphi(n)} \bmod n \iff n \neq 4 \text{ and } n \neq p^\alpha \text{ and } n \neq 2p^\alpha,$$

where $p \in \mathbb{P} \setminus \{2\}$ and $\alpha \in \mathbb{N}_1$.

We need the following known result.

THEOREM 3.6
The group $(\Phi(n), \cdot_n)$ is a cyclic group if and only if $n = 2$ or $n = 4$ or $n = p^k$ or $n = 2p^k$, where $p \in \mathbb{P} \setminus \{2\}$ and $k \in \mathbb{N}_1$.

From Theorems 3.1, 3.3, 3.5 and 3.6 we conclude finally.

THEOREM 3.7
For an $n \in \mathbb{N}_3$ the following condition are equivalent:

(A) *$n = 4$ or $n = p^\alpha$ or $n = 2p^\alpha$, where $p \in \mathbb{P} \setminus \{2\}$ and $\alpha \in \mathbb{N}_1$;*

(B) *$(\Phi(n), \cdot_n)$ is a cyclic group;*

(C) $\operatorname{ord} \Phi(n)_{\operatorname{ord} 2} = 2$;

(D) $\prod_{k\in\Phi(n)} k + 1 \equiv 0 \bmod n$;

(E) $\prod_{\substack{k\in\Phi(n)\\ k\le[\frac{n}{2}]}} k^2 + (-1)^{\frac{1}{2}\varphi(n)} \equiv 0 \bmod n$.

References

[1] Lin Cong, Zhipeng Li, *On Wilson's theorem and Polignac conjecture*, Math. Medley **32** (2005), 11–16. (arXiv:math/0408018v1). Cited on 7.

[2] J.B. Cosgrave, K. Dilcher, *Extensions of the Gauss-Wilson theorem*, Integers **8** (2008), A39, 15pp. Cited on 7 and 13.

[3] M. Hassani, M. Momeni-Pour, *Euler type generalization of Wilson's theorem*, arXiv:math/0605705v1 28 May, 2006. Cited on 10.

[4] G.A. Miller, *A new proof of the generalized Wilson's theorem*, Ann. of Math. (2) **4** (1903), 188–190. Cited on 7.

Institute of Mathematics
Pedagogical University
Podchorążych 2, PL-30-084 Kraków
Poland
E-mail: jangorowski@interia.pl,
alomnicki@poczta.fm

Received: January 13, 2014; final version: January 28, 2014;
available online: April 15, 2014.