FOLIA 141

Annales Universitatis Paedagogicae Cracoviensis

Studia ad Didacticam Mathematicae Pertinentia V (2013)

Jan Górowski, Adam Łomnicki

Around the Wilson's theorem*

Abstract. In this paper some known conditions and new congruences characterising prime numbers are given. Some of them are obtained by the generalised Wilson theorem given by Gauss. The elementary proof of this theorem is also presented.

Some considerations on the Wilson's theorem and, in particular, deep analysis of the numerous proofs of this theorem let us formulate a number of criteria for an integer to belong to $\mathbb{P}$ – the set of all primes.

The first result is based on the following theorem.

THEOREM 1 (LAGRANGE)
Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, *where* $a_k \in \mathbb{Z}$ *for* $k \in \{0, 1, \ldots, n\}$ *and* $a_n \neq 0$. *Let* $p \in \mathbb{P}$ *and* $p \nmid a_n$, *then* $p \mid f(x_j)$ *for at most* n *numbers* $x_1, x_2, \ldots, x_p$ *such that* $p \nmid (x_j - x_i)$ *for* $i, j \in \{1, 2, \ldots, n\}$, $j \neq i$.

Theorem 1 yields

REMARK 1
Let $p \in \mathbb{P}$ *and* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, *where* $a_k \in \mathbb{Z}$ *for* $k \in \{0, 1, \ldots, n\}$ *and* $a_n \neq 0$. *If there exist numbers* $x_1, x_2, \ldots, x_n, x_{n+1}$ *such that* $p \nmid (x_j - x_i)$ *for* $i, j \in \{1, 2, \ldots, n+1\}$, $j \neq i$ *and* $p \mid f(x_j)$ *for* $j \in \{1, 2, \ldots, n+1\}$, *then* $p \mid a_k$ *for* $k \in \{0, 1, \ldots, n\}$.

We now prove the following

THEOREM 2
If $p \in \mathbb{P}$, $x_1, x_2, \ldots, x_{p-1} \in \mathbb{Z}$, $p \nmid x_j$ *for* $j \in \{1, 2, \ldots, p-1\}$ *and* $p \nmid (x_j - x_i)$ *for* $i, j \in \{1, 2, \ldots, p-1\}$ *such that* $j \neq i$, *then*

$$p \mid \left(\prod_{j=1}^{p-1} x_j + (-1)^{p-1} \right).$$

*Wokół twierdzenia Wilsona

2010 Mathematics Subject Classification: Primary: 11A41, 11A07
Key words and phrases: prime number, Wilson's theorem, congruence

Proof. Set $f(x) = \prod_{j=1}^{p-1}(x-x_j) - x^{p-1}+1$ and notice that $f(x)$ is a polynomial of degree at most $p-2$. The definition of $f(x)$ and the Fermat's little theorem imply that $p \mid f(x_j)$ for $j \in \{1, 2, \ldots p-1\}$. Hence by Remark 1 the number p divides each coefficient of $f(x)$, in particular,

$$p \mid \left((-1)^{p-1} \prod_{j=1}^{p-1} x_j + 1 \right).$$

Let $[x]$ denote the integer part of $x \in \mathbb{R}$. Put $0!! = 1$, $1!! = 1$ and $n!! = (n-2)!!n$ for $n \in \mathbb{N}$, $n \geqslant 2$. From Theorem 2 we have

Remark 2
If $p \in \mathbb{P}$, then

a) $p \mid ((p-1)! + 1)$,
b) $p \mid ([\frac{p}{2}]!^2 + (-1)^{[\frac{p}{2}]})$,
c) $p \mid ((p-1)!!^2 + (-1)^{[\frac{p}{2}]})$,
d) $p \mid ((p-2)!!^2 + (-1)^{[\frac{p}{2}]})$.

Proof. Obviously for $p = 2$, conditions a), b), c), d) hold true. Suppose $p \geqslant 3$. Observe that to obtain a), b), c), d) it suffices to take for $x_1, x_2, x_3, \ldots, x_{p-1}$ in Theorem 2:

in case a): $1, 2, 3, \ldots, p-1$,
in case b): $-\frac{p-1}{2}, -\frac{p-3}{2}, \ldots, -1, 1, 2, \ldots, \frac{p-1}{2}$,
in case c): $-(p-1), -(p-3), \ldots, -2, 2, 4, \ldots, (p-1)$,
in case d): $-(p-2), -(p-4), \ldots, -1, 1, 3, 5, \ldots, p-2$.

Theorem 3
If k is an integer such that $k \geqslant 2$, then

a) $k \in \mathbb{P} \Leftrightarrow k \mid ((k-1)! + 1)$,
b) $k \in \mathbb{P} \Leftrightarrow k \mid ([\frac{k}{2}]!^2 + (-1)^{[\frac{k}{2}]})$,
c) $k \in \mathbb{P} \Leftrightarrow k \mid ((k-1)!!^2 + (-1)^{[\frac{k}{2}]})$,
d) $k \in \mathbb{P} \Leftrightarrow k \mid ((k-2)!!^2 + (-1)^{[\frac{k}{2}]})$.

Proof. Notice that in view of Remark 2 in each case we need to show that the implication "$\Leftarrow$" holds true.

To prove a) suppose that $k \mid ((k-1)! + 1)$ and $k \notin \mathbb{P}$. Hence $k = a \cdot b$, where $a = \min\{q : q \in \mathbb{P} \text{ and } q \mid k\}$. Thus $1 < a < \frac{k}{2}$, $a \mid (k-1)!$ and $a \mid ((k-1)! + 1)$. It follows that $a \mid 1$, a contradiction. Observe that condition a) is in fact the Wilson's theorem.

The proof of b) runs similarly.

To prove c) assume that $k \geqslant 3$, $k \notin 2\mathbb{N}$ and $k \mid ((k-1)!!^2 + (-1)^{[\frac{k}{2}]})$.
If $k \notin \mathbb{P}$, we would have $k = a \cdot b$, where $a = \min\{q : q \in \mathbb{P} \text{ and } q \mid k\}$ and $1 < a < \left[\frac{k}{2}\right]$.
Since $(k-1)!! = 2 \cdot 4 \cdot \ldots \cdot (k-1) = 2^{\frac{k-1}{2}}(\frac{k-1}{2})!$ we obtain $a \mid (\frac{k-1}{2})!$ and $a \mid ((k-1)!!^2 + (-1)^{[\frac{k}{2}]})$. Hence $a \mid (-1)^{[\frac{k}{2}]}$, a contradiction.

Suppose now that $k \in 2\mathbb{N}$, $k \geqslant 4$ and $k \mid ((k-1)!!^2 + (-1)^{[\frac{k}{2}]})$. Consider two following cases:

i) $k = 2^\beta$, where $\beta \geqslant 2$,

ii) $k = 2^\alpha \cdot t$, where $\alpha \geqslant 1$, $t \geqslant 3$ and $t \notin 2\mathbb{N}$.

If $k = 2^\beta$, where $\beta \geqslant 2$, then the fact that $k \mid ((k-1)!!^2 + (-1)^{[\frac{k}{2}]})$ implies $2^\beta \mid ((2^\beta - 1)!!^2 + 1)$. This is a contradiction as $4 \mid 2^\beta$ and $4 \nmid ((2^\beta - 1)!!^2 + 1)$. Therefore i) cannot occur.

Let $k = 2^\alpha \cdot t$, where $\alpha \geqslant 1$, $t \geqslant 3$ and $t \notin 2\mathbb{N}$. Then $t \mid (k-1)!!$, which yields $t \nmid ((k-1)!!^2 + (-1)^{[\frac{k}{2}]})$, a contradiction.

Finally, in order to prove d) suppose that $k > 2$. If $k \mid ((k-2)!!^2 + (-1)^{[\frac{k}{2}]})$, then k is an odd integer. If k were not a prime, we would have $k = a \cdot b$, where $a = \min\{q : q \in \mathbb{P} \text{ and } q \mid k\}$ and $1 < a < \left[\frac{k}{2}\right]$. Hence $a \mid (k-2)!!$ and $a \mid (k-2)!!^2 + (-1)^{[\frac{k}{2}]}$ and, in consequence, $a \mid (-1)^{[\frac{k}{2}]}$ which is impossible. This ends the proof of d) and the proof od the theorem.

A generalization of the Wilson's theorem is the following known result.

THEOREM 4
Let k, n be integer and such that $k \geqslant 2$, $0 \leqslant n \leqslant k-1$, then

$$k \in \mathbb{P} \Leftrightarrow k \mid (n!(k-1-n)! + (-1)^n).$$

In (Dence, Dence, 1995) as a corollary of Theorem 4 condition b) of our Theorem 3 was obtained.

Now we prove another characterisation of a prime number.

THEOREM 5
Let k, n be integer and such that $k \geqslant 2$, $0 \leqslant n \leqslant k-2$, then

$$k \in \mathbb{P} \Leftrightarrow k \mid (n!!^2(k-2-n)!!^2 + (-1)^{[\frac{k}{2}]}). \tag{1}$$

Proof. The proof is by induction on n. For $n = 0$ the assertion follows from condition d) of Theorem 3. For $n = 1$ we have $k \geqslant 3$ and by condition c) of Theorem 3 we obtain $k \in \mathbb{P} \Leftrightarrow k \mid ((k-1)!!^2 + (-1)^{[\frac{k}{2}]})$. As $k \mid ((k-1)!!^2 + (-1)^{[\frac{k}{2}]})$ is equivalent to each of the following

$$k \mid ((k-1)^2(k-3)!!^2 + (-1)^{[\frac{k}{2}]}),$$

$$k \mid ((k-3)!!^2 + (-1)^{[\frac{k}{2}]})$$

we get $k \in \mathbb{P} \setminus \{2\} \Leftrightarrow k \mid ((k-3)!!^2 + (-1)^{[\frac{k}{2}]})$. This proves (1) for $n = 1$.

Now fix $n \in 2\mathbb{N}$ such that $0 \leqslant n \leqslant k-5$, where $k \geqslant 5$ and suppose that (1) holds true. Condition $k \mid (n!!^2(k-2-n)!!^2 + (-1)^{[\frac{k}{2}]})$ is equivalent to

$$k \mid (n!!^2(k-2-n)^2(k-2-(n+2))!!^2 + (-1)^{[\frac{k}{2}]})$$

and

$$k \mid ((n+2)!!^2(k-2-(n+2))!!^2 + (-1)^{[\frac{k}{2}]}).$$

This gives (1) for $n \in 2\mathbb{N}$ and $n \leqslant k-2$.

Finally, assume (1) for arbitrary fixed $n \geqslant 1$ such that $n \notin 2\mathbb{N}$ and $n \leqslant k-3$. Then $k \mid (n!!^2(k-2-n)!!^2 + (-1)^{[\frac{k}{2}]})$ is equivalent to

$$k \mid (n!!^2(k-2-n)^2(k-2-(n+2))!!^2 + (-1)^{[\frac{k}{2}]})$$

and

$$k \mid ((n+2)!!^2(k-2-(n+2))!!^2 + (-1)^{[\frac{k}{2}]}).$$

This in view of the principle of induction finishes the proof.

THEOREM 6
If $k > 1$ is an odd integer, then

$$k \in \mathbb{P} \Leftrightarrow (k-2)!!^2 + (-4)^{\frac{k-1}{2}} \equiv 0 \bmod k.$$

Proof. If $k \in \mathbb{P}$ then from Fermat's little theorem and Theorem 3 we get

$$\begin{aligned}(k-2)!!^2 + (-4)^{\frac{k-1}{2}} &= ((k-2)!!^2 + (-1)^{\frac{k-1}{2}}) + (-1)^{\frac{k-1}{2}}(4^{\frac{k-1}{2}} - 1) \\ &= ((k-2)!!^2 + (-1)^{\frac{k-1}{2}}) + (-1)^{\frac{k-1}{2}}(2^{k-1} - 1) \equiv 0 \bmod k.\end{aligned}$$

To obtain a contradiction suppose that $(k-2)!!^2 + (-4)^{\frac{k-1}{2}} \equiv 0 \bmod k$ and $k \notin \mathbb{P}$. Then $k = a \cdot b$, where $a > 1$ and $b > 1$ and $a, b \notin 2\mathbb{N}$. Hence $a \mid (k-2)!!$ and in consequence $a \mid 4^{\frac{k-1}{2}}$, which is impossible.

A similar proof can be used to show the following result.

THEOREM 7
If $n > 1$ is an odd integer and $m > 1$ is an integer such that $\gcd(n, m) = 1$*, then*

$$n \in \mathbb{P} \setminus \{2\} \Leftrightarrow (n-2)!!^2 + (-m^2)^{\frac{n-1}{2}} \equiv 0 \bmod n.$$

THEOREM 8
If $p \in \mathbb{P} \setminus \{2\}$, then $(p-2)!! + (-1)^{\frac{p-1}{2}}(p-3)!! \equiv 0 \bmod p$.

Proof. By Theorems 3 and 4 we get

$$1 \equiv (p-2)! \bmod p,$$

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

Hence

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

$$(p-2)!!((p-2)!! + (-1)^{\frac{p-1}{2}}(p-3)!!) \equiv 0 \bmod p,$$

$$(p-2)!! + (-1)^{\frac{p-1}{2}}(p-3)!! \equiv 0 \bmod p.$$

This ends the proof.

Notice that the reverse to Theorem 8 is not true. Indeed, $7!! + (-1)^4 6!! \equiv 0 \bmod 9$.

Remark 3 (Leibniz theorem (Sierpiński, 1988, p. 214))
Let $n > 1$ be an integer. Then the following conditions are equivalent:

(i) *n is prime,*

(ii) $(n-2)! \equiv 1 \mod n$.

Now we recall the notion of the quadratic residue. Let $p \in \mathbb{P} \setminus \{2\}$ and $a \in \mathbb{Z}$ be such that $p \nmid a$, if there exists a $b \in \mathbb{Z}$ satisfying $a \equiv b^2 \bmod p$, then we call a the *quadratic residue modulo p.*

If $p \in \mathbb{P} \setminus \{2\}$ and $a \in \mathbb{Z}$ are such that $p \nmid a$ and $a \not\equiv b^2 \bmod p$ for each $b \in \mathbb{Z}$. Then we call a the *quadratic non-residue modulo p.*

For $a \in \mathbb{Z}$ and $p \in \mathbb{P} \setminus \{2\}$ the so-called Legendre symbol $\left(\frac{a}{p}\right)$ is defined as follows.

$$\left(\frac{a}{p}\right) := \begin{cases} 1, \text{ if } a \text{ is a quadratic residue modulo } p, \\ -1, \text{ if } a \text{ is a quadratic non-residue modulo } p, \\ 0, \text{ if } p \mid a. \end{cases}$$

Some standard properties of the Legendre symbol may be found in (Yan, 2006).

L. Euler proved the following result.

Theorem 9 (Ribenboim, p. 50)
If $a \in \mathbb{Z}, p \in \mathbb{P} \setminus \{2\}$, then $a^{\frac{p-1}{2}} - \left(\frac{a}{p}\right) \equiv 0 \bmod p$.

Theorems 3 and 9 imply

Theorem 10
If $p \in \mathbb{P} \setminus \{2\}$ and $a \in \mathbb{Z}$ are such that $p \nmid a$, then

(i) $(p-2)!!^2 + (-1)^{\frac{p-1}{2}}\left(\frac{a}{p}\right)a^{\frac{p-1}{2}} \equiv 0 \bmod p$,

(ii) $a^{\frac{p-1}{2}}(p-2)!!^2 + (-1)^{\frac{p-1}{2}}\left(\frac{a}{p}\right) \equiv 0 \bmod p$.

Proof. By Theorems 3 and 9 and by the properties of the congruence relation we get

$$(p-2)!!^2 + (-1)^{\frac{p-1}{2}} + (-1)^{\frac{p-1}{2}}\left(\frac{a}{p}\right)\left(a^{\frac{p-1}{2}} - \left(\frac{a}{p}\right)\right) \equiv 0 \bmod p.$$

This implies (i) as $\left(\frac{a}{p}\right) \cdot \left(\frac{a}{p}\right) = 1$.

Using again Theorems 3 and 9 we obtain

$$\left[a^{\frac{p-1}{2}}(p-2)!!^2 + (-1)^{\frac{p-1}{2}} a^{\frac{p-1}{2}}\right] - (-1)^{\frac{p-1}{2}}\left(a^{\frac{p-1}{2}} - \left(\frac{a}{p}\right)\right) \equiv 0 \bmod p,$$

which yields (ii).

Theorems 3 and 9 and a similar reasoning as in the proof of Theorem 10 may be used to prove the following result.

THEOREM 11
If $p \in \mathbb{P} \setminus \{2\}$ and $a \in \mathbb{Z}$ are such that $p \nmid a$, then

(i) $\left(\frac{p-2}{2}\right)!^2 + (-1)^{\frac{p-1}{2}}\left(\frac{a}{p}\right) a^{\frac{p-1}{2}} \equiv 0 \bmod p,$

(ii) $a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!^2 + (-1)^{\frac{p-1}{2}}\left(\frac{a}{p}\right) \equiv 0 \bmod p,$

(iii) $(p-1)!!^2 + (-1)^{\frac{p-1}{2}}\left(\frac{a}{p}\right) a^{\frac{p-1}{2}} \equiv 0 \bmod p,$

(iv) $a^{\frac{p-1}{2}}(p-1)!!^2 + (-1)^{\frac{p-1}{2}}\left(\frac{a}{p}\right) \equiv 0 \bmod p.$

To finish let us notice, that analogous conditions to (i) and (ii) of Theorem 10 and to conditions (i), (ii), (iii), (iv) of Theorem 11 can be obtained by Theorems 5 and 9.

Bibliography

Dence, J. B., Dence, T. P.: 1995, Anecessary and sufficient conditions for twin primes, *Missouri J. Math. Sci.* **7**(3), 129-131.

Ribenboim, P.: 1991, *The little book of big primes*, Springer Verlag, New York.

Sierpiński, W.: 1988, *Elementary theory of numbers.* second edition, North-Holland Publishing Co, Amsterdam.

Yan, S. Y.: 2006, *Number theory for computing*, Springer Verlag, Berlin.

Instytut Matematyki
Uniwersytet Pedagogiczny
ul. Podchorążych 2
PL-30-084 Kraków
e-mail alomnicki@poczta.fm
e-mail jangorowski@interia.pl