On the relationship between prime numbers and double factorials

Juan Moreno Borrallo

June 25, 2020

email: juan.morenoborrallo@gmail.com

Abstract

In this paper it is studied the relationship between prime numbers and double factorials, obtaining some new theorems regarding the characterization of prime numbers.

1 Introduction

One of the oldest and most famous theorems regarding the characterization of prime numbers is Wilson’s theorem, which states that a natural number $n > 1$ is a prime number if and only if the product of all the positive integers less than $n$ is one less than a multiple of $n$. That is, if we denote as $(n-1)!$ the mentioned product, and with $P$ the set of prime numbers, Wilson’s theorem states that

$$n \in P \Leftrightarrow (n-1)! \equiv -1 \pmod{n}$$

In this paper, we expose some interesting results regarding the relationship between prime numbers and double factorials, which leads to a better characterization of prime numbers $p \equiv 1 \pmod{4}$ and $p \equiv 3 \pmod{4}$.

2 Prime numbers and double factorials

Double factorial or semifactorial of a positive integer $n$ (denoted by $n!!$) is the product of all the integers up to $n$ that have the same parity (odd or even) as $n$; that is,

$$n!! = n(n-2)(n-4)\ldots$$

Once defined double factorials, we can expose the first theorem of this paper:
Theorem 1. Let it be $n = 4k + 3$ some positive integer; then, we can affirm that

$$n \in P, n \equiv 3 \pmod{4} \Rightarrow \begin{cases} (n-1)!! \equiv \pm1 \pmod{n} \\ and \\ (n-2)!! \equiv \pm1 \pmod{n} \end{cases}$$ (1)

Proof.

Let it be some odd positive integer $n = 2k + 1$.

For the sake of clarity, from now on we will establish the following change of variables:

- $a = (n-1)!!$
- $b = (n-2)!!$

To express that some positive integer $n$ divides some other positive integer $m$, we will use the notation $n \mid m$.

From the definitions of factorials and double factorials, it can be seen that

$$(n-1)! = ab$$

Therefore, from Wilson’s theorem we get that for every $n \in P$

$$n \mid ab + 1$$

Other hand, expanding $(n-1)!!$, and grouping under $P(n)$ all the terms divisible by $n$, we have that

$$(n-1)!! = (n-1)(n-3)(n-5)\ldots = P(n) + (-1)^\frac{n-1}{2}(n-2)!!$$

Therefore, for all odd positive integers it holds that

- $n \mid a - b$ for odd positive integers $n = 4k + 1$
- $n \mid a + b$ for odd positive integers $n = 4k + 3$

Other hand, by Wilson’s theorem, if $n \in P$, then $n \mid ab + 1$. Therefore, if $n \in P$ and $n \equiv 3 \pmod{4}$, we have that

$$n \mid ab - a - b + 1$$

$$n \mid ab + a + b + 1$$
As

\[ ab - a - b + 1 = (a - 1)(b - 1) \]

\[ ab + a + b + 1 = (a + 1)(b + 1) \]

We get that if \( n \in P \) and \( n = 4k + 3 \), then \( n \mid a - 1 \) or \( n \mid b - 1 \), and \( n \mid a + 1 \) or \( n \mid b + 1 \). In fact, as \( n \mid a + b \) if \( n \mid a - 1 \), then it follows that \( n \mid b + 1 \); and if \( n \mid b - 1 \), then it follows that \( n \mid a + 1 \).

The biconditionality derives from the fact that, if \( n \) is some odd composite number, then \((n - 1)!! \equiv (n - 2)!! \equiv 0 \pmod{n}\). A proof can be found in Aebi et al.[1].

It can be known if \( n \mid a - 1 \) or \( n \mid b - 1 \) based on the fact that if \( n \in P \) and \( n \equiv 3 \pmod{4} \), then \((p - 1)!! \equiv (-1)^v \pmod{p} \), where \( v \) denotes the number of nonquadratic residues \( j \) with \( 2 < j < \frac{p}{2} \), as showed in Aebi et al[2].

It follows from Theorem 1 that

\[(p - 2)!! \equiv (-1)^{v-1} \pmod{p} \quad \text{(2)}\]

Taking into account Theorem 1, we can derive the second theorem of this paper:

**Theorem 2.**

\[ n \in P, n \equiv 1 \pmod{4} \iff \begin{cases} (n - 1)!! \equiv k \pmod{n} & |k| > 1 \\ (n - 2)!! \equiv k \pmod{n} & |k| > 1 \end{cases} \quad \text{(3)} \]

**Proof.**

If \( n \in P \) and \( n \equiv 1 \pmod{4} \) we have that \( a \equiv -k \pmod{n} \), or which is the same, \( n \mid a + k \). As \( n \mid a - b \), we get that \( n \mid b + k \). Subsequently, if \( n \in P \) and \( n \equiv 1 \pmod{4} \),

\[(n - 1)!! \equiv (n - 2)!! \equiv -k \pmod{n} \quad \text{(4)}\]
Also, if \( n \in P \) and \( n \equiv 1 \pmod{4} \) we have by Wilson’s theorem that \( n \mid ab + 1 \), and thus we have that \( n \nmid a \); other hand, if \( n \) is some odd composite number, then, as already mentioned, \( a \equiv b \equiv 0 \pmod{n} \); subsequently, and taking into account Theorem 1, we guarantee the biconditionality of Theorem 2.

References
