

# An extension of Wilson's Theorem

Gennady Butov

January 23, 2025

## Abstract

The aim of this work is to optimize the existing formula based on Wilson's theorem to reduce the magnitude of the computation results.

## 1. Introductions

Wilson's theorem [1] states: if  $p$  is a prime number, then  $(p-1)! + 1$  is divisible by  $p$

$$(p-1)! \equiv -1 \pmod{p} \quad (1)$$

The function  $(p-1)!$  increases very rapidly and reaches huge values. Stirling's formula [2] clearly demonstrates the increase in  $(p-1)!$ :

$$(p-1)! \sim \sqrt{2 \cdot \pi \cdot (p-1)} \cdot \left(\frac{p-1}{e}\right)^{p-1}$$

There are many formulas and theorems derived from Wilson's theorem. Here is one of the formulas [3]:

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p} \quad (2)$$

The function  $\left(\left(\frac{p-1}{2}\right)!\right)^2$  also increases rapidly:

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \sim \left(\sqrt{2 \cdot \pi \cdot \left(\frac{p-1}{2}\right)} \cdot \left(\frac{p-1}{2 \cdot e}\right)^{\frac{p-1}{2}}\right)^2 = 2 \cdot \pi \cdot \left(\frac{p-1}{2}\right) \cdot \left(\frac{p-1}{2 \cdot e}\right)^{p-1}$$

When the values of  $p$  are large, the calculations become resource-intensive, so it is necessary to reduce the upper limit of the calculation results.

## 2. Main results

**Theorem.** *If  $p$  is a prime number, then the following formula will be true:*

$$\left((2 \cdot k - 1)!! \cdot \left(\left\lfloor \frac{p}{2} \right\rfloor - k\right)! \cdot \frac{1}{2^k}\right)^2 \equiv (-1)^{\left\lceil \frac{p}{2} \right\rceil} \pmod{p} \quad (3)$$

where  $\lfloor \cdot \rfloor$  is the rounding down operator,  $\lceil \cdot \rceil$  is the rounding up operator,  $k$  is a natural number.

*Proof.* Let's optimize formula (2).

$$\begin{aligned}
\left(\frac{p-1}{2}\right)! &= 1 \cdot 2 \cdot 3 \cdot \dots \cdot \left(\frac{p-1}{2} - 3\right) \cdot \left(\frac{p-1}{2} - 2\right) \cdot \left(\frac{p-1}{2} - 1\right) \cdot \left(\frac{p-1}{2} - 0\right) \\
\left(\frac{p-1}{2}\right)! &= 1 \cdot 2 \cdot 3 \cdot \dots \cdot \left(\frac{p+1}{2} - 4\right) \cdot \left(\frac{p+1}{2} - 3\right) \cdot \left(\frac{p+1}{2} - 2\right) \cdot \left(\frac{p+1}{2} - 1\right) \\
\left(\frac{p-1}{2}\right)! &= 1 \cdot 2 \cdot 3 \cdot \dots \cdot \left(\frac{p+1}{2} - k - 1\right) \cdot \left(\frac{p+1}{2} - k\right) \cdot \dots \cdot \left(\frac{p+1}{2} - 1\right) \\
\left(\frac{p-1}{2}\right)! &= 1 \cdot 2 \cdot 3 \cdot \dots \cdot \left(\frac{p-1}{2} - k\right) \cdot \left(\frac{p+1}{2} - k\right) \cdot \dots \cdot \left(\frac{p+1}{2} - 1\right) \\
\left(\frac{p-1}{2}\right)! &\stackrel{\text{mod } p}{\equiv} 1 \cdot 2 \cdot 3 \cdot \dots \cdot \left(\frac{p-1}{2} - k\right) \cdot \left(\frac{0+1}{2} - k\right) \cdot \dots \cdot \left(\frac{0+1}{2} - 1\right) \\
\left(\frac{p-1}{2}\right)! &\stackrel{\text{mod } p}{\equiv} 1 \cdot 2 \cdot 3 \cdot \dots \cdot \left(\frac{p-1}{2} - k\right) \cdot \left(\frac{1}{2} - k\right) \cdot \dots \cdot \left(\frac{1}{2} - 1\right) \\
\left(\frac{p-1}{2}\right)! &\stackrel{\text{mod } p}{\equiv} \left(\frac{p-1}{2} - k\right)! \cdot \left(\frac{1}{2} - k\right) \cdot \dots \cdot \left(\frac{1}{2} - 1\right) \\
\left(\frac{p-1}{2}\right)! &\stackrel{\text{mod } p}{\equiv} \left(\frac{p-1}{2} - k\right)! \cdot \left(\frac{1-2 \cdot k}{2}\right) \cdot \dots \cdot \left(\frac{1-2 \cdot 1}{2}\right) \\
\left(\frac{p-1}{2}\right)! &\stackrel{\text{mod } p}{\equiv} \left(\frac{p-1}{2} - k\right)! \cdot (1-2 \cdot k) \cdot \dots \cdot (1-2 \cdot 1) \cdot \frac{1}{2^k} \\
\left(\frac{p-1}{2}\right)! &\stackrel{\text{mod } p}{\equiv} \left(\frac{p-1}{2} - k\right)! \cdot (-1)^k \cdot 1 \cdot \dots \cdot (2 \cdot k - 1) \cdot \frac{1}{2^k} \\
\left(\frac{p-1}{2}\right)! &\stackrel{\text{mod } p}{\equiv} (-1)^k \cdot (2 \cdot k - 1)!! \cdot \left(\frac{p-1}{2} - k\right)! \cdot \frac{1}{2^k} \\
\left(\left(\frac{p-1}{2}\right)!\right)^2 &\stackrel{\text{mod } p}{\equiv} \left((2 \cdot k - 1)!! \cdot \left(\frac{p-1}{2} - k\right)! \cdot \frac{1}{2^k}\right)^2 \\
\left((2 \cdot k - 1)!! \cdot \left(\frac{p-1}{2} - k\right)! \cdot \frac{1}{2^k}\right)^2 &\equiv (-1)^{\frac{p+1}{2}} \pmod{p}
\end{aligned} \tag{4}$$

Let a prime number  $p$  be expressed in the following form:

$$p = 2 \cdot n + 1$$

where  $n$  is a natural number.

Then

$$\frac{p-1}{2} = \frac{2 \cdot n + 1 - 1}{2} = n \tag{5}$$

$$\left\lfloor \frac{p}{2} \right\rfloor = \left\lfloor \frac{2 \cdot n + 1}{2} \right\rfloor = \left\lfloor n + \frac{1}{2} \right\rfloor = n \tag{6}$$

It follows from equations (5) and (6):

$$\frac{p-1}{2} = \left\lfloor \frac{p}{2} \right\rfloor \quad (7)$$

$$\frac{p+1}{2} = \frac{2 \cdot n + 1 + 1}{2} = n + 1 \quad (8)$$

$$\left\lceil \frac{p}{2} \right\rceil = \left\lceil \frac{2 \cdot n + 1}{2} \right\rceil = \left\lceil n + \frac{1}{2} \right\rceil = n + 1 \quad (9)$$

It follows from equations (8) and (9):

$$\frac{p+1}{2} = \left\lceil \frac{p}{2} \right\rceil \quad (10)$$

By substituting (7) and (10) into equation (4), we obtain the previously mentioned formula (3):

$$\left( (2 \cdot k - 1)!! \cdot \left( \left\lfloor \frac{p}{2} \right\rfloor - k \right)! \cdot \frac{1}{2^k} \right)^2 \equiv (-1)^{\left\lceil \frac{p}{2} \right\rceil} \pmod{p}$$

Suitable values of  $k$  can be found from the following condition:

$$\left( \left\lfloor \frac{p}{2} \right\rfloor - k \right)! \equiv 0 \pmod{2^k}$$

Proposal.

Allowed values of  $k$  can be taken from the following ranges:

$k = 0$  for  $2 \leq p \leq 5$ ,

$0 \leq k \leq 1$  for  $7 \leq p \leq 11$ ,

for  $p \geq 13$ :

$$0 \leq k \leq \left\lfloor \frac{p-1}{4} \right\rfloor - \left\lfloor \ln \left\lfloor \frac{p-1}{4} \right\rfloor \right\rfloor$$

or, what is the same:

$$0 \leq k \leq \left\lfloor \frac{\left\lfloor \frac{p}{2} \right\rfloor}{2} \right\rfloor - \left\lfloor \ln \left\lfloor \frac{\left\lfloor \frac{p}{2} \right\rfloor}{2} \right\rfloor \right\rfloor$$

## References

- [1] Eric W. Weisstein. *CRC Concise Encyclopedia of Mathematics, Second Edition. Wilson's Theorem*, Chapman and Hall/CRC, pp. 3211, 2002.
- [2] Philippe Flajolet, Robert Sedgewick. *Analytic Combinatorics, 1st Edition. Stirling's formula*, Cambridge University Press, United Kingdom, Cambridge, pp. 37, 2009.
- [3] Leonard Eugene Dickson, *History of the Theory of Numbers, Volume I, Divisibility and Primality*, Chelsea Publishing Company, Publication No. 256, New York, pp. 275, 1952.
- [4] Eric W. Weisstein. *CRC Concise Encyclopedia of Mathematics, Second Edition. Double Factorial*, Chapman and Hall/CRC, pp. 823, 2002.