Wilson's theorem

From Wikipedia, the free encyclopedia

In number theory, **Wilson's theorem** states that a natural number $n > 1$ is a prime number if and only if

$$(n-1)! \equiv -1 \pmod{n}.$$

That is, it asserts that the factorial $(n-1)! = 1 \times 2 \times 3 \times \cdots \times (n-1)$ is one less than a multiple of n exactly when n is a prime number.

Contents

History

This theorem was stated by Ibn al-Haytham (c. 1000 AD),[1] and John Wilson.[2] Edward Waring announced the theorem in 1770, although neither he nor his student Wilson could prove it. Lagrange gave the first proof in 1771.[3] There is evidence that Leibniz was also aware of the result a century earlier, but he never published it.[4]

Example

The following table shows the values of n from 2 to 30, $(n-1)!$, and the remainder when $(n-1)!$ is divided by n. (In the notation of modular arithmetic, the remainder when m is divided by n is written $m \bmod n$.) The background color is blue for prime values of n, gold for composite values.

Table of remainder modulo *n*

n	$(n-1)!$ **(sequence A000142 in OEIS)**	$(n-1)! \bmod n$ **(sequence A061006 in OEIS)**
2	1	1
3	2	2
4	6	2
5	24	4
6	120	0
7	720	6
8	5040	0
9	40320	0
10	362880	0
11	3628800	10
12	39916800	0
13	479001600	12
14	6227020800	0
15	87178291200	0
16	1307674368000	0
17	20922789888000	16
18	355687428096000	0
19	6402373705728000	18
20	121645100408832000	0
21	2432902008176640000	0
22	51090942171709440000	0
23	1124000727777607680000	22
24	25852016738884976640000	0
25	620448401733239439360000	0
26	15511210043330985984000000	0
27	403291461126605635584000000	0
28	10888869450418352160768000000	0
29	304888344611713860501504000000	28
30	8841761993739701954543616000000	0

Proofs

Both of the proofs (for prime moduli)[5] below make use of the fact that the residue classes modulo a prime number are a field—see the article prime field for more details. Lagrange's theorem, which states that in any field a polynomial of degree n has at most n roots, is needed for both proofs.

Composite modulus

If n is composite it is divisible by some prime number q, where $2 \le q \le n-2$. If $(n-1)!$ were congruent to $-1 \pmod{n}$ then it would also be congruent to $-1 \pmod{q}$. But $(n-1)! \equiv 0 \pmod{q}$.

In fact, more is true. With the sole exception of 4, where $3! = 6 \equiv 2 \pmod 4$, if n is composite then $(n-1)!$ is congruent to $0 \pmod{n}$. The proof is divided into two cases: First, if n can be factored as the product of two unequal numbers, $n = ab$, where $2 \le a < b \le n-2$, then both a and b will appear in the product $1 \times 2 \times \ldots \times (n-1) = (n-1)!$ and $(n-1)!$ will be divisible by n. If n has no such factorization, then it must be the square of some prime q, $q > 2$. But then $2q < q^2 = n$, both q and $2q$ will be factors of $(n-1)!$, and again n divides $(n-1)!$.

Prime modulus

Elementary proof

The result is trivial when $p = 2$, so assume p is an odd prime, $p \ge 3$. Since the residue classes $\pmod p$ are a field, every non-zero a has a unique multiplicative inverse, a^{-1}. Lagrange's theorem implies that the only values of a for which $a \equiv a^{-1} \pmod p$ are $a \equiv \pm 1 \pmod p$ (because the congruence $a^2 \equiv 1$ can have at most two roots $\pmod p$). Therefore, with the exception of ± 1, the factors of $(p-1)!$ can be arranged in unequal pairs,[6] where the product of each pair is $\equiv 1 \pmod p$. This proves Wilson's theorem.

For example, if $p = 11$,

$$10! = [(1 \cdot 10)] \cdot [(2 \cdot 6)(3 \cdot 4)(5 \cdot 9)(7 \cdot 8)] \equiv [-1] \cdot [1 \cdot 1 \cdot 1 \cdot 1] \equiv -1 \pmod{11}.$$

Proof using Fermat's little theorem

Again, the result is trivial for $p = 2$, so suppose p is an odd prime, $p \ge 3$. Consider the polynomial

$$g(x) = (x-1)(x-2)\cdots(x-(p-1)).$$

g has degree $p-1$, leading term x^{p-1}, and constant term $(p-1)!$. Its $p-1$ roots are 1, 2, ..., $p-1$.

Now consider

$$h(x) = x^{p-1} - 1.$$

h also has degree $p-1$ and leading term x^{p-1}. Modulo p, Fermat's little theorem says it also has the same $p-1$ roots, 1, 2, ..., $p-1$.

Finally, consider

$$f(x) = g(x) - h(x).$$

f has degree at most $p-2$ (since the leading terms cancel), and modulo p also has the $p-1$ roots 1, 2, ..., $p-1$. But Lagrange's theorem says it cannot have more than $p-2$ roots. Therefore f must be identically zero $\pmod p$, so its constant term $(p-1)! + 1 \equiv 0 \pmod p$. This is Wilson's theorem.

Proof using the Sylow theorems

It is possible to deduce Wilson's theorem from a particular application of the Sylow theorems. Let *p* be a prime. It is immediate to deduce that the symmetric group S_p has exactly $(p-1)!$ elements of order *p*, namely the *p*-cycles C_p. On the other hand, each Sylow *p*-subgroup in S_p is a copy of C_p. Hence it follows that the number of Sylow *p*-subgroups is $n_p = (p-2)!$. The Sylow theorems imply

$$(p-2)! \equiv 1 \pmod{p}.$$

Multiplying both sides by (*p* - 1) gives

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

that is, the result.

Applications

Primality tests

In practice, Wilson's theorem is useless as a primality test because computing (*n* − 1)! modulo *n* for large *n* is computationally complex, and much faster primality tests are known (indeed, even trial division is considerably more efficient).

Quadratic residues

Using Wilson's Theorem, for any odd prime $p = 2m + 1$, we can rearrange the left hand side of

$$1 \cdot 2 \cdots (p-1) \equiv -1 \pmod{p}$$

to obtain the equality

$$1 \cdot (p-1) \cdot 2 \cdot (p-2) \cdots m \cdot (p-m) \equiv 1 \cdot (-1) \cdot 2 \cdot (-2) \cdots m \cdot (-m) \equiv -1 \pmod{p}.$$

This becomes

$$\prod_{j=1}^{m} j^2 \equiv (-1)^{m+1} \pmod{p}$$

or

$$(m!)^2 \equiv (-1)^{m+1} \pmod{p}.$$

We can use this fact to prove part of a famous result: for any prime *p* such that $p \equiv 1 \pmod 4$, the number (−1) is a square (quadratic residue) mod *p*. For suppose $p = 4k + 1$ for some integer *k*. Then we can take $m = 2k$ above, and we conclude that $(m!)^2$ is congruent to (−1).

Formulas for primes

Wilson's theorem has been used to construct formulas for primes, but they are too slow to have practical value.

p-adic gamma function

Wilson's theorem allows to define the p-adic gamma function.

Gauss's generalization

Gauss proved[7] that if $m > 2$

$$\prod_{\substack{k=1 \\ \gcd(k,m)=1}}^{m} k \equiv \begin{cases} -1 \pmod{m} & \text{if } m = 4,\ p^\alpha,\ 2p^\alpha \\ 1 \pmod{m} & \text{otherwise} \end{cases}$$

where p is an odd prime, and α is a positive integer. The values of m for which the product is -1 are precisely the ones where there is a primitive root modulo m.[8]

This further generalizes to the fact that in any finite abelian group, either the product of all elements is the identity, or there is precisely one element a of order 2 (but not both). In the latter case, the product of all elements equals a.

See also

- Primitive root modulo n
- Wilson prime
- Ibn al-Haitham
- Table of congruences

Notes

1. O'Connor, John J.; Robertson, Edmund F., "Abu Ali al-Hasan ibn al-Haytham", *MacTutor History of Mathematics archive*, University of St Andrews.
2. Edward Waring, *Mediationes Algebraicae* (Cambridge, England: 1770), page 218 (in Latin). In the third (1782) edition of Waring's *Mediationes Algebraicae*, Wilson's theorem appears as problem 5 on page 380 (http://books.google.co.uk/books?id=1MNbAAAAQAAJ&pg=PA380#v=onepage&f=false). On that page, Waring states: "Hanc maxime elegantem primorum numerorum proprietatem invenit vir clarissimus, rerumque mathematicarum peritissimus Joannes Wilson Armiger." (A man most illustrious and most skilled in mathematics, Squire John Wilson, found this most elegant property of prime numbers.)
3. Joseph Louis Lagrange, "Demonstration d'un théorème nouveau concernant les nombres premiers" (http://books.google.com/books?id=_-U_AAAAYAAJ&pg=PA125#v=onepage&q&f=false) (Proof of a new theorem concerning prime numbers), *Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres* (Berlin), vol. 2, pages 125–137 (1771).
4. Giovanni Vacca (1899) "Sui manoscritti inediti di Leibniz" (On unpublished manuscripts of Leibniz), *Bollettino di bibliografia e storia delle scienze matematiche* ... (Bulletin of the bibliography and history of mathematics), vol. 2, pages 113–116; see page 114 (http://books.google.com/books?id=vqwSAQAAMAAJ&pg=PA114#v=onepage&q&f=false) (in Italian). Vacca quotes from Leibniz's mathematical manuscripts kept at the Royal Public Library in Hanover (Germany), vol. 3 B, bundle 11, page 10:

> *Original* : Inoltre egli intravide anche il teorema di Wilson, come risulta dall'enunciato seguente:
>
> "Productus continuorum usque ad numerum qui antepraecedit datum divisus per datum relinquit 1 (vel complementum ad unum?) si datus sit primitivus. Si datus sit derivativus relinquet numerum qui cum dato habeat communem mensuram unitate majorem."
>
> Egli non giunse pero a dimostrarlo.

Translation : In addition, he [Leibniz] also glimpsed Wilson's theorem, as shown in the following statement:

"The product of all integers preceding the given integer, when divided by the given integer, leaves 1 (or the complement of 1?) if the given integer be prime. If the given integer be composite, it leaves a number which has a common factor with the given integer [which is] greater than one."

However, he didn't succeed in proving it.

See also: Giuseppe Peano, ed., *Formulaire de mathématiques*, vol. 2, no. 3, page 85 (http://books.google.com/books?id=bfDuAAAAMAAJ&pg=PA85#v=onepage&q&f=false) (1897).

5. Landau, two proofs of thm. 78
6. When $n = 3$, the only factors are ± 1
7. Gauss, DA, art. 78
8. $m = 1$ and 2 have to be excluded because $1 \equiv -1 \pmod{1 \text{ or } 2}$.

References

The *Disquisitiones Arithmeticae* has been translated from Gauss's Ciceronian Latin into English and German. The German edition includes all of his papers on number theory: all the proofs of quadratic reciprocity, the determination of the sign of the Gauss sum, the investigations into biquadratic reciprocity, and unpublished notes.

- Gauss, Carl Friedrich; Clarke, Arthur A. (translator into English) (1986), *Disquisitiones Arithemeticae (Second, corrected edition)*, New York: Springer, ISBN 0-387-96254-9
- Gauss, Carl Friedrich; Maser, H. (translator into German) (1965), *Untersuchungen über hohere Arithmetik (Disquisitiones Arithemeticae & other papers on number theory) (Second edition)*, New York: Chelsea, ISBN 0-8284-0191-8
- Landau, Edmund (1966), *Elementary Number Theory*, New York: Chelsea
- Ore, Oystein (1988). *Number Theory and its History*. Dover. pp. 259–271. ISBN 0-486-65620-9.

External links

- Hazewinkel, Michiel, ed. (2001), "Wilson theorem", *Encyclopedia of Mathematics*, Springer, ISBN 978-1-55608-010-4
- Weisstein, Eric W., "Wilson's Theorem" (http://mathworld.wolfram.com/WilsonsTheorem.html), *MathWorld*.
- Mizar system proof: http://mizar.org/version/current/html/nat_5.html#T22

Categories: Modular arithmetic | Factorial and binomial topics | Theorems about prime numbers

---