Wilson's theorem

In algebra and number theory, **Wilson's theorem** 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 (using the notations of modular arithmetic), the factorial $(n-1)! = 1 \times 2 \times 3 \times \cdots \times (n-1)$ satisfies

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

exactly when n is a prime number. In other words, any integer $n > 1$ is a prime number if, and only if, $(n-1)! + 1$ is divisible by n.[1]

History

The theorem was first stated by Ibn al-Haytham c. 1000 AD.[2] Edward Waring announced the theorem in 1770 without proving it, crediting his student John Wilson for the discovery.[3] Lagrange gave the first proof in 1771.[4] There is evidence that Leibniz was also aware of the result a century earlier, but never published it.[5]

Example

For each of the values of n from 2 to 30, the following table shows the number $(n-1)!$ 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 factorial and its remainder modulo *n*

n	$(n-1)!$ (sequence A000142 in the OEIS)	$(n-1)! \mod n$ (sequence A061006 in the 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

As a biconditional (if and only if) statement, the proof has two halves: to show that equality *does not* hold when n is composite, and to show that it *does* hold when n is prime.

Composite modulus

Suppose that n is composite. Therefore, it is divisible by some prime number q where $2 \leq q < n$. Because q divides n, there is an integer k such that $n = qk$. Suppose for the sake of contradiction that $(n-1)!$ were congruent to -1 modulo n. Then $(n-1)!$ would also be congruent to -1 modulo q: indeed, if $(n-1)! \equiv -1 \pmod{n}$ then $(n-1)! = nm - 1 = (qk)m - 1 = q(km) - 1$ for some integer m, and consequently $(n-1)!$ is one less than a multiple of q. On the other hand, since $2 \leq q \leq n-1$, one of the factors in the expanded product $(n-1)! = (n-1) \times (n-2) \times \cdots \times 2 \times 1$ is q. Therefore $(n-1)! \equiv 0 \pmod{q}$. This is a contradiction; therefore it is not possible that $(n-1)! \equiv -1 \pmod{n}$ when n is composite.

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

Prime modulus

The first two proofs below use the fact that the residue classes modulo a prime number are a finite field—see the article Prime field for more details.[6]

Elementary proof

The result is trivial when $p = 2$, so assume p is an odd prime, $p \geq 3$. Since the residue classes modulo p form a field, every non-zero residue a has a unique multiplicative inverse a^{-1}. Euclid's lemma implies[a] that the only values of a for which $a \equiv a^{-1} \pmod{p}$ are $a \equiv \pm 1 \pmod{p}$. Therefore, with the exception of ± 1, the factors in the expanded form of $(p-1)!$ can be arranged in disjoint pairs such that product of each pair is congruent to 1 modulo p. This proves Wilson's theorem.

For example, for $p = 11$, one has

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

Proof using Fermat's little theorem

Again, the result is trivial for $p = 2$, so suppose p is an odd prime, $p \geq 3$. 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 (mod p), so its constant term is $(p - 1)! + 1 \equiv 0 \pmod{p}$. 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 third Sylow theorem implies

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

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).

Used in the other direction, to determine the primality of the successors of large factorials, it is indeed a very fast and effective method. This is of limited utility, however.

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 this, 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) (mod p).

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 one to define the p-adic gamma function.

Gauss's generalization

Gauss proved[7] that

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

where p represents an odd prime and α a positive integer. That is, the product of the positive integers less than m and relatively prime to m is one less than a multiple of m when m is equal to 4, or a power of an odd prime, or twice a power of an odd prime; otherwise, the product is one more than a multiple of m. The values of m for which the product is −1 are precisely the ones where there is a primitive root modulo m.

See also

- Wilson prime

- Table of congruences
- Agoh–Giuga conjecture

Notes

a. Because if $a \equiv a^{-1} \pmod{p}$ then $a^2 - 1 \equiv 0 \pmod{p}$, and if the prime p divides $a^2 - 1 = (a-1)(a+1)$, then by Euclid's lemma it divides either $a - 1$ or $a + 1$.

1. *The Universal Book of Mathematics.* David Darling, p. 350.
2. O'Connor, John J.; Robertson, Edmund F., "Abu Ali al-Hasan ibn al-Haytham" (https://mathshistory.st-andrews.ac.uk/Biographies/Al-Haytham.html) , *MacTutor History of Mathematics Archive*, University of St Andrews
3. Edward Waring, *Meditationes Algebraicae* (Cambridge, England: 1770), page 218 (in Latin). In the third (1782) edition of Waring's *Meditationes Algebraicae*, Wilson's theorem appears as problem 5 on page 380 (https://books.google.com/books?id=1MNbAAAAQAAJ&pg=PA380) . 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.)
4. Joseph Louis Lagrange, "Demonstration d'un théorème nouveau concernant les nombres premiers" (https://books.google.com/books?id=_-U_AAAAYAAJ&pg=PA125) (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).
5. 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 (https://books.google.com/books?id=vqwSAQAAMAAJ&pg=PA114) (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 (https://archive.org/details/formulairedemat02peangoog/page/n231) (1897).

6. Landau, two proofs of thm. 78
7. Gauss, DA, art. 78

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. (1986), *Disquisitiones Arithemeticae* (2nd corrected ed.), New York: Springer, ISBN 0-387-96254-9(translated into English).
- Gauss, Carl Friedrich; Maser, H. (1965), *Untersuchungen über hohere Arithmetik (Disquisitiones Arithemeticae & other papers on number theory)* (2nd ed.), New York: Chelsea, ISBN 0-8284-0191-8(translated into German).
- Landau, Edmund (1966), *Elementary Number Theory*, New York: Chelsea.
- Ore, Øystein (1988). *Number Theory and its History* (https://archive.org/details/numbertheoryitsh0000orey/page/259) . Dover. pp. 259–271 (https://archive.org/details/numbertheoryitsh0000orey/page/259) . ISBN 0-486-65620-9.

External links

- "Wilson theorem" (https://www.encyclopediaofmath.org/index.php?title=Wilson_theorem) , *Encyclopedia of Mathematics*, EMS Press, 2001 [1994]
- Weisstein, Eric W. "Wilson's Theorem" (https://mathworld.wolfram.com/WilsonsTheorem.html) . *MathWorld*.
- Mizar system proof: http://mizar.org/version/current/html/nat_5.html#T22
- Ohana, Andrew. "A Generalization of Wilson's Theorem" (https://sites.math.washington.edu/~morrow/336_09/papers/Andrew.pdf) (PDF).