Wilson’s Theorem

APS - Presentation

USN: 01FE15BCS136
NAME: Prashant Kumar

Wilson's Theorem.

Let p be an integer greater than one. p is prime if and only if $(p-1)! = -1 \pmod{p}$

Proof

It is easy to check the result when p is 2 or 3, so let us assume $p > 3$. If p is composite, then its positive divisors are among the integers
$1, 2, 3, 4, \ldots, p-1$

and it is clear that $\gcd((p-1)!, p) > 1$, so we can not have $(p-1)! = -1 \pmod{p}$.
However if p is prime, then each of the above integers are relatively prime to p. So for each of these integers a there is another b such that $ab = 1 \pmod{p}$. It is important to note that this b is unique modulo p, and that since p is prime, $a = b$ if and only if a is 1 or p-1. Now if we omit 1 and p-1, then the others can be grouped into pairs whose product is one showing
$2 \cdot 3 \cdot 4 \cdot \ldots \cdot (p-2) = 1 \pmod{p}$

(or more simply $(p-2)! = 1 \pmod{p}$). Finally, multiply this equality by p-1 to complete the proof.

Examples

Table of 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

References

[1] https://en.wikipedia.org/wiki/Wilson%27s_theorem

[2] https://primes.utm.edu/notes/proofs/Wilsons.html