Wilson's Theorem

Wilson's theorem provides us a relation between (p - 1)! and its remainder modulo p for some prime p. It states that a number p is prime if and only if -

(p - 1) != -1 mod p

For example :-
i) Say p = 3
(p - 1)! = 2! = 2
2%3 = (3 - 1) mod 3

ii) Say p = 5
(p-1)! = 24
24 % 5 = 4

Formal Proof

1) We take the base case of p <= 3 and it can be solved manually.

2) Now we assume p > 3. If p is composite, then its positive divisors are among the integers 1, 2, 3, 4, ... , p-1 and it is clear that gcd((p-1)!, p) > 1, so we can not have (p-1)! = -1 (mod p) since remainder between 2 numbers is always a multiple of their gcd.

3) If p is a prime, then all numbers in [1, p-1] are relatively prime to p. And for every number x in range [2, p-2], there must exist exactly one other number y such that (x * y) % p = 1. So

[1 * 2 * 3 * ... (p-1)] % p
= [1 * 1 * 1 ... (p-1)] mod p.
= (p-1) mod p = -1 mod p

Applications

1. We can efficiently compute n! % p using this theorem. When n < p we can use the fact that
   n! % p = (p - 1)! % p * (p - 1)^(-1) * (p - 2)^-1 ... (n + 1)^(-1).
   So when n is close to p we can compute n! efficiently.

2. This can be used as a primality test for some number p. If (p-1)! mod p is equal to p - 1 then we can conclude that p is prime.
3. It is also used to derive a famous result that for any prime p of the form 4k + 1, (-1) is a square (quadratic residue) mod p.