5.5 Wilson's theorem

Example 118. What can you say about factors of $n!+1$? Is $n!+1$ composite infinitely often. Is it prime infinitely often?

Solution.

n	1	2	3	4	5	6	7	8	9	10	11	12
$n!+1$	2	3	7	5^2	11^2	$7\cdot 103$	71^2	$61\cdot 661$	$19\cdot 71\cdot 269$	$11\cdot 329,891$	$39,916,801$	$13^2\cdot 2,834,329$

- Every factor $m \geqslant 2$ of $n!+1$ has to be bigger than n. That's because, if $m \leqslant n$, then $n!+1 \equiv 1 \pmod{m}$.

  Comment. In other words, the number $n!+1$ has the property that all its prime factors are bigger than n. This observation provides us with another proof that there is infinitely many primes (see below).

- By Wilson's theorem (which we discuss below), if p is a prime, then p divides $(p-1)!+1$. Hence, $n!+1$ is composite whenever $n+1$ is prime (so that $n=p-1$ for some prime p).

- It is not known whether $n!+1$ is prime infinitely often. $n!+1$ is prime for $n=1,2,3,11,27,37,41,73,77,116,\ldots$. The largest such value known (proven in 2000) is $n=6380$.

  Comment. As of 2016, $6380!+1$ is the 515th largest known prime number (it has $712,355$ decimal digits). For comparison, the largest known prime is $2^{74207281}-1$ (a Mersenne prime). It has a bit over 22.3 million (decimal) digits.

Another proof of Euclid's theorem. In order to show that there are infinitely many primes, it is sufficient to observe that there doesn't exist a largest prime number. But, as noted above, the number $n!+1$ has the property that all its prime factors are bigger than n, so that arbitrarily large primes exist.

The data in the above table suggests the following:

If p is a prime, then p divides $(p-1)!+1$.

Apparently, this was guessed by John Wilson, a student of Waring who mentions this in his 1770 algebra book. Neither of these two could prove it at the time (and were pessimistic about it); Lagrange proved it in 1771.

The first few cases. As in the table above:

If $p=2$, then $(p-1)!+1=2$ is divisible by 2.

If $p=3$, then $(p-1)!+1=3$ is divisible by 3.

If $p=5$, then $(p-1)!+1=25$ is divisible by 5.

[If $p=6$, then $(p-1)!+1=121$ is not divisible by 6.]

If $p=7$, then $(p-1)!+1=721$ is divisible by 7.

Theorem 119. (Wilson) If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

Proof. We can check the case $p=2$ directly (as we did in the previous example).

Note that $(p-1)! = 1\cdot 2\cdot \ldots\cdot (p-1)$ modulo p is the product of all invertible values modulo p.

Each x among these, we can pair with its unique inverse x^{-1} modulo p. Unless, $x \equiv x^{-1} \pmod{p}$ or, equivalently, $x^2 \equiv 1 \pmod{p}$. In the last homework, you showed that, because p is a prime, this equation has only the solutions $x \equiv \pm 1 \pmod{p}$.

[Indeed: $x^2 \equiv 1 \pmod{p} \iff p|(x^2-1)=(x-1)(x+1) \iff p|(x-1)$ or $p|(x+1) \iff x \equiv \pm 1 \pmod{p}$]

Hence, $(p-1)! \equiv 1\cdot(-1) = -1 \pmod{p}$ because the contribution of any other value x is cancelled, modulo p, by its inverse x^{-1}. □

For instance. Go through the proof for $p=7$. In that case, $2^{-1} \equiv 4$, $3^{-1} \equiv 5$.

Armin Straub
straub@southalabama.edu

Corollary 120. n is a prime if and only if $(n-1)! \equiv -1 \pmod{n}$.

Proof. It only remains to show that, if n is not a prime, then $(n-1)! \not\equiv -1 \pmod{n}$.
But this is obvious, if we realize that -1 is invertible modulo n but $(n-1)!$ is not. (Why?!) □

Review. A residue a is invertible modulo n if and only if $\gcd(a, n) = 1$.

Comment. In fact, can you see why $(n-1)! \equiv 0 \pmod{n}$ if $n > 4$ is not a prime?

If we can write $n = ab$ where $a, b > 1$ and $a \neq b$, then $(n-1)! = \ldots \cdot a \cdot \ldots \cdot b \cdot \ldots \equiv 0 \pmod{n}$. This works (for instance, we can let a be the smallest divisor of n) unless $n = p^2$.

If $n = p^2$, then $(p^2-1)! = \ldots \cdot p \cdot \ldots \cdot (2p) \cdot \ldots \equiv 0 \pmod{p^2}$. Unless $2p > p^2 - 1$, which excludes $p = 2$ ($n = 4$).

Example 121. Show that, for a given odd prime p, half of the values $1, 2, \ldots, p-1$ are squares.

A residue which is a square modulo p is also called a **quadratic residue**.

Comment. As the only noninvertible residue, 0 plays a special role. It is always a square because $0^2 = 0$.

For instance. If $p = 7$, then 1, 2, 4 are squares modulo 7 but $3, 5, 6$ are not.

That's because $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$, $(\pm 3)^2 \equiv 2$. Hence, $1, 2, 4$ are the only quadratic residues modulo 7.

Solution. This is best seen if, instead of $1, 2, \ldots, p-1$, we look at the residues $\pm 1, \pm 2, \ldots, \pm (p-1)/2$. It is then clear that each residue a and its negative $-a$ square to the same result. Therefore, there are at most $(p-1)/2$ many different squares.

So far, we haven't used that p is a prime. This is important for the next step: namely, to show that there are exactly $(p-1)/2$ many squares. This requires us to show that each square a^2 only comes from the residues $\pm a$. In other words, we need to show that $x^2 \equiv a^2 \pmod{p}$ only has the solutions $x = a$ and $x = -a$.

Indeed, $x^2 \equiv a^2 \pmod{p} \iff p | (x^2 - a^2) = (x-a)(x+a) \iff p | (x-a)$ or $p | (x+a) \iff x \equiv \pm a \pmod{p}$.