

14

Wilson's Theorem

Wilson's Theorem is elegant. It is not very useful, but like a lot of other people, I like it. So that is why it is here. Consider an integer $n > 1$. If the integer $(n-1)! + 1$ is divided by any number from 2 to $n-1$, it yields a remainder of 1. Hence the smallest number (other than 1) that can divide it is n .¹ Wilson's theorem simplifies this situation remarkably. It says:

$$(n-1)! \equiv -1 \pmod{n} \text{ iff } n \text{ is prime}$$

Wilson's Theorem

Remember that *iff* stands for *if and only if*. Frequently in statements of Wilson's theorem only the *if* part is stated.

The Case n is a Composite

We are going to reach the proof of this theorem in stages. First, we will look at the situation where n is composite. Suppose $n=r \cdot s$ where $r \neq s$. Then $n \mid (n-1)!$ and thus $(n-1)! \equiv 0 \pmod{n}$. This leaves the case where $n = p^2$ where p is a prime. If n is greater than $2p$, then $p \cdot 2p \mid (n-1)!$ and hence once again $(n-1)! \equiv 0 \pmod{n}$. This leaves the case where $2p \geq n$. Hence, $2p \geq p^2$, and then $2 \geq p$. There is only one such case and that is $p=2$. We can see that $3! \equiv 2 \pmod{4}$. All together we have shown that $(n-1)! \not\equiv -1 \pmod{n}$, if n is not a prime. In fact, $(n-1)! \equiv 0 \pmod{n}$, if n is a composite other than 4. Actually we have shown more than we need to. To merely prove that if n is composite then $n \mid (n-1)! + 1$, we note that if n is composite that

¹This fact can be used to give a variation on Euclid's proof that there are an infinite number of primes. If on the contrary there are a finite number of primes then there must be a largest prime P . Then the number $P!+1$ can be divided only by numbers bigger than P . Furthermore if n divides $P!+1$, any prime factor of n must divide $P!+1$ and thus must be bigger than P . This is of course a contradiction, and therefore there must be an infinite number of primes.

it has a prime factor p that is smaller than n . Hence if $n|(n-1)! + 1$ then $p|(n-1)! + 1$. But this is impossible since $p|(n-1)!$.

A Different Problem

Let's consider a different problem altogether. Given some integer $n > 1$ denote the numbers from 1 to n that are relatively prime to n by a_1, a_2, \dots, a_k . What is the product of all of these numbers mod n ? It is tempting to think that the product must be one. Each of these numbers has a multiplicative inverse mod n (and these are the only integers in that range for which this is true) and the inverse is in this range. Hence each number cancels out its inverse and this gives us 1. However, some numbers may be their own inverses. 1 and $n-1$ are always their own inverses. Each of the numbers 1, 3, 5, 7 is its own inverse mod 8, so apparently there can be more than two numbers that are their own inverses. Suppose that h is its own inverse mod n . Then $(n-h)^2 \equiv n^2 - 2hn + h^2 \equiv 1 \pmod{n}$. We could prove using Bezout's Lemma that $n-h$ is relatively prime to n , but the fact that it has an inverse (mod n) proves the same thing. Note that $h \neq n-h$, otherwise $n = 2h$ and n and h are not relatively prime. We have also that $h(n-h) \equiv -1 \pmod{n}$. Hence when we multiply the self-inverse numbers (mod n) they pair up, and the product is 1 or -1 depending on how many pairs or self-inverse integers there are.

The Case n is Prime

We will show that if n is some prime p , that the only numbers between 1 and p that are self inverses are 1 and $n-1$. Their product (mod p) is -1. All of the other numbers between 1 and p are also relatively prime to p (since it is a prime) and under multiplication (mod p) cancel out their inverses giving 1. Putting this together we get $(p-1)! \equiv -1 \pmod{p}$, which is the half of Wilson's theorem there remained to be proven.

So our last problem is to consider the equation $x^2 \equiv 1 \pmod{p}$ and to prove that the only solutions are 1 and $p-1$. We have $x^2 - 1 \equiv 0 \pmod{p}$, or equivalently $p|(x-1)(x+1)$. Now if p does not divide $x-1$, then by Euclid's lemma it must divide $x+1$. If p divides a proper multiple of one or the other, we have x outside of our range from 1 to p . If $p = x-1$, then $x = 1 \pmod{p}$ and that

is one of our two known solutions. If $p = n+1$, then $n = p-1$ and that is the other, and we are done.

Example $10! \equiv -1 \pmod{11}$ since 11 is a prime.

Example $11! \equiv 0 \pmod{12}$ since 12 is a composite other than 4.

Example Consider $8! \pmod{11}$. Since 10 is its own inverse mod 11, and the inverse of 9 is 5, we have that $8! \equiv 10! \cdot 10 \cdot 5 \pmod{11}$. Hence $8! \equiv (-1)10 \cdot 5 \equiv 5 \pmod{11}$.