Sketch of Lecture 19 Tue, 11/6/2018

16 Wilson's theorem

Example 129. 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 $n=1,2,3,11,27,37,41,73,77,116,\ldots$. Only 21 such "factorial primes" are currently known, the largest being $n=150209$.

  https://en.wikipedia.org/wiki/Factorial_prime

  Comment. As of 11/2018, $150209!+1$ is the 924th largest known prime number (it has $712,355$ decimal digits). For comparison, the largest known prime is $2^{77,232,917}-1$ (a Mersenne prime; possibly the 50th). It has a bit over 23.2 million (decimal) digits.

  https://primes.utm.edu/largest.html

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 130. (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, $x^2\equiv 1 \pmod{p}$. 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, $2^{-1}\equiv 4$, $3^{-1}\equiv 5$.

Corollary 131. 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?!) □

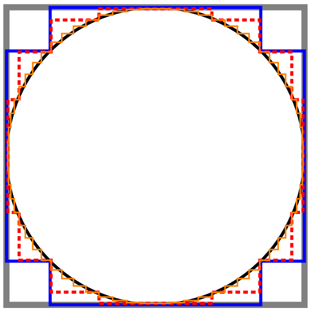
Review. A residue a is invertible modulo n if and only if $\gcd(a,n)=1$.

Comment. Unfortunately, this criterion is not a a good practical primality test. That's becaause computing the factorial is as much work as trial division by all numbers $2, \ldots, n-1$.

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 $p=2$ ($n=4$).



(Halloween scare: $\pi = 4$) π is the perimeter of a circle enclosed in a square with edge length 1. The perimeter of the square is 4, which approximates π. To get a better approximation, we "fold" the vertices of the square towards the circle (and get the blue polygon). This construction can be repeated for even better approximations and, in the limit, our shape will converge to the true circle. At each step, the perimeter is 4, so we conclude that $\pi = 4$, contrary to popular belief.

What is going wrong?

We are constructing curves c_n with the property that $c_n \to c$ where c is the circle. This convergence can be understood, for instance, in the sense $\|c_n - c\| \to 0$ where the norm measures the maximum distance between c_n and c.

Since $c_n \to c$ we then want to conclude that $\mathrm{perimeter}(c_n) \to \mathrm{perimeter}(c)$, leading to $4 \to \pi$.

However, in order to conclude from $x_n \to x$ that $f(x_n) \to f(x)$ we need that f is continuous (at x)!!

The "function" $\mathrm{perimeter}$, however, is not continuous. In words, this means that (as we see in this example) curves can be arbitrarily close, yet have very different arc length.

We can dig a little deeper: as you learned in Calculus II, the arc length of a function $y = f_n(x)$ for $x \in [a,b]$ is

$$\int_a^b \sqrt{(\mathrm{d}x)^2 + (\mathrm{d}y)^2} = \int_a^b \sqrt{1 + f_n'(x)^2}\,\mathrm{d}x.$$

Observe that this involves $f_n'(x)$. Try to see why the operator D that sends f to f' is not continuous. In words, two functions f and g can be arbitrarily close, yet have very different derivatives f' and g'.

That's a huge issue in **functional analysis**, which is the generalization of linear algebra to infinite dimensional spaces (like the space of all differentiable functions). The linear operators ("matrices") on these spaces frequently fail to be continuous.