ANOTHER PROOF OF WILSON'S THEOREM

DAVID LOWRY-DUDA

While teaching a largely student-discovery style elementary number theory course to high schoolers at the Summer@Brown program, we were looking for instructive but interesting problems to challenge our students. By we, I mean Alex Walker, my academic little brother, and me. After a bit of experimentation with generators and orders, we stumbled across a proof of Wilson's Theorem, different than the standard proof.

Wilson's theorem is a classic result of elementary number theory, and is used in some elementary texts to prove Fermat's Little Theorem, or to introduce primality testing algorithms that give no hint of the factorization.

Theorem 1 (Wilson's Theorem)**.** *For a prime number p, we have*

$$(p-1)! \equiv -1 \pmod{p}. \tag{1}$$

The theorem is clear for $p = 2$, so we only consider proofs for "odd primes p."

The standard proof of Wilson's Theorem included in almost every elementary number theory text starts with the factorial $(p-1)!$, the product of all the units mod p. Then as the only elements which are their own inverses are ± 1 (as $x^2 \equiv 1 \pmod{p} \iff p \mid (x^2-1) \iff p \mid x+1$ or $p \mid x-1$), every element in the factorial multiples with its inverse to give 1, except for -1. Thus $(p-1)! \equiv -1 \pmod{p}$. □

Now we present a different proof.

Take a primitive root g of the unit group $(\mathbb{Z}/p\mathbb{Z})^\times$, so that each number $1, \dots, p-1$ appears exactly once in $g, g^2, \dots, g^{p-1}$. Recalling that $1 + 2 + \dots + n = \frac{n(n+1)}{2}$ (a great example of classical pattern recognition in an elementary number theory class), we see that multiplying these together gives $(p-1)!$ on the one hand, and $g^{(p-1)p/2}$ on the other.

As $g^{(p-1)/2}$ is a solution to $x^2 \equiv 1 \pmod{p}$, and it is not 1 since g is a generator and thus has order $p-1$. So $g^{(p-1)/2} \equiv -1 \pmod{p}$, and raising -1 to an odd power yields -1, completing the proof. □

After posting this, we have since seen that this proof is suggested in a problem in Ireland and Rosen's extremely good number theory book. But it was pleasant to see it come up naturally, and it's nice to suggest to our students that you can stumble across proofs.

It may be interesting to question why $x^2 \equiv 1 \pmod{p} \iff x \equiv \pm 1 \pmod{p}$ appears in a fundamental way in both proofs.

This material is based upon work supported by the National Science Foundation Graduate Research Fellowship Program under Grant No. DGE 0228243.

This post appears on the author's personal website davidlowryduda.com and on the Math.Stackexchange Community Blog math.blogoverflow.com. It is also available in pdf note form. It was typeset in TEX, hosted on Wordpress sites, converted using the utility github.com/davidlowryduda/mse2wp, and displayed with MathJax.

Brown University
E-mail address: djlowry@math.brown.edu
URL: http://davidlowryduda.com