Wilson's Theorem

P. Reany

July 29, 2022

Wilson's Theorem is a result used in number theory. My approach to its proof will use group theory.[1] The statement of the theorem follows: Let p be an odd prime, then

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

where the congruence is of modulo arithmetic. Since we are going to use group theory to prove this theorem, we'd better introduce a suitable group to help us out.

Consider the group $G = (Z/p\backslash\{0\}, \odot) = (Z/p)^\times$, where Z/p is the set of integers modulo p. Thus G has $p-1$ elements in it. Also, the symbol $\odot$ means that the group operation is multiplication modulo p.

Definition: A unipotent element

A **unipotent element** of a group, ring, or algebra is a number u other than ± 1 that squares to unity. Or, in other words, a unipotent element is its own inverse, in which case

$$u^2 = 1\,. \tag{2}$$

Lemma: $(Z/p)^\times$ has no unipotent elements

A unipotent element must satisfy the quadratic equation

$$x^2 - 1 \equiv 0 \pmod{p}\,, \tag{3}$$

with the understanding that this equation admits at most two distinct solutions. So, let's try an arbitrary element $p - r$ in $(Z/p)^\times$ and solve for r:

$$(p-r)^2 - 1 \equiv 0 \pmod{p}\,, \tag{4}$$

or

$$r^2 \equiv 1 \pmod{p}\,, \tag{5}$$

which we already know has roots $r = 1$ and $r = -1$, which are not unipotent.[2]

[1] If the reader is not familiar with group theory, it can be look up on the Internet.

[2] The set of all square roots of unity consists of ± 1 and the unipotents. We might think of the unipotents as the nonstandard squareroots of unity.

Proof of Wilson's Theorem:

So, we want to show that something is true about $(p-1)!$ (mod p). But each factor of $(p-1)!$ is a distinct element of G and vise versa. Hence, $(p-1)!$ is the product of all the elements of G:

$$(p-1)! = \prod g_j = (p-1)\cdots(1)\,, \tag{6}$$

Taking this last equation modulo p, we get

$$(p-1)! \equiv (p-1)(p-2)\cdots(2)(1) \equiv (p-1)\cdot(1) \equiv -1 \pmod{p}\,, \tag{7}$$

where all the factors, other than 1 and -1, have cancelled in pairs. And this finishes the proof.