Three proofs of Wilson's theorem

Wilson's theorem states the following.

> Let p be a prime. Then
> $$(p-1)! \equiv -1 \pmod{p}.$$

This is obvious whenever $p = 2$. Hence I'll assume from now on that p is an odd prime.

First proof This is the one I gave in the lectures.

We use the fact that if a polynomial $f(X)$ has integer coefficients, degree d and there are more that d values of $a \in \{0, 1, 2, \ldots, p-1\}$ with $f(a) \equiv 0 \pmod{p}$ then all the coefficients of f are multiples of p. (It is essential that p be prime for this to hold!)

We apply this observation to the polynomial

$$f(X) = X^{p-1} - 1 - (X-1)(X-2)\cdots(X-(p-1)) = X^{p-1} - 1 - \prod_{k=1}^{p-1}(X-k).$$

If we substitute $X = a$ for $a \in \{1, 2, \ldots, p-1\}$ in the product above, one of the factors becomes zero and it vanishes. Hence for $a \in \{1, 2, \ldots, p-1\}$,

$$f(a) = a^{p-1} - 1 \equiv 1 - 1 = 0 \pmod{p}$$

by Fermat's little theorem. The degree of f is less than $p-1$ as the coefficient of X^{p-1} is $1 - 1 = 0$. As there are $p-1$ solutions of $f(a) \equiv 0 \pmod{p}$ in $\{1, 2, \ldots, p-1\}$, then all the coefficients of f are divisible by p. It follows that $f(0) \equiv 0 \pmod{p}$, that is

$$0 \equiv -1 - \prod_{k=1}^{p-1}(-k) = -1 - (-1)^{p-1}\prod_{k=1}^{p-1} k = -1 - (p-1)! \pmod{p}$$

(noting that as p is odd, $(-1)^p = 1$.) Rearranging gives

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

Second proof This is the most common textbook proof.

Each a in $\{1, 2, \ldots, p-1\}$ has an *inverse* $a^* \in \{1, 2, \ldots, p-1\}$ modulo p, that is $aa^* \equiv 1 \pmod{p}$. This inverse is unique and it follows that $(a^*)^* = a$. If $a = a^*$ then $1 \equiv aa^* = a^2 \pmod{p}$. We have seen that this necessitates $a \equiv \pm 1 \pmod p$ and so $a = 1$ or $a = p - 1$. In the product $(p-1)! = 1 \times 2 \times 3 \times \cdots \times (p-2) \times (p-1)$ we pair off each term, save for 1 and $p-1$ with its inverse modulo p. We thus get $(p-1)! \equiv 1 \times (p-1) \equiv -1 \pmod p$.

As an illustration, consider the case $p = 11$. Then

$$\begin{aligned} 10! &= 1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10 \\ &= 1 \times (2 \times 6) \times (3 \times 4) \times (5 \times 9) \times (7 \times 8) \times 10 \\ &\equiv 1 \times 1 \times 1 \times 1 \times 1 \times 10 = 10 \equiv -1 \pmod{11}. \end{aligned}$$

Third proof This requires the fact that each prime has a primitive root.

Let g be a primitive root modulo p. Then the numbers 1, g, $g^2, \ldots, g^{p-2}$ are congruent modulo p, in some order, to $1, 2, \ldots, p-1$. Hence

$$(p-1)! \equiv 1 g g^2 \cdots g^{p-2} = g^{1+2+\cdots+(p-2)} \pmod p.$$

The sum $1 + 2 + \cdots + (p-2)$ is the sum of an arithmetic progression with $p-2$ terms, and so equals

$$(p-2)\frac{(p-2)+1}{2} = \frac{(p-2)(p-1)}{2}.$$

Hence

$$(p-1)! \equiv g^{(p-2)(p-1)/2} \pmod p.$$

To analyse this further, recall that p is odd. Thus $p = 2k+1$ where k is a natural number. As $k < 2k = p-1$ then $g^k \not\equiv 1 \pmod p$ but $g^{2k} = g^{p-1} \equiv 1 \pmod p$ by Fermat's little theorem. As $(g^k)^2 = g^{2k} \equiv 1 \pmod p$ then $g^k \equiv \pm 1 \pmod p$ and so $g^k \equiv -1 \pmod p$.

We finally conclude that

$$(p-1)! \equiv g^{(p-2)(p-1)/2} = g^{(2k-1)k} = (g^k)^{2k-1} \equiv (-1)^{2k-1} = -1 \pmod p.$$

RJC 24/3/2005