An Inclusion-Exclusion Proof of Wilson's Theorem

Wilson's Theorem states that for a prime number p, $(p-1)! \equiv -1 \bmod p$. The statement can be easily verified for $p = 2$, so we'll restrict ourselves to odd p. The first proofs of Wilson's theorem were given by Lagrange in [**1**]. In his paper, Lagrange gave two proofs that are unusual compared to modern proofs that use multiplicative inverses modulo p. We give our own proof that uses inclusion-exclusion:

Consider the number of permutations on $A = \{1, 2, \dots, p\}$. On the one hand, the number is $p!$. On the other hand, we can think of a permutation on A as a function $f : A \to A$ that is onto. The number of functions $g : A \to A$ is p^p (for each input, we have p possible inputs). To find the onto functions, we have to remove whichever ones are not onto. Therefore, we must remove those that miss at least 1 value. There are $\binom{p}{1}$ ways of choosing the missed value and $(p-1)^p$ functions missing that particular value (for each input, we have $p-1$ possibilities). But when we remove all of these functions, we took out some too many times, indeed, any function that misses at least 2 values was over counted. So we have to add it back in. We get $\binom{p}{2}(p-2)^p$ such functions. We continue in this fashion using inclusion-exclusion to get the formula

$$p! = \sum_{k=0}^{p} (-1)^k \binom{p}{k} (p-k)^p. \tag{1}$$

Now divide by p and analyze modulo p:

$$\begin{aligned}(p-1)! = \frac{1}{p}\sum_{k=0}^{p}(-1)^k\binom{p}{k}(p-k)^p &= \sum_{k=0}^{p}(-1)^k\frac{(p-1)!}{k!(p-k)!}(p-k)^p \\ &\equiv (-1)^p\sum_{k=1}^{p-1}(-1)^k\frac{(p-1)!}{k!(p-k)!}k^p \bmod p. \qquad (2)\end{aligned}$$

Now

$$\begin{aligned}k!(p-k)! &\equiv k(-1)^{k-1}(p-(k-1))(p-(k-2))\cdots(p-1)(p-k)! \bmod p \\ &\equiv k(-1)^{k-1}(p-1)! \bmod p. \qquad (3)\end{aligned}$$

Therefore, from (2) and (3), we get

$$(p-1)! \equiv (-1)^p \sum_{k=1}^{p-1}(-1)\frac{(p-1)!}{k(p-1)!}k^p \equiv \sum_{k=1}^{p-1} k^{p-1} \bmod p.$$

From Fermat's Little Theorem, $k^{p-1} \equiv 1 \bmod p$. Therefore, the right-hand sum consists of $p-1$ ones and the proof is complete.

Remark. Lagrange's second proof uses (1) applied to $p-1$ instead of p. He says the formula "est facile de voir, par la théorie des différences" which translates to "easy to see, by the theory of differences". What is meant by this is that the formula pops up from repeatedly applying the difference operator Δ, where $\Delta(f)(x) = f(x) - f(x-1)$, to $f(x) = x^{p-1}$. He then uses Fermat's Little Theorem, followed by the expansion of $(1-1)^{p-1}$ to finish off the proof. There's another proof in the literature that uses (1). This proof was done by Ruiz in [**2**], and he calls the formula an algebraic identity. Ruiz proves (1) by induction using Calculus, then he uses Pascal's identity $\mod p$ to get a formula similar to (3). He finishes the proof in a similar fashion as here.

Acknowledgment. I would like to thank the referee for pointing out Lagrange's original proof and other suggestions that helped improved this paper. I would also like to thank Paul Pollack for reading drafts of this paper and pointing out what Lagrange meant by “théorie de differences”.

Summary. We present an inclusion-exclusion proof of Wilson's Theorem.

References

1. Joseph Louis Lagrange, *Demonstration d'un thorme nouveau concernant les nombres premiers*, Nouveaux Mmoires de l'Acadmie Royale des Sciences et Belles-Lettres **2** (1771), 125–137.
2. Sebastin Martn Ruiz, *An algebraic identity leading to wilsons theorem*, The Mathematical Gazette **80** (1996), no. 489, 579-582.