Fermat's Little Theorem and Wilson's Theorem

Jose Chavez

December 27, 2021

Abstract

We cover a pair of fascinating and elementary theorems in number theory due to Pierre de Fermat and Wilson. The theorem due to Wilson is dependent on Fermat's theorem and gives a sufficient and necessary condition for a number p being *prime*, a rare occurrence.

Discussion

Throughout this brief article we will be interested in the demonstration not only of proofs of the two Fermat and Wilson's theorems but also in the way that one goes about proving statements in mathematics.

Background Definitions and Lemmas

Recall that we say that given integers a and m we say that a is congruent to integer b modulo m iff

$$a - b = k \cdot m \text{ for some integer } k.$$

Theorem (Least Residue Theorem (LRT))**.** *Every integer a is congruent to a unique member of $\{0, \cdots, m-1\}$ mod n , in other words:*

$$a \equiv k \ (\ \textit{mod}\ n) \textit{ for some } k \in \{0, \cdots, m-1\}$$

Definition. *Given an integer a we say define the* least residue of a modulo m *to be the unique integer from the previous theorem.* {}

That's it! We are now ready to state and prove Fermat's Little Theorem.

Theorem (Fermat's Little Theorem (FLT)). *If p is prime and $(a, p) = 1$, then*

$$a^{p-1} \equiv 1 \ (\ \textit{mod}\ p)$$

Let's consider the situation. We have theorem LRT at our disposal. It also involves congruence modulo an integer so maybe it will be useful in proving FLT.

Proving the Theorems

Theorem.

$$a^{p-1} \equiv 1(\textit{mod}\ p)\ \textit{for every}\ a \not\equiv 0(\textit{mod}\ p)$$

Proving Wilson's Theorem

Next on the menu is Wilson's Theorem which partially characterizes prime numbers. Let's vary our style a bit. Assume that you know the following to facts:

1. $x^2 \equiv 1(\ \text{mod}\ p)$ has exactly two solutions, namely: p and $p - 1$;
2.

¡++¿

Theorem (Wilson's Theorem). *p is prime if and only if*

$$(p-1)! \equiv -1 \quad \textit{mod}\ p.$$

¡++¿

Appendix

Lemma ? proof. Let r be any solution of $x^2 \equiv 1\ (\ \text{mod}\ p)$. Recall that this means that r is a least residue that satisfies the congruence.

□