Fermat's Little Theorem

April 25, 2020

Conjecture. *If* $a, p \in \mathbb{N}$*,* p *is prime and* $gcd(a,p) = 1$ *then* $a^{p-1} \equiv 1 \pmod{p}$.

Proof. We claim that the first $(p-1)$ multiples of $a = \{a, 2a, 3a, \ldots, (p-1)a\}$, when divided by p, have distinct, non-zero remainders. Let $\mathbb{Z}_{p-1}$ represent the set of first $(p-1)$ positive integers. Let $k \in \mathbb{Z}_{p-1}$. If ka had a zero remainder on division by p, it would mean $p \mid ka$.

We will prove that this means $p \mid k$ or $p \mid a$. Since $p \mid ka$ there must exist $x \in \mathbb{Z}$ so that $px = ka$. Assume $p \nmid k$.

$\square$