Fermat's Little Theorem Proof

Saksham Sethi

1 Statement

$n^p \equiv n \pmod{p}$ where p is a prime.

2 Proof

Indirectly, this means that any $n^p - n$ is divisible by p for a certain prime p. Fix p. Let's take some examples first:

$n^2 - n = (n)(n-1)$. Since one of two consecutive numbers must be even (a multiple of 2), the whole product is too.

$n^3 - n = (n)(n^2 - 1) = (n)(n+1)(n-1)$. Using the same logic from the first example, this works too!

Whenever we factor this kind of expression, we get $(n)(n^{p-1} - 1)$. Finding a general expression gives us an idea of using induction.

Base Case: $n = 1$: Plugging $n = 1$ into the original statement, we get $1^p \equiv 1 \pmod{p}$, which is obviously true since $1^p = 1$ no matter what p is.

Inductive step: $(n+1)^p \equiv n + 1 \pmod{p}$**.** We have to show that if the relationship is true for n, it must be true for $n+1$. Plugging in $n+1$ into the original statement instead of n, we get $(n+1)^p \equiv n \pmod{p}$. Using the binomial theorem, we get that

$$(n+1)^p = n^p + \binom{p}{1} n^{p-1} + \binom{p}{2} n^{p-2} + \cdots + \binom{p}{p-1} n + 1.$$

Since $\binom{p}{q} = \frac{p!}{q!(p-q)!}$, p divides all $\binom{p}{q}$ for $1 \leq q \leq p-1$. Using this fact and taking $\pmod{p}$ on $(n+1)^p$, we get $(n+1)^p \equiv n^p + 1 \pmod{p}$. Since we know that $n^p \equiv n \pmod{p}$, we conclude that $(n+1)^p \equiv n + 1 \pmod{p}$, as desired in the inductive step.

$n^p \equiv n \pmod{p}$ $\square$