An Induction Proof for Prime Numbers—C.E. Mungan, Fall 2004

Prove that there exists some non-negative integer $m$ such that $n^p - n = mp$ where $n$ is any positive integer and $p$ is any prime number.

1. Claim is true for $n = 1$. Namely $m = 0$.

2. Assume claim is true for $n$, ie. $n^p = pm + n$ for some integer $m$.

3. Now prove that it holds for $n + 1$, i.e., show that $(n + 1)^p - (n + 1)$ is divisible by $p$. Using the binomial expansion, this expression becomes

$$n^p + \sum_{i=1}^{p-1} \frac{p!}{i!(p-i)!} n^i + 1 - n - 1$$

Substitute in claim 2 for the first term and simplify to get

$$pm + \sum_{i=1}^{p-1} \frac{p!}{i!(p-i)!} n^i$$

The proof is now complete if we can show that every binomial coefficient in this summation is divisible by $p$. First verify that this is true for the special cases of $p$ equaling 2 or 3. For $p=2$, we have only one binomial coefficient, equal to 2, which is clearly divisible by 2. For $p=3$, we have two binomial coefficients, both of which are equal to 3, divisible by 3.

So we can now restrict ourselves to the case of $p \geq 5$. In that case, the binomial coefficient for $i$ equaling 1 or $p-1$ is $p$, which is evidently divisible by $p$. So we are only left with the binomial coefficients for $2 \leq i \leq p-2$. An arbitrary coefficient in this range is

$$p \times \frac{(p-1)\times \cdots \times (p-i+1)}{i!}$$

Both the quantity in the square brackets and the denominator $i!$ are integers greater than or equal to 2. Since $p$ is prime, $i!$ cannot divide it. Thus $i!$ must divide the integer in square brackets because the binomial coefficient itself is an integer. Therefore this coefficient is $p$ times an integer, and is thereby divisible by $p$. QED

As an application, this result proves Fermat’s Little Theorem. Specifically, we have $n^{p-1} = 1 + pm / n$. But $pm / n = n^{p-1} - 1$ is an integer. Since $p$ is prime, $n$ must thereby divide $m$. It therefore follows that $n^{p-1} = 1 (mod p)$. 