Prime power of an integer modulo the prime

11/11/2020

Problem. *To prove that for a prime n, every integer smaller than n raised to the power n is equivalent to itself modulo n ($a^n \equiv a \mod n$). In other words a^n when divided by n leaves a as remainder.*

Solution. *We prove this by induction. Using $a = 1$ for the **basis step**, we can see that $1^n \equiv 1 \mod n$ (i.e., when divided by n, 1 leaves the remainer 1).*

*For the **induction step** assume the claim is true for an arbitrary $a = k < n$. I.e., $k^n \equiv k \mod n$, or for a quotient, q:*

$$k^n = n \cdot q + k \tag{1}$$

*Now consider, for $k + 1 < n$, the **binomial expansion**:*

$$\begin{aligned}(k+1)^n &= k^n + \sum_{r=1}^{n} \binom{n}{r} k^{n-r} + 1 \\ &= (n \cdot q + k) + \sum_{r=1}^{n} \binom{n}{r} k^{n-r} + 1\end{aligned}$$

$$(k+1)^n = n \cdot q + \sum_{r=1}^{n} \binom{n}{r} k^{n-r} + (k+1) \tag{2}$$

The binomial coefficient, $\binom{n}{r}$ also expressed as $\frac{n!}{j}$ is an integer. However n, being prime, can be extracted from it leaving behind an integer i_r (j does not divide n). Thus (2) can be re-written as:

$$\begin{aligned}(k+1)^n &= n\left(q + \sum_{r=1}^{n} i_r k^{n-r}\right) + (k+1) \\ &= n \cdot p + (k+1) && \textit{for an integer } p\end{aligned}$$

But since $k + 1 < n$, $(k+1)^n \equiv (k+1) \mod n$. In other words, $(k+1)^n$ when divided by n leaves $k + 1$ as remainder. Which means the claim is true for $a = (k + 1) < n$. And since we got to this conclusion by assuming the claim were true for $a = k < n$ it must be true for all $a < n$.