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).*

Now let's assume the claim is true for an arbitrary $a = k$: I.e., $k^n \equiv k \mod n$, or for a quotient, q

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

*Now consider the **binomial expansion**:*

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

The binomial coefficient, $\binom{n}{r}$ is an integer. However since n, being prime, can be extracted from it still leaving an integer i_r. Therefore

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

Thus we see that assuming the claim is true for $a = k$ we prove that it is true for $a = k + 1$. Hence it's true for all $a < n$