IMOSL N4

March 21, 2025

Problem. *Let $p \geq 5$ be a prime number. Prove that there exists an integer a with $1 \leq a \leq p-2$ such that neither $a^{p-1}-1$ nor $(a+1)^{p-1}-1$ is divisible by p^2.*

Solution. *Note that if $p = 5$, we choose $a = 2$, therefore we can assume $p \geq 7$*

Lemma. *For all x we have $(x+p)^p \equiv x^p \mod p^2$*

Proof. *Note that $(x+p)^p \equiv \sum_{i=0}^{i=p} \binom{p}{i} p^i x^{p-i} \equiv x^p + \binom{p}{1} p x^{p-1} \equiv x^p \mod p^2$*

Note that the given condition is equivalent to finding a number a such that neither $a - a^p$ nor $(a+1)-(a+1)^p$ is divisible by p^2. Let $f(a) = a - a^p$ then note that
$f(a) + f(p-a) = p + (a^p - (a-p)^p)$
Therefore $f(a) + f(p-a) \equiv p \mod p^2$
Hence at least one of $f(a)$ or $f(p-a)$ is not divisible by p^2.
Let's suppose for the sake of contradiction that there exists a prime p for which there exists no such a s.t. both $f(a)$ and $f(a+1)$ are not divisible by p^2 for all $1 \leq a \leq p-2$.Now if for some $t, 1 \leq t \leq p-2$ both $f(t)$ and $f(t+1)$ are divisible by p^2 then this implies both of $f(p-t)$ and $f(p-t-1)$ are not divisible by p^2 which is a contradiction, hence only one of $f(t)$ and $f(t+1)$ are divisible by p^2. Hence the divisibility by p^2 alternates and as we have $f(1) = 0$, this implies $f(a) \equiv 0 \mod p^2$ for all odd a s.t. $1 \leq a \leq p-1$. As $f(a) + f(p-a) \equiv p \mod p^2$, we get $f(a) \equiv p \mod p^2$ for all even a s.t. $1 \leq a \leq p-1$. Therefore we have
$f(2) \equiv p \mod p^2$ *, hence $2^p \equiv 2 - p$ and $f(3) \equiv 0 \mod p^2$, hence $3^p \equiv 3 \mod p^2$ and $f(6) \equiv p \mod p^2$, hence $6^p \equiv 6 - p$. So we have*
$2^p \cdot 3^p \equiv 6 - p \mod p^2$ *, hence*
$3(2-p) \equiv 6 - p \mod p^2$ *so $2p \equiv 0\ mod p^2$ which is a contradiction. Hence our original claim was true. QED*

Exploration. *Lots of primitive root thinking, but simply adding in reverse works*

Tags. *NT , Number Theory , modulo*