Bilkent University
Department of Mathematics

Problem Of The Month

March 2016

Problem:

Show that for each square free integer $n > 1$ there are prime p and integer m such that

$$p \mid n \quad \text{and} \quad n \mid p^2 + p \cdot m^p$$

Solution: Let p be the greatest prime divisor of n. We want to show that there exists m with $m^p \equiv -p \pmod{\frac{n}{p}}$. Then the two problem conditions will hold.

Let $m_1, m_2, \ldots, m_t$ be all the numbers between 0 and $\frac{n}{p}$ that are coprime to $\frac{n}{p}$. If all the numbers $m_1^p, m_2^p, \ldots, m_t^p$ happen to be different $\pmod{\frac{n}{p}}$, one would get $\{m_1^p, m_2^p, \ldots, m_t^p\} \equiv \{m_1, m_2, \ldots, m_t\} \pmod{\frac{n}{p}}$. But, $-p$ is an element of the right-hand side set, so it must be in the left-hand side set as well. This implies the existence of an integer m with the desired properties.

Thus, it is now sufficient to prove that no two of the numbers $m_1^p, m_2^p, \ldots, m_t^p$ are the same. Suppose otherwise and let $x^p \equiv y^p \pmod{\frac{n}{p}}$ where $x \not\equiv y \pmod{\frac{n}{p}} \Rightarrow s^p \equiv 1 \pmod{\frac{n}{p}}$ and $s \not\equiv 1 \pmod{\frac{n}{p}}$ where $s \equiv \frac{x}{y}$.

Let d be the least positive integer such that $s^d \equiv 1 \pmod{\frac{n}{p}}$. Then, one has $d > 1$, $d \mid p$ and $d \mid \phi(\frac{n}{p}) \Rightarrow p \mid \phi(\frac{n}{p})$. But $\phi(\frac{n}{p}) = (q_1 - 1) \cdots (q_k - 1)$ where $q_1, \ldots, q_k$ are the other prime divisors of n. By choice of p, one has $p > q_1, \ldots, q_k$ and this contradicts with $p \mid (q_1 - 1) \cdots (q_k - 1)$. Done.

Note. There is another, more constructive way of obtaining m with the desired properties. Keeping notation from previous part, the condition $m^p \equiv -p \pmod{\frac{n}{p}}$ can be equivalently characterized, by Chinese Remainder Theorem, as a set of conditions:

$$m^p \equiv -p \pmod{q_1}, \ldots, m^p \equiv -p \pmod{q_k}$$

But these conditions are symmetric, so it is sufficient to demonstrate one. In other words, one needs to prove that there exists m with $m^p \equiv -p \pmod{q}$ where $p > q$ are prime numbers. Let g be a primitive root $\pmod{q}$, r be such that $g^r \equiv -p \pmod{q}$ and s be a multiplicative inverse of $p \pmod{q-1}$. Note that p is indeed invertible $\pmod{q-1}$ as $p > q$ implies $\gcd(p, q-1) = 1$. Then $m = g^{rs}$ clearly works.