Rex H. Wu
Brooklyn, NY
RexHWu@aol.com

Solution to Problem 1057.

As suggested by the proposer, we will characterize the natural numbers p, q and r such that r divides $p^n - q$ for all $n \in \mathbb{N}$.

Case (I), $q \equiv 0 \pmod{r}$.

It follows that $p \equiv 0 \pmod{r}$.

Case (II), $q \not\equiv 0 \pmod{r}$.

Since we know

$$\begin{aligned} p - q &\equiv 0 \pmod{r} \\ p^2 - q &\equiv 0 \pmod{r} \\ p^3 - q &\equiv 0 \pmod{r} \\ &\vdots \\ p^n - q &\equiv 0 \pmod{r} \end{aligned}$$

we have $p^2 - q = p^2 - pq + pq - q = p(p-q) + q(p-1) \equiv 0 \pmod{r}$, or $p \equiv 1 \pmod{r}$. Similarly, $p^3 - q = p(p^2 - q) + q(p-1) \equiv 0 \pmod{r}$, again, $p \equiv 1 \pmod{r}$. In general, $p^n - q = p(p^{n-1} - q) + q(p-1) \equiv 0 \pmod{r}$, and $p \equiv 1 \pmod{r}$. This implies $q \equiv 1 \pmod{r}$.

Therefore, the only two cases we have to consider are (I) $q \equiv p \equiv 0 \pmod{r}$ and (II) $q \equiv p \equiv 1 \pmod{r}$.

Once we know this, it is not difficult to see that $p^n - q \equiv 0 \pmod{r}$ implies $q^n - p \equiv 0 \pmod{r}$ and vice versa.

■