Bilkent University
Department of Mathematics

PROBLEM OF THE MONTH

July-August 2008

Problem:

Let $k > 1$ be an integer and $p = 6k + 1$ be a prime number. Prove that for each $m = 2^p - 1$

$$\frac{2^{m-1} - 1}{127m}$$

is an integer.

Solution:

Let us show that both m and 127 divide $2^{m-1} - 1$. By Fermat's little theorem $2^p \equiv 2(mod p) \Rightarrow m = 2^p - 1 \equiv 1(mod p) \Rightarrow p \mid m - 1$. Therefore, $2^p - 1 \mid 2^{m-1} - 1$ $\Rightarrow m \mid 2^{m-1} - 1$. On the other hand, $6 \mid p - 1 \Rightarrow 63 = 2^6 - 1 \mid 2^{p-1} - 1 \Rightarrow 7 \mid 2^p - 2 \Rightarrow 7 \mid m - 1 \Rightarrow 127 = 2^7 - 1 \mid 2^{m-1} - 1$. We complete the solution by showing that m and 127 are relatively prime. Since 127 is prime, it is enough to show that m is not divisible by 127. Let $p = 7k + n(0 \leq n < 7)$. $k > 1 \Rightarrow p > 7$ and p is not divisible by $7 \Rightarrow n \neq 0$. Now $127 = 2^7 - 1 \mid 2^{7k} - 1 \Rightarrow 127 \mid 2^{7k+n} - 2^n = 2^p - 2^n$. If $127 \mid m$, then $127 \mid 2^n - 1$ which is impossible since $0 < 2^n - 1 < 127$. Done.