SOLUTION TO MS-2015, NOS. 1-2: PROBLEM-4

MANJIL P. SAIKIA

1. Problem Statement

Show that n divides $2^n - 1$ over $\mathbb{Z}$ if and only if $n = 1$.

2. Solution

If $n = 1$, then $2^n - 1 = 1$ and thus one direction is trivial.

Let us now assume that n divides $2^n - 1$. Let if possible p be the smallest prime factor of n, then p also divides $2^n - 1$. So, we have $2^n \equiv 1 \pmod{p}$. Since $2^n - 1$ is odd and $p > 2$ we have by Fermat's Little Theorem $2^{p-1} \equiv 1 \pmod{p}$.

Let d be the smallest value of k such that $2^k \equiv 1 \pmod{p}$. Then we have d divides n and $p - 1$. This shows that there is a factor of n which is smaller than p, and thus the only possibility for d is $d = 1$, but then it gives $2^1 \equiv 1 \pmod{p}$ which is not possible. So, we see that n has no prime factors and hence $n = 1$ or $n = -1$. But clearly if $n = -1$ then $2^{-1} - 1$ is not an integer.

Diploma Student, Mathematics Section, The Abdus Salam International Centre for Theoretical Physics, Trieste 34151, Italy

E-mail address: manjil@gonitsora.com, msaikia@ictp.it