NNTDM 6 (2000) 1, 28

SHORT REMARK ON NUMBER THEORY. I

Krassimir T. Atanassov
Centre for Biomedical Engineering - Bulgarian Academy of Sciences,
Acad. G. Bonchev Str., Bl. 105, Sofia-1113, BULGARIA
e-mail: krat@bgcict.acad.bg

In this short remark we shall prove that

For all natural numbers $k \geq 1, m \geq 2$ at least one member of the set

$$S = \{m^1 - 1, m^2 - 1, m^3 - 1, ..., m^{m.k} - 1\}$$

is divisible by $m.k + 1$.

Let us suppose that no member of S is divisible by $m.k + 1$. In this case, each of the $m.k$ members of S must be congruent, modulo $m.k + 1$, to one of the $m.k$ nonzero remainders 1, 2, ..., $m.k$. By the pigeonhole principle, then, either:
(a) some two members of S are congruent to the same remainder, and therefore, to each other:

$$m^r - 1 \equiv m^s - 1 (\text{mod } m.k + 1)$$

where $r > s$, or
(b) each of 1, 2, ..., $m.k$ is congruent to different members of S.

In the event of case (a), we have

$$m^r - m^s \equiv 0 (\text{mod } m.k + 1)$$

$$m^s.(m^{r-s} - 1) \equiv 0 (\text{mod } m.k + 1).$$

Since $(m.k + 1, m) = 1$, the factor m^s does not contribute toward the satisfaction of the congruence, and it follows that

$$m^{r-s} - 1 \equiv 0 (\text{mod } m.k + 1).$$

But $m^{r-s} - 1$ is a member of S, and therefore, a member of S would be divisible by $m.k + 1$, which is a contradiction with our assumption.

If (b) were to hold, then some members of S would be congruent to $m.k$ and let it be $a-$th member, i.e.,

$$m^a - 1 \equiv m.k (\text{mod } m.k + 1).$$

Therefore,

$$m^a \equiv m.k + 1 \equiv 0 (\text{mod } m.k + 1),$$

as obvious contradiction. The conclusion follows.

The above assertion is a direct generalization of a similar one from [1], where the case $m = 2$ is discussed.

REFERENCE:

[1] Honsberger R., Mathematical Gems. III. Mathematical Assoc. of America, 1985.