NNTDM 8 (2002) 4, 120-124

A NOTE ON THE ELEMENTARY NUMBER THEORY

Krassimir T. Atanassov
CLBME - Bulg. Academy of Sci., P.O.Box 12, Sofia-1113, Bulgaria,
e-mail: *krat@bas.bg*

The Bulgarian schoolboy Todor Eliseev formulated in the Bulgarian journal *"Mathematics"*, Vol. 31 (1992), No. 5, the following problem, which was included in the monthly competition of the journal: *Prove that* n *is a divisor of* $\sum_{d/n} \varphi(d).p^{\frac{n}{d}}$, *where* p *is an arbitrary prime number,* φ *is the Euler's function and the sum (here and below) is over all divisors of* n.

The Bulgarian schoolboys Yasen Siderov and Detelin Dosev solved the problem (their solution was published in "Mathematics" Vol. 32 (1993), No. 4)) generalizing it with the change of p with an arbitrary natural number a.

Below we shall formulate a next generalization of the above problem, following [1].

Let $g : \mathcal{N} \times \mathcal{N} \to \mathcal{Q}$ (where $\mathcal{N}$ and $\mathcal{Q}$ are the sets of all natural and rational numbers, respectively) be a function, for which:
a) $g(n, k) \in \mathcal{N}$, if k is a divisor of n;
b) for every three natural numbers k, m and n:

$$g(k.m, k.n) = g(m, n); \tag{1}$$

c) for every three natural numbers k, m and n, for which n is a divisor of k:

$$g(k.m, n) = m.g(k, n). \tag{2}$$

From where it follows that

$$g(k, k) = g(1, 1), \tag{3}$$

$$g(k, 1) = k.g(1, 1), \tag{4}$$

$$g(1, 1).g(k.l, m.n) = g(k, m).g(l, n) \tag{5}$$

for every four natural numbers k, l, m and n, for which m and n are divisors of k and l, respectively.

The last equality is valid, because by condition there are natural numbers x and y, for which $k = x.m$ and $l = y.n$ and, therefore,

$$g(1, 1).g(k.l, m.n)$$

(from (2))

$$= g(1, 1).x.y.g(m.n, m.n)$$

(from (1))

$$= x.g(m, m).y.g(n, n)$$

(from (2))

$$= g(k,m).g(l,n).$$

Let everywhere below $b = g(1,1)$.

The last problem and its Y. Siderov - D. Dosev's generalization can be extended to the form:

Prove that if n and a are natural numbers and if

$$S_n(a) = \sum_{d/n} \varphi(d).a^{b^{cas(n)}.g(n,d)}, \tag{6}$$

then

$$S_n(a) \equiv 0(mod\ LCM(n, a^{b^{cas(n)}.g(n,d)})), \tag{7}$$

where LCM is the integer function "the lowest common multiple" and $cas(n)$ is the number of the different prime divisors of n.

Firstly, we shall note, that the right hand of (7) is divided by $a^{b^{cas(n)}}$, because all terms of the sum are divided by the same divisor. Therefore, we must prove that

$$S_n(a) \equiv 0(\text{mod } n). \tag{8}$$

We shall apply an induction in relation to $cas(n)$.

Let $cas(n) = 1$, i.e. $n = p^m$ for some prime number p and some natural number $m \geq 1$. Then, $S_n(a)$ from (6) can be represented in the form

$$S_n(a) = T_m(n,a) = \sum_{k=0}^{m} \varphi(p^k).a^{b \cdot g(p^m,p^k)} \tag{9}$$

and, hence, (8) must be proved in the form

$$T_m(n,a) \equiv 0(\text{mod } n). \tag{10}$$

The validity of (10) is proved, e.g., by induction according to m.

For $m = 1$, (9) has the form:

$$T_1(n,a) = a^{b.g(p,1)} + (p-1).a^{b.g(p,p)}$$

(from (3) and (4))

$$= p.a^{b^2} + ((a^{b^2})^p - a^{b^2})$$

and from the Little Fermat's Theorem (see, e.g., [2]) it follows that for every $a =\in \mathcal{N}$:

$$T_1(n,a) \equiv 0(\text{mod } n).$$

Let us assume that (10) is valid for some natural number m. Now, we will use the identity

$$\sum_{k=0}^{m} A(k).B(k+1) = \sum_{k=1}^{m+1} A(k-1).B(k),$$

which is valid for arbitrary arithmetical functions A and B.

Let us put in it:

$$A(s) = a^{b.g(p^m,p^s)}$$

and

$$B(s) = \varphi(p^s).$$

Then, we obtain:

$$\sum_{k=0}^{m} \varphi(p^{k+1}).a^{b.g(p^m,p^k)} = \sum_{k=1}^{m+1} \varphi(p^k).a^{b.g(p^m,p^{k-1})}$$

and from $\varphi(p^{k+1}) = p.\varphi(p^k)$ for $k \geq 1$, and $g(p^m,p^{k-1}) = g(p^{m+1},p^k)$ we obtain:

$$\varphi(p).a^{b.g(p^m,1)} + p. \sum_{k=1}^{m} \varphi(p^k).a^{b.g(p^m,p^k)} = \sum_{k=1}^{m+1} \varphi(p^k).a^{b.g(p^{m+1},p^k)}$$

which from (9) can be written in the following form:

$$T_{m+1}(n,a) = p.T_m(n,a) + R,$$

where

$$R = a^{b.g(p^{m+1},1)} - a^{b.g(p^m,1)}.$$

Therefore, we must show that

$$R \equiv 0 (\text{mod } p^{m+1}). \qquad (11)$$

From (4) it follows that $g(p^m,1) = p^m.b$ and $g(p^{m+1},1) = p^{m+1}.b$ and hence,

$$R = (a^{b^2})p^m.((a^{b^2.\varphi(p^{m+1})} - 1). \qquad (12)$$

If $a \equiv 0(\text{mod } p)$, then,

$$(a^b)^p \equiv 0(\text{mod } p^{m+1})$$

and therefore (11) is valid. If $(a,p) = 1$, then from Euler's theorem (see, e.g. [2]) it follows that

$$(a^{b^2})^{\varphi(p^{m+1})} \equiv 1(\text{mod } p^{m+1})$$

and therefore from (12) it follows that (11) is valid, too.

With this, the induction step about m has ended and, therefore, the validity of (10) is proved, i.e. (8) is valid for $cas(n) = 1$.

Let us assume that (8) holds for every natural numbers n, for which $cas(n) \leq s$, where s is a natural number. We must prove (8) for some natural number n, for which $cas(n) = s+1$. Therefore, $n = n'.p^m$ for some prime number p that does not divide n, and for some natural number $m \geq 1$, where $cas(n') = s$. Obviously,

$$cas(n) = cas(n') + cas(p^m) = s + 1.$$

Let us put for brevity $n'' = p^m$ and hence $n = n'.n''$.

We must prove that

$$S_n(a) = S_{n'.n''}(a) \equiv 0 (\text{mod } n)$$

By induction assumption

$$S_{n'}(a') \equiv 0 (\text{mod } n')$$

for every natural number a' and from the first step of the induction

$$S_{n''}(a'') \equiv 0 (\text{mod } n'')$$

for every natural number a''.

From (6) and from the fact that φ is a multiplicative function, we obtain

$$S_n(a) = \sum_{d/n'} \sum_{e/n''} \varphi(n').\varphi(n'').a^{b^{cas(n')+cas(n'')}.g(n'.n'',d.e)}$$

(from (5))

$$= \sum_{d/n'} \varphi(n').(\sum_{e/n''} \varphi(n'').a^{b^{s-1}.g(n',d).b.g(n'',e)})$$

(from (6))

$$= \sum_{d/n'} \varphi(n').S_{n''}(a^{b^{s-1}.g(n',d)}).$$

But it follows from the first induction step that

$$S_{n''}(a^{b^{s-1}.g(n',d)}) \equiv 0 (\text{mod } n'')$$

and, therefore, $S_n(a) \equiv 0(\text{mod } n'')$.

On the other hand, it can be analogously seen that

$$S_n(a) = \sum_{e/n''} \varphi(n'').S_{n'}(a^{g(n'',e)})$$

and from the induction assumption it follows that

$$S_n(a) \equiv 0 (\text{mod } n').$$

But $(n', n'') = 1$. Therefore,

$$S_n(a) \equiv 0 (\text{mod } n'.n''),$$

i.e. (8) and, hence, (7), also, are valid.

With this the problem is proved.

The following question is interesting, too: can the above problem be generalized more with the change of φ with an arbitrary arithmetical function?

From the above construction it is seen that f must be a multiplicative function (therefore, if it is not identically equal to 0, it must satisfy equality $f(1) = 1$) for which the conditions for every prime number p must be valid and for every natural number $k \geq 1$:

$$f(p^{k+1}) = p.f(p^k),$$

$$f(p) = (p - 1).f(1).$$

But in this case one can directly see that function f coincides with function φ. Therefore the above problem cannot be extended in this direction.

Are there other directions for its generalization?

REFERENCES:

[1] Atanassov K., A note on the elementary number theory. *Notes on Number Theory and Discrete Mathematics,* Vol. 8 (2002), No. 4 (in press).

[2] Nagell T., Introduction to number theory, John Wiley & Sons, New York, 1950.