Stanislav Jakubec
Note on a certain sums of integer parts

Mathematica Slovaca, Vol. 51 (2001), No. 1, 59--62

Persistent URL: http://dml.cz/dmlcz/129885
NOTE ON A CERTAIN SUMS OF INTEGER PARTS

STANISLAV JAKUBEC

(Communicated by Pavol Zlatoš)

ABSTRACT. In the paper a connection between sums of integral parts and the class number is given.

Let \( p \) be odd primes. Let \( H_0 \) be a subgroup of the group \((\mathbb{Z}/p^n\mathbb{Z})^*\) of index \( l \). The cosets of \((\mathbb{Z}/p^n\mathbb{Z})^*\) with respect to the subgroup \( H_0 \) will be denoted by \( H_i, \ i \in \{0, 1, 2, \ldots, l-1\} = I \).

The following definitions are taken from [1].

DEFINITION 1. ([1]) A subset \( T \) of a coset \( H_i \) will be called a semisystem (in \( H_i \)) if for each \( x \in H_i \) exactly one of the residue classes \( x, -x \) belongs to \( T \). Clearly

\[
\#T_i = \frac{\#H_0}{2} = \frac{\varphi(p^n)}{2l} = \frac{p^{n-1}(p-1)}{2l}
\]

for every semisystem \( T_i \).

DEFINITION 2. ([1]) Given a positive integer \( a \) coprime to \( p \) and a semisystem \( T_i \) for some \( i \in I \), let

\[
g(a, i) = \sum_{z \in T_i} \left( \left\lfloor \frac{az}{p^n} \right\rfloor + \left\lfloor \frac{z}{p^n} \right\rfloor \right) \quad \text{for } a \text{ odd,} \quad (1)
\]

\[
g(a, i) = \sum_{z \in T_i} \left( \left\lfloor \frac{2az}{p^n} \right\rfloor + \left\lfloor \frac{2z}{p^n} \right\rfloor \right) \quad \text{for } a \text{ even.} \quad (2)
\]

Note that in [1: Proposition 2] it is proved that the value \( g(a, i) \mod 2 \) is independent from the choice of the representant of \( a \) modulo \( p^n \).

2000 Mathematics Subject Classification: Primary 11R29.
Key words: class number.
STANISLAV JAKUBEC

DEFINITION 3. ([1]) Denote by $G$ the set of all $a \in (\mathbb{Z}/p^n\mathbb{Z})^*$ such that $g(a,i) \equiv g(a,j) \pmod{2}$ for all $i, j \in I$.

In [1] it is proved that $G$ is a group and it holds that either $G = H_0$ or $G = (\mathbb{Z}/p^n\mathbb{Z})^*$.

The aim of this paper is to give a necessary and sufficient condition for $G = (\mathbb{Z}/p^n\mathbb{Z})^*$ (hence $n = 1$) in case that 2 is primitive root modulo $l$ (hence $l = 3, 5, 11, 13, 19, \ldots$) and 2 is not an $l$th power modulo $p$. If $l = 3$, then $p = 163$ is the first prime such that $G = (\mathbb{Z}/p\mathbb{Z})^*$.

**Theorem 1.** Let $K$ be a real number field with prime conductor $p$, where $[K : \mathbb{Q}] = l$ is prime. Let 2 be a primitive root modulo $l$. Suppose that 2 is not an $l$th power modulo $p$. Then $G = (\mathbb{Z}/p\mathbb{Z})^*$ if and only if $h_K$ is even.

**Proof.**

1. We shall prove that if $G = (\mathbb{Z}/p\mathbb{Z})^*$, then $2 \mid h_K$. Let $U_K$, $U_K^+$ and $U_K^2$ be the group of units, the group of total positive units and the group of quadrates of $K$, respectively. Suppose that $U_K^+ \neq U_K^2$, hence $\dim_2 U_K^+ / U_K^2 = d > 0$. O r i a t [3] has proved that if $-1$ is a power of 2 modulo $l$, then $2^d \mid h_K$. Since 2 is a primitive root modulo $l$, $-1$ is a power of 2 modulo $l$, and from $d > 0$ we have $2 \mid h_K$.

Let $U_K^+ = U_K^2$. Since $G = (\mathbb{Z}/p\mathbb{Z})^*$, according to [1; Proposition 6] all positive units of the group $C(K)$ (the group of cyclotomic units of $K$) are totally positive, and from $U_K^+ = U_K^2$ it follows that they are quadrates. It easily implies that the index $[U_K^+ : C(K)]$ is of divisibility $2^{l-1}$. By [4] and [5], $h_K = \text{index}[U_K^+ : C(K)]$.

2. We shall prove that $2 \mid h_K$, then $G = (\mathbb{Z}/p\mathbb{Z})^*$. Here, the following theorem proved by Metsänkylä [2] will be used.

**Theorem (Metsänkylä).** Let $K$ be a real abelian field with conductor $p$, an odd prime. If the class number of $K$ is even, then

$$
\prod_{\chi \neq 1} \sum_{i=1}^{p-1} a_i \chi(i) \equiv 0 \pmod{2},
$$

where the product extends over all nonprincipal characters $\chi$ of $K$ and where

$$
a_i = \begin{cases} 0 & \text{for } i \equiv 0 \text{ or } p \pmod{4}, \\ 1 & \text{otherwise}. \end{cases}
$$

If this Theorem is applied on the case that the degree $[K : \mathbb{Q}] = l$ is prime and 2 is a primitive root modulo $l$, we have: If $2 \mid h_K$, then

$$
\sum_{i=1}^{p-1} a_i \chi(i) \equiv 0 \pmod{2}.
$$
NOTE ON A CERTAIN SUMS OF INTEGER PARTS

The above congruence can be rewritten to the form

\[ A_0 + A_1 \zeta_l + A_2 \zeta_l^2 + \cdots + A_{l-1} \zeta_l^{l-1} \equiv 0 \pmod{2}, \]

hence

\[ A_0 \equiv A_1 \equiv A_2 \equiv \cdots \equiv A_{l-1} \pmod{2}, \]

where

\[ A_i = \#\{z : z \equiv 1 \text{ or } 2 \pmod{4}, \ z \in H_i, \ z < \frac{p}{2} \} \quad \text{for } p \equiv 3 \pmod{4}, \]

and

\[ A_i = \#\{z : z \equiv 2 \text{ or } 3 \pmod{4}, \ z \in H_i, \ z < \frac{p}{2} \} \quad \text{for } p \equiv 1 \pmod{4}. \]

It is enough to prove that if

\[ A_0 \equiv A_1 \equiv A_2 \equiv \cdots \equiv A_{l-1} \pmod{2}, \]

then \( G = (\mathbb{Z}/p\mathbb{Z})^* \).

Let \( p \equiv 3 \pmod{4} \). Since \( 2 \notin H_0 \), we have \( \frac{p-1}{2} \notin H_0 \). The number \( \frac{p-1}{2} \) is odd. Substituting \( a = \frac{p-1}{2} \) into (1) we have

\[
\sum_{z \in H_i \atop z < \frac{p}{2}} \left\lfloor \frac{p-1}{2} \frac{z}{p} \right\rfloor = \sum_{z \in H_i \atop z < \frac{p}{2}} \left\lfloor \frac{z}{2} - \frac{z}{2p} \right\rfloor.
\]

It is easy to see that there holds

\[
\left\lfloor \frac{z}{2} - \frac{z}{2p} \right\rfloor = \begin{cases}
\frac{z}{2} - 1 & \text{if } z \equiv 0 \pmod{2}, \\
\frac{z}{2} & \text{if } z \equiv 1 \pmod{2}.
\end{cases}
\]

From the above we get that

\[
\sum_{z \in H_i \atop z < \frac{p}{2}} \left\lfloor \frac{p-1}{2} \frac{z}{p} \right\rfloor \equiv \#\{z : z \equiv 2 \pmod{4}, \ z \in H_i, \ z < \frac{p}{2} \} \\
+ \#\{z : z \equiv 0 \pmod{2}, \ z \in H_i, \ z < \frac{p}{2} \} \\
+ \#\{z : z \equiv 3 \pmod{4}, \ z \in H_i, \ z < \frac{p}{2} \} \\
\equiv \#\{z : z \equiv 2 \pmod{4}, \ z \in H_i, \ z < \frac{p}{2} \} \\
+ \frac{p-1}{2l} \ - \#\{z : z \equiv 1 \pmod{4}, \ z \in H_i, \ z < \frac{p}{2} \} \\
- \#\{z : z \equiv 3 \pmod{4}, \ z \in H_i, \ z < \frac{p}{2} \} \\
+ \#\{z : z \equiv 3 \pmod{4}, \ z \in H_i, \ z < \frac{p}{2} \} \\
\equiv \frac{p-1}{2l} + \#\{z : z \equiv 1 \pmod{4}, \ z \in H_i, \ z < \frac{p}{2} \} \\
+ \#\{z : z \equiv 2 \pmod{4}, \ z \in H_i, \ z < \frac{p}{2} \} \pmod{2}.
\]
It follows that $\frac{p-1}{2} \in G$, hence $G = (\mathbb{Z}/p\mathbb{Z})^*$. If $p \equiv 1 \pmod{4}$, then $\frac{p+1}{2} \notin H_0$. The number $\frac{p+1}{2}$ is odd. Substituting $a = \frac{p+1}{2}$ into (1) we have

$$
\sum_{z \in H_i, \ z < \frac{p}{2}} \left[ \frac{p+1}{2} \frac{z}{p} \right] = \sum_{z \in H_i, \ z < \frac{p}{2}} \left[ \frac{z}{2} + \frac{z}{2p} \right].
$$

Clearly

$$
\left[ \frac{z}{2} + \frac{z}{2p} \right] = \begin{cases} 
\frac{z}{2} & \text{if } z \equiv 0 \pmod{2}, \\
\frac{z-1}{2} & \text{if } z \equiv 1 \pmod{2}.
\end{cases}
$$

Hence

$$
\sum_{z \in H_i, \ z < \frac{p}{2}} \left[ \frac{p+1}{2} \frac{z}{p} \right] \equiv \# \{ z : z \equiv 2 \pmod{4}, \ z \in H_i, \ z < \frac{p}{2} \}
$$

$$
+ \# \{ z : z \equiv 3 \pmod{4}, \ z \in H_i, \ z < \frac{p}{2} \} \pmod{2}.
$$

Hence $\frac{p+1}{2} \in G$, therefore $G = (\mathbb{Z}/p\mathbb{Z})^*$. Theorem 1 is proved.

REFERENCES

[1] JAKUBEC, S.: Note on the congruences $2^{p-1} \equiv 1 \pmod{p^2}$, $3^{p-1} \equiv 1 \pmod{p^2}$, $5^{p-1} \equiv 1 \pmod{p^2}$, Acta Math. Inform. Univ. Ostraviensis 6 (1998), 115–120.


Received March 24, 1999