Math. Student 35 (1967), 47-50.

AN ELEMENTARY NUMBER-THEORETIC FORMULA

By

KENNETH S. WILLIAMS

(*Received*: 28-1-1964)

It is well-known [1] that

$$\sum_{x=0}^{p-1}\left\{\frac{ax+b}{p}\right\}=p'$$

where p is an odd prime not dividing a, $p'=\frac{1}{2}(p-1)$ and $\{x\}$ denotes the fractional part of x. I wondered if there is a similar formula for

$$\sum_{x=0}^{p-1}\left\{\frac{ax^2+bx+c}{p}\right\}.$$

I find a formula for this sum, which depends on a sum of Legendre symbols over an incomplete residue system and also on the class number $h(-p)$ if $p\equiv 3 \pmod 4$. I first prove a simple lemma.

Lemma. If n is a positive integer then

$$\sum_{x=0}^{p-1}x\left(\frac{x+n}{p}\right)-p\sum_{x=0}^{n-1}\left(\frac{x}{p}\right)$$

$$=\begin{cases}0 & p\equiv 1 \pmod 4\\ -\frac{p}{3}\left(2+\left(\frac{2}{p}\right)\right)h(-p) & p\equiv 3 \pmod 4\end{cases}$$

Proof. For $n\geqslant 1$

$$\sum_{x=0}^{p-1}x\left(\frac{x+n}{p}\right)=\sum_{x=1}^{p}(x-1)\left(\frac{x+n-1}{p}\right)$$

$$=\sum_{x=1}^{p}x\left(\frac{x+n-1}{p}\right)$$

since
$$\sum_{x=1}^{p}\left(\frac{x+n-1}{p}\right)=\sum_{y=0}^{p-1}\left(\frac{y}{p}\right)=0$$

Thus
$$\sum_{x=0}^{p-1} x\left(\frac{x+n}{p}\right)-\sum_{x=0}^{p-1} x\left(\frac{x+n-1}{p}\right)=p\left(\frac{n-1}{p}\right)$$

for $n \geqslant 1$, yielding
$$\sum_{x=0}^{p-1} x\left(\frac{x+n}{p}\right)=\sum_{x=0}^{p-1} x\left(\frac{x}{p}\right)+p\sum_{x=0}^{p-1}\left(\frac{x}{p}\right)$$

and the lemma follows [2]
$$\sum_{x=0}^{p-1} x\left(\frac{x}{p}\right)=\begin{cases}0 & p\equiv 1 \pmod 4\\ -\frac{1}{3}p\left(2+\left(\frac{2}{p}\right)\right)h(-p) & p\equiv 3 \pmod 4\end{cases}$$

I can now deduce the formula for the sum in question.

Theorem. If p is an odd prime and $p \nmid a$ then
$$\sum_{x=0}^{p-1}\left\{\frac{ax^2+bx+c}{p}\right\}=p'+\left(\frac{a}{p}\right)\sum_{x=0}^{d-1}\left(\frac{x}{p}\right)$$
$$+\begin{cases}0 & p\equiv 1 \pmod 4\\ -\frac{1}{3}\left(\frac{a}{p}\right)\left(2+\left(\frac{2}{p}\right)\right)h(-p) & p\equiv 3 \pmod 4\end{cases}$$

where d is such that $0 \leqslant d \leqslant p-1$ and $b^2-4ac \equiv 4ad \pmod p$.

Proof. Define r by $b \equiv 2ar \pmod p$, $0 \leqslant r \leqslant p-1$.

Then since $\left\{\frac{x}{p}\right\}$ is periodic with period p
$$\sum_{x=0}^{p-1}\left\{\frac{ax^2+bx+c}{p}\right\}=\sum_{x=0}^{p-1}\left\{\frac{a(x+r)^2+(c-ar^2)}{p}\right\}$$

$$= \sum_{x=0}^{p-1} \left\{ \frac{ax^2 - d}{p} \right\}$$

$$= \sum_{x=0}^{p-1} \left\{ \frac{ax - d}{p} \right\} + \sum_{x=0}^{p-1} \left(\frac{x}{p} \right) \left\{ \frac{ax - d}{p} \right\}.$$

$$= p' + \sum_{x=0}^{p-1} \left(\frac{a^{-1}(x + d)}{p} \right) \left\{ \frac{x}{p} \right\}$$

$$= p' + \left(\frac{a}{p} \right) \sum_{x=0}^{p-1} \left(\frac{x + d}{p} \right) \frac{x}{p}$$

and the result follows on using the lemma.

In general, $\sum_{x=0}^{d-1} \left(\frac{x}{p} \right)$ cannot be given more simply. However when $p \equiv 1 \pmod 4$ and $d = 0, 1, 2, p'$ or $p' + 1$ its value is immediate.

In these special cases, setting $p'' = \frac{p+1}{2} = p' + 1$, we have immediately from the theorem :

Corollary : For $p \equiv 1 \pmod 4$, $p \nmid a$,

(*i*) $$\sum_{x=0}^{p-1} \left\{ \frac{ax^2}{p} \right\} = p'$$

(*ii*) $$\sum_{x=0}^{p-1} \left\{ \frac{ax^2 - 1}{p} \right\} = p'$$

(*iii*) $$\sum_{x=0}^{p-1} \left\{ \frac{ax^2 - 2}{p} \right\} = p' + \left(\frac{a}{p} \right)$$

(*iv*) $$\sum_{x=0}^{p-1} \left\{ \frac{ax^2 - p'}{p} \right\} = p' + (-1)^{p'/2+1} \left(\frac{a}{p} \right)$$

(*v*) $$\sum_{x=0}^{p-1} \left\{ \frac{ax^2 - p''}{p} \right\} = p'$$

From (*iv*) and (*v*) with $a = 1$ and $p \equiv 5 \pmod 8$ I have the "reciprocal" relations

$$\sum_{x=0}^{p-1} \left\{ \frac{x^2 - p'}{p} \right\} = p'', \quad \sum_{x=0}^{p-1} \left\{ \frac{x^2 - p''}{p} \right\} = p'.$$

REFERENCES

1. I.M. Vinogradov, Elements of Number Theory (Dover) 1954 (See Ex. 2 (*a*) (*α*) *P*. 50.)
2. L.E. Dickson "History of the Theory of Numbers". Vol. 3. (Chelsea) 1952 (See . *p* 118).

Department of Mathematics
Carleton University
Ottawa 1
Ontario, Canada