JNSF 9-1-77

J. Natn. Sci. Coun. Sri Lanka 1981 9 (1)

A Theorem on the Congruences $[\frac{1}{2}(p-1)]! \equiv \pm 1 \pmod{p}$.

M. VELUPPILLAI

Department of Mathematics, University of Peradeniya, Peradeniya, Sri Lanka.

(Date of receipt : 16 May 1979)

(Date of acceptance : 30 January 1981)

1. Introduction.

From Wilson's theorem, we have for any prime $p \equiv 3 \pmod 4$,

$[\frac{1}{2}(p-1)]! \equiv \pm 1 \pmod p$. For some primes the plus sign holds and for some the minus sign hold. Kr ö necker has derived a rule, mentioned in [1], to decide which of the two signs $\pm$ holds in the above congruence. The object of this paper is to derive a simple formula depending only on the class number $h(-p)$.

2. Theorem:

If p is a prime $\equiv 3 \pmod 4$, then

$[\frac{1}{2}(p-1)]! \equiv -1 \pmod p$, if $h(-p) \equiv 1 \pmod 4$

$\equiv +1 \pmod p$, if $h(-p) \equiv 3 \pmod 4$

3. Proof:

We have $[\frac{1}{2}(p-1)]! \equiv \pm 1 \pmod p$.

Then $\left(\frac{[\frac{1}{2}(p-1)]!}{p}\right) \equiv \left(\frac{\pm 1}{p}\right) = \pm 1$

Hence $[\frac{1}{2}(p-1)]! \equiv (-1)^n \pmod p$ where n is the number of positive quadratic non residues of p which are less than or equal to $\frac{1}{2}(p-1)$.

Now, let m be the number of positive quadratic residues of p which are less than or equal to $\frac{1}{2}(p-1)$.

Then $m+n=\frac{1}{2}(p-1)$ (1)

If $p \equiv -1 \pmod 8$ then $h(-p)=m-n$ (2)

and if $p \equiv 3 \pmod 8$,

$h(-p)=\frac{1}{3}(m-n)$. (See e.g. [2])

From (1) and (2), we have, if $p \equiv -1 \pmod 8$, then

$$n=\tfrac{1}{4}(p-2h-1)$$

and from (1) and (3), we have, if $p \equiv 3 \pmod 8$, then

$$n=\tfrac{1}{4}(p-6h-1).$$

In both cases n is odd if $h \equiv 1 \pmod 4$ and n is even if $h \equiv 3 \pmod 4$

Hence the theorem.

References

1. AYOUB, R. (1963) *An Introduction to the Analytic Theory of numbers*, Amer. Math. Soc. p. 300—301.

2. USPENSKY, J.V. & HEASLET, M.A. (1939) *Elementary Number Theory*, New York and London p 156—157.