Acta Math. Hung.
46 (3—4) (1985), 265—267.

GENERALIZATION OF EISENSTEIN'S CONGRUENCE

P. JOTHILINGAM (Shillong)

We shall use the letter p to denote an odd prime number. Fermat's little theorem asserts that the residue of 2^{p-1} modulo p is 1. Regarding the residue of 2^{p-1} modulo p^2, Eisenstein [1], proved the following.

THEOREM A. *For any integer* s, $1 \leqq s \leqq p-1$, *let* $\bar{s}$ *represent the inverse class of* $s \bmod p$. *Then*

$$2^{p-1} \equiv 1 + p(\bar{1} + \bar{3} + \ldots + \overline{p-2}) \pmod{p^2}.$$

In this note, Eisenstein's congruence is extended to include residue of 2^{p-1} modulo p^3. We state

THEOREM B. *Let* $p > 3$ *and define* $\lambda = \frac{p-1}{2}$. *For any integer* s, $1 \leqq s \leqq p-1$; *let* $\tilde{s}$ *be a representative of the inverse class of* $s \bmod p^2$. *Then*

$$2^{p-1} \equiv 1 + p(\tilde{1} + \tilde{3} + \ldots + \widetilde{p-2}) - p^2 \sum_{s=1}^{\lambda} \left\{\theta_s + \left(\frac{2}{p}\right)\theta_{\lambda-s+1}\right\} 2^{s-1} \pmod{p^3}$$

where $\left(\frac{2}{p}\right)$ *stands for the Legendre's symbol and* $\theta_1, \theta_2, \ldots, \theta_\lambda$ *are the quadratic residues* $\bmod p$ *in a certain order.*

REMARK. Since $p\tilde{s} \equiv p\bar{s} \pmod{p^2}$, it is clear that Theorem A follows from Theorem B.

PROOF OF THEOREM B. We start from the identity

$$1 - \frac{1}{2} + \frac{1}{3} - \ldots + \frac{(-1)^{n-1}}{n} = \sum_{s=1}^{n} (-1)^{s-1} \binom{n}{s} \frac{2^s - 1}{s}. \tag{1}$$

This identity is easily established through induction. Take $n = p$ in this identity and use the fact that $\binom{p}{s} = \frac{p}{s}\binom{p-1}{s-1}$; we get

$$1 - \frac{1}{2} + \frac{1}{3} - \ldots - \frac{1}{p-1} - \frac{2^p - 2}{p} = p \sum_{s=1}^{p-1} (-1)^{s-1} \binom{p-1}{s-1} \frac{2^s - 1}{s^2}. \tag{2}$$

Since $\binom{p-1}{s-1} \equiv (-1)^{s-1} \pmod{p}$, the identity (2) implies that the numerator of the fraction (in reduced form)

$$1-\frac{1}{2}+\frac{1}{3}-\ldots-\frac{1}{p-1}-\frac{2^p-2}{p}-p\sum_{s=1}^{p-1}\frac{2^s-1}{s^2} \tag{3}$$

is divisible by p^2. Multiplying the fraction (3) by $[(p-1)!]^2$ we find that p^2 divides the integer

$$\tilde{1}-\tilde{2}+\tilde{3}-\ldots-\widetilde{p-1}-\frac{2^p-2}{p}-p\sum_{s=1}^{p-1}(2^s-1)\bar{s}^2 \tag{4}$$

where $\bar{s}$ denotes inverse of $s \bmod p$.

But it is well known that [1]

$$\tilde{1}-\tilde{2}+\tilde{3}-\ldots-\widetilde{p-1} \equiv 2(\tilde{1}+\tilde{3}+\ldots+\widetilde{p-2}) \pmod{p^2}$$

and that

$$\overline{1^2}+\overline{2^2}+\ldots+\overline{p-1^2} \equiv 0 \pmod{p}.$$

Using these informations in (4) we find that the integer

$$2(\tilde{1}+\tilde{3}+\ldots+\widetilde{p-2})-\frac{2^p-2}{p}-2p\sum_{s=1}^{p-1}2^{s-1}\bar{s}^2$$

is divisible by p^2. Cancelling the factor 2 and multiplying by p we find that

$$2^{p-1} \equiv 1+p(\tilde{1}+\tilde{3}+\ldots+\widetilde{p-2})-p^2\sum_{s=1}^{p-1}2^{s-1}\bar{s}^2 \pmod{p^3}. \tag{5}$$

By Euler's criterion, $2^{(p-1)/2} \equiv \left(\frac{2}{p}\right) \pmod{p}$ i.e. $2^\lambda \equiv \left(\frac{2}{p}\right) \pmod{p}$. Hence $2^{\lambda+1} \equiv$

$\equiv 2\left(\frac{2}{p}\right)$, $2^{\lambda+2} \equiv 2^2\left(\frac{2}{p}\right)$, ..., $2^{p-2} \equiv 2^{(p-3)/2}\left(\frac{2}{p}\right) \pmod{p}$. This implies

$$\sum_{s=1}^{p-1}2^{s-1}\bar{s}^2 = \sum_{s=1}^{\lambda}2^{s-1}\bar{s}^2+\sum_{s=1}^{\lambda}2^{\lambda+s-1}\overline{(\lambda+s)^2} \equiv \sum_{1}^{\lambda}2^{s-1}\bar{s}^2+\sum_{1}^{\lambda}2^{s-1}\left(\frac{2}{p}\right)\overline{(\lambda+s)^2} \equiv$$

$$\equiv \sum_{1}^{\lambda}\left\{\bar{s}^2+\left(\frac{2}{p}\right)\overline{(\lambda+s)^2}\right\}2^{s-1} \equiv \sum_{1}^{\lambda}\left\{\bar{s}^2+\left(\frac{2}{p}\right)\overline{(\lambda-s+1)^2}\right\}2^{s-1} \pmod{p}$$

since $\lambda+s \equiv -(\lambda-s+1) \pmod{p}$. Let $\theta_1, \theta_2, \ldots, \theta_\lambda$ be the residues of $\overline{1^2}, \overline{2^2}, \ldots$ $\ldots, \overline{\lambda^2} \bmod p$, in this order. It is clear then that $\theta_1, \theta_2, \ldots, \theta_\lambda$ are the quadratic

residues modulo p. Moreover, from what precedes,

$$\sum_{s=1}^{p-1} 2^{s-1}\bar{s}^2 \equiv \sum_{s=1}^{\lambda}\left\{\theta_s+\left(\frac{2}{p}\right)\theta_{\lambda-s+1}\right\}2^{s-1} \pmod{p}.$$

Using this in (5) we get Theorem B.

References

[1] G. H. Hardy and E. M. Wright, *An Introduction to Number Theory*, Oxford Univ. Press (1959).

(Received August 8, 1983)

DEPARTMENT OF MATHEMATICS
NORTH EASTERN HILL UNIVERSITY
BIJNI CAMPUS, LAITUMKHRAH
SHILLONG 793 003, MEGHALAYA, INDIA