SOME CONGRUENCE THEOREMS

BY P. KESAVA MENON
(*Annamalai University*)

Received January 26, 1942
(Communicated by Dr. A. Narasinga Rao)

1. In two papers entitled "A Theorem on Congruence" I have proved the theorem :

if p be an odd prime, then

$$\sum_{i=1}^{p-1} n^{p-1} - p - (p-1)! \equiv 0 \pmod{p^2}$$

and its generalization:

if $n_1, n_2, \ldots, n_\phi$ $[\phi = \phi(m)]$ be a reduced residue system, (mod m), then

$$\sum_{r=1}^{\phi} n_r^{\phi} \pm \phi . \quad n_1 n_2 \ldots n_r \equiv 0 \pmod{m^2},$$

where the positive sign is to be chosen when $m = 4$, p^n *or* $2p^n$, p being an odd prime, and the negative sign when m has any other value.

The first of these results has been previously obtained by M. Lerch in a paper entitled "Zur Theorie des Fermatschen Quotienten" by a method which is practically the same as that employed to obtain the second result. In the same paper Lerch proves a number of other Congruence relations some of which are similar to those proved in this paper.

The results of this paper are obtained by the same method as that by which the second of the above results was obtained.

2. Let the numbers p_i $(i = 1, 2, \ldots\ldots, k)$ satisfy the following conditions :

$$p_i^l \equiv r_i \pmod{m} \quad (i = 1, 2, \ldots k)$$

$$p_1 p_2 \ldots p_k \equiv a \pmod{m}.$$

Then we have

THEOREM 1.

$$\left(1 - k + \sum_{i=1}^{l} p_i^l / r_i\right) \prod_{i=1}^{k} r_i \equiv a^{l-1} \left\{(1-l)\, a + l \prod_{i=1}^{k} p_i\right\}, \pmod{m^2}$$

PROOF :

$$\prod_{i=1}^{k} (x + p_i^l) = \prod_{i=1}^{k} (x + r_i + p_i^l - r_i)$$

$$\equiv \left[1 + \sum_{i=1}^{k} \frac{p_i^l - r_i}{x + r_i}\right] \prod_{i=1}^{k} (x + r_i), \pmod{m^2}.$$

Putting $x = 0$ we get

$$\left(\prod_{i=1}^{k} p_i\right)^l \equiv \left[1 - k + \sum_{i=1}^{k} p_i^l / r_i\right] \prod_{i=1}^{k} r_i, \pmod{m^2}.$$

But

$$\prod_{i=1}^{k} p_i = \lambda m + a$$

λ being an integer, so that

$$\{\Pi\, p_i\} = (\lambda m + a)^l$$

$$\equiv a^l + l\lambda m\, a^{l-1}, \pmod{m^2}$$

$$\equiv a^l (1 - l) + l\, a^{l-1} \prod_{i=1}^{k} p_i, \pmod{m^2},$$

whence we get the required result.

THEOREM 2. If e be the exponent of p modulo the prime m,

$$(p^{e^2} - 1)/(p^e - 1) \equiv (-1)^{e-1}\, e\, p^{\frac{e(e-1)}{2}}, \pmod{m^2}.$$

PROOF : Take $p_i \equiv p^{i-1}$ and $k = l = e$ in Theorem 1. Then

$$\Pi\, p_i = p^{\frac{(e-1)e}{2}} \equiv (-1)^{e-1} \pmod{m},$$

so that $a = (-1)^{e-1}$, and $r_i = 1$.

Therefore

$$1 - e + \frac{p^{e^2} - 1}{p^e - 1} \equiv 1 - e + (-1)^{e-1}\, e\, p^{\frac{e(e-1)}{2}}, \pmod{m^2}$$

from which we get the required result.

Let $\left(\frac{i}{p}\right)$ be Legendre's symbol equal to $+1$ if i be a quadratic residue of the prime p and to -1 if i be a quadratic non-residue of p. Then we have

THEOREM 3. If p be prime and x be prime to p,

$$(x^{(p-1)^2} - 1)/(x^{p-1} - 1) \equiv \left(\frac{x}{p}\right) (p - 1)\, x^{(p-1)(p-2)/2}, \pmod{p^2}.$$

PROOF : Take $p_i = x^{i-1}$ and $k = l = p-1$ in Theorem 1. Then

$$\prod_{i=1}^{p-1} p_i = x^{(p-2)(p-1)/2} \equiv \left(\frac{x}{p}\right)^{p-2} \equiv \left(\frac{x}{p}\right), \text{ (mod } p),$$

so that $a = \left(\frac{x}{p}\right)$.

Also, by Fermat's Theorem, $r_i = 1$. Therefore

$$1-(p-1)+\frac{x^{(p-1)^2}-1}{x^{p-1}-1} \equiv 1-(p-1)+\left(\frac{x}{p}\right)(p-1)\prod_{i=1}^{p-1} x^{i-1}, \text{ (mod } p^2),$$

whence the theorem follows.

THEOREM 4. If p be an odd prime, then

$$\sum_{i=1}^{p-1} \left(\frac{i}{p}\right) i^{\frac{p-1}{2}} \equiv \frac{p-1}{2}\left\{1-(p-1)\,!\right\} \text{ (mod } p^2).$$

PROOF : Take $p_i = i$, $l = \frac{p-1}{2}$, $k = p-1$ in Theorem 1.

Then we have

$$p_i^l \equiv \left(\frac{i}{p}\right) \text{ (mod } p)$$

and

$$\prod_{i=1}^{p-1} p_i \equiv -1 \text{ (mod } p), \text{ by Wilson's Theorem.}$$

so that $\quad r_i = \left(\frac{i}{p}\right)$, $a = -1$ and $\Pi\, r_i = (-1)^{\frac{p-1}{2}}$.

Therefore

$$\left[1-(p-1)+\sum_{i=1}^{p-1}\left(\frac{i}{p}\right) i^{\frac{p-1}{2}}\right](-1)^{\frac{p-1}{2}} \equiv$$

$$(-1)^{\frac{p-1}{2}}\left[\left(1-\frac{p-1}{2}\right)-\frac{p-1}{2}(p-1)\,!\right], \text{ (mod } p^2).$$

From this we get the required result.

THEOREM 5. If p be an odd prime and α runs through the quadratic residues of p, then

$$\Sigma\, \alpha^{\frac{p-1}{2}} + (-1)^{\frac{p-1}{2}} \frac{p-1}{2}\, \Pi\, \alpha \equiv 0 \text{ (mod } p^2).$$

PROOF : In Theorem 1 take the p_i's to be the α's so that

$$k = \frac{p-1}{2}, \text{ and } l = \frac{p-1}{2}. \quad \text{Then}$$

$$\alpha^{\frac{p-1}{2}} \equiv 1 \text{ (mod } p)$$

and

$$\Pi\, \alpha \equiv (-1)^{\frac{p+1}{2}} \text{ (mod } p).$$

Therefore

$$\left(1-\frac{p-1}{2}+\Sigma\, a^{\frac{p-1}{2}}\right) \equiv 1-\frac{p-1}{2}+(-1)^{\frac{p+1}{2}}\frac{p-1}{2}\,\Pi\, a \pmod{p^2}$$

from which the theorem follows.

In a similar manner we may prove

THEOREM 6. If β runs through the quadratic non-residues of an odd prime p, then

$$\Sigma\, \beta^{\frac{p-1}{2}}+(-1)^{\frac{p-1}{2}}\frac{p-1}{2}\,\Pi\, \beta \equiv 0 \pmod{p^2}$$

From Theorems 4, 5 and 6 we get

THEOREM 7. If α, β run through the quadratic residues and the quadratic non-residues respectively of an odd prime p, then

$$(p-1)\,! \equiv 1+(-1)^{\frac{p-1}{2}}\left[\Pi\, \alpha-\Pi\, \beta\right], \pmod{p^2}.$$

3. We require the following

Lemma.—Let a_1, $a_2, \ldots,$ a_k be all divisible by m. Then

$$(1-a_1)\,(1-a_2)\ldots(1-a_k) \equiv 1-\sum_{i=1}^{k} a_i \pmod{m^2}.$$

THEOREM 8. If p be an odd prime,

$$\left\{1\,!\;2\,!\;3\,!\ldots(p-1)\,!\right\}^2 \equiv \frac{(-1)^{\frac{p-1}{2}}}{p-1}, \bmod p^2.$$

PROOF : We know that

$$1+\frac{(-1)^{i-1}}{(p-i)\,!\,(i-1)\,!} \equiv 0 \pmod{p} \quad (i=1, 2, \ldots, p-1).$$

Take $\quad a_i=1+\dfrac{(-1)^{i-1}}{(p-i)\,!\,(i-1)\,!}$, $k=p$ in the lemma.

Then we have

$$\prod_{i=1}^{p}\frac{(-1)^{i}}{(p-i)\,!\,(i-1)\,!} \equiv 1-p, \pmod{p^2},$$

since
$$\sum_{i=1}^{p}\frac{(-1)^{i-1}}{(p-i)\,!\,(i-1)\,!}=0.$$

i.e.,

$$\frac{(-1)^{\frac{p(p+1)}{2}}}{\{1\,!\;2\,!\cdots(p-1)\,!\}^2} \equiv 1-p, \bmod p^2$$

from which the required result follows.

It will be noticed that Theorem 8 gives a necessary and sufficient condition for p to be an odd prime.

Theorem 8 may also be proved as follows :—

$$1\,!\;2\,!\ldots.(p-1)\,!=(p-1)\;(p-2)^2\;(p-3)^2\ldots.2^{p-2}.\;1^{p-1}$$

$$\text{Now}\quad p-1\equiv 1\;(p-1)\;(\text{mod }p^2)$$

$$(p-2)^2\equiv\;-2^2\,(p-1)\;(\text{mod }p^2)$$

$$(p-i)^i\equiv(-1)^{i-1}\,i^i\;(p-1)\;(\text{mod }p^2)$$

$$\text{so that}\quad (p-1)\,(p-2)^2\ldots.(p-i)^i\equiv(-1)^{\frac{(i-1)\,i}{2}}1\cdot 2^2\cdot 3^3\ldots.\;i^i\;(p-1)^i\;(\text{mod }p^2),$$

$$\{(p-1)\;(p-2)^2\ldots.(p-i)^i\}^2\equiv(1\cdot 2^2\cdot 3^3\ldots.i^i)^2\,(p-1)^{2i}\;(\text{mod }p^2)$$

Taking $i=\frac{p-1}{2}$ and multiplying both sides by

$$\left\{1^{p-1}.2^{p-2}\ldots.\left(\frac{p-1}{2}\right)^{\frac{p+1}{2}}\right\}^2$$

we get

$$[1\,!\,2\,!\ldots.(p-1)\,!]^2\equiv\left(\frac{p-1}{2}\,!\right)^{2p}(p-1)^{p-1},(\text{mod }p^2).$$

If p be an odd prime

$$\left(\frac{p-1}{2}\,!\right)^2+(-1)^{\frac{p-1}{2}}\equiv 0\;(\text{mod }p),$$

$$\text{so that}\;\left(\frac{p-1}{2}\,!\right)^{2p}\equiv\left[\left(\frac{p-1}{2}\,!\right)^2+(-1)^{\frac{p-1}{2}}-(-1)^{\frac{p-1}{2}}\right]^p$$

$$\equiv(-1)^{\frac{p+1}{2}}\;(\text{mod }p^2),$$

$$\text{and}\;\;(p-1)^{p-1}\equiv\frac{-1}{p-1}\;(\text{mod }p^2),$$

whence we get Theorem 8.

From Theorem 8 we readily get

THEOREM 9. The necessary and sufficient condition that p be an odd prime of the form $1+x^2$ is $1\,!\;2\,!\ldots.(p-1)\,!\equiv\frac{\pm 1}{\sqrt{p-1}}$ mod p^2.

If $a_i\equiv 0$ (mod m) ($i=1, 2, \ldots. k$) we have $\Pi\;(1-a_i)\equiv 1-\Sigma\,a_i+\Sigma\,a_i\,a_j$, (mod m^3).

Therefore taking $a_i \equiv 1 + \frac{(-1)^{i-1}}{(p-i)!\,i!}$, we get, as for Theorem 8,

THEOREM 10. If p be an odd prime

$$\frac{(-1)^{\frac{p-1}{2}}}{\left\{1!\,2!\,3!\ldots\left(\frac{p-1}{2}\right)!\right\}^2} \equiv \frac{p-1\,(p-2)}{2} - \frac{(2p-2)!}{\{(p-1)!\}^4}, \pmod{p^3}.$$

REFERENCES

"A Theorem on Congruence," *Journal of the Indian Mathematical Society*, 1937, **2** (New Series).

"A Theorem on Congruence," *The Mathematics Student*, 1940, **8**, No. 4.

Zur Theorie des Fermatschen Quotienten," *Math. Annalen*, **60**, 471–90.