SOME THEOREMS ON RESIDUES*

By P. Kesava Menon

(*Annamalai University*)

Received March 23, 1942

(Communicated by Dr. A. Narasinga Rao, F.A.Sc.)

In this paper an attempt is made to throw more light on the following statement of Hardy and Wright in their book *Introduction to the Theory of Numbers*.

"Fermat's and Wilson's theorems show that 2^{p-1} and $(p-1)!$ have the residues 1 and -1, mod p (p being prime). Little is known about their residues, mod p^2, but they can be transformed in interesting ways."

Theorems 1 to 4, under some restrictions, give such transformations for general values of the modulus m. Theorems 5 and 6 are equivalents of Gauss' lemma regarding $\left(\frac{n}{p}\right)$. The remaining theorems give results of these types.

THEOREM 1. Let m, n and d be integers such that $m-1=nd$. Then

$$\frac{d^{\phi(m)}-1}{m} \equiv \frac{1}{d}\,\Sigma\,\frac{\left\langle \frac{x}{n}\right\rangle}{x}, \text{ mod } m$$

where $<x>$ denotes the smallest integer greater than or equal to x, and the summation is for all x less than and prime to m.

Proof.—Consider the array

$$\begin{array}{lll}
1 & d+1 \cdots\cdots\cdots & (n-1)\,d+1 \\
2 & d+2 & (n-1)\,d+2 \\
3 & \cdot & \cdot \\
\cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot \\
d & 2d & nd
\end{array}$$

from which all numbers not prime to $m\,[=nd+1]$ are removed. Let the product of the elements of the ith row be denoted by $\Pi'_j\,(i+jd)$. Then

* I am thankful to the referee for some very helpful suggestions.

we have

$$\prod_j{}' (i+jd) = \prod_j{}' \{i(nd+1) - d(ni-j)\}$$

$$= \left\{\prod_j{}' (-d)(ni-j)\right\} \prod_j{}' \left\{1 - \frac{im}{d(ni-j)}\right\}$$

$$\equiv \left\{\prod_j{}' (-d)(ni-j)\right\} \left\{1 - \frac{im}{d} \sum_j{}' \frac{1}{ni-j}\right\}, \bmod m^2$$

where, Σ' denotes summation over such values of $j < n$ for which $ni-j$ is prime to m. Taking the product for $i = 1, 2, 3, \ldots d$ it is easily seen that

$$\Pi a \equiv (-d)^{\phi(m)}\, \Pi a \prod_{i=1}^{d} \left\{1 - \frac{im}{d} \sum_j{}' \frac{1}{ni-j}\right\}, \bmod m^2$$

$$\equiv (-d)^{\phi(m)}\, \Pi a \left\{1 - \frac{m}{d} \sum_{i,j}{}' \frac{i}{ni-j}\right\}, \bmod m^2,$$

where Πa denotes the product of all numbers less than m and prime to it.

Therefore

$$1 \equiv (-d)^{\phi(m)} \left\{1 - \frac{m}{d} \sum_{i,j}{}' \frac{i}{ni-j}\right\}, \bmod m^2.$$

On writing $d^{\phi(m)} = 1 + \lambda m$, this gives

$$1 \equiv 1 + m\left\{\lambda - \frac{1}{d} \sum_{i,j}{}' \frac{i}{ni-j}\right\}, \bmod m^2,$$

so that

$$\lambda \equiv \frac{1}{d} \sum_{i,j}{}' \frac{i}{ni-j}, \bmod m$$

i.e.,
$$\frac{d^{\phi(m)} - 1}{m} = \frac{1}{d} \Sigma \frac{\left\langle \frac{x}{n} \right\rangle}{x}, \bmod m.$$

Corollary 1.—If m is prime and $m-1 = nd$, then

$$\frac{d^m - d}{m} \equiv \sum_{i=1}^{d} i\left(\frac{1}{ni} + \frac{1}{ni-1} + \ldots + \frac{1}{ni-n+1}\right), \bmod m.$$

Corollary 2.—Taking $d = 2$ in Theorem 1, which is possible if m is odd, we get

$$\frac{2^{\phi(m)} - 1}{m} \equiv \frac{1}{2}\left[\sum_j{}' \frac{1}{n-j} + 2 \sum_j{}' \frac{1}{2n-j}\right], \bmod m.$$

But $\displaystyle\sum_j{}' \frac{1}{2n-j} \equiv -\sum_j{}' \frac{1}{n-j}, \bmod m,$

so that, if m is odd,

$$\frac{2^{\phi(m)}-1}{m} = -\frac{1}{2}\sum_j{}' \frac{1}{n-j}, \bmod m,$$

$$= -\frac{1}{2}\Sigma\frac{1}{x}, \bmod m.$$

where Σ denotes summation over all x less than $\frac{m}{2}$ and prime to m.

Corollary 3.—Taking $d=3$ in Theorem 1, which is possible if m is of the form $3n+1$, we get

$$\frac{3^{\phi(m)}-1}{m} \equiv \frac{1}{3}\left[\sum_j{}' \frac{1}{n-j} + 2\sum_j{}' \frac{1}{2n-j} + 3\sum_j{}' \frac{1}{3n-j}\right] \bmod m.$$

It is easily seen that

$$\sum_j{}' \frac{1}{3n-j} \equiv -\sum_j{}' \frac{1}{n-j}, \bmod m$$

and

$$\sum_j{}' \frac{1}{2n-j} \equiv 0, \bmod m.$$

Therefore

$$\frac{3^{\phi(m)}-1}{m} \equiv -\frac{2}{3}\sum_j{}' \frac{1}{n-j}, \bmod m$$

$$= -\frac{2}{3}\,\Sigma\,\frac{1}{x}, \bmod m$$

where m is of the form $3n+1$, and Σ denotes summation over all $x < \frac{m}{3}$ and prime to m.

THEOREM 2. Let $m+1=nd$, and $[x]$ the greatest integer $\leqslant x$. Then

$$\frac{d^{\phi(m)}-1}{m} \equiv \frac{1}{d}\Sigma\frac{\left[\frac{x}{n}\right]}{x}, \bmod m.$$

This is proved exactly like Theorem 1, by observing that

$$\prod_j{}' (i+jd) = \prod_j{}' \{-i(nd-1)+d(ni+j)\}, \begin{pmatrix} i=1, 2, \ldots, d-1 \\ j<n \end{pmatrix}$$

and $\prod_j{}' (1+j)\,d = d^{\phi(m,n)} \times \prod_j{}' (j+1)$,

where $\phi(m,n)$ denotes the number of numbers not greater than n and prime to m.

Corollary.—Take $d=3$. Then

$$\frac{3^{\phi(m)}-1}{m} \equiv \frac{1}{3}\left[\sum_j{}' \frac{1}{n+j} + 2\sum_j{}' \frac{1}{2n+j}\right], \bmod m.$$

But $$\sum_j' \frac{1}{n+j} \equiv 0, \text{ mod } m$$

and $$\sum_j' \frac{1}{2n+j} \equiv -\sum_j' \frac{1}{n-j-1}, \text{ mod } m.$$

Therefore, if m is of the form $3n-1$,

$$\frac{3^{\phi(m)}-1}{m} \equiv -\frac{2}{3}\sum_j' \frac{1}{n-j-1}, \text{ mod } m$$

$$=-\frac{2}{3}\Sigma\frac{1}{x}, \text{ mod } m,$$

where Σ denotes summation over all $x < \frac{m}{3}$ and prime to m.

We therefore see that Corollary 3 of Theorem 1 is true for all values of m prime to 3.

THEOREM 3. If α runs through all numbers less than m and prime to it and β through all numbers less than $\frac{m}{2}$ and prime to m, and m is odd, then

$$\Pi\alpha \equiv (-1)^{\frac{1}{2}\phi(m)} (\Pi\beta)^2 \, 2^{2\phi(m)}, \text{ mod } m^2.$$

This can be proved in the same way as theorem 133 of Hardy and Wright's book, making use of Corollary 2 of Theorem 1 in the place of the more particular result used there.

THEOREM 4. If α, β, γ run through all numbers prime m and are such that $\alpha < m$, $\beta < \frac{2m}{3}$ and $\gamma < \frac{m}{3}$ and $\phi\,(m, n)$ denotes the number of numbers not greater than n and prime to m, and m is prime to 3, then

$$\Pi\alpha \equiv (-1)^{\phi(m,\, m/3)} \tfrac{1}{2}\, \Pi\beta\cdot\Pi\gamma\, \{3^{\phi(m)+1}-1\}, \text{ mod } m^2.$$

First, let us assume that $m = 3n+1$.

Then, if Π' denotes the product for numbers prime to m, and $j < n$,

$$\prod_j' (1+3j) = \prod_j' \{(3n+1) - 3\,(n-j)\}$$

$$\equiv \left\{\prod_j' (-3)\,(n-j)\right\} \left\{1-\frac{m}{3}\sum' \frac{1}{n-j}\right\}, \text{ mod } m^2$$

and $\prod_j' (2+3j) = \prod_j' \{(m+3\,(n+j+1\})$

$$\equiv \left\{\prod_j' 3\,(n+j+1)\right\} \left\{1-\frac{m}{3}\sum_j' \frac{1}{n+j+1}\right\}, \text{ mod } m^2.$$

Therefore

$$\Pi'_j (1+3j)\, \Pi'_j (2+3j)\, \Pi'_j (3+3j) \equiv (-1)^{\phi(m,n)}\, 3^{\phi(m)}\, \Pi'_j (n-j)\, \Pi'_j (n+j+1) \times$$
$$\times\, \Pi'_j (1+j) \left\{1 - \frac{m}{3}\left(\Sigma'_j \frac{1}{n-j} + \Sigma'_j \frac{1}{n+j+1}\right)\right\}, \text{ mod } m^2.$$

But $\Sigma'_j \dfrac{1}{n+j+1} \equiv 0 \text{ mod } m,$

and hence we get the required result for $m = 3n+1$ by making use of Corollary 3 of Theorem 1 and the fact that $3^{\phi(m)} \equiv 1$ mod m.

The case $m = 3n-1$ can be treated as above, using corollary of Theorem 2.

THEOREM 5. If $m - 1 = 2nd$, then $d^{\phi(m)/2} \equiv (-1)^{\nu}$ mod m,

where

$$\nu = \begin{cases} \sum\limits_{i=1}^{n} \left\{\phi\left(m, \frac{2i-1}{2} d\right) - \phi(m, id)\right\} & \text{if } d \text{ is even} \\ \sum\limits_{i=1}^{n} \left\{\phi\left(m, \frac{(2i-1)d - 1}{2}\right) - \phi(m, id)\right\} & \text{if } d \text{ is odd.} \end{cases}$$

Alternately, ν may be given by the relations

$$\nu = \begin{cases} \sum\limits_{i=1}^{d/2} [\phi(m, 2ni) - \phi\{m, 2(i-1)n\}] & \text{if } d \text{ is even} \\ \sum\limits_{i=1}^{(d-1)/2} [\phi(m, 2ni) - \phi\{m, 2(i-1)n\}] & \text{if } d \text{ is odd.} \end{cases}$$

Proof.—Consider the array

$$\begin{array}{llll} 1 \quad d+1 & 2d+1 \ldots\ldots & (n-1)\,d+1 \\ 2 \quad d+2 & 2d+2 & (n-1)\,d+2 \\ 3 \quad \cdot & \cdot & \cdot \\ \cdot \quad \cdot & \cdot & \cdot \\ \cdot \quad \cdot & \cdot & \cdot \\ \cdot \quad \cdot & \cdot & \cdot \\ d \quad 2d & 3d & nd \end{array}$$

from which all numbers not prime to m are removed. If we denote the product of the elements of the ith row by $\Pi'_j (i+jd)$ it is clear that j runs through all values from 0 to $n-1$ such that $i+jd$ is prime to m. We have

$$\Pi'_j (i+jd) \equiv \Pi'_j \{im - d(2ni-j)\}$$
$$\equiv \Pi'_j (-d)(2ni-j), \text{ mod } m.$$

Similarly

$$\Pi'_j \{d-i+jd\} = \Pi'_j \{d(2in+j+1)-im\}$$
$$\equiv \Pi'_j \{d(2ni+j+1)\}, \text{ mod } m.$$

Therefore

$$\prod_{i=1}^{k} \Pi'_j (i+jd) \prod_{i=0}^{d-k-1} \Pi'_j (d-i+jd)$$
$$\equiv \prod_{i=1}^{k} \Pi'_j (-d)(2ni-j) \prod_{i=0}^{d-k-1} \Pi'_j (d)(2ni+j+1), \text{ mod } m.$$

Taking $k = d/2$ or $(d-1)/2$ according as d is even or odd we get

$$\Pi a = (-1)^{\nu} d^{\phi\frac{1}{2}(m)} \Pi a, \text{ mod } m,$$

where a runs through the numbers prime to m and not greater than $m/2$. Dividing both sides by Πa we get the required result.

In a similar manner we may prove

THEOREM 6. If $m+1 = 2nd$,

$$d^{\frac{1}{2}\phi(m)} \equiv (-1)^{\mu} \text{ mod } m,$$

where $\mu = \begin{cases} \sum_{i=1}^{n} \left\{\phi(m, id-1) - \phi\left(m, \frac{2i-1}{2} d - 1\right)\right\}, & \text{if } d \text{ is even} \\ \sum_{i=2}^{n} \left\{\phi(m, id-1) - \phi\left(m, \frac{\overline{2i-1}\, d-1}{2}\right)\right\}, & \text{if } d \text{ is odd.} \end{cases}$

As corollaries of Theorems 5 and 6 we get,

THEOREM 7. If $m = 2nd + 1$ be prime, then to the modulus m

$$d^{\frac{m-1}{2}} \equiv (-1)^{\frac{m-1}{4}}, \text{ if } d \text{ is even}$$
$$\equiv (-1)^{n(d-1)/2}, \text{ if } d \text{ is odd;}$$

and

THEOREM 8. If $m = 2nd - 1$ be prime, then to the modulus m

$$d^{\frac{m-1}{2}} \equiv (-1)^{\frac{m+1}{4}}, \text{ if } d \text{ is even}$$
$$\equiv (-1)^{n(d-1)/2}, \text{ if } d \text{ is odd.}$$

By combining the methods of Theorems 1 and 5 we get

THEOREM 9. If residues are taken to the modulus $m = 2nd + 1$, and

$\langle x \rangle$ and $[x]$ are as in Theorems 1 and 2.

$$\frac{(-1)^{\nu}\, d^{\frac{1}{2}\phi(m)}-1}{m} \equiv \frac{1}{d}\,\Sigma\,\frac{\left\{\frac{x}{2n}\right\}}{x} \bmod m,$$

where the summation is for all $x < \frac{m}{2}$ and prime to m, and $\left\{\frac{x}{2n}\right\}$ denotes $\left\langle\frac{x}{2n}\right\rangle$ or $\left[\frac{x}{2n}\right]$ according as $\left\langle\frac{x}{n}\right\rangle$ is even or odd, and ν has the same meaning as in Theorem 5;

and

THEOREM 10. If residues are taken to the modulus $m = 2nd - 1$, then

$$\frac{(-1)^{\mu}\, d^{\frac{1}{2}\phi(m)}-1}{m} \equiv \frac{1}{d}\,\Sigma\,\frac{\left[\frac{x}{2n}\right]}{x}, \bmod m,$$

where the summation is for all $x < \frac{m}{2}$ and prime to m, and $\left[\frac{x}{2n}\right]$ denotes $\left[\frac{x}{2n}\right]$ or $\left\langle\frac{x}{2n}\right\rangle$ according as $\left[\frac{x}{n}\right]$ is even or odd, and μ has the same meaning as in Theorem 6.