A congruence equation involving the factorisation in residue class ring mod n.

K. NAGESWARA RAO (New Delhi)

1. Introduction

If n is any integer $\geqq 1$ and r, s are any two non-negative integers, the object of the paper is to obtain the number of solutions $N_{r,s}(a, n)$ in $x_i^{(j)} \pmod{n}$ $(i=1, \ldots, r+1;\ j=0, \ldots, s)$ of the congruence

$$(1.1) \qquad a \equiv a_0 x_1^{(0)} \ldots x_{r+1}^{(0)} + a_1 x_1^{(1)} \ldots x_{r+1}^{(1)} + \ldots + a_s x_1^{(s)} \ldots x_{r+1}^{(s)} \pmod{n}$$

Where $(a_i, n)=1$ $(i=0, \ldots, s)$, in terms of the Ramanujan's sum $C(m, n)$ (see (2. 1)) and establish the related arithmetical identities involving $N_{r,s}(a, n)$ and some known functions. We also establish the multiplicative property of the function $N_{r,s}(a, n)$ in the sense of Vaidyanathaswamy [8; Section I; 1] i.e.

$$(1.2) \qquad N_{r,s}(a_1 a_2, n_1 n_2) = N_{r,s}(a_1, n_1) \cdot N_{r,s}(a_2, n_2).$$

Whenever $(a_1 n_1, a_2 n_2)=1$.

We observe that these results generalise some of the results of GYIRES ([7]) and also COHEN ([6], Theorem 3). In the proofs we use representation theorems due to Cohen ([1]), which in fact simplify the discussion, and also employ Cauchy Composition to evaluate $N_{r,s}(a, n)$.

2. Preliminaries and notation

Let F be a field of characteristic zero containing the nth rooths of unity. We say that an arithmetic function $f(a)$ is said to be (n, F)-arithmetic or simply arithmetic when there is no ambiguity, if it defines a single valued function in F for every rational integer a, with the condition $f(a)=f(a^1)$ for $a \equiv a^1 \pmod{n}$.

Ramanujan's trigonometrical sum $c(m, n)$ is defined by the following formula.

$$(2.1) \qquad c(m, n) = \sum_{(z, n)=1} \varepsilon_z(m)$$

where the summation is over all Z of a reduced residue system $(\bmod n)$ and $\varepsilon_z(m) = e^{\frac{2\pi i z m}{n}}$

E. Cohen ([1]; Theorem 1) has shown that every (n, F)-arithmetic function can be represented uniquely in the form

$$f(a) = \sum_{z \,(\mathrm{mod}\, n)} a_z \varepsilon_z(a) \tag{2.2}$$

where

$$a_z = \frac{1}{n} \sum_{v (\mathrm{mod}\, n)} f(v) \varepsilon_z(-v) \tag{2.3}$$

An (n, F) arithmetic function $f(a)$ is said to be even $(\mathrm{mod}\, n)$, if $f(a) = f(g)$, where $g = (a, n)$, for every integral a. E. Cohen ([2]; Theorem 1) has also shown that an even function $f(a)$ has the unique representation given by

$$f(a) = \sum_{d/n} \alpha_d c(m, d) \tag{2.4}$$

Where

$$\alpha_d = \frac{1}{n} \sum_{\delta/n} f\left(\frac{n}{\delta}\right) c\left(\frac{n}{d}, \delta\right). \tag{2.5}$$

If f and g are two (n, F)-arithmetic functions we define their Cauchy product h by the relation

$$h(m) = \sum_{m \equiv a+b (\mathrm{mod}\, n)} f(a) g(b) \tag{2.6}$$

If f and g are any two (n, F)-arithmetic functions having the representations

$$\begin{aligned} f(m) &= \sum_{z (\mathrm{mod}\, n)} a_z \varepsilon_z(m) \\ g(m) &= \sum_{z (\mathrm{mod}\, n)} b_z \varepsilon_z(m) \end{aligned} \tag{2.7}$$

then their Cauchy product h is given by

$$h(m) = n \sum_{z (\mathrm{mod}\, n)} a_z b_z \varepsilon_z(m) \qquad \text{(see Cohen [1], (2.6))}. \tag{2.8}$$

If f and g are even functions $(\mathrm{mod}\, n)$ and have the representation

$$\begin{aligned} f(a) &= \sum_{d/n} \alpha_d c(a, d) \\ g(a) &= \sum_{d/n} \beta_d c(a, d) \end{aligned} \tag{2.9}$$

then their Cauchy product h is given by

$$h(m) = n \sum_{d/n} \alpha_d \beta_d c(m, d) \qquad \text{(see Cohen [1], (3.10))}. \tag{2.10}$$

We now go to the main results of this paper.

3. Main results

Let $N_r(a, n)$ denote the number of solutions of the congruence in X_i (mod n) $(i=1, \dots, r+1)$

(3. 1) $$a \equiv x_1, \dots, x_{r+1} \pmod n$$

two solutions $X_i \equiv b_i$ and $X_i \equiv c_i$ being considered identical if and only if $b_i \equiv c_i$ (mod n) $(i=1, \dots, r+1)$.

We now have the following theorem.

Theorem 1. *The function* $N_r(a, n)$ *is even* (mod n) i.e.

(3. 2) $$N_r(a, n) = N_r((a, n), n).$$

Proof. It is clear that $N_r(a, n)$ depends on a (mod n) and hence it has the Fourier expansion by (2. 2) and (2. 3)

(3. 3) $$N_r(a, n) = \sum_{z \pmod n} a_z \varepsilon_z(a)$$

Where

$$a_Z = \frac{1}{n} \sum_{u \pmod n} N_r(u, n) \varepsilon_z(-u) = \frac{1}{n} \sum_{u \pmod n} \sum_{x_1 \dots x_{r+1} \equiv u \pmod n} \varepsilon_z(-x_1 \dots x_{r+1}) =$$

(3. 4) $$= \frac{1}{n} \sum_{zx_1 \dots x_r \equiv 0 \pmod n} n = \sum_{zx_1 \dots x_r \equiv 0 \pmod n} 1 =$$

$$= d^r \sum_{x_1 \dots x_r \equiv 0 \left(\bmod \frac{n}{d}\right)} 1, \qquad \text{Where} \qquad (z, n) = d.$$

(see Cohen [1], (2. 2))

$$a_z = d^r N_{r-1}\left(o, \frac{n}{d}\right).$$

This shows that a_z as a function of Z, is even (mod n) and hence so is $N_r(a, n)$. This completes the proof.

We now obtain a recurring relation for $N_r(a, n)$ in terms of the Ramanujan's sum.

Theorem 2.

$$N_r(a, n) = \sum_{d/n} d^r N_{r-1}\left(o, \frac{n}{d}\right) c\left(a, \frac{n}{d}\right)$$

Proof. This is a direct consequence of Theorem 1, since a_z's are even (mod n) as functions of Z.

We now extend the above result as follows.

Let $M_{r,s}(a, n)$ represent the number of solutions of the congruence equation in $x_i^{(j)}$ (mod n) $(i=1, \dots, r+1; j=0, \dots, s)$

(3. 5) $$a \equiv x_1^{(0)} \dots x_{r+1}^{(0)} + \dots + x_1^{(s)} \dots x_{r+1}^{(s)} \pmod n$$

We now evaluate $M_{r,s}(a, n)$. Set $X_i = x_1^{(i)} \dots x_{r+1}^{(i)}$. Now it is clear that

$$M_{r,s}(a,n) = \sum_{a \equiv X_0 + \dots + X_s \pmod n} \prod_{i=0}^{s} N_r(X_i, n) \tag{3.6}$$

But the right side of the equation (3. 6) is the Cauchy product of $(s+1)$ functions $N_r(m, n)$ at $a \pmod n$. Also we have that

$$N_r(a, n) = \sum_{d/n} \alpha_d c(a, d) \tag{3.7}$$

Where

$$\alpha_d = \left(\frac{n}{d}\right)^r N_{r-1}(o, d) \qquad \text{(from Theorem 2)} \tag{3.8}$$

By (2. 9) and (2. 10) we have

$$M_{r,s}(a, n) = n^s \sum_{d/n} \left(\frac{n}{d}\right)^{r(s+1)} N_{r-1}^{s+1}(o, d) c(a, d)$$

Hence we have

Theorem 3. *The number of solutions $M_{r,s}(a, n)$ of the congruence* (3. 5) *is equal to*

$$n^s \sum_{d/n} \left(\frac{n}{d}\right)^{r(s+1)} N_{r-1}^{s+1}(o, d) c(a, d)$$

We note that for $r=1$, this reduces to a result of COHEN ([6], Theorem 3). For similar discussions see also COHEN ([4], § 3, [5], (3. 7)).

Theorem 3 aids us in obtaining the number of solutions of the congruence equation (1. 1).

Theorem 4. The number of solutions of (1. 1) is same as the number of solutions of (3. 5) i.e.

$$N_{r,s}(a, n) = M_{r,s}(a, n).$$

PROOF. Observe that the congruence equation

$$a \equiv a_i x, \dots, x_{r+1} \pmod n \tag{3.9}$$

has the same number of solutions as

$$b_i a \equiv x_1 \dots x_{r+1} \pmod n, \tag{3.10}$$

where

$$a_i b_i \equiv 1 \pmod n. \tag{3.11}$$

So the number of solutions of the congruence (3. 9) is $N_r(ab_i n) = N_r(a, n)$, since $N_r(a, n)$ is even $\pmod n$ and $(ab_i, n) = (a, n)$. Hence the result now follows as on the lines of the proof of Theorem 3.

For a discussion of some other equation of similar nature we refer to COHEN ([3]; Theorems 5 & 6).

We now obtain some identities involving $N_{r,s}(a, n)$.

Let $E(m)=1$ for all integral m, then $E(m)$ is even (mod n) and by (2. 4) and (2. 5), $E(m)$ has the representation given by

$$E(m)=\sum_{d/n}\gamma_\alpha C(m, d). \tag{3. 12}$$

Where

$$\gamma_d=\begin{cases}1 & \text{if} \quad d=1\\ 0 & \text{otherwise.}\end{cases} \tag{3. 13}$$

Now consider the Cauchy product of $N_{r,s}(a, n)$ and $E(m)$ namely

$$\sum_{\substack{m\equiv a+b\\ (\mathrm{mod}\, n)}} N_{r,s}(a, n)E(b)$$

By (2. 9) and (2. 10), this is equal to

$$n\cdot n^s\cdot n^{r(s+1)}\cdot N_{r-1}^{s+1}(o, 1)c(m, 1)$$

But $N_{r-1}(0, 1)\equiv 1$ and also $c(m, 1)\equiv 1$.

$$\sum_{\substack{m\equiv a+b\\ (\mathrm{mod}\, n)}} N_{r,s}(a, n)E(b) = n^{(s+1)(r+1)}. \tag{3. 14}$$

If we put $m=0$ in (3. 14) we obtain the following result:

$$\sum_{a=1}^{n} N_{r,s}(a, n) = n^{(s+1)(r+1)}. \tag{3. 15}$$

Hence, we state the following Theorem which reduces to a result of GYIRES ([7], (9)) when $s=0$.

Theorem 5.

$$\sum_{a=1}^{n} N_{r,s}(a, n) = \sum_{d/n}\Phi\left(\frac{n}{d}\right)N_r(d, n) = n^{(r+1)(s+1)}.$$

We note that the intermediate result follows since $N_{r,s}(a, n)$ is an even function of a (mod n), Φ being Euler's totient.

We now establish the multiplicative property of $N_{r,s}(a, n)$. Let us first obtain a lemma which is useful in establishing the multiplicative property of $N_{r,s}(a, n)$.

Lemma *The function $N_r(a, n)$ is multiplicative.*

The lemma follows by inductive hypothesis on r and from the fact that $C(a, n)$ is multiplicative with respect to both the arguments i.e. $C(a_1 a_2, n_1 n_2)=C(a_1, n_1)$ $C(a_2, n_2)$ whenever $(a_1 n_1, a_2 n_2)=1$ (see VENKATRAMAN [9], § 4).

Now we go to the proof of Theorem 6.

Theorem 6. *The function $N_{r,s}(a, n)$ is multiplicative.*

Let a_1, r_1, a_2, n_2 be integers such that $(a_1 n_1, a_2 n_2) = 1$. If $D|n_1, n_2$ then there exist two integers d_1, d_2 so that $d_1|n_1$, $d_2|n_2$ and $d_1 d_2 = D$.

$$N_{r,s}(a_1 a_2, n_1 n_2) = (n_1 n_2)^s \sum_{d_1 d_2/n_1 n_2} \left(\frac{n_1 n_2}{d_1 d_2}\right)^{r(s+1)} N_{r-1}(o, d_1 d_2) c(a_1 a_2, d_1 d_2) =$$

$$(3.16) \quad = n_1^s n_2^s \sum_{\substack{d_1/n_1 \\ d_2/n_2}} \left(\frac{n_1}{d_1}\right)^{r(s+1)} \left(\frac{n_2}{d_2}\right)^{r(s+1)} N_{r-1}(o, d_1) N_{r-1}(o, d_2) c(a_1, d_2) c(a_2, d_2) =$$

$$= \left[n_1^s \sum_{d_1/n_1} \left(\frac{n_1}{d_1}\right)^{r(s+1)} N_{r-1}(o, d_1) c(a_1, d_1)\right] \left[n_2^s \sum_{d_2/n_2} \left(\frac{n_2}{d_2}\right)^{r(s+1)} N_{r-1}(o, d_2) c(a_2, d_1)\right] =$$

$$= N_{r,s}(a_1, n_1) N_{r,s}(a_1, n_2)$$

This completes the proof.

References

[1] ECKFORD COHEN, Rings of arithmetic functions, *Duke Math. J.* **19** (1952), 115—129.
[2] ECKFORD COHEN, A class of arithmetic functions, *Proc. Nat. Acad. Sci. U.S.A.* **41** (1955), 937—944.
[3] ECKFORD COHEN, An extension of Ramujan sum II. Additi veproperties, *Duke Math. J.* **22** (1955), 543—550
[4] ECKFORD COHEN, Some totient functions, *Duke Math. J.* **23** (1956), 515—522.
[5] ECKFORD COHEN, Representations of even functions (mod r) I. Arithmetical identities, *Duke Math. J.* **25** (1958), 401—421.
[6] ECKFORD COHEN, Trigonometric sums in elementary number theory, *Amer. Math. Monthly* **66** (1959), 105—116.
[7] B. GYIRES, Über die Faktorisation im Restklassenring mod n, *Publ. Math. Debrecen* **1** (1949), 51—55.
[8] R. VAIDYANATHA SWAMY, The theory of multiplicative arithmetic functions, *Trans. Amer. Math. Soc.* **33** (1931), 579—662.
[9] C.'S. VENKATRAMAN, A new identical equation for multiplicative functions of two arguments and its applications to Ramanujan's sum C_M (N), *Proc. Indian Acad. Sci. Sect* A **24** (1946), 518—529.

(Received December 17, 1965.)