Canad. Math. Bull. Vol. **22** (2), 1979

SQUARE-REDUCED RESIDUE SYSTEMS (MOD r) AND RELATED ARITHMETICAL FUNCTIONS

BY

R. SIVARAMAKRISHNAN

ABSTRACT. We define a square-reduced residue system (mod r) as the set of integers $a \pmod r$ such that the greatest common divisor of a and r, denoted by (a, r), is a perfect square ≥ 1 and contained in a residue system (mod r). This leads to a Class-division of integers (mod r) based on the 'square-free' divisors of r. The number of elements in a square-reduced residue system (mod r) is denoted by $b(r)$. It is shown that

(1) $b(r)=\sum_{d \mid r} \lambda(r/d)d$, where $\lambda(r)$ is Liouville's function.

(2) $$b(n)b(r)=\sum_{d \mid (n,r)} b(nr/d^2)d\lambda(d)$$

In view of (2), $b(r)$ is said to be 'specially multiplicative'. The exponential sum associated with a square-reduced residue system (mod r) is defined by

$$B(n, r)=\sum_{\substack{h \pmod r \\ (h,r)=\text{a square}}} \exp(2\pi ihn/r)$$

where the summation is over a square-reduced residue system (mod r).

$B(n, r)$ belongs to a new class of multiplicative functions known as 'Quasi-symmetric functions' and

(3) $$B(n, r)=\sum_{d \mid (n,r)} \lambda(r/d)d=\lambda(r/g)b(g); \quad g=(n, r).$$

As an application, the sum $\sum_{(a,r)=\text{a square}}^{a \pmod r} (a-1, r)$ is considered in terms of the Cauchy-composition of even functions (mod r). It is found to be multiplicative in r. The evaluation of the above sum gives an identity involving Pillai's arithmetic function

$$\beta(r)=\sum_{a \pmod r} (a, r) \quad \text{and } b(r).$$

1. **Introduction.** It is well-known that Euler's function $\phi(r)$ represents the number of elements in a reduced-residue system (mod r). In [1], Eckford Cohen obtains the unitary analogue of $\phi(r)$, by defining a semi-reduced residue system (mod r). The notion of the 'unitary divisor' plays a major role in the derivation of identities connected with the analogue $C^*(n, r)$ [1] of Ramanujan's Sum $C(n, r)$ [5, §5.6].

Received by the editors March 13, 1978 and, in revised form, August 3, 1978.

https://doi.org/10.4153/CMB-1979-028-1 Published online by Cambridge University Press

In this paper, we introduce a third subset of the residue system $S(\bmod r)$ which leads to an interesting analogue of $C(n, r)$ having certain special properties not possessed by either $C(n, r)$ or $C^*(n, r)$. The counter-part of the 'unitary divisor' in this case would be the 'square-free' divisor.

We define a square-reduced residue system (mod r) as follows: For $r \geq 1$, the set K of integers $a(\bmod r)$ such that the greatest common divisor of a and r denoted by (a, r) is a square ≥ 1 and contained in a residue system $S(\bmod r)$ will be designated "the square-reduced residue system (mod r)" contained in S. If S consists of the integers $1, 2, 3, \ldots, r$; then K will be called a least positive square-reduced residue system (mod r). The number of elements in a square-reduced residue system (mod r) is denoted by $b(r)$.

It may be shown that if $f(r)$ is any arithmetic function, then

$$\sum_{a(\bmod r)} f((a, r)) = \sum_{d \mid r} f(d)\phi(r/d) \tag{1.1}$$

In particular, $\beta(r) = \sum_{a(\bmod r)} (a, r)$ [10] has the representation

$$\beta(r) = \sum_{d \mid r} d\phi(r/d) \tag{1.2}$$

If

$$\varepsilon(r) = \begin{cases} 1, & \text{if } r \text{ is a perfect square} \\ 0, & \text{otherwise} \end{cases} \tag{1.3}$$

then $b(r)$ representing the number of integers $a(\bmod r)$ such that (a, r) is a square, may be expressed as

$$b(r) = \sum_{d \mid r} \varepsilon(d)\phi(r/d) = \sum_{tD^2 = r} \phi(t) \tag{1.4}$$

The proposed analogue of $C(n, r)$ is the function $B(n, r)$ defined by

$$B(n, r) = \sum_{\substack{h(\bmod r) \\ (h,r) = \text{a square}}} \exp(2\Pi ihn/r) \tag{1.5}$$

the summation extending over a square-reduced residue system (mod r). Among the applications of the function $b(r)$, we prove in §6 the following identity:
For $r > 1$,

$$\sum_{\substack{a(\bmod r) \\ (a,r) = \text{a square}}} (a-1, r) = \Pi\{\beta(p_i^{a_i}) - b(p_i^{a_i - 1})\} \tag{1.6}$$

where $r = \Pi\, p_i^{a_i}$, p_i being distinct primes and $a_i \geq 1$.

2. **Preliminaries.** An arithmetic function $f(r)$ is said to be *multiplicative* in r, if

$$f(r)f(r')=f(rr') \tag{2.1}$$

whenever $(r, r')=1$. f is said to be *completely multiplicative* if (2.1) holds for all pairs of numbers r, r'.

The Dirichlet Convolution of two functions $f(r)$ and $g(r)$ is defined by

$$(f\cdot g)(r)=\sum_{d\mid r} f(d)g(r/d) \tag{2.2}$$

where d runs through the divisors of r. It is known that the set A of arithmetic functions f for which $f(1)$ is not equal to zero, forms an abelian group under Dirichlet Convolution with identity element $e_0(r)=[1/r]$, where $[x]$ denotes the greatest integer not greater than x. The Dirichlet inverse of $f(r)$ when it exists, is written as $f^{-1}(r)$. We need the following elementary functions:

$$e(r)=1, \qquad r\geq 1 \tag{2.3}$$

$$I(r)=r. \tag{2.4}$$

$$\mu(r)=\begin{cases}1, & \text{if} \quad r=1\\ 0, & \text{if} \quad a^2\mid r, \quad a>1\\ (-1)^k, & \text{if} \quad r=p_1p_2\cdots p_k \ (p_i \text{ being distinct primes})\end{cases} \tag{2.5}$$

It may be easily verified that $\mu(r)=e^{-1}(r)$. Further,

$$\phi(r)=(I\cdot e^{-1})(r) \tag{2.6}$$

$$\lambda(r)=(-1)^{\Omega(r)} \tag{2.7}$$

where $\Omega(r)$ represents the total number of prime factors of r (each being counted according to its multiplicity)

In terms of $\lambda(r)$, $\varepsilon(r)$ (1.3) may be expressed as

$$\varepsilon(r)=(\lambda\cdot e)(r). \tag{2.8}$$

If

$$\delta(r)=\begin{cases}1, & \text{whenever } r \text{ is square-free}\\ 0, & \text{otherwise}\end{cases}$$

we note that

$$\delta(r)=\lambda^{-1}(r) \tag{2.9}$$

This leads to the following *Inversion Formula*:

(2.10) If $f(r)$ is such that $\displaystyle\sum_{\substack{t\mid r\\ t \text{ square-free}}} f(r/t)=g(r)$

https://doi.org/10.4153/CMB-1979-028-1 Published online by Cambridge University Press

then

$$f(r)=(g\cdot\lambda)(r)=\sum_{d\mid r} g(d)\lambda(r/d)$$

If $\Theta(r)$ denotes the number of square-free divisors (including unity) of r, it is known that

$$\Theta(r)=2^{\omega(r)}$$

where $\omega(r)$ is the number of distinct prime factors of r. Also, as

$$\Theta(r)=\sum_{\substack{t\mid r\\ t \text{ square-free}}} e(r/t)$$

we have

$$\Theta(r)=(e\cdot\delta)(r). \tag{2.11}$$

Let $g(r)$ be a completely multiplicative function. If a multiplicative function f is such that

$$f(n)f(r)=\sum_{d\mid(n,r)} f(nr/d^2)g(d) \tag{2.12}$$

where the summation extends over all common divisors d of n, r; f is said to be *specially multiplicative* [8]. It is shown [8] that a specially multiplicative function $f(r)$ is the Dirichlet product of two completely multiplicative functions.

Next, we give some relevant results concerning arithmetic functions of two variables say n, r.

An arithmetic function $f(n,r)$ is said to be *multiplicative* in both the variables n, r if

$$f(n,r)f(n',r')=f(nn',rr') \tag{2.13}$$

whenever $(nr,n'r')=1$. A multiplicative function $f(n,r)$ is determined if the values of $f(p^b,p^a)$ are known; $a\geq 0$, $b\geq 0$; p being a prime. It is obvious that $f(1,1)=1$. Also, $f(1,r)$ is multiplicative in r and $f(n,1)$ is multiplicative in n.

An arithmetic function $f(n,r)$ is said to be an '*even function of* $n \pmod r$' if $f(n,r)=f((n,r),r)$ for all n and $r\geq 1$. Here, we assume $n\geq 1$. It is shown [2, Theorem 1] that $f(n,r)$ is even $(\bmod r)$ if and only if it possesses a Fourier expansion of the form

$$f(n,r)=\sum_{d\mid r}\alpha(d,r)C(n,d) \tag{2.14}$$

where $C(n,r)$ is Ramanujan's Sum and $\alpha(d,r)$ is determined by the formula

$$\alpha(d,r)=\frac{1}{r}\sum_{s\mid r} f(s,r)C(r/d,r/s) \tag{2.15}$$

The *Cauchy-composition* (mod r) [4] of two even functions f and g is defined by

$$h(n, r) = \sum_{n \equiv a+b \pmod r} f(a, r)g(b, r) \tag{2.16}$$

the summation in (2.16) extending over $a, b \pmod r$ such that $n \equiv a + b \pmod r$. If $f(n, r)$ has the representation (2.14) and

$$g(n, r) = \sum_{d \mid r} \beta(d, r)C(n, d) \tag{2.17}$$

then the Cauchy-product h of f and g is given [4, Theroem 1] by

$$h(n, r) = r \sum_{d \mid r} \alpha(d, r)\beta(d, r)C(n, d) \tag{2.18}$$

It is proved in [9, Theorem 3.2] that if f and g are multiplicative in the sense of (2.13), so is their Cauchy-product.

3. **Properties of $b(r)$.** We first observe that any positive integer $a \leq r$ can be uniquely represented in the form $a = tx^2$, where t is a square-free divisor of r and x^2 is contained in a least positive square-reduced residue system (mod r/t). Of course, if a is a square-free divisor of r, we take $x^2 = 1$. Now, $\varepsilon(r)$ (1.3) and $\delta(r)$ (2.9) are multiplicative in r. That is, $\varepsilon(1) = 1$, where 1 is treated as a perfect square. At the same time $\delta(1) = 1$, where 1 is treated as square-free. Therefore, we make a convention that 1 is to be considered as both 'square-free' and 'square-ful'. In other words, 1 is included in the set of square-free divisors of r and simultaneously, as $(1, r) = 1^2 = 1$, 1 is included in the set of integers $a \pmod r$ such that (a, r) is a square.

If $a = tx^2$, where t is a square-free divisor of r, $(a, r) = (tx^2, r) = t(x^2, r/t)$. For fixed t, $(a, r) = t$ will mean $(x^2, r/t)$ is a square including unity. Therefore, the number of integers $a \pmod r$ such that $(a, r) = t$, a fixed square-free divisor of r is precisely $b(r/t)$. This idea is manifested in the following

3.1 THEOREM. *The integers tx^2, where t runs through the square-free divisors of r and for each t, x^2 ranges over a square-reduced residue system* (mod r/t) *constitute a residue system* (mod r).

Proof. Using (1.4)

$$\begin{aligned} b(r) &= (\varepsilon \cdot \phi)(r) \\ &= (\varepsilon \cdot (I \cdot e^{-1})(r) \quad \text{by} \quad (2.6) \\ &= ((\varepsilon \cdot e^{-1}) \cdot I)(r) \end{aligned}$$

As, $(\lambda \cdot e)(r) = \varepsilon(r)$ (2.8) we get

$$b(r) = ((\lambda \cdot e \cdot e^{-1}) \cdot I)(r)$$
$$= (\lambda \cdot e_0 \cdot I)(r)$$
$$= (\lambda \cdot I)(r)$$

Or,

$$(b \cdot \lambda^{-1})(r) = I(r)$$

But, $\lambda^{-1}(r) = \delta(r)$ (2.9). Therefore,

$$\sum_{\substack{t \mid r \\ t \text{ square-free}}} b(r/t) = r$$

Hence, as t runs through the square-free divisors of r including unity, the integers tx^2 such that x^2 ranges over a square-reduced residue system (mod r/t) will exhaust the residue system (mod r).

COROLLARIES.
(3.1.1) *The function* $b(r)$ *is multiplicative in* r *and* $b(r) = (I \cdot \lambda)(r)$.
(3.1.2) $b(r)$ *is specially multiplicative in the sense of* (2.12).

For, $b(r)$ *is the Dirichlet product of the two completely multiplicative functions* $I(r)$ *and* $\lambda(r)$. *Therefore, by* [8, Theorem 3.2] (3.1.2) *follows.*

(3.1.3) $$b(n)b(r) = \sum_{d \mid (n, r)} b(nr/d^2) d\lambda(d)$$

Proof of (3.1.3). As $b(r) = (I \cdot \lambda)(r)$, the completely multiplicative function $g(r)$ associated with $b(r)$ is given [8, Theorem 3.2] by $g(r) = I(r)\lambda(r)$. So, (3.1.3) is deduced from (2.12) with $f(r) = b(r)$ and $g(r) = I(r)\lambda(r)$.

3.2 THEOREM. *If* $f(r)$ *is any arithmetic function, then*

$$\sum_{\substack{a \pmod r \\ (a,r) = \text{a square}}} f((a, r)) = \sum_{\substack{t \mid r \\ t \text{ square-free}}} f(t) b(r/t)$$

Proof is omitted as it is a direct consequence of Theorem 3.1.

COROLLARY.

(3.2.1) $$\sum_{\substack{a \pmod r \\ (a,r) = \text{a square}}} (a, r) = \sum_{d \mid r} d\Theta(d)\lambda(r/d)$$

where $\Theta(r)$ is the number of square-free divisors of r.

https://doi.org/10.4153/CMB-1979-028-1 Published online by Cambridge University Press

Proof of (3.2.1). Using Theorem 3.2, we have

$$\sum_{\substack{a \pmod r \\ (a,r)=\text{a square}}} (a, r) = \sum_{\substack{t \mid r \\ t \text{ square-free}}} tb(r/t)$$
$$= (I\delta, b)(r)$$
$$= (I\delta \cdot (I \cdot \lambda))(r), \text{ by (3.1.1)}$$
$$= (I(\delta \cdot e) \cdot \lambda)(r)$$
$$= (I\Theta \cdot \lambda)(r), \quad \text{as} \quad (\delta \cdot e)(r) = \Theta(r), \text{ by (2.11)}$$

This yields (3.2.1).

3.3 THEOREM. *If $\sigma(r)$ denotes the sum of the divisors of r, then*

$$\sum_{d \mid r} b(r/d)\Theta(d) = \sigma(r)$$

where $\Theta(r)$ is as given in (3.2.1)

Proof.

$$\sum_{d \mid r} b(r/d)\Theta(d) = (b \cdot \Theta)(r)$$
$$= ((I \cdot \lambda) \cdot (\delta \cdot e))(r)$$
$$= (I \cdot (\lambda \cdot \delta) \cdot e)(r)$$
$$= (I \cdot e_0 \cdot e)(r) \text{ by (2.9)}$$
$$= (I \cdot e)(r)$$
$$= \sigma(r).$$

4. **Properties of $B(n, r)$.** The function $B(n, r)$ defined in (1.5) is independent of the residue system in the summation. It is evident that if x^2 ranges over a square-reduced residue system (mod r) and $(a, r) = 1$, then ax^2 also ranges over a square-reduced residue system (mod r). Hence,

(4.1) $$B(an, r) = B(n, r) \quad \text{whenever} \quad (a, r) = 1.$$

Also,

(4.2) $$B(r, r) = b(r).$$

Now, we give below the properties of $B(n, r)$.

4.3 THEOREM.

$$\sum_{\substack{t \mid r \\ t \text{ square-free}}} B(n, r/t) = \begin{cases} r, & \text{if } r \mid n \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Let

$$\eta(n, r) = \sum_{h \pmod r}{}' \exp(2\Pi ihn/r)$$

It is clear that $\eta(n, r) = \begin{cases} r, & \text{if } r \mid n \\ 0, & \text{otherwise.} \end{cases}$

https://doi.org/10.4153/CMB-1979-028-1 Published online by Cambridge University Press

From Theorem 3.1, we have

$$\eta(n, r) = \sum_{\substack{tt'=r \\ t \text{ square-free}}} \sum_{\substack{x^2 \pmod{r/t} \\ (x^2, r/t) = \text{a square}}} \exp\left(\frac{2\Pi i x^2 n}{r/t}\right)$$

$$= \sum_{\substack{t \mid r \\ t \text{ square-free}}} B(n, r/t)$$

Hence the theorem.

COROLLARY.

(4.3.1) $$B(1, r) = \lambda(r)$$

For,

$$\sum_{\substack{t \mid r \\ t \text{ square-free}}} B(1, r/t) = e_0(r).$$

Therefore, by Inversion formula (2.10) $B(1, r) = (e_0 \cdot \lambda)(r) = \lambda(r)$.

4.4 THEOREM.

$$B(n, r) = \sum_{d \mid (n, r)} \lambda(r/d)d$$

Proof. From Theorem 4.3 and by applying Inversion formula (2.10) we have

$$B(n, r) = \sum_{d \mid r} \eta(n, d)\lambda(r/d)$$

$$= \sum_{d \mid r,\, d \mid n} d\lambda(r/d)$$

$$= \sum_{d \mid (n, r)} \lambda(r/d)d$$

REMARK. The relation between $C(n, r)$ and $B(n, r)$ is

$$\sum_{dD^2 = r} C(n, d) = B(n, r) \quad [3, \text{Corollary } 4]$$

4.5 THEOREM. *$B(n, r)$ is multiplicative in r.*

Proof. Let $(r, r') = 1$. If x and x' range over residue systems (mod r) and (mod r') respectively, then $xr' + x'r$ ranges over a residue system (mod rr'). Suppose $(xr' + x'r, rr') =$ a square. Since $(r, r') = 1$, it must follow that $(x, r) =$ a square, $(x', r') =$ a square. Conversely, if $(x, r) =$ a square, $(x', r') =$ a square, then $(xr' + x'r, rr') =$ a square. That is, $xr' + x'r$ yields a square-reduced residue system (mod rr'). x and x' range over square-reduced residue systems (mod r),

https://doi.org/10.4153/CMB-1979-028-1 Published online by Cambridge University Press

(mod r') respectively. So,

$$B(n, rr') = \sum_{\substack{x \pmod r,\ x' \pmod{r'} \\ (x, r)=\text{a square},\ (x', r')=\text{a square}}} \exp\left(\frac{2\Pi in(xr'+x'r)}{rr'}\right)$$

$$= B(nr', r)B(nr, r')$$

$$= B(n, r)B(n, r'), \quad \text{as} \quad (r, r')=1, \text{ by (4.1).}$$

4.6 Theorem. *$B(n, r)$ is multiplicative in both the variables n, r in the sense of* (2.13)

Proof. From Theorem 4.4 we note that $B(n, r)$ is even (mod r). Also, it is multiplicative in r, by Theorem 4.5. Therefore, by Theorem 2.2 in [11], $B(n, r)$ is multiplicative in n, r.

Corollary.

(4.6.1) *$B(n, r)$ is quasi-multiplicative in n. That is,*

$$B(n, r)B(n', r) = \lambda(r)B(nn', r) \quad \textit{whenever} \quad (n, n')=1$$

Proof of (4.6.1). If $f(n, r)$ is multiplicative in n, r, it is known [12, Lemma 2.1] that

$$f(n, r)f(n', r) = f(1, r)f(nn', r) \quad \text{whenever} \quad (n, n')=1.$$

This is referred to as quasi-multiplicative nature in n. Here, as $B(n, r)$ is multiplicative in n, r, we get

$$B(n, r)B(n', r) = B(1, r)B(nn', r) \quad \text{when} \quad (n, n')=1.$$

But, $B(1, r) = \lambda(r)$ (4.3.1). Hence, the corollary follows.

4.7 Theorem. $B(n, r) = \lambda(r/g)b(g)$; $g = (n, r)$.

Proof. We have

$$B(n, r) = \sum_{d \mid (n, r)} \lambda(r/d)d$$

As $\lambda(r)$ is completely multiplicative, $\lambda(r/d) = \lambda(r/g)\lambda(g/d)$ for every divisor d of $g = (n, r)$. So,

$$B(n, r) = \lambda(r/g) \sum_{d \mid g} \lambda(g/d)d$$

$$= \lambda(r/g)b(g), \text{ using (3.1.1)}$$

Remark. The above formula for $B(n, r)$ suggests that $B(n, r)$ has the form

$$B(n, r) = B(1, r/g)B(g, g); \qquad g = (n, r)$$

$B(n, r)$ is a typical example of a 'Quasi-symmetric function' [7] whose properties we discuss in §5.

Now, we are in a position to compare the arithmetic functions connected with (i) a reduced-residue system (mod r) (ii) a semi-reduced residue system (mod r) and (iii) a square-reduced residue system (mod r).

(i) $\phi(r)$ is multiplicative and has totient structure. The associated exponential sum is Ramanujan's Sum $C(n, r)$ with $C(r, r)=\phi(r)$.

(ii) $\phi^*(r)$ is multiplicative and has unitary totient structure. The associated exponential sum is the unitary analogue $C^*(n, r)$ of Ramanujan's Sum with $C^*(r, r)=\phi^*(r)$.

(iii) $b(r)$ is multiplicative and has 'specially multiplicative' structure. The associated exponential sum is the square-reduced analogue $B(n, r)$ of Ramanujan's Sum with $B(r, r)=b(r)$.

5. **Quasi-symmetric functions.** There exist multiplicative functions $f(n, r)$ for which $f(p^b, p^a)=(-1)^{a+b}f(p^a, p^b)$; p any prime; $a\geq 0$, $b\geq 0$. For instance, if $f(n, r)=\lambda(r)F(nr)$ where F is multiplicative in a single variable, $f(n, r)=\lambda(nr)f(r, n)$.

5.1 Definition. A multiplicative function $f(n, r)$ is said to be *quasi-symmetric* if f has the property

$$f(n, r)=h(nr)f(r, n) \tag{5.1.1}$$

where $h(r)$ is completely multiplicative in r.

The above definition of a quasi-symmetric function implies that $f(r, r)=h(r^2)f(r, r)$. Therefore, $h(r)$ occurring in (5.1.1) should satisfy

$$h(r^2)=h^2(r)=1. \tag{5.1.2}$$

We may take $h(r)=e(r)$ in which case $f(n, r)=f(r, n)$. That is, when $h(r)=e(r)$, $f(n, r)$ becomes a *symmetric multiplicative function* [13].

5.2 Definition. Given two positive integers n, r, the *greatest common unitary divisor* (g.c.u.d) of n and r is the integer g' such that g' is a unitary divisor of n as well as r and is the greatest divisor common to n and r having this property.

For example, if $n=\Pi p_i^{b_i}$ and $r=\Pi p_i^{a_i}$ (p_i being distinct primes), the g.c.u.d of n and r is given by $g'=\Pi p_j^{a_j}$, where a_j is the power of a common prime factor p_j (occurring in n and r) when $b_j=a_j$.

We shall denote the least common multiple (l.c.m) of n and r by $\ell=\{n, r\}$.

5.3 Theorem. *If $f(n, r)$ is quasi-symmetric and as defined in* (5.1.1) *then*

$$f(n, r)=h(n'r')f(g, \ell)$$

where $g=(n, r)$, $\ell=\{n, r\}$, n' is the g.c.u.d of n and ℓ; r' is the g.c.u.d of r and g.

Proof. Let

$$n=\prod_{i=1}^{s} p_i^{b_i}\prod_{i=s+1}^{k} p_i^{b_i}, \qquad r=\prod_{i=1}^{s} p_i^{a_i}\prod_{i=s+1}^{k} p_i^{a_i}$$

https://doi.org/10.4153/CMB-1979-028-1 Published online by Cambridge University Press

where $a_i \geq b_i$ $(i=1$ to $s)$; $a_i < b_i$ $(i=s+1$ to $k)$. Then,

$$g=\prod_{i=1}^{s} p_i^{b_i} \prod_{i=s+1}^{k} p_i^{a_i} \tag{5.3.1}$$

$$\ell=\prod_{i=1}^{s} p_i^{a_i} \prod_{i=s+1}^{k} p_i^{b_i} \tag{5.3.2}$$

Now,

$$f(n,r)=\prod_{i=1}^{s} f(p_i^{b_i}, p_i^{a_i}) \prod_{i=s+1}^{k} f(p_i^{b_i}, p_i^{a_i}) \tag{5.3.3}$$

As f is quasi-symmetric,

$$f(p_i^{b_i}, p_i^{a_i})=h(p_i^{a_i+b_i})f(p_i^{a_i}, p_i^{b_i}) \qquad (i=1 \text{ to } k)$$

Applying this to the product from $i=s+1$ to k in (5.3.3), we get

$$\begin{aligned} f(n,r) &= \prod_{i=1}^{s} f(p_i^{b_i}, p_i^{a_i}) \prod_{i=s+1}^{k} h(p_i^{a_i+b_i}) \prod_{i=s+1}^{k} f(p_i^{a_i}, p_i^{b_i}) \\ &= f(g,\ell) \prod_{i=s+1}^{k} h(p_i^{a_i}) \prod_{i=s+1}^{k} h(p_i^{b_i}) \end{aligned}$$

From the definition of n' and r', it follows that

$$\begin{aligned} f(n,r) &= f(g,\ell)h(r')h(n') \\ &= h(n'r')f(g,\ell) \end{aligned}$$

as h is completely multiplicative.

REMARK. In particular, if $h(r)=e(r)=1$, $f(n,r)=f(g,\ell)$. That is, if $f(n,r)=f(r,n)$; $f(n,r)=f(g,\ell)$. This property is characteristic of a symmetric multiplicative function considered in [13, Lemma of Theorem 6].

5.4 THEOREM. *If $f(n,r)$ is quasi-symmetric and even* (mod r) *then*

$$f(n,r)=f(1,r/g)f(g,g); \qquad g=(n,r).$$

Proof. As f is quasi-symmetric, there exists a completely multiplicative function $h(r)$ such that $f(n,r)=h(nr)f(r,n)$; where $h^2(r)=1$. As f is also even (mod r)

$$\begin{aligned} f(n,r) &= f(g,r) \\ &= h(gr)f(r,g) \\ &= h(gr)f(g,g) \quad \text{as} \quad g \mid r \\ &= h(g^2r/g)f(g,g) \\ &= h(g^2)h(r/g)f(g,g) \\ &= h(r/g)f(g,g), \quad \text{as} \quad h(g^2)=h^2(g)=1. \end{aligned}$$

https://doi.org/10.4153/CMB-1979-028-1 Published online by Cambridge University Press

Now,

$$\begin{aligned} f(1, r/g) &= h(r/g)f(r/g, 1) \\ &= h(r/g)f(1, 1) \\ &= h(r/g) \end{aligned}$$

Hence, $f(n, r) = f(1, r/g)f(g, g)$.

REMARK. It may be noted that if $f(n, r) = f(1, r/g)f(g, g)$, f need not be quasi-symmetric. For example, let

$$f(n, r) = \frac{r}{(n, r)} \phi((n, r))$$

If $f(n, r) = h(nr)f(r, n)$, then $h(r) = r$. Thus, $h^2(r) \neq 1$.

We observe that $B(n, r)$ is quasi-symmetric with $h(r) = \lambda(r)$. For, by Theorem 4.7 $B(n, r) = \lambda(r/g)b(g)$ and so

$$B(n, r) = B(1, r/g)B(g, g); \qquad g = (n, r).$$

Next, we proceed to the proof of (1.6) which may be treated as an analogue of Menon's Identity [6].

6. **An analogue of Menon's identity.** We first give a lemma that is needed in the calculation of Fourier Coefficients of even functions (mod r).

6.1 LEMMA. [9, Theorem 4.3] *If $f(n, r) = F((n, r))$ where F is multiplicative, then the Fourier Coefficient of $f(n, r)$ is given by*

$$\alpha(d, r) = \frac{1}{r} \sum_{s \mid r/d} G(r/s)s$$

where $G(r) = (F \cdot e^{-1})(r)$.

If $f(n, r) = (n, r)$, it follows that

(6.1.1) $$\alpha(d, r) = \sum_{s \mid r/d} \frac{1}{r} \phi(r/s)s$$

In the same manner, the Fourier Coefficient $\beta(d, r)$ of $\varepsilon((n, r))$ is calculated as

$$\begin{aligned} \beta(d, r) &= \frac{1}{r} \sum_{s \mid r/d} \lambda(r/s)s \\ &= \frac{1}{r} \sum_{s \mid r/d} \lambda(d)\lambda(r/ds)s \end{aligned}$$

Or,

(6.1.2) $$\beta(d, r) = \frac{1}{r} \lambda(d)b(r/d), \text{ using (3.1.1)}$$

https://doi.org/10.4153/CMB-1979-028-1 Published online by Cambridge University Press

Next, if $h(n, r)$ is the Cauchy-product of (n, r) and $\varepsilon((n, r))$ we have from (2.18), (6.1.1) and (6.1.2)

$$h(n,r)=\frac{1}{r}\sum_{d\mid r}\left\{\sum_{s\mid r/d}\phi(r/s)s\right\}\lambda(d)b(r/d)C(n,d) \tag{6.1.3}$$

We make use of (6.1.3) to prove

6.2 THEOREM. *Let*

$$(n,r)=1 \quad \text{and} \quad r=\prod_{i=1}^{k} p_i^{a_i} \quad (a_i \geq 1)$$

Then,

$$\sum_{\substack{a(\mathrm{mod}\, r)\\(a,r)=\text{a square}}} (|n-a|, r)=\prod_{i=1}^{k}\{\beta(p_i^{a_i})-b(p_i^{a_i-1})\}$$

Proof. If $h(n, r)$ is as defined in (6.1.3) $h(n, r)$ is even (mod r) and is multiplicative in n, r. Further, when $(n, r)=1$, $h(n, r)=h(1, r)$. Moreover, $h(1, r)$ is multiplicative in r. Therefore, if $(n, r)=1$

$$\sum_{\substack{a(\mathrm{mod}\, r)\\(a,r)=\text{a square}}} (|n-a|, r)=h(1,r)=\prod_{i=1}^{k} h(1, p_i^{a_i})$$

So, it will suffice if we evaluate $h(1, p^a)$ where p is a prime and $a \geq 1$. We note that $C(1, r)=\mu(r)$ (2.5) and $(I\cdot\phi)(r)=\beta(r)$. Appealing to the property of the Mobius function and after a little calculation, we arrive at

$$p^a h(1,p^a)=\beta(p^a)\{b(p^a)+b(p^{a-1})\}-p^a b(p^{a-1})$$

But,

$$b(p^a)+b(p^{a-1})=p^a.$$

Therefore,

$$p^a h(1,p^a)=p^a\{\beta(p^a)-b(p^{a-1})\}$$

Thus,

$$h(1,p^a)=\beta(p^a)-b(p^{a-1})$$

Now, the desired result follows on account of the multiplicativity of $h(1, r)$.

REMARK. (1.6) is a particular case of the above theorem when $n=1$.

ACKNOWLEDGEMENT. The author is grateful to Dr. K. Nageswara Rao who suggested the evaluation of the left side of (1.6). He is also thankful to the referee for valuable comments which improved the original version of this paper.

REFERENCES

1. Eckford Cohen, *Arithmetical functions associated with the unitary divisors of an integer*, Math. Zeitschr **74** (1960) 66–80.

2. ——, *A class of arithmetical functions*, Proc. Nat. Acad. Sc., **41** (1955) 939–944.

3. ——, *Representations of Even Functions* (mod r) *I Arithmetical Identities*, Duke Math. J., **25** (1958) 401–422.

4. ——, *Representations of Even Functions* (mod r) *II Cauchy Products*, Duke Math. J., **26** (1959) 165–182.

5. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, ELBS and Oxford University Press (1971 Edition).

6. P. Kesava Menon, *On the Sum* $\sum_{(a,n)=1}(a-1,n)$, J. Ind. Math. Soc. (New Series) **29** (1963) 155–163.

7. R. Sivaramakrishnan, *Contributions to the study of multiplicative arithmetic functions*, Ph.D Thesis University of Kerala (1971).

8. ——, *On a class of multiplicative arithmetic functions*, J. Reine. Angew. Math., **280** (1976) 157–162.

9. ——, *Multiplicative Even Functions* (mod r) *I Structural properties*, J. Reine. Angew. Math. **302** (1978).

10. S. S. Pillai, *On an arithmetic function*, J. Annamalai University **II** No. 2 243–248.

11. C. S. Venkataraman, *Modular Multiplicative Functions*, J. Madras University **XIX** (1950) 69–78.

12. ——, *A new Identical Equation for multiplicative functions of two arguments and its applications to Ramanujan's Sum* $C_M(N)$, Proc. Ind. Acad. Sc., **XXIV** No. 6 Sec. A (1946) 518–529.

13. ——, *On Von Sterneck Ramanujan Function*, J. Ind. Math. Soc. (New Series) **13** (1949) 65–72.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF CALICUT
KERALA 673635, INDIA