ARITHMETICAL NOTES, VII. SOME CLASSES OF EVEN FUNCTIONS (mod r)

by

ECKFORD COHEN

1. INTRODUCTION. With n and r representing integers, $r > 0$, a complex-valued function $f(n, r)$ is defined to be even (mod r) if $f((n, r), r) = f(n, r)$ for all n. Here (n, r) has its usual meaning as the greatest common divisor of n and r. The class of even functions (mod r), to be denoted E_r, was discussed in [2], [3], [4], [5].

In this note we consider some subclasses of E_r. It will be observed that for a fixed divisor δ of r, $E_\delta \equiv E_\delta(r) \subseteq E_r$. We define the class $B_\delta \equiv B_\delta(r)$ to consist of the functions of E_r contained in E_δ but not contained in E_D for any proper divisor D of δ. The classes E_δ and B_δ are characterized in § 2 (Theorem 2.1) in terms of FOURIER expansions. This criterion is applied to the classification of some important functions of E_r. In particular, we consider the functions $\theta_s(n, r)$, $P_t(n, r)$, $S_m(n, r)$, defined for positive integers s, t, m, as follows: $\theta_s(n, r)$ is the number of solutions (mod r) of

$$n \equiv x_1 + \dots + x_s \pmod{r}, \quad (x_i, r) = 1, \tag{1.1}$$

$(i = 1, \dots, s)$; $P_t(n, r)$ is the number of solutions (mod r) of

$$n \equiv p_1 y_1 + \dots + p_t t_t \pmod{r}, \quad p_i \text{ prime}, \quad p_i \mid r, \quad (y_i, r) = 1, \tag{1.2}$$

$(i = 1, \dots, t)$; and $S_m(n, r)$ is the number of solutions (mod r) of

$$n \equiv z_1^2 + \dots + z_{2m}^2 \pmod{r}, \quad (r \text{ odd}). \tag{1.3}$$

If n is viewed as an element of the residue class ring J_r of the ring of integers (mod r), then the above functions can be interpreted in the following manner: $\theta_s(n, r)$ is the number of representations of n as a sum of s units of J_r; $P_t(n, r)$ is the number of representations of n as a weighted sum of t prime elements of J_r; $S_m(n, r)$ is the number of representations of n as the sum of squares of an even number $(2m)$ of elements of J_r.

Section 3 is devoted to generalizations of the congruence (1.1) and includes some explicit formulas. For a discussion of some other classes of functions of E_r we mention McCarthy [8].

REMARK 1.1. In this paper r is to be assumed fixed. However, in the arithmetical inversion theory of the papers referred to above, r must be treated as an integral variable.

2. CLASSIFICATION OF EVEN FUNCTION (mod r). Let $c(n, r)$ denote Ramanujan's sum and place $\phi(r) = c(0, r)$, $\mu(r) = c(1, r)$, the EULER and Möbius function, respectively. The function $c(n, r)$ is contained in E_r; moreover, we have the following characterization [2, Theorem 1] of E_r in terms of the Ramanujan sums: *A function $f(n, r)$ is contained in E_r if and only if it is representable in the form*

$$f(n, r) = \sum_{d|r} \alpha(d, r)\, c(n, d); \tag{2.1}$$

the coefficients $\alpha(d, r)$ are uniquely determined ([2, (7)].

This result may be restated in the alternative form : E_r is a vector space over complex field with basis $c(n, d)$, d ranging over the divisors of r. This result leads directly to the following criterion for the subclasses of E_r defined in the Introduction.

THEOREM 2.1. *Let δ denote a divisor of r. A function $f(n, r)$ is contained in E_δ if and only if it possesses an expansion* (2.1) *in which $\alpha(d, r) = 0$ for each d which is not a divisor of δ. A function $f(n, r)$ is contained in B_δ if and only if it possesses an expansion* (2.1) *in which $d \nmid \delta$ implies that $\alpha(d, r) = 0$, but such that for each proper divisor D of δ there exists a D', $D' \nmid D$, for which $\alpha(D', r) \neq 0$.*

Let $\nu_k(r)$ denote the maximal $(k+1)$ — free divisor of r, for each positive integer k, and place $\nu(r) = \nu_1(r)$. We note the following chain of function classes,

$$E_{\nu(r)} = E_{\nu_1(r)} \subset E_{\nu_2(r)} \subset E_{\nu_3(r)} \subset \ldots \subset E_{\nu_e(r)} = E_r, \tag{2.2}$$

where $e = e(r)$ is the maximum exponent to which any prime divides r. The class $E_{\nu(r)}$ was discussed in [3] under the name of *primitive functions* (mod r). For a more precise classification of functions we have the hierarchy of classes,

$$B_{\nu(r)} = B_{\nu_1(r)},\ B_{\nu_2(r)},\ \ldots,\ B_{\nu_e(r)} = B_r; \tag{2.3}$$

note that $B_{\nu_i(r)} \subset E_{\nu_i(r)}$, while for each $f(n, r)$ in $B_{\nu_i(r)}$, it follows that $f(n, r) \notin E_{\nu_{i-1}(r)}$, $i = 1, \ldots, e$, if $\nu_0(r) = 1$. Proceeding from left to right in (2.3), (or 2.2)), one passes from the class of functions with the simplest structure, $B_{\nu(r)}$ (or $E_{\nu(r)}$), to the class with the most complicated structure, B_r (or E_r).

In order to identify the functions $\theta_s(n, r)$, $P_t(n, r)$, $S_m(n, r)$ in terms of the above classification, we recall their expansions of the form (2.1), that is, their Fourier expansions as even functions (mod r). Placing $\alpha = (-1)^m$ and letting (α/d) denote the LEGENDRE-JACOBI symbol, we have [1, Theorem 11, $s = 2m$],

$$(2.4) \qquad S_m(n, r) = r^{2m-1} \sum_{d|r} \left(\frac{\alpha}{d}\right) \frac{c(n, d)}{d^m} \qquad (r \text{ odd}).$$

Let $\omega(r)$ and $\varrho(r)$ denote respectively, the number and sum of the (distinct) prime divisors of r and place $Q(d, r) = \omega(r) - \tau(d)$, $\mu^*(r) = (-1)^{\omega(r)}$. Also define

$$\pi(r) = \begin{cases} p \text{ if } r = p^2 d, \ p \text{ prime}, \ d \text{ square-free}, \ p \nmid d, \\ 0 \text{ otherwise.} \end{cases}$$

Then by [5, Theorem 4]

$$(2.5) \quad P_t(n, r) = \frac{\phi^t(r)}{r} \left\{ \sum_{d|r} \left(\frac{\mu(d) Q(d, r)}{\phi(d)}\right)^t c(n, d) + \sum_{d|r} \left(\frac{\pi(d)\mu^*(d)}{\phi(d)}\right)^t c(n, d) \right\}.$$

Finally, by [2, Theorem 6 (Note)], we have

$$(2.6) \qquad \theta_s(n, r) = \frac{\phi^s(r)}{r} \sum_{d|r} \left(\frac{\mu(d)}{\phi(d)}\right)^s c(n, d).$$

By the definition of the functions $\mu(r)$, (α/r), and $\pi(r)$, the following result follows on applying Theorem 2.1 to (2.4), (2.5), and (2.6).

THEOREM 2.2.

$$(2.7) \qquad S_m(n, r) \ \varepsilon \ B_r, \qquad (r \text{ odd}),$$

$$(2.8) \qquad P_t(n, r) \ \varepsilon \ B_{\nu_2(r)},$$

$$(2.9) \qquad \theta_s(n, r) \ \varepsilon \ B_{\nu(r)}.$$

Let now $g(n, r)$ denote a function of E_r with Fourier expansion,

$$(2.10) \qquad g(n, r) = \sum_{d|r} \beta(d, r) \, c(n, d).$$

It is recalled from [4, Theorem 1] that

$$(2.11)\qquad \sum_{n\equiv a+b \pmod r} f(a, r)\, g(b, r) = r \sum_{d|r} \alpha(d, r)\, \beta(d, r)\, c(n, d).$$

We apply this result to the function $Q_{s,m}(n, r)$, defined to be the number of solutions (mod r) of

$$(2.12)\qquad n \equiv x_1 + \ldots + x_s + z_1^2 + \ldots + z_{2m}^2 \pmod r,\ (x_i, r) = 1,$$

$i = 1, \ldots, s$. In particular, application of (2.11) with $f(n, r) = \theta_s(n, r)$, $g(n, r) = S_m(n, r)$, leads on the basis of (2.4) and (2.6) to

THEOREM 2.3. *If r is odd, then for $s > 0$,*

$$(2.13)\qquad Q_{s,m}(n, r) = r^{2m-1} \phi^s(r) \sum_{d|r} \left(\frac{\mu(d)}{\phi(d)}\right)^s \left(\frac{\alpha}{d}\right) \frac{c(n, d)}{d^m};$$

in particular, $Q_{s,m}(n, r)\ \varepsilon\ B_{\nu(r)}$.

To obtain a product representation of $Q_{s,m}(n, r)$, we recall that $c(n, r)$ is multiplicative in r and that for $e > 0$ and primes p,

$$(2.14)\qquad c(n, p^s) = \begin{cases} p^e - p^{e-1} & \text{if } p^e | n \\ -p^{e-1} & \text{if } p^{e-1} | n,\ p^e + n \\ 0 & \text{otherwise.} \end{cases}$$

Hence (2.13) becomes.

THEOREM 2.3′. *If r is odd, then*

$$(2.15)\qquad \frac{Q_{s,m}(n, r)}{r^{2m-1}\phi^s(r)} = \prod_{p|(n,r)} \left(1 + \left(\frac{\alpha}{p}\right) \frac{(-1)^s}{p^m(p-1)^{s-1}}\right) \prod_{\substack{p|r \\ p\nmid n}} \left(1 + \left(\frac{\alpha}{p}\right) \frac{(-1)^{s+1}}{p^m(p-1)^s}\right)$$

3. SOME FURTHER CONGRUEMCE PROBLEMS. In generalizing the problem (1.1), we need the function $g_k(n, r)$, defined for positive integers k, by

$$(3.1)\qquad g_k(n, r) = \sum_{d|r} d\mu_k\left(\frac{r}{d}\right),$$

where $\mu_k(r)$ is the function, multiplicative in r, with the evaluation,

$$(3.2)\qquad \mu_k(p^e) = \begin{cases} -1 & (e = k) \\ 0 & (e \neq k), \end{cases}$$

for primes p and positive integers e. Clearly, $\mu_1(r) = \mu(r)$, and by the well-known evaluation of $c(n, r)$, $g_1(n, r) = g(n, r)$. For an equivalent trigonometric definition of $g_k(n, r)$, we mention [6, § 4 and (6.3)].

Evidently, $g_k(n, r)$ is even (mod r) and is multiplicative as a function of r; it is therefore sufficient to consider the case $r = p^e$, $n = p^l$, $0 \leq l \leq e$, where p and e have the same significance as above.

In particular, it is easily seen that

$$g_k(p^l, p^e) = \begin{cases} p^e & (l = e < k) \\ p^e - p^{e-k} & (l = e \geq k) \\ -p^{e-k} & (0 \leq e - k \leq l < e) \\ 0 & (l < e < k \text{ or } e > k + l), \end{cases} \tag{3.3}$$

$g_k(n, 1) = 1$.

Define now $\theta_{k,s}(n, r)$ to be the number of solutions of

$$n \equiv x_1 + \ldots + x_s \pmod{r}, \quad (x_i, r)_k = 1, \tag{3.4}$$

($i = 1, \ldots, s$), where $(n, r)_k$ denotes the greatest common *k-th* power divisor of n and r. The following FOURIER expansion of $\theta_{k,s}(n, r)$ as an even function (mod r) was proved in [6, (6.10)]:

$$\theta_{k,s}(n. r) = \frac{1}{r} \sum_{d|r} \left(g_k\left(\frac{r}{d}, r\right)\right)^s c(n, d). \tag{3.5}$$

Let r_k denote the product of the prime powers p^e such that $p^e|r$, $p^{e+1} + r$ and $e \geq k$. Then we have

THEOREM 3.1. *The function $\theta_{k,s}(n, r)$ is contained in the class $B_{\nu_k(r_k)}$. Moreover, if $k > 1$, then $\theta_{k,s}(n, r) = 0$ if and only if $s = 1$ and $(n, r)_k \neq 1$.*

PROOF. The first statement of the theorem results from (3.3), (3.5) and Theorem 2.1. Using e, l as in (3.3), a computation based on (3.5) yields, for prime factors p of π_k).

$$\frac{p^e \phi_{k,s}(p^l, p^e)}{p^{(e-k)s}} = \begin{cases} (p^k - 1)^s + (-1)^{s+1} & \text{if } k > l, \\ (p^k - 1)\left[(p^k - 1)^{s-1} + (-1)^s\right] & \text{if } k \leq l. \end{cases} \tag{3.6}$$

By the multiplicativity of $\theta_{k,s}(n, r)$ as a function of π, the proof is now complete.

REMARK 3.1. Since $\theta_{1,s}(n, r) = \theta_s(n, r)$, the first statement of Theorem 3.1 reduces to (2.9) in case $k = 1$. A complete discussion of the solvability of (3.4) in this case is contained in [7].

For positive integral h, k, s, t, let $\phi_{h,s}^{k,t}(n, r)$ denote the number of solutions of

$$(3.7)\quad n \equiv x_1 + \ldots + x_s + y_1 + \ldots + y_t \pmod r, (x_i, r)_h = (y_j, r)_k = 1,$$

$(i = 1, \ldots, s; j = 1, \ldots, t)$. Applying (2.11) with $f(n, r) = \theta_{h,s}(n, r)$, $g(n, r) = \theta_{k,t}(n, r)$, it follows by (3.5) that

$$(3.8)\qquad \theta_{h,s}^{k,t}(n, r) = \frac{1}{r} \sum_{d|r} \left(g_h\left(\frac{r}{d}, r\right)\right)^s \left(g_k\left(\frac{r}{d}, r\right)\right)^t c(n, d)\,.$$

Let e and l have the same meaning as in (3.6). Then by (3.3) and (3.8), with $h \leq k \leq e$, it can be verified that

$$(3.9)\quad \frac{p^e\,\theta_{h,s}^{k,t}(p^l, p^e)}{p^{(e-h)s+(e-k)t}} = \begin{cases} (p^h-1)^s(p^k-1)^t + (-1)^{s+t+1} & \text{if } h > l, \\ (p^h-1)\,[(p^h-1)^{s-1}(p^k-1)^t + (-1)^{s+t}] & \text{if } h \leq l. \end{cases}$$

Clearly (3.7) is solvable if $k > e$, $r = p^e$; therefore, by (3.9) and multiplicativity one obtains.

Remark 3.2. *If* $\max(h, k) > 1$, *then* (3.7) *is always solvable.*

Remark. 3.3. The formula (3.6) determines $\theta_{k,s}(n, p^e)$, $k \geq e$, while (3.9) evaluates $\theta_{h,s}^{k,t}(n, p^e)$, $h \leq k \leq e$. The excluded case, $k > e$, is of course trivial.

The result in Remark 3.2 can also be verified directly.

BIBLIOGRAPHY

1. ECKFORD COHEN, *Rings of arithmetic functions*, II. *The number of solutions of quadratic congruences*, Duke Mathematical Journal, vol. 21 (1954), pp. 9-28.

2. ECKFORD COHEN, *A class of arithmetical functions*, Proceedings of the National Academy of Sciences, vol. 41 (1955), pp. 939-944.

3. ECKFORD COHEN, *Representations of even functions* (mod r), I. *Arithmetical identities*, Duke Mathematical Journal, vol. 25 (1958), pp. 401-422.

4. ECKFORD COHEN, *Representations of even functions* (mod r), II. *Cauchy products* (mod r), Duke Mathematical Journal, vol. 26 (1959), pp. 165-182.

5. ECKFORD COHEN, *Representations of even functions* (mod r), III. *Special topics*, vol. 26 (1959), pp. 491-500.

6. ECKFORD COHEN, *A class of residue systems* (mod r) *and related arithmetical functions*, I. *A generalization of Mobius inversion*, Pacific Journal of Mathematics, vol. 9 (1959), pp. 13-23.

7. J. D. DIXON, *A finite analogue of the Goldbach problem*, Canadian Mathematical Bulletin, vol. 3 (1960), pp. 121-126.

8. P. J. McCARTHY, *The generation of arithmetical identities*, Journal für die reine und die angewandte Mathematik, vol. 203 (1960), pp. 55-63.

The University of Tennessee.