COLLOQUIUM MATHEMATICUM

VOL. XXII 1971 FASC. 2

REGULAR ARITHMETICAL CONVOLUTIONS AND THE SOLUTIONS OF LINEAR CONGRUENCES

BY

P. J. McCARTHY (LAWRENCE, KANSAS)

The Ramanujan sum, and its k-analogue which was introduced by Cohen in [2], have been used to obtain identities involving arithmetical functions and to determine the number of restricted solutions of certain congruences; see, for example, [3]-[8], [12]-[15], [21], [23]-[25]. We shall refer to the results contained in these papers as the classical results. In [9], Cohen introduced the unitary analogue of the Ramanujan sum, and the unitary analogues of many of the classical results were obtained in subsequent papers [10], [11], [15], [17]-[20].

The classical Dirichlet convolution and the unitary convolution of [9] are regular arithmetical convolutions. The notion of regular arithmetical convolution was introduced by Narkiewicz in [22], and will be discussed below. In terms related to this notion we can formulate questions involving analogues of the classical arithmetical functions and concerning the number of restricted solution of congruences. The purpose of this note is to point out how the answers to these questions may be obtained easily from the classical results. We shall discuss in some detail the number of restricted solutions of certain congruences. It will be clear how the analogues of the classical arithmetical identities can be obtained. Of course, our results will include certain known unitary analogues of the classical results.

For each positive integer r, let $A(r)$ be a non-empty set of positive divisors of r. If f and g are arithmetical functions, we define a new arithmetical function h by

$$h(r) = \sum_{d\in A(r)} f(d)g(r/d).$$

This furnishes us with a binary operation on the set F of all arithmetical functions; it is called the *arithmetical convolution A*. Two examples of arithmetical convolutions are the classical *Dirichlet convolution D*, where $D(r)$ is the set of all positive divisors of r, and the *unitary con-*

volution U, where $U(r)$ is the set of all positive divisors d of r such that $(d, r/d) = 1$ (the unitary divisors of r).

An arithmetical convolution A is called *regular* if: (a) F is a commutative ring with respect to addition and the convolution A, (b) the convolution of multiplicative functions is multiplicative, and (c) the function e defined by $e(r) = 1$ for all r has an inverse μ_A in the ring F and $\mu_A(r) = 0$ or -1 whenever r is a prime power. The convolutions D and U are regular. Narkiewicz characterized regular arithmetical convolutions in terms of the sets $A(r)$ ([22], Theorems I and II). In particular, he showed that a regular arithmetical convolution is completely determined by the sets $A(p^a)$ for all prime powers $p^a > 1$, and that for each such prime power there is a positive divisor t of a such that

$$A(p^a) = \{1, p^t, p^{2t}, \ldots, p^{st}\}, \qquad st = a,$$

and for $1 \leqslant j \leqslant a/t$, $A(p^{jt}) = \{1, p^t, \ldots, p^{jt}\}$. The integer t is called the *type* of p^a and is denoted by $\tau_A(p^a)$. Note that for all $p^a > 1$, $\tau_D(p^a) = 1$ and $\tau_U(p^a) = a$. We shall assume complete familiarity with the first three sections of [22].

Let A be a regular arithmetical convolution. The function μ_A is multiplicative, and for every prime p and positive integer a,

$$\mu_A(p^a) = \begin{cases} -1 & \text{if } \tau_A(p^a) = a, \\ 0 & \text{otherwise.} \end{cases}$$

If n is a non-negative integer and r is a positive integer, we denote by $(n, r)_A$ the largest divisor of n which is contained in $A(r)$. The function φ_A is defined by

$\varphi_A(r) =$ the number of integers x such that $1 \leqslant x \leqslant r$ and $(x, r)_A = 1$.

We have shown in [16] that φ_A is multiplicative and that if p is a prime and a a positive integer, then $\varphi_A(p^a) = p^a - p^{a-t}$, where $t = \tau_A(p^a)$. The analogue of the Ramanujan sum is defined by

$$c_A(n, r) = \sum_{(x,r)_A = 1} \exp(2\pi i n x/r),$$

where the sum is over the $\varphi_A(r)$ integers x such that $1 \leqslant x \leqslant r$ and $(x, r)_A = 1$. We have investigated this sum in [16], and it follows from results given there that if $(r_1, r_2) = 1$, then $c_A(n, r_1 r_2) = c_A(n, r_1) c_A(n, r_2)$. Furthermore, if p is a prime and a a positive integer, then

$$c_A(n, p^a) = \begin{cases} p^a - p^{a-t} & \text{if } p^a \mid n, \\ -p^{a-t} & \text{if } p^{a-t} \mid n, p^a \nmid n, \\ 0 & \text{if } p^{a-t} \nmid n, \end{cases}$$

where $t = \tau_A(p^a)$.

We denote by $c_k(n, r)$ Cohen's extension of the Ramanujan sum. If $(r_1, r_2) = 1$, then $c_k(n, r_1 r_2) = c_k(n, r_1) c_k(n, r_2)$, and if p is a prime and β a positive integer, then ([2], Theorem 3)

$$c_k(n, p^\beta) = \begin{cases} p^{\beta k} - p^{\beta k - k} & \text{if } p^{\beta k} \mid n, \\ -p^{\beta k - k} & \text{if } p^{\beta k - k} \mid n, p^{\beta k} \nmid n, \\ 0 & \text{if } p^{\beta k - k} \nmid n. \end{cases}$$

If we compare this formula with the one given above for $c_A(n, p^a)$, we see that for all primes p and positive integers a we have

$$c_A(n, p^a) = c_t(n, p^{a/t})$$

for all non-negative integers n, where $t = \tau_A(p^a)$. It is this observation that is the starting point for the remarks which follow.

First, we shall show that the sum $c_A(n, r)$ has the same value as the proper analogue of the von Sterneck function (see [23]).

THEOREM 1. *If A is a regular arithmetical convolution, then*

$$(1) \qquad c_A(n, r) = \frac{\varphi_A(r)\mu_A(m)}{\varphi_A(m)}, \quad m = \frac{r}{(n, r)_A}.$$

For fixed n, the function on the right-hand side of (1) is a multiplicative function of r. Hence, it is enough to verify this identity when r is a prime power $p^a > 1$. If $t = \tau_A(p^a)$, then

$$c_A(n, p^a) = c_t(n, p^{a/t}) = \frac{\varphi_t(p^{a/t})\mu(q)}{\varphi_t(q)},$$

where $q^t = p^a/(n, p^a)_t$ ([4], Theorem 1; [13], p. 61). The function φ_t is the t-analogue of Euler's function, and $(n, p^a)_t$ is the largest t-th power divisor of n which divides p^a. Now, $(n, p^a)_A$ and $(n, p^a)_t$ are both equal to p^{jt}, where j is the largest integer $\leqslant a/t$ such that $p^{jt} \mid n$. If $a = st$, then both m and q^t are equal to $p^{(s-j)t}$. Hence, $\varphi_A(m) = \varphi_A(p^{(s-j)t}) = \varphi_t(p^{s-j}) = \varphi_t(q)$. Furthermore,

$$\mu_A(m) = \mu_A(p^{(s-j)t}) = \begin{cases} 1 & \text{if } j = s, \\ -1 & \text{if } j = s-1, \\ 0 & \text{if } j \leqslant s-2, \end{cases}$$

which is precisely the value of $\mu(q)$. Thus, the asserted equality holds.

When $A = U$, (1) was given in [15], p. 56, and, in an equivalent form, in [11], Lemma 2.2.

We now turn to the determination of the number of solutions, restricted in various ways, of the congruence

$$(2) \qquad n \equiv x_1 + \ldots + x_s \pmod{r}.$$

Two solutions of this congruence, $x_1, \ldots, x_s$ and $x_1', \ldots, x_s'$, are counted as the same if and only if $x_i \equiv x_i' \pmod{r}$ for $i = 1, \ldots, s$.

Let $N_A(n, r, s)$ be the number of solutions of (2) such that $(x_i, r)_A = 1$ for $i = 1, \ldots, s$. Then

$$N_A(n, r, s) = \frac{1}{r} \sum_{d \in A(r)} c_A(r/d, r)^s c_A(n, d). \tag{3}$$

If $(r_1, r_2) = 1$, then $N_A(n, r_1 r_2, s) = N_A(n, r_1, s) N_A(n, r_2, s)$. Thus, it is sufficient to verify (3) when r is a prime power $p^a > 1$. Let $M_k(n, r, s)$ be the number of solutions of

$$n \equiv x_1 + \ldots + x_s \pmod{r^k} \tag{4}$$

such that $(x_i, r^k)_k = 1$ for $i = 1, \ldots, s$. As we have seen, $(x, p^a)_t = (x, p^a)_A$, where $t = \tau_A(p^a)$. Hence, $N_A(n, p^a, s) = M_t(n, p^{a/t}, s)$. Therefore, by [4], Theorem 12,

$$N_A(n, p^a, s) = \frac{1}{p^a} \sum_{d | p^{a/t}} c_t(p^a/d^t, p^{a/t})^s c_t(n, d).$$

As d runs over the divisors of $p^{a/t}$, d^t runs over the elements of $A(p^a)$, and $c_t(p^a/d^t, p^{a/t}) = c_A(p^a/d^t, p^a)$ and $c_t(n, d) = c_A(n, d^t)$ since $t = \tau_A(d^t)$. Thus, (3) holds whenever r is a prime power, and so for all r.

THEOREM 2. *If A is a regular arithmetical convolution, then*

$$N_A(n, r, s) = \frac{\varphi_A(r)^s}{r} \sum_{d \in A(r)} \frac{\mu_A(d)^s}{\varphi_A(d)^s} c_A(n, d)$$

$$= r^{s-1} \prod_{\substack{p | r \\ p^t | n}} \frac{(p^t - 1)\big((p^t - 1)^{s-1} - (-1)^{s-1}\big)}{p^{ts}} \prod_{\substack{p | r \\ p^t \nmid n}} \frac{(p^t - 1)^s - (-1)^s}{p^{ts}},$$

where, for each prime p which divides r, $t = \tau_A(p^a)$, where $p^a | r$ and $p^{a+1} \nmid r$.

The first of these expressions for $N_A(n, r, s)$ follows immediately from (1) and (3); when $A = U$, this evaluation was given by Cohen [10], Theorem 6.1.

The second expression extends to the case of an arbitrary regular arithmetical convolution a formula for $N_D(n, r, s) = M_1(n, r, s)$ which was given by Rademacher many years ago [1], and derived in another way by Rearick in [25]. The analogous formula for $M_k(n, r, s)$ was given by Vietoris [26] (see also [27]). We shall indicate how this latter formula can be obtained by using the k-analogue of still another evaluation of $M_1(n, r, s)$ due to Cohen [6], Theorem 7. We have

$$M_k(n, r, s) = \frac{1}{r^k} \sum_{d^k | (n, r^k)} d^k c_k\big((r/d)^k, r\big)^s \psi_k^{(s)}(d, r), \tag{5}$$

where

$$\psi_k^{(s)}(d, r) = \prod_{\substack{p|r\\ p\nmid d}} \left(1+\frac{(-1)^{s+1}}{(p^k-1)^s}\right).$$

Here, p runs over the distinct prime divisors of r which do not divide d; if there are no such primes then $\psi_k^{(s)}(d, r) = 1$. Using this to evaluate the right-hand side of (5) when r is a prime power, we obtain

$$M_k(n, r, s)$$

$$= r^{k(s-1)} \prod_{p^k|(n,r^k)} \frac{(p^k-1)\left((p^k-1)^{s-1}-(-1)^{s-1}\right)}{p^{ks}} \prod_{\substack{p|r\\ p^k\nmid n}} \frac{(p^k-1)^s-(-1)^s}{p^{ks}}.$$

When $k = 1$, this is the formula of Rademacher. From this formula we obtain immediately the second expression for $N_A(n, r, s)$ in Theorem 2.

Now we can easily obtain necessary and sufficient conditions for the non-existence of solutions of (2) which are resticted in the prescribed manner.

COROLLARY. $N_A(n, r, s) = 0$ *if and only if one of the following conditions hold*:

(i) $s = 1$ *and* $(n, r)_A \neq 1$,

(ii) $s > 1, 2 \in A(r)$, *and* $n \not\equiv s \pmod 2$.

When $A = U$, this result was obtained by Cohen [10], Theorem 6.2.

The function $\theta_A(n, r) = N_A(n, r, 2)$ is the analogue of the Nagell totient function [12]. Various results for $\theta_A(n, r)$ can be obtained by specializing those for $N_A(n, r, s)$. For the special case when $A = U$, see [17] and [18]. In particular, we have $\theta_A(n, r) = 0$ if and only if n is odd and $2 \in A(r)$.

Let $N'_A(n, r, s)$ be the number of solutions of (2) such that $\left((x_1, \ldots, x_s), r\right)_A = 1$. If we let $M'_k(n, r, s)$ be the number of solutions of (4) such that $\left((x_1, \ldots, x_s), r^k\right)_k = 1$, then for every prime power $p^a > 1$ we have $N'_A(n, p^a, s) = M'_t(n\, p^{a/t}, s)$, where $t = \tau_A(p^a)$. If we try to use this fact and the known formulas for $M'_k(n, r, s)$ ([15], p. 49) to evaluate $N'_A(n, p^a, s)$, we run into difficulties. For, these formulas involve not only the k-analogue of the Ramanujan sum (or Euler's function), but the ks-analogue or the $k(s-1)$-analogue. However, when $s = 2$, we can evaluate $\theta'_A(n, r) = N'_A(n, r, 2)$ in this way; from the formula at the bottom of p. 49 of [15] we have

$$\theta'_A(n, r) = \frac{r}{(n, r)_A}\varphi_A\left((n, r)_A\right).$$

It follows that for a prime power $p^a > 1$ we have

$$\theta'_A(n, p^a) = \begin{cases} p^a - p^{a-t} & \text{if } p^t \mid n, \\ p^a & \text{if } p^t \nmid n, \end{cases}$$

where $t = \tau_A(p^a)$. Thus, we see that for every A, $\theta'_A(n, r) \neq 0$ for all n and r. Consequently, if $s > 1$, then for every A, $N'_A(n, r, s) \neq 0$ for all n and r.

By applying the inclusion-exclusion principle, as was done on p. 50 of [15], we obtain

$$N'_A(n, r, s) = \sum_{d \in A((n,r)_A)} \mu_A(d)(r/d)^{s-1}.$$

When $A = U$ this becomes

$$N'_U(n, r, s) = \frac{r^{s-1}}{(n, r)_U^{s-1}} J_s^*\big((n, r)_U\big),$$

where J_s^* is the unitary analogue of the Jordan function; it was studied in [20].

Let $N''_A(n, r, s)$ be the number of solutions of (2) such that $(x_i, r)_A$ is a square for $i = 1, \ldots, s$. By using now familiar arguments we can evaluate this number; we use the formula of [14], Theorem 3. Let $\lambda(r) = (-1)^{\Omega(r)}$, where $\Omega(r)$ is the number of primes dividing r with repetitions counted, and let λ_A be the multiplicative function such that for every prime power $p^a > 1$, $\lambda_A(p^a) = \lambda(p^{a/t})$, where $t = \tau_A(p^a)$. If we set

$$\beta_A(r) = \sum_{d \in A(r)} d\lambda_A(r/d),$$

then

$$N''_A(n, r, s) = \frac{1}{r} \sum_{d \in A(r)} \big(\beta_A(d)\lambda_A(r/d)\big)^s c_A(n, d).$$

Let $\theta''_U(n, r) = N''_U(n, r, 2)$. For every prime power p^a we have $\lambda_U(p) = 1$, and so $\beta_U(r)$ is the sum of the unitary divisors of r. Hence, for a prime power $p^a > 1$,

$$\theta''_U(n, p^a) = \begin{cases} p^a + 3 & \text{if } p^a \mid n, \\ p^a + 2 & \text{if } p^a \nmid n. \end{cases}$$

Consequently, $\theta''_U(n, r)$ never vanishes.

REFERENCES

[1] A. Brauer, *Lösung der Aufgabe 30*, Jahresbericht der Deutschen Mathematiker-Vereinigung 35 (1926), 2. Abteilung, p. 92–94.

[2] Eckford Cohen, *An extension of Ramanujan's sum*, Duke Mathematical Journal 16 (1949), p. 85–90.

[3] — *An extension of Ramanujan's sum II. Additive properties*, ibidem 22 (1955), p. 543–550.

[4] — *An extension of Ramanujan's sum. III. Connection with totient functions*, ibidem 23 (1956), p. 623–630.

[5] — *Some totient functions*, ibidem 23 (1956), p. 515–522.

[6] — *A class of arithmetical functions*, Proceedings of the National Academy of Sciences 41 (1955), p. 939–944.

[7] — *Representations of even functions* (mod r). *I. Arithmetical identities*, Duke Mathematical Journal 25 (1958), p. 561–571.

[8] — *Representations of even functions* (mod r). *II. Cauchy products*, ibidem 26 (1959), p. 165–182.

[9] — *Arithmetical functions associated with the unitary divisors of an integer*, Mathematische Zeitschrift 74 (1960), p. 66–80.

[10] — *Unitary functions* (mod r), *I*, Duke Mathematical Journal 28 (1961), p. 475–486.

[11] — *Unitary functions* (mod r), *II*, Publicationes Mathematicae, Debrecen 9 (1962), p. 94–104.

[12] — *Nagell's totient function*, Mathematica Scandinavica 8 (1960), p. 55–58.

[13] P. J. McCarthy, *The generation of arithmetical identities*, Journal für die Reine und Angewandte Mathematik 203 (1960), p. 55–63.

[14] — *Some remarks on arithmetical identities*, American Mathematical Monthly 67 (1960), p. 539–548.

[15] — *Some more remarks on arithmetical identities*, Portugaliae Mathematica 21 (1962), p. 45–57.

[16] — *Regular arithmetical convolutions*, ibidem 27 (1968), p. 1–13.

[17] J. Morgado, *Unitary analogue of the Nagell totient function*, ibidem 21 (1962), p. 221–232.

[18] — *Some remarks on the unitary analogue of the Nagell totient function*, ibidem 22 (1963), p. 127–135.

[19] K. Nageswara Rao, *Unitary class division of integers* mod n *and related arithmetical identities*, Journal of the Indian Mathematical Society 30 (1966), p. 195–205.

[20] — *On the unitary analogues of certain totients*, Monatshefte für Mathematik 70 (1966), p. 149–154.

[21] — *On a congruence equation and related arithmetical identities*, ibidem 71 (1967), p. 24–31.

[22] W. Narkiewicz, *On a class of arithmetical convolutions*, Colloquium Mathematicum 10 (1963), p. 81–94.

[23] C. A. Nicol and H. S. Vandiver, *A von Sterneck arithmetical function and restricted partitions with respect to a modulus*, Proceedings of the National Academy of Sciences 40 (1954), p. 825–835.

[24] K. G. Ramanathan, *Some applications of Ramanujan's trigonometrical sum* $C_m(n)$, Proceedings of the Indian Academy of Sciences (A) 20 (1944), p. 62–69.

[25] David Rearick, *A linear congruence with side conditions*, American Mathematical Monthly 70 (1963), p. 837–840.

[26] L. Vietoris, *Über die Zahl der in einem k-reduzierten Restsystem liegenden Lösungen einer Kongruenz* $x_1+x_2+\ldots+x_r \equiv a(m^k)$, Monatshefte für Mathematik 71 (1967), p. 55–63.

[27] — *Über eine Zahlfunktion von K. Nageswara Rao*, ibidem 72 (1968), p. 147–151.

THE UNIVERSITY OF KANSAS

Reçu par la Rédaction le 23. 6. 1969