REGULAR CLASS DIVISION OF INTEGERS (mod r)

PENTTI HAUKKANEN

Department of Mathematics, Statistics and Philosophy,
FIN-33014 University of Tampere, Finland

1 Introduction

Let r be an integer > 1. Let $t_1(=1), t_2, \ldots, t_s(=r)$ be the divisors of r, where s is the number of divisors of r. The integers x with $1 \leq x \leq r$ fall into s mutually disjoint classes

$$C_1, C_2, \ldots, C_s,$$

where

$$C_i = \{x : 1 \leq x \leq r, \quad (x,r) = t_i\}.$$

The number of elements in C_i is equal to $\phi(r/t_i)$, where ϕ is the Euler totient function.

The sum of C_i and C_j, denoted by $C_i \oplus C_j$, is defined as the multiset given by

$$C_i \oplus C_j = \{x + y \pmod r : x \in C_i, y \in C_j\}.$$

It is known that in $C_i \oplus C_j$ elements of a class C_k occur the same number $M(i,j,k)$ of times, see R. Vaidyanathaswamy [11]. For a concrete example, see [10, Chapter XV] or [11]. The coefficients $M(i,j,k)$ can be evaluated in terms of Ramanujan sums $c(n,r)$, see K. G. Ramanathan [9]. To be more precise,

$$C_i \oplus C_j = \bigcup_{k=1}^{s} M(i,j,k)C_k, \tag{1.1}$$

where

$$M(i,j,k) = r^{-1} \sum_{d|r} c(r/d, r/t_i)c(r/d, r/t_j)c(t_k, d). \tag{1.2}$$

The product $M(i,j,k)C_k$ means the multiset, where each of the elements of the set C_k occurs $M(i,j,k)$ times.

A divisor d of r is said to be a unitary divisor of r and is denoted by $d \| r$ if $(d, r/d) = 1$. K. Nageswara Rao [7] gives class division of integers mod r with respect to unitary divisors of r. In this paper we give a class division of integers mod r with respect to A-divisors of r, where A is Narkiewicz's regular convolution [8]. This class division contains as special cases the usual class division of integers mod r and class division of integers mod r with respect to unitary divisors of r.

2 Regular convolution

In this section we introduce the concept of Narkiewicz's regular convolution. Background material on regular convolutions can be found e.g. in [6, Chapter 4] and [8]. We here review the concepts and notations needed in this paper.

For each n let $A(n)$ be a subset of the set of positive divisors of n. The elements of $A(n)$ are said to be the A-divisors of n. The A-convolution of two arithmetical functions f and g is defined by

$$(f *_A g)(n) = \sum_{d \in A(n)} f(d)g(n/d).$$

Narkiewicz [8] defines an A-convolution to be regular if

(a) the set of arithmetical functions forms a commutative ring with unity with respect to the ordinary addition and the A-convolution,

(b) the A-convolution of multiplicative functions is multiplicative,

(c) the constant function 1 has an inverse μ_A with respect to the A-convolution, and $\mu_A(n) = 0$ or -1 whenever n is a prime power.

It can be proved [8] that an A-convolution is regular if and only if

(i) $A(mn) = \{de : d \in A(m), e \in A(n)\}$ whenever $(m, n) = 1$,

(ii) for each prime power p^a (> 1) there exists a divisor $t = t_A(p^a)$ of a such that

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

where $rt = a$, and

$$A(p^{it}) = \{1,\ p^t, p^{2t}, \ldots, p^{it}\}, 0 \leq i < r.$$

The positive integer $t = t_A(p^a)$ in part (ii) is said to be the A-type of p^a. A positive integer n is said to be A-primitive if $A(n) = \{1, n\}$. The A-primitive numbers are 1 and p^t, where p runs through the primes and t runs through the A-types of the prime powers p^a with $a \geq 1$.

For all n let $D(n)$ denote the set of all positive divisors of n and let $U(n)$ denote the set of all unitary divisors of n, that is,

$$U(n) = \{d > 0 : d \mid n, (d, n/d) = 1\} = \{d > 0 : d \parallel n\}.$$

The D-convolution is the classical Dirichlet convolution and the U-convolution is the unitary convolution [3]. These convolutions are regular with $t_D(p^a) = 1$ and $t_U(p^a) = a$ for all prime powers p^a (> 1).

Throughout the rest of the paper A will be an arbitaray but fixed regular convolution.

The A-analogue of the Möbius function μ_A is the multiplicative function given by

$$\mu_A(p^a) = \begin{cases} -1 & \text{if } p^a (> 1) \text{ is } A\text{-primitive}, \\ 0 & \text{if } p^a \text{ is non-}A\text{-primitive}. \end{cases}$$

In particular, $\mu_D = \mu$, the classical Möbius function, and $\mu_U = \mu^*$, the unitary analogue of the Möbius function [3].

The symbol $(m,n)_A$ denotes the greatest divisor of m, which belongs to $A(n)$. In particular, $(m,n)_D$ is the usual greatest common divisor (m,n) of m and n.

The generalized Ramanujan's sum $c_A(n;r)$ is defined [5] by

$$c_A(n;r) = \sum_{\substack{x \pmod r \\ (x,r)_A=1}} \exp(2\pi inx/r).$$

An arithmetical evaluation is given [5] by

$$c_A(n;r) = \sum_{d \in A((n,r)_A)} d\mu_A(r/d).$$

In particular, denote

$$\phi_A(r) = c_A(0;r).$$

Then $\phi_A(r)$ is the number of integers $x \pmod r$ such that $(x,r)_A = 1$. Also

$$\phi_A(r) = \sum_{d \in A(r)} d\mu_A(r/d).$$

Cohen [1] defined an arithmetical function $f(n;r)$ to be even $\pmod r$ if

$$f(n;r) = f((n,r);r)$$

for all n. An arithmetical function $f(n;r)$ is said to be A-even $\pmod r$ [5] if

$$f(n;r) = f((n,r)_A;r)$$

for all integers n. Alternatively, we may say that $f(n;r)$ is A-even $\pmod r$ if

$$f((n,r)_A;r) = f((m,r)_A;r)$$

whenever $(n,r)_A = (m,r)_A$. In particular, D-even functions $\pmod r$ are even functions $\pmod r$.

The Cauchy product of two A-even functions $f(n;r)$ and $g(n;r) \pmod r$ is defined by

$$(f \circ g)(n;r) = \sum_{n \equiv a+b \pmod r} f(a;r)g(b;r).$$

The concept of the Cauchy product of even functions $\pmod r$ originates in Cohen [2].

It is known [5] that an arithmetical function $f(n;r)$ is A-even $\pmod r$ if and only if it has a unique representation of the form

$$f(n;r) = \sum_{d \in A(r)} \alpha(d;r)c_A(n;d),$$

where

$$\alpha(d;r) = r^{-1} \sum_{\delta \in A(r)} f(r/\delta; r) c_A(r/d; \delta)$$

The numbers $\alpha(d;r)$ are called the Fourier coefficients of f. If $f(n;r)$ and $g(n;r)$ are A-even functions (mod r) with Fourier coefficients $\alpha(d;r)$ and $\beta(d;r)$, respectively, then their Cauchy product is given as

$$(f \circ g)(n;r) = r \sum_{d \in A(r)} \alpha(d;r)\beta(d;r) c_A(n;d)$$

and so the Cauchy product $(f \circ g)(n;r)$ is also an A-even function (mod r), cf. [4].

3 Regular class division of integers (mod r)

Let r be an integer > 1 and let A be a regular convolution. Let $t_1(=1), t_2, \ldots, t_s(=r)$ be the A-divisors of r, where s is the number of A-divisors of r. The integers x with $1 \leq x \leq r$ fall into s mutually disjoint classes

$$C_1, C_2, \ldots, C_s,$$

where

$$C_i = \{x : \ 1 \leq x \leq r, \quad (x,r)_A = t_i\}. \tag{3.1}$$

The number of elements in C_i is equal to $\phi_A(r/t_i)$.

The sum of C_i and C_j, denoted by $C_i \oplus C_j$, is defined as the multiset given by

$$C_i \oplus C_j = \{x + y \pmod r : x \in C_i, y \in C_j\}. \tag{3.2}$$

We show that in $C_i \oplus C_j$ elements of a class C_k occur the same number of times and give a generalization for the formula (1.2), see Theorem 3.1.

We begin with a concrete example. Let $r = 12$ and let $A = U$, the unitary convolution. The unitary divisors of 12 are $1, 3, 4, 12$. Further, $C_1 = \{1,2,5,7,10,11\}$, $C_2 = \{3,6,9\}$, $C_3 = \{4,8\}$ and $C_4 = \{12\}$. It is easy to verify that

$$\begin{aligned}
C_1 \oplus C_1 &= 2C_1 \cup 4C_2 \cup 3C_3 \cup 6C_4, \\
C_1 \oplus C_2 &= 2C_1 \cup 3C_3, \\
C_1 \oplus C_3 &= C_1 \cup 2C_2, \\
C_1 \oplus C_4 &= C_1, \\
C_2 \oplus C_2 &= 2C_2 \cup 3C_4, \\
C_2 \oplus C_3 &= C_1, \\
C_2 \oplus C_4 &= C_2, \\
C_3 \oplus C_3 &= C_3 \cup 2C_4, \\
C_3 \oplus C_4 &= C_3, \\
C_4 \oplus C_4 &= C_4.
\end{aligned}$$

Theorem 3.1 *Let C_i and $C_i \oplus C_j$ be given as in* (3.1) *and* (3.2). *Then*

$$C_i \oplus C_j = \bigcup_{k=1}^{s} M(i,j,k)C_k, \tag{3.3}$$

where

$$M(i,j,k) = r^{-1} \sum_{d \in A(r)} c_A(r/d, r/t_i)c_A(r/d, r/t_j)c_A(t_k, d). \tag{3.4}$$

Proof Let

$$\rho^{(i)}(n;r) = \begin{cases} 1 & \text{if } (n,r)_A = t_i \text{ (or } n \in C_i), \\ 0 & \text{otherwise.} \end{cases}$$

The function $\rho^{(i)}(n;r)$ is A-even (mod r) with Fourier coefficients given as

$$\alpha(d;r) = r^{-1} \sum_{\delta \in A(r)} \rho^{(i)}(r/\delta;r)c_A(r/d;\delta) = r^{-1}c_A(r/d;r/t_i).$$

Thus $\rho^{(i)} \circ \rho^{(j)}(n;r)$ is A-even (mod r) and

$$\rho^{(i)} \circ \rho^{(j)}(n;r) = r^{-1} \sum_{;} d \in A(r)c_A(r/d;r/t_i)c_A(r/d;r/t_j)c_A(n;d). \tag{3.5}$$

Let $m \in C_k$. The number of the element m in $C_i \oplus C_j$ is equal to

$$\sum_{\substack{m \equiv a+b \pmod r \\ a \in C_i, b \in C_j}} 1$$

or

$$\rho^{(i)} \circ \rho^{(j)}(m;r).$$

Since the function $\rho^{(i)} \circ \rho^{(j)}(n;r)$ is A-even (mod r), we have $\rho^{(i)} \circ \rho^{(j)}(n;r) = \rho^{(i)} \circ \rho^{(j)}(m;r)$ whenever $(n,r)_A = (m,r)_A$ or whenever $n \in C_k$. This proves (3.3). Further,

$$\rho^{(i)} \circ \rho^{(j)}(m;r) = \rho^{(i)} \circ \rho^{(j)}((m,r)_A;r) = \rho^{(i)} \circ \rho^{(j)}(t_k;r).$$

Thus, by (3.5), we obtain (3.4). 2

References

[1] E. Cohen: A class of arithmetical functions, Proc. Nat. Acad. Sci. (USA) 41 (1955), 939–944.

[2] E. Cohen: Representations of even functions (mod r), II. Cauchy products, Duke Math. J. 26 (1959), 165–182.

[3] E. Cohen: Arithmetical functions associated with the unitary divisors of an integer, Math. Z. 74 (1960), 66–80.

[4] P. Haukkanen and P. J. McCarthy: Sums of values of even functions, Portugal. Math. 48 (1991), 53–66.

[5] P. J. McCarthy: Regular arithmetical convolutions, Portugal. Math. 27 (1968), 1-13.

[6] P. J. McCarthy: Introduction to Arithmetical Functions, Springer-Verlag Universitext (1986).

[7] K. Nageswara Rao: Unitary class division of integers mod n and related arithmetical identities, J. Indian Math. Soc., n. Ser. 30 (1966), 195–205.

[8] W. Narkiewicz: On a class of arithmetical convolutions, Colloq. Math. 10 (1963), 81–94.

[9] K. G. Ramanathan: Some applications of Ramanujan's trigonometrical sum $C_m(n)$, Proc. Ind. Acad. Sci. (A) 20 (1944), 62–69.

[10] R. Sivaramakrishnan: Classical Theory of Arithmetic Functions, Marcel Dekker: Monographs and Text Books in Pure and Applied Mathematics No. 126 (1989).

[11] R. Vaidyanathaswamy: A remarkable property of integers (mod N) and its bearing on group theory, Proc. Ind. Acad. Sci. Section A (1937), 63–75.