Collect. Math. **42**, 1 (1991), 33–44

Cauchy multiplication and periodic functions (mod r)

PENTTI HAUKKANEN

Department of Mathematical Sciences, University of Tampere,

P.O. Box 607, SF-33101 Tampere, Finland

R. SIVARAMAKRISHNAN

Department of Mathematics, University of Calicut, Calicut 673 635, India

Received 12/MAR/91

ABSTRACT

We analyse periodic functions (mod r), keeping Cauchy multiplication as the basic tool, and pay particular attention to even functions (mod r), the subclass of periodic functions (mod r) having the property $f(n) = f((n,r))$ for all n. We provide some new aspects into the Hilbert space structure of even functions (mod r) and make use of linear transformations to interpret the known number-theoretic formulae involving solutions of congruences.
1980 Mathematics Subject Classification (1985 Revision) 11A25.

1. Introduction

Let r be an arbitrary but fixed positive integer and F a field of characteristic 0 containing the rth roots of unity. In [2], Cohen defined an F-valued function f on the set of rational integers to be (r,F) arithmetic if $f(n) = f(n')$ whenever $n \equiv n' \pmod{r}$. For example, the function ϵ_j, defined by $\epsilon_j(n) = \exp(2\pi ijn/r)$, is (r,F) arithmetic for any integer j. We denote by $A_r(F)$ the set of all (r,F)

arithmetic functions. Any (r, F) arithmetic function f can be expressed uniquely in the form [11, p. 328]

$$f(n) = \sum_{j=0}^{r-1} a_j \epsilon_j(n), \tag{1}$$

where

$$a_j = r^{-1} \sum_{u \pmod r} f(u)\epsilon_j(-u). \tag{2}$$

It may be noted that (r, F) arithmetic functions are, in fact, periodic functions (mod r) [1, 9, 11].

Now, $f \in A_r(F)$ is said to be even (mod r) if $f(n) = f((n, r))$, where (n, r) is the greatest common divisor of n and r. Taking $F = \mathbb{C}$, the field of complex numbers, we consider the subclass $B_r(\mathbb{C})$ of even functions (mod r). If $f \in B_r(\mathbb{C})$, then it is known [3] that f can be written uniquely in the form

$$f(n) = \sum_{d|r} \alpha(d)\, C(n, d), \tag{3}$$

where $C(n, r)$ is Ramanujan's trigonometric sum. The coefficients $\alpha(d)$, $d \mid r$, are called the Fourier coefficients of f. They have the expressions [9, p 80, 11, p. 335]

$$\alpha(d) = r^{-1} \sum_{\delta|r} f(r/\delta) C(r/d, \delta), \tag{4}$$

$$\alpha(d) = (r\phi(d))^{-1} \sum_{a \pmod r} f(a) C(a, r), \tag{5}$$

where ϕ is the Euler totient.

E. Cohen has made an extensive study of the theory of even functions (mod r) in a series of papers [3–7]. Though the idea of an even function (mod r) is implicit in counting solutions of the linear congruence

$$n \equiv x_1 + x_2 + \cdots + x_s \pmod r \tag{6}$$

under the restriction $(x_i, r) = 1, i = 1, 2, \ldots, s$, the theory as developed by Cohen gave the clue to various number-theoretic identities [9, 11].

The purpose of this paper is to analyse certain standard properties of even functions (mod r), keeping Cauchy multiplication (for definition, see equation (7)) as the basic tool. We also make use of linear transformations to interpret the known number-theoretic formulae involving solutions of congruences. A measure theoretic approach provides a new insight into the structure of even functions (mod r).

2. The Cauchy product

The Cauchy product of $f, g \in A_r(F)$ is defined by

$$(f \circ g)(n) = \sum_{n \equiv a+b \pmod{r}} f(a)g(b), \tag{7}$$

where a, b range over the elements of a complete residue system (mod r) such that $n \equiv a + b \pmod{r}$. If

$$f(n) = \sum_{j=0}^{r-1} a_j \epsilon_j(n)$$

and

$$g(n) = \sum_{j=0}^{r-1} b_j \epsilon_j(n),$$

then their Cauchy product is given by [11, p. 329]:

$$(f \circ g)(n) = r \sum_{j=0}^{r-1} a_j b_j \epsilon_j(n). \tag{8}$$

The set $A_r(F)$ forms a commutative ring relative to ordinary addition and Cauchy multiplication. Furthermore, $A_r(F)$ has the structure of a semi-simple algebra over F and it can be expressed as the direct sum of r fields each isomorphic to F [2]. The function e_0, defined by

$$e_0(n) = \begin{cases} 1 & \text{if } n \equiv 0 \pmod{r}, \\ 0 & \text{otherwise,} \end{cases}$$

serves as the identity under Cauchy multiplication. It can be written as

$$e_0(n) = r^{-1} \sum_{j=0}^{r-1} \epsilon_j(n). \tag{9}$$

We call g the Cauchy inverse of f if $f \circ g = e_0$.

Theorem 1

Let $f \in A_r(F)$ and denote

$$f(n) = \sum_{j=0}^{r-1} a_j \epsilon_j(n).$$

Then f possesses a Cauchy inverse if and only if $a_j \neq 0$ for all $j = 0, 1, \ldots, r-1$. The Cauchy inverse is given by

$$f^{-1}(n) = r^{-2} \sum_{j=0}^{r-1} a_j^{-1} \epsilon_j(n).$$

Proof. Let

$$g(n) = \sum_{j=0}^{r-1} b_j \epsilon_j(n).$$

Then, by (8) and (9), $f \circ g = e_0$ if and only if $ra_jb_j = r^{-1}$, $j = 0, 1, \ldots, r-1$. This proves Theorem 1. □

Next, we shall confine ourselves to even functions (mod r). The Cauchy product of even functions f, g (mod r) is an even function (mod r) and is given by

$$(f \circ g)(n) = r \sum_{d|r} \alpha(d)\beta(d)C(n,d), \tag{10}$$

where $\alpha(d)$ and $\beta(d)$, $d \mid r$, are the Fourier coefficients of f and g, respectively [9, p. 84, 11, p. 338]. The identity function e_0 can also be written as

$$e_0(n) = r^{-1} \sum_{d \mid r} C(n,d). \tag{11}$$

Theorem 2

Let $f \in B_r(\mathbb{C})$ with the Fourier coefficients $\alpha(d)$, $d|r$. Then f possesses a Cauchy inverse in $B_r(\mathbb{C})$ if and only if $\alpha(d) \neq 0$ for all $d \mid r$. The Fourier coefficients of the Cauchy inverse are $r^{-2}\alpha(d)^{-1}$, $d \mid r$.

Proof. Theorem 2 follows on the lines of proof of Theorem 1 using (10) and (11). □

3. The unitary space of even functions (mod r)

It is known [8, p. 194] that the vector space $B_r(\mathbb{C})$ forms a complex Hilbert space (and therefore a unitary space) under the inner product

$$\langle f,g\rangle = \sum_{d|r} \phi(d) f(r/d)\bar{g}(r/d) = (\phi * f\bar{g})(r), \tag{12}$$

where $\bar{g}(n) = \overline{g(n)}$, the complex conjugate of $g(n)$, and $*$ is the Dirichlet convolution. We shall show this adopting a measure theoretic approach in Section 5. There we shall also prove that the above inner product can be written as

$$\langle f,g\rangle = r \sum_{d|r} \alpha(d)\overline{\beta(d)}\phi(d) = (f \circ \bar{g})(0), \tag{13}$$

where $\alpha(d)$ and $\beta(d)$, $d \mid r$, are the Fourier coefficients of f and g, respectively.

The inner product $\langle f,g\rangle$ given in (13) leads to the definition of a norm of $f \in B_r(\mathbb{C})$ naturally. That is, we define

$$\|f\| = \langle f,f\rangle^{1/2} = \left\{ r \sum_{d\,|\,r} |\alpha(d)|^2 \phi(d) \right\}^{1/2}. \tag{14}$$

The Cauchy-Schwarz inequality states that

$$|\langle f,g\rangle| \le \|f\|\,\|g\|, \qquad f,g \in B_r(\mathbb{C}). \tag{15}$$

Incidentally, we remark about the analogous inequality about $\|f \circ g\|$.

Theorem 3

For $f,g \in B_r(\mathbb{C})$,

$$\|f \circ g\| \le \sqrt{r}\,\|f\|\,\|g\|. \tag{16}$$

Proof. Suppose $\alpha(d),\beta(d)$, where $d \mid r$, are the Fourier coefficients of f and g, respectively. Then, by (10) and (14), we can write

$$\|f \circ g\|^2 = r \sum_{d\,|\,r} r^2 |\alpha(d)|^2 |\beta(d)|^2 \phi(d). \tag{17}$$

Also,

$$\|f\|^2\|g\|^2 = r^2 \sum_{d\,|\,r} \sum_{t\,|\,r} |\alpha(d)|^2 |\beta(t)|^2 \phi(d)\phi(t). \tag{18}$$

For $d = t$, the right-hand side of (18) contains

$$r^2 \sum_{d|r} |\alpha(d)|^2 |\beta(d)|^2 \phi^2(d).$$

Since, in addition, $\phi(d) \leq \phi^2(d)$ for each $d|r$, we have

$$\begin{aligned} \sum_{d|r} r^2 |\alpha(d)|^2 |\beta(d)|^2 \phi(d) &\leq r^2 \sum_{d|r} |\alpha(d)|^2 |\beta(d)|^2 \phi^2(d) \\ &\leq r^2 \sum_{d|r} \sum_{t|r} |\alpha(d)|^2 |\beta(t)|^2 \phi(d)\phi(t). \end{aligned}$$

Now, the desired inequality follows from (17) and (18). □

Next, we shall construct subspaces of $B_r(\mathbb{C})$. For $f \in B_r(\mathbb{C})$, the Fourier coefficients $\alpha(d)$, $d\,|\,r$, are known. Let q be a fixed divisor of r. Associated with f, we can contsruct an even function $f(n,q)$ (even (mod r)) by defining

$$f(n,q) = \sum_{d\,|\,q} \alpha(d)\, C(n,d). \tag{19}$$

If $d\,|\,r$, $d \nmid q$, then $\alpha(d) = 0$ in the representation of $f(n,q)$ as an element of $B_r(\mathbb{C})$. In (19) we are actually forming a 'truncated sum'.

Let $S_q(\mathbb{C})$ be the set of functions of the form (19). Then $S_q(\mathbb{C})$ forms a subspace of $B_r(\mathbb{C})$ of dimension $\tau(q)$, where $\tau(q)$ is the number of divisors of q. Since $B_r(\mathbb{C})$ is a unitary space, the orthogonal complement of $S_q(\mathbb{C})$, written $S_q^{\perp}(\mathbb{C})$, exists and we have

$$B_r(\mathbb{C}) = S_q(\mathbb{C}) \oplus S_q^{\perp}(\mathbb{C}). \tag{20}$$

In (20), $S_q^{\perp}(\mathbb{C})$ consists of functions of the form

$$f(n) = \sum_{\substack{d|r \\ d \nmid q}} \alpha(d)\, C(n,d).$$

Its dimension is $\tau(r) - \tau(q)$.

Remark 1. If $\tau(r) = m$, the complex inner product space $B_r(\mathbb{C})$ is isomorphic to the weighted Euclidean inner product space $\mathbb{C}^m$ with weights $\phi(d)$, $d\,|\,r$. In particular, when r is a prime, $B_r(\mathbb{C})$ is isomorphic to $\mathbb{C}^2$.

4. Linear transformations

Given two unitary spaces $B_r(\mathbb{C})$ and $B_{r'}(\mathbb{C})$, a transformation $T : B_r(\mathbb{C}) \to B_{r'}(\mathbb{C})$ is said to be linear if, for $f, g \in B_r(\mathbb{C})$,

$$T(z_1 f + z_2 g) = z_1 T(f) + z_2 T(g), \ z_1, z_2 \in \mathbb{C}.$$

Let $L(B_r, B_{r'})$ denote the set of linear transformations from $B_r(\mathbb{C})$ into $B_{r'}(\mathbb{C})$. Then $L(B_r, B_{r'})$ endowed with addition and scalar multiplication gives a vector space of dimension $\tau(r)\tau(r')$.

A linear transformation from $B_r(\mathbb{C})$ into itself is called a linear operator.

DEFINITION. Let $\gamma \in B_r(\mathbb{C})$. The linear operator T_γ is defined by

$$T_\gamma(f) = \gamma \circ f, \ f \in B_r(\mathbb{C}).$$

For e_0, the identity element under Cauchy multiplication,

$$T_{e_0}(f) = e_0 \circ f = f.$$

Theorem 4

If $\gamma, \eta \in B_r(\mathbb{C})$, the composition of operators T_γ and T_η has the property

$$(T_\gamma \cdot T_\eta)(f) = T_{\gamma \circ \eta}(f), \qquad f \in B_r(\mathbb{C}).$$

Proof. We have

$$(T_\gamma \cdot T_\eta)(f) = T_\gamma(T_\eta(f)) = T_\gamma(\eta \circ f) = \gamma \circ \eta \circ f = T_{\gamma \circ \eta}(f).$$

This proves Theorem 4. □

As an illustration, let

$$\rho(n) = \begin{cases} 1 & \text{if } (n, r) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

The Fourier coefficients of ρ are $r^{-1}C(r/d, r)$, $d \mid r$. We note that

$$T_\rho(f)(n) = \sum_{\substack{a=1 \\ (a,r)=1}}^{r} f(n-a), \qquad f \in B_r(\mathbb{C}).$$

If $\alpha(d)$, $d \mid r$, are the Fourier coefficients of f, then we have

$$T_\rho(f)(n) = \sum_{d \mid r} \alpha(d)\, C(r/d, r)\, C(n, d).$$

In particular,

$$T_\rho(\rho)(n) = r^{-1} \sum_{d \mid r} C(r/d, r)^2 C(n, d). \tag{21}$$

The function $T_\rho(\rho)$ is the well-known Nagell totient [9, p. 119, 11, p. 343]. Let $N(n, r, s)$ denote the number of solutions of (6). Then

$$N(n, r, s) = T_\rho^{(s-1)}(\rho), \tag{22}$$

where $T_\rho^{(s)} = T_\rho \cdot \ldots \cdot T_\rho$ (s factors), and so

$$N(n, r, s) = r^{-1} \sum_{d \mid r} C(r/d, r)^s C(n, d). \tag{23}$$

For Ramanujan's sum $C(n, r)$, we have

$$T_\rho(C)(n) = \sum_{\substack{a=1 \\ (a,r)=1}}^{r} C(n - a, r) = \mu(r)\, C(n, r) \tag{24}$$

[9, p. 86]. Thus we can write

$$(T_\rho - \mu(r) T_{e_0})(C) \equiv 0$$

and so we may look upon $\mu(r)$ as an eigenvalue of the operator $T\rho$.

If

$$\epsilon(n) = \begin{cases} 1 & \text{if } (n, r) \text{ is a square,} \\ 0 & \text{otherwise,} \end{cases}$$

we may consider the operator T_ϵ and give algebraic interpretation to the number $M(n, r, s)$ of solutions of

$$n \equiv x_1 + x_2 + \cdots + x_s \pmod{r}$$

under the restriction (x_i, r), $i = 1, 2, \ldots, s$, is a square [5]. The Fourier coefficients of the function ϵ are $r^{-1}B(r/d, r)$, $d \mid r$, where $B(n, r)$ is an analogue of Ramanujan's sum and is given by [10]

$$B(n,r) = \sum_{\substack{a \pmod r \\ (a,r) \text{ is a square}}} \exp(2\pi i a n/r) = \sum_{d \mid (n,r)} \lambda(r/d)d = \sum_{dD^2=r} C(n,d).$$

Here λ is the well-known Liouville function. Now, analogous to (21), (22), (23), and (24), we have

$$T_\epsilon(\epsilon)(n) = r^{-1} \sum_{d \mid r} B(r/d, r)^2 C(n,d), \tag{25}$$

$$M(n,r,s) = T_\epsilon^{(s-1)}(\epsilon), \tag{26}$$

$$M(n,r,s) = r^{-1} \sum_{d \mid r} B(r/d, r)^s C(n,d), \tag{27}$$

and

$$T_\epsilon(C)(n) = \lambda(r)C(n,r). \tag{28}$$

Remark 2. Since $B_r(\mathbb{C})$ is a Hilbert space, it is a complete normed linear space under the norm given in (14). It can be verified that the sequences $\{N(\cdot, r, s)\}_{s=1}^{\infty}$ and $\{M(\cdot, r, s)\}_{s=1}^{\infty}$ $(r \geq 2)$ of $B_r(\mathbb{C})$ are not Cauchy sequences. Therefore these sequences do not converge in $B_r(\mathbb{C})$.

5. Measure theoretic approach

Given the positive integer r, we write

$$X = \{d > 0 : d \mid r\}.$$

Let B denote the power set of X. Then (X, B) is a measurable space. Define a measure m on B such that

$$m(d) = \phi(r/d) \text{ for all } d \mid r.$$

It is clear that then (X, B, m) is a measure space.

Let f be a complex-valued function on X. The integral of f over X is

$$\int_X f dm = \sum_{d \mid r} f(d)\phi(r/d).$$

Then the vector space $L^2(X, B, m)$ of all measurable functions $f : X \to \mathbb{C}$ such that $|f|^2$ is integrable over X consists of all complex-valued functions on X. Since every even function $f \pmod r$ is uniquely determined by its values on X, the vector spaces $L^2(X, B, m)$ and $B_r(\mathbb{C})$ are identical. It is well known from linear algebra that the vector space $L^2(X, B, m)$ forms a Hilbert space under the inner product

$$\langle f, g \rangle = \int_X f \bar{g}\, dm.$$

This proves that the vector space $B_r(\mathbb{C})$ forms a Hilbert space under the inner product given in (12).

Theorem 5

The set

$$\{(r\phi(d))^{-1/2} C(\cdot, d) : d \mid r\} \tag{29}$$

forms an orthonormal basis of the Hilbert space $B_r(\mathbb{C})$.

Proof. It is plain that the dimension of the vector space of the complex-valued functions on X is $\tau(r)$, that is, the dimension of $B_r(\mathbb{C})$ is $\tau(r)$. Therefore it suffices to prove that the set (29) is orthonormal. For $d \mid r$, $\delta \mid r$, we have, by [6, (2.1)] and [3, (6)],

$$\sum_{e \mid r} C(r/e, d) C(r/e, \delta)\phi(e) = \phi(\delta) \sum_{e \mid r} C(r/e, d) C(r/\delta, e) = \begin{cases} r\phi(d) & \text{if } d = \delta, \\ 0 & \text{otherwise.} \end{cases}$$

This proves Theorem 5. For a similar proof of this theorem we refer to §2 of Chapter 7 of [8]. □

Remark 3. Since the set in (29) is an orthonormal basis, we have, for each $f \in B_r(\mathbb{C})$,

$$f(n) = \sum_{d \mid r} \langle f, (r\phi(d))^{-1/2} C(\cdot, d)\rangle (r\phi(d))^{-1/2} C(n, d). \tag{30}$$

Since $C(r/\delta, d)\phi(\delta) = C(r/d, \delta)\phi(d)$ [9, p. 93, 11, p. 333], we have

$$\begin{aligned}\langle f, (r\phi(d))^{-1/2} C(\cdot, d)\rangle &= \sum_{\delta \mid r} \phi(\delta) f(r/\delta)(r\phi(d))^{-1/2} C(r/\delta, d) \\ &= r^{-1/2}\phi(d)^{1/2} \sum_{\delta \mid r} f(r/\delta) C(r/d, \delta).\end{aligned}$$

Therefore,

$$\langle f, (r\phi(d))^{-1/2} C(\cdot, d)\rangle = (r\phi(d))^{1/2}\alpha(d), \qquad d \mid r, \tag{31}$$

where $\alpha(d)$ is as given in (4). Thus the equation (30) with the inner product (12) gives the Fourier expansion (3) with the Fourier coefficients given by (4).

Theorem 6

The inner products of the vector space $B_r(\mathbb{C})$ given by (12) and (13) are equal.

Proof. By Theorem 5 and Parseval's identity, for $f, g \in B_r(\mathbb{C})$,

$$\langle f, g\rangle = \sum_{d \mid r} \langle f, (r\phi(d))^{-1/2} C(\cdot, d)\rangle \overline{\langle g, (r\phi(d))^{-1/2} C(\cdot, d)\rangle}.$$

Using (31), this can be written as

$$\langle f, g\rangle = r \sum_{d \mid r} \alpha(d)\overline{\beta(d)}\phi(d),$$

where $\alpha(d)$ and $\beta(d)$, $d \mid r$, are the Fourier coefficients of f and g, respectively. Since $C(0, d) = \phi(d)$, applying (10) we see that

$$\langle f, g\rangle = (f \circ \bar{g})(0).$$

This proves Theorem 6. □

Remark 4. The equation (30) with the inner product (13) gives the Fourier expansion (3) of $f \in B_r(\mathbb{C})$ with the Fourier coefficients given by (5).

Acknowledgement. The authors are grateful to Professor Paul J. McCarthy for suggesting the inner product given in (13) and for the proof of Theorem 3.

References

1. T. M. Apostol, *Introduction to Analytic Number Theory*, Springer, New York, 1976.
2. E. Cohen, Rings of arithmetic functions, *Duke Math. J.* **19** (1952), 115–129.
3. E. Cohen, A class of arithmetical functions, *Proc. Nat. Acad. Sci. U.S.A.* **41** (1955), 939–944.
4. E. Cohen, Representations of even functions (mod r), I. Arithmetical identities, *Duke Math. J.* 25 (1958), 401–421.
5. E. Cohen, Representations of even functions (mod r), II. Cauchy products, *Duke Math. J.* **26** (1959), 105–117.
6. E. Cohen, Representations of even functions (mod r), III. Special topics, *Duke Math. J.* 26 (1959), 491–500.
7. E. Cohen, Arithmetical notes VIII. Some classes of even functions (mod r), *Collect. Math.* **16** (1964), 81–87.
8. J. Knopfmacher, *Abstract Analytic Number Theory*, North Holland, Amsterdam1975.
9. P. J. McCarthy, *Introduction to Arithmetical Functions*, Springer, New York, 1986.
10. R. Sivaramakrishnan, Square-reduced residue systems (mod r) and related arithmetical functions, *Canad. Math. Bull.* **22** (1979), 207–220.
11. R. Sivaramakrishnan, *Classical Theory of Arithmetic Functions*, Marcel Dekker, New York, 1989.