AN ARITHMETIC FUNCTION

BY LEONARD CARLITZ

1. *Introduction*. The function*

$$\psi(k, m) = \sum_{st=k} \mu(s)m^t, \tag{1}$$

where $\mu(s)$ is the Möbius function, has the property

$$\psi(k, m) \equiv 0 \pmod{k}, \tag{2}$$

for arbitrary integral m. Gegenbauer† has generalized this by replacing $\mu(s)$ by an arbitrary integral-valued function $w(s)$ for which

$$\sum_{s|k} w(s) \equiv 0 \pmod{k}, \tag{3}$$

for all k. Clearly (3) holds for the function $\mu(s)$. Since (1) is equivalent to

$$\sum_{s|k} \psi(s, m) = m^k,$$

we put

$$W(k, m) = \sum_{st=k} w(s)m^t = \sum_{sde=k} w(s)\psi(e, m) = \sum_{te=k} \psi(e, m) \sum_{s|t} w(s) \tag{4}$$

and therefore by (2) and (3),

$$W(k, m) \equiv 0 \pmod{k}, \tag{5}$$

for all m. Conversely it is easy to show, by an induction on k, that (5) implies (3). Indeed, if (3) holds for all integers $<k$, it follows from (4) and (5) that

$$\psi(1, m) \sum_{s|k} w(s) = m \sum_{s|k} w(s) \equiv 0 \pmod{k}.$$

Since this must hold for all m, we may select an m prime to k, and therefore we have (3).

---

* For references see Dickson's *History of the Theory of Numbers*, vol. 1, pp. 84–86. Cited as Dickson.

† See Dickson, p. 86.

2. *The Generalized Function.* In the right member of (1) replace m^t by an arbitrary integral-valued function $g(t)$, and define

$$\psi(k) = \psi(k, g) = \sum_{st=k} \mu(s)g(t). \tag{6}$$

From the definition it follows at once that

$$g(k) = \sum_{s|k} \psi(s),$$

and for $(h, k) = 1$,

$$\psi(hk) = \sum_{st=k} \mu(s)\psi(ht).$$

We shall now show that

$$\psi(k) \equiv 0 \pmod{k} \tag{7}$$

for all integers k if and only if

$$g(p^e t) \equiv g(p^{e-1}t) (\mathrm{mod}\ p^e) \tag{8}$$

for all primes p and all integers t. Clearly we may assume in (8) that $p \nmid t$. Then if we write $k = p^e K$, where $p \nmid K$, it is easily seen that (6) implies

$$\psi(p^e k) = \sum_{st=k} \mu(s) \{ g(p^e t) - g(p^{e-1}t) \}. \tag{9}$$

This shows that if (8) holds, then $\psi(k) \equiv 0 \pmod{p^e}$ for every p^e that divides k. Hence (8) is certainly a sufficient condition. Interchanging K and t in (9), and then inverting, we get

$$g(p^e K) - g(p^{e-1}k) = \sum_{s|k} \psi(p^e s),$$

from which it follows that (8) is also a necessary condition that (7) hold. Note that if (8) holds for each of two functions, it holds also for their product.

If now we replace the $\mu(s)$ of (6) by an integral-valued function $w(s)$ for which (3) is satisfied, we may define

$$W(k) = W(k, g) = \sum_{st=k} w(s)g(t)$$

as generalizing $\psi(k, g)$. Then as above,

$$W(k, g) = \sum_{st=k} \psi(s, g) \sum_{d \mid t} w(d),$$

and therefore if (7) and (3) hold, it follows that

$$W(k, g) \equiv 0 \pmod{k}. \tag{10}$$

Conversely it can be proved that (10) and (7) imply (3); similarly (10) and (3) imply (7).

3. *Connection with Irreducible Polynomials.* As is well known, if in (1) we put $m = p^n$, the power of a prime, the resulting function $\psi(k, p^n)$ is k times the number of irreducible polynomials of degree k in a single indeterminate, and with coefficients in the Galois field $GF(p^n)$. More generally, the number of irreducible *factorable* polynomials* in $GF(p^n)$,

$$G \equiv \prod_{j=1}^{k} (\alpha_{j0} + \alpha_{j1}x_1 + \cdots + \alpha_{js}x_s), \qquad \prod_{j=1}^{k} \alpha_{js} \neq 0,$$

is $\psi(k, p^{ns})/k$.

In the case of the general function $\psi(k) = \psi(k, g)$, for which (7) is assumed to hold, we consider a set of polynomials M with coefficients in a field (the precise nature of which need not be defined). The degree of M is assumed defined; the number of polynomials M of fixed degree m will be denoted by $f(m)$, $f(0) = 1$. It is assumed that M can be factored into a product of powers of irreducible polynomials (of the set) in essentially one way. If $\psi(k)/k$ be the number of irreducible polynomials P of degree k, we shall show that

$$mf(m) = \sum_{s=1}^{m} \psi(s) \{ f(m - s) + f(m - 2s) + \cdots \}, \tag{11}$$

or what is the same thing,

$$mf(m) = \sum_{s=1}^{m} g(s) f(m - s). \tag{12}$$

We put

$$F(m) = \prod_{\deg M = m} M, \qquad \Theta(m) = \prod_{\deg P = m} P, \tag{13}$$

* Duke Mathematical Journal, vol. 2 (1936), pp. 660–670.

so that $F(m)$ is the product of all the polynomials of degree m, $\Theta(m)$ the product of the irreducible polynomials. To express $F(m)$ in terms of Θ, let

$$M = P^e A, \qquad P \nmid A,$$

where P is of degree s, say. Then by (13),

$$F(m) = \prod_{P,e} P^{e\phi_{m-es}(P)}, \tag{14}$$

the product extending over all P, e such that $es \leqq m$, and $\phi_k(P)$ denotes the number of polynomials of degree k, not divisible by P. Evidently

$$\phi_k(P) = \begin{cases} f(k) \text{ for } k < s, \\ f(k) - f(k-s) \text{ for } k \geqq s. \end{cases}$$

Thus (14) becomes

$$F(m) = \prod_P P^{\Sigma_e e\phi_{m-es}(P)};$$

the exponent in the right member is

$$\{f(m-s) - f(m-2s)\} + 2\{f(m-2s) - f(m-3s)\} + \cdots \\ + rf(m-rs) = f(m-s) + f(m-2s) + \cdots + f(m-rs),$$

where $r = [m/s]$, the greatest integer $\leqq m/s$. Grouping together all P of equal degree, we have finally

$$F(m) = \prod_{s=1}^{m} \{\Theta(s)\}^{f(m-s)+\cdots+f(m-rs)}. \tag{15}$$

Comparison of the degree of the two members of (15) leads to

$$\begin{aligned} mf(m) &= \sum_{s=1}^{m} \psi(s) \sum_{e=1}^{r} f(m-es) \\ &= \sum_{es \leqq m} \psi(s) f(m-es) \\ &= \sum_{k \leqq m} f(m-k) \sum_{es=k} \psi(s) \\ &= \sum_{k=1}^{m} f(m-k) g(k), \end{aligned}$$

so that we have proved both (11) and (12).

4. *The L.C.M. Property.* In the paper previously referred to, the following formula appears incidentally:

$$\sum_{[s,t]=k} \psi(s, p^n)\psi(t, p^n) = \psi(k, p^{2n}), \tag{16}$$

the summation on the left extending over all s, t with least common multiple equal to k. This formula may be proved very easily; indeed it follows at once from a formula due to von Sterneck.*

Let $g_1(m)$, $g_2(m)$ denote arbitrary arithmetic functions, and $g(m) = g_1(m)g_2(m)$. Then for $\psi(k, g)$ as defined by (6), von Sterneck's formula is

$$\sum_{[s,t]=k} \psi(s, g_1)\psi(t, g_2) = \psi(k, g). \tag{17}$$

To prove this, consider the equivalent formula

$$\sum_{k|m} \sum_{[s,t]=k} \psi(s, g_1)\psi(t, g_2) = \sum_{k|m} \psi(k, g). \tag{18}$$

The summation conditions on the left are equivalent to $s|m$, $t|m$, that is, s and t independently ranging over the divisors of m. Thus we have

$$\sum_{s|m} \psi(s, g_1) \sum_{t|m} \psi(t, g_2) = g_1(m)g_2(m) = \sum_{k|m} \psi(k, g_1g_2),$$

which proves (18), and therefore (17).

If in (17) we take

$$g_1(s) = m^s, \qquad g_2(s) = n^s,$$

the formula becomes

$$\sum_{[s,t]=k} \psi(s, m)\psi(t, n) = \psi(k, mn),$$

a direct generalization of (16).

Formula (17) may be generalized to the case of m functions $g_1, \cdots, g_m$, $g = g_1g_2 \cdots g_m$,

$$\sum_{[s_1,\cdots,s_m]=k} \psi(s_1, g_1) \cdots \psi(s_m, g_m) = \psi(k, g),$$

* See Dickson, p. 151. For details of the L.C.M. calculus, see D. H. Lehmer, American Journal of Mathematics, vol. 53 (1931), pp. 843–854.

the summation extending over all sets $s_1, \cdots, s_m$, with least common multiple equal to 1.

5. *A Polynomial Analog of* $\psi(k)$. It is easy to define analogs of $\psi(k)$ having the property (2). For example, for an algebraic field, we have*

$$\psi(\mathfrak{m}, \beta) = \sum_{\mathfrak{a}\mathfrak{b}=\mathfrak{m}} \mu(\mathfrak{a})\beta^{n(\mathfrak{b})} \equiv 0 \pmod{\mathfrak{m}},$$

where $\mathfrak{m}$ is an ideal and β an integer in the field.

We now define an analog in the domain of polynomials in a single indeterminate, with coefficients in a $GF(p^n)$:

$$\psi(M, G) = \sum_{AB=M} \mu(A)G^{|B|}. \tag{19}$$

Here $\mu(A)$ is the Möbius function for the polynomial domain, and the *absolute value* $|B|$ is defined by

$$|B| = p^{nb}, \qquad b = \deg B.$$

Then it is easy to show that

$$\psi(M, G) \equiv 0 \pmod{M}, \tag{20}$$

for arbitrary polynomials G. For M irreducible, (20) reduces to Fermat's theorem.

More generally if $g(M)$ is a function of the polynomial M whose values are polynomials in $GF(p^n)$, we may define

$$\psi(M, g) = \sum_{AB=M} \mu(A)g(B),$$

and prove, exactly as above, that $\psi(M, g) \equiv 0 \pmod{M}$ if and only if

$$g(P^e M) \equiv g(P^{e-1}M) \pmod{P^e}.$$

Generally speaking, all our results for $\psi(m, g)$ carry over to the polynomial $\psi(M, g)$. In particular this is true of the L.C.M. property. The one exception is §3; there seems to be no connection between $\psi(M, G)$ and classes of irreducible polynomials.

DUKE UNIVERSITY

* Due to J. Westlund; see Dickson, p. 86.