A CLASS OF POLYNOMIALS*

BY

LEONARD CARLITZ

1. **Introduction.** For an indeterminate x in the $GF(p^n)$, put

$$[k] = x^{p^{nk}} - x, \quad F_k = [k][k-1]^{p^n} \cdots [1]^{p^{n(k-1)}}, \quad F_0 = 1; \tag{1.1}$$

then we define the function† $\psi(t)$ by means of

$$\psi(t) = \sum_{k=0}^{\infty} \frac{(-1)^k}{F_k} t^{p^{nk}}, \tag{1.2}$$

where t takes on the values

$$t = \sum_{j=0}^{\infty} c_{m-j} x^{m-j} \qquad (c_j \text{ in } GF(p^n)).$$

Then $\psi(t)$ has the linearity properties

$$\psi(t+u) = \psi(t) + \psi(u), \qquad \psi(ct) = c\psi(t), \tag{1.3}$$

for arbitrary c in $GF(p^n)$; further from (1.2) it follows that

$$-\psi(xt) = \psi^{p^n}(t) - x\psi(t). \tag{1.4}$$

In turn (1.4) implies the general relation

$$(-1)^m \psi(Mt) = \omega_M(\psi(t)), \tag{1.5}$$

where M is a polynomial in $GF(p^n)$ of degree m in x, and

$$\omega_M(u) = \sum_{j=0}^{m} \frac{(-1)^{m-j}}{F_j} \psi_j(M) u^{p^{nj}}. \tag{1.6}$$

It remains to define $\psi_j(t)$. We put

$$\begin{bmatrix} k \\ i \end{bmatrix} = \frac{F_k}{F_i L_{k-i}^{p^{ni}}}, \qquad \begin{bmatrix} k \\ 0 \end{bmatrix} = \frac{F_k}{L_k}, \qquad \begin{bmatrix} k \\ k \end{bmatrix} = 1,$$

for F_k as defined in (1.1), and

$$L_k = [k][k-1] \cdots [1], \qquad L_0 = 1;$$

then we have

* Presented to the Society, December 29, 1936; received by the editors November 23, 1936.

† For a discussion of $\psi(t)$ and $\psi_k(t)$ see the Duke Mathematical Journal, vol. 1 (1935), pp. 137–168.

$$\psi_k(t) = \sum_{i=0}^{k} (-1)^{k-i} \begin{bmatrix} k \\ i \end{bmatrix} t^{p^{ni}}, \qquad \psi_0(t) = t. \tag{1.7}$$

In this paper we shall be interested first in the polynomials $\omega_M(u)$. Evidently (1.5) implies

$$\omega_{MN}(u) = \omega_M(\omega_N(u)), \tag{1.8}$$

for arbitrary polynomials M, N. Assume next that M is *primary*, that is, the coefficient of the highest power of x occurring in M is the unit element of $GF(p^n)$. Then we define a class of polynomials $W_M(u)$ related to $\omega_M(u)$ by means of

$$\omega_M(u) = \prod_{A|M} W_A(u), \tag{1.9}$$

the product extending over all (primary) polynomials A dividing M.

As we shall see below, the polynomials $W_M(u)$ have many properties analogous to those of the well-known cyclotomic polynomials.* In particular $W_M(u)$ is irreducible in the ring $F[u]$, where $F=F(x, p^n)$ is the field of rational functions of x with coefficients in $GF(p^n)$. Again if P is an irreducible polynomial in x, the factorization of $W_M(u)$ (mod P) is determined by a very simple rule. For example, if $P \nmid M$, define $e>0$ as the smallest exponent such that

$$P^e \equiv 1 \pmod{M},$$

and put $\phi(M)=er$, where $\phi(M)$ is the Euler function for polynomials M; then we have the factorization

$$W_M(u) \equiv f_1(u)f_2(u) \cdots f_r(u) \pmod{P},$$

where each $f_i(u)$ is irreducible (mod P) and of degree e in u. Applications are made to the congruence $\omega_M(u) \equiv \delta \pmod{P}$.

2. **Notation; properties of $\omega_M(u)$.** It will be convenient to fix certain notation. If $GF(p^n)$ denotes a fixed Galois field of order p^n, we denote by $R=R(x, p^n)$ the ring of polynomials in the indeterminate x with coefficients in $GF(p^n)$. Similarly $F=F(x, p^n)$ denotes the field of rational functions of x with coefficients in $GF(p^n)$. For an additional indeterminate u, $R[u]$ and $F[u]$ denote rings of polynomials in u with coefficients in R and F, respectively. Elements of $GF(p^n)$ will usually be denoted by c, c_j; elements of R (in other words, polynomials in x over the Galois field) by A, B, C, D, H, M, N, P, where P denotes a typical irreducible polynomial in x. The poly-

* The cyclotomic polynomial $F_m(x)$ is the polynomial (with leading coefficient=1) whose roots are the primitive mth roots of unity.

nomial M is said to be *primary* if the coefficient of the highest power of x occurring in M is the unit element of $GF(p^n)$. Typical elements of $R[u]$ or $F[u]$ will be denoted by $f(u)$, $g(u)$, $h(u)$. The degree of M (for M in R) has the obvious meaning; the degree of $f(u)$ means the degree in u. If the coefficient of the highest power of u occurring in $f(u)$ is the unit element of $R(x, p^n)$, $f(u)$ is primary.

According to the formula (1.5), $\omega_M(u)$ is defined by means of the function $\psi(t)$. However as the present paper is concerned only with algebraic properties, we shall define $\omega_M(u)$ directly and show that all the properties of the polynomials follow readily from the new definition. One possibility is to take (1.6) as the definition, but it is perhaps more satisfactory to proceed somewhat differently.

For defining properties* we shall take

$$(2.1)\qquad \begin{cases} \omega_{M+N} = \omega_M + \omega_N, & \\ \omega_{cM} = c\omega_M & (c \text{ in } GF(p^n)), \\ \omega_{x^{k+1}} = (\omega_{x^k})^{p^n} - x\omega_{x^k} & (k = 0, 1, 2, \cdots), \\ \omega_1 = u, & \end{cases}$$

where M, N are arbitrary polynomials in R, and for brevity we write ω_M in place of $\omega_M(u)$. Then it is easy to see, to begin with, that for all M,

$$(2.2)\qquad \omega_{xM} = \omega_M{}^{p^n} - x\omega_M,$$

thus generalizing the third equation in (2.1). Again if in that equation we take $k=0$, we have

$$\omega_x = \omega_1{}^{p^n} - x\omega_1 = u^{p^n} - xu;$$

combining this with (2.2) we see that

$$(2.3)\qquad \omega_{xM} = \omega_x(\omega_M).$$

In this equation replace M by xM; then (2.3) becomes

$$\omega_{x^2M} = \omega_x(\omega_{xM}) = \omega_x\{\omega_x(\omega_M)\} = \omega_{x^2}(\omega_M),$$

since by the third equation in (2.1)

$$\omega_{x^2} = \omega_x{}^{p^n} - x\omega_x = \omega_x(\omega_x).$$

Continuing in this way we may show by an easy induction on k that

$$(2.4)\qquad \omega_{x^kM} = \omega_{x^k}(\omega_M),$$

* If the operator Ω is defined by $\Omega u = u^{p^n}$, then the third equation in (2.1) implies $\omega_x = (\Omega - x)u$, and it is easy to see that generally $\omega_M = M(\Omega - x)u$, where $M(\Omega - x)$ is the operator obtained by substituting $\Omega - x$ for x in M.

thus generalizing (2.2). If now we take (2.4) together with the first two equations in (2.1), we have at once

$$\omega_{MN} = \omega_M(\omega_N) = \omega_N(\omega_M), \tag{2.5}$$

for arbitrary M, N. Thus we see that (1.8) follows from the new definition (2.1). For the sequel this property is apparently fundamental.

It is now not difficult to derive the explicit formula (1.6) for the polynomial $\omega_M(u)$. Because of the linearity (with respect to t) of the polynomial $\psi_k(t)$ it is sufficient to prove (1.6) in the case $M = x^m$. The formula is clearly true for $m = 0$. Assume it true up to and including the value m. Then by the third equation in (2.1),

$$\begin{aligned}\omega_{x^{m+1}} &= \left\{\sum_{j=0}^{m} \frac{(-1)^{m-j}}{F_j}\psi_j(x^m)u^{p^nj}\right\}^{p^n} - x\sum_{j=0}^{m}\frac{(-1)^{m-j}}{F_j}\psi_j(x^m)u^{p^nj} \\ &= (-1)^{m+1}x\psi_0(x^m)u + \sum_{j=1}^{m+1}\frac{(-1)^{m+1-j}}{F_j}\left\{x\psi_j(x^m) + [j]\psi_{j-1}^{p^n}(x^m)\right\}u^{p^nj}.\end{aligned} \tag{2.6}$$

But it is easily seen that (1.7) implies*

$$\psi_k(xt) = x\psi_k(t) + [k]\psi_{k-1}^{p^n}(t);$$

also $\psi_0(x^m) = x^m$ and $F_k = [k]F_{k-1}^{p^n}$; thus (2.6) becomes

$$\omega_{x^{m+1}} = \sum_{j=0}^{m+1}\frac{(-1)^{m+1-j}}{F_j}\psi_j(x^{m+1})u^{p^nj};$$

this completes the induction, and therefore establishes (1.6). It is also evident from the induction that the coefficient of u^{p^nj} in (1.6) is integral, that is, $\psi_j(M)/F_j$ is a polynomial in x. Our results may be summed up in the following:

THEOREM 1. *The polynomial $\omega_M(u)$ defined by* (2.1) *for all M (where M is a polynomial in x with coefficients in $GF(p^n)$) satisfies the equation* (2.5). *The polynomial has the explicit expression* (1.6) *in which the coefficients of u^{p^nj} are polynomials in x. In particular $\omega_M(u)$ is linear in u† as well as in M.*

In the next place from (2.5) it follows that $\omega_M(u)$ is a divisor of $\omega_{MN}(u)$. The coefficients of u^i in the quotient are polynomials in x. This is a consequence of the following:

THEOREM 2. *If in the equation*

$$u^{m+r} + M_1u^{m+r-1} + \cdots + M_{m+r} = (u^m + A_1u^{m-1} + \cdots + A_m)(u^r + B_1u^{r-1} + \cdots + B_r)$$

* Duke Mathematical Journal, vol. 1 (1935), p. 141.

† That is, of the form $\sum_i \alpha_i u^{p^ni}$.

all the coefficients M, A, B are rational functions of x in the $GF(p^n)$, then the M's are polynomials if and only if all the A's and B's are polynomials.

This is an analogue of a well-known theorem of Gauss; the proof need not be given.

Consider now two polynomials $\omega_M(u)$, $\omega_N(u)$. We seek the greatest common divisor (ω_M, ω_N). Clearly if A is a common divisor of M and N, then ω_A is a common divisor of ω_M and ω_N. Let $D=(N, M)$ the greatest common divisor of M and N—to make it unique assume D primary—then

$$D = AM + BN,$$

for properly chosen polynomials A, B. Then by the first of (2.1),

$$\omega_D = \omega_{AM} + \omega_{BN},$$

from which follows

$$\omega_D = f(u)\omega_M + g(u)\omega_N, \tag{2.7}$$

where $f(u)$ and $g(u)$ are polynomials in u (whose coefficients are polynomials in x). But (2.7) shows that any common divisor of ω_M and ω_N is necessarily a divisor of ω_D. This proves the following theorem:

THEOREM 3. *For arbitrary M, N, the greatest common divisor of ω_M and ω_N is determined by*

$$\omega_D = (\omega_M, \omega_N), \tag{2.8}$$

where $D=(M, N)$, the greatest common divisor of M and N.

If P is an irreducible polynomial in x, then it follows from (1.6) that

$$\omega_P(u) \equiv u^{p^{nk}} \pmod{P}, \tag{2.9}$$

where k is the degree of P. Therefore by (2.5),

$$\omega_{PM} \equiv (\omega_M)^{p^{nk}} \pmod{P}.$$

If then M and e are arbitrary, we have

$$\omega_{P^eM} \equiv (\omega_M)^{p^{nke}} \pmod{P}. \tag{2.10}$$

It will be convenient for a later purpose to alter slightly the notation for the greatest common divisor in order to indicate that we are reducing coefficients (mod P). We shall use the symbol $(f(u), g(u))_P$ to denote the G.C.D. in this situation. Thus usually,

$$(f(u), g(u))_P \not\equiv (f(u), g(u)) \pmod{P}.$$

In the present case, because of (2.7), the two symbols are equivalent, and we may state

THEOREM 4. *If MN is not a multiple of the irreducible polynomial P, then for $D=(M, N)$, we have*

$$(\omega_{P^eM}, \omega_{P^fN})_P \equiv (\omega_D)^{p^{nks}} \pmod{P}.$$

where P is of degree k, and $e \leqq f$.

The theorem is an immediate consequence of (2.8) and (2.10).

Finally, we ask whether ω_M can have repeated factors. Since by (1.6) the derivative with respect to u is $(-1)^m M$, which is independent of u, there can clearly be no repeated factor. Also if the polynomial be taken (mod P), this indicates that for $P \nmid M$ there is no repeated factor. If $P \mid M$, we make use of (2.10).

THEOREM 5. *The polynomial $\omega_M(u)$ has only simple factors in $F[u]$. For $P \nmid M$, $\omega_M(u)$ has no repeated factors* (mod P). *For $M=P^eN$, $P \nmid N$, $\omega_M(u) \equiv \omega_N{}^{p^{nks}}$ (mod P), where ω_N has only simple factors.*

3. **Definition* of $W(u)$.** For convenience assume M primary. Then suppose $\omega_M(u)$ exhibited as a product of (necessarily distinct) primary polynomials f_i in $R[u]$:

$$\omega_M(u) = f_1(u)f_2(u) \cdots f_k(u), \tag{3.1}$$

so that the coefficients of $f_i(u)$ are polynomials in x. Consider those $f_i(u)$ in the right member of (3.1) that divide no $\omega_A(u)$, where A is a *proper* divisor of M. The product of those $f_i(u)$ is by definition $W_M(u)$, so that in particular $W_M(u)$ is primary. Since $A \mid M$ implies $\omega_A(u) \mid \omega_M(u)$, it is evident that $W_A(u) \mid \omega_M(u)$. Again for A a proper divisor of M, it is clear from the definition that $(W_M(u), W_A(u))=1$; thus $\omega_M(u)$ is divisible by the product $\prod W_A(u)$, extended over all A dividing M. On the other hand since to each $f_i(u)$ in the right member of (3.1) corresponds by the definition a unique $W_A(u)$ of which it is a divisor, it follows that

$$\omega_M(u) = \prod_{A \mid M} W_A(u). \tag{3.2}$$

By inversion we have for $W_M(u)$ the formula

$$W_M(u) = \prod_{M=AB} \{\omega_A(u)\}^{\mu(B)}, \tag{3.3}$$

where $\mu(B)$ is the Möbius function† for polynomials in $R(x, p^n)$.

From (3.3) certain properties of $W_M(u)$ are immediate. For example the degree of $W_M(u)$ is

* Cf. Kronecker, *Vorlesungen über Zahlentheorie*, vol. 1, 1901, p. 283.

† See American Journal of Mathematics, vol. 54 (1932), p. 39.

$$\phi(M) = \sum_{M=AB} \mu(A) \mid B \mid = \mid M \mid \prod_{P \mid M} (1 - \mid P \mid^{-1}), \tag{3.4}$$

the product extending over all irreducible divisors of M. Here $\mid M \mid = p^{nm}$, where m is the degree of M, so that $\mid M \mid$ is the degree of $\omega_M(u)$. Comparison of the degree of both members of (3.2) leads to

$$\sum_{A \mid M} \phi(A) = \mid M \mid,$$

which is of course a direct consequence of (3.4). We remark that $\phi(M)$ may be defined independently as the number of quantities in a reduced residue system (mod M).

In the next place we evaluate $W_M(0)$. Since $W_1(u) = \omega_1(u) = u$, $W_1(0) = 0$. We now assume $M \neq 1$. For $M = P^e$, P irreducible, it follows from (1.6) and (1.7) that $W_P(0) = \pm P$. In general (3.3) implies

$$W_M(u) = \prod_{M=AB} \left\{ \frac{\omega_A(u)}{u} \right\}^{\mu(B)},$$

so that

$$W_M(0) = \prod_{M=AB} (-1)^a A^{\mu(B)} = \begin{cases} (-1)^k P & \text{for } M = P^e, \\ 1 & \text{otherwise,} \end{cases} \tag{3.5}$$

where a, k is the degree of A, P, respectively.

Suppose next that M and N are arbitrary, $M \neq N$; then (3.2) implies that $W_M(u) W_N(u)$ is a divisor of $\omega_{MN}(u)$. Since $\omega_A(u)$ has no repeated factors it follows at once that

$$(W_M, W_N) = 1 \qquad (M \neq N). \tag{3.6}$$

If the irreducible $P \nmid MN$, we may assert slightly more:

$$(W_M, W_N)_P \equiv 1 \qquad (M \neq N, P \nmid MN). \tag{3.7}$$

In the general case, note that for $P \nmid M$, (3.3) implies

$$W_{P^e M} = \prod_{M=AB} \{\omega_{P^e A}\}^{\mu(B)} \prod_{M=AB} \{\omega_{P^{e-1} A}\}^{\mu(PB)} \equiv \prod_{M=AB} \{\omega_A^{\mu(B)}\}^{p^e - p^{e-1}} \pmod{P},$$

by (2.10); and therefore (for $P \nmid M$)

$$W_{P^e M} \equiv W_M^{p^e - p^{e-1}} \pmod{P}. \tag{3.8}$$

Hence we conclude that for $P \nmid MN$

$$(W_{P^e M}, W_{P^f N})_P \equiv 1 \qquad (M \neq N), \tag{3.9}$$

while

$$(W_{P^eM}, W_{P^fM})_P \equiv (W_M)^{p^e-p^{e-1}} \pmod{P} \tag{3.10}$$

for $e \leqq f$.

Consider* now the greatest common divisor of $W_M(\omega_N(u))$ and $W_N(\omega_M(u))$, or briefly

$$(W_M(\omega_N), W_N(\omega_M)).$$

We take first the case $(M, N) = 1$. Then by (3.3) and (2.5),

$$W_M(\omega_N) = \prod_{M=AB} (\omega_{AN})^{\mu(B)} = \prod_{M=AB} \prod_{AN=DE} W_D^{\mu(B)}. \tag{3.11}$$

Now since $(M, N) = 1$, the factorization DE may be obtained by factoring A and N independently and then combining in all possible ways. Thus (3.11) becomes

$$\prod_{M=ABC} \prod_{N=DE} W_{AD}^{\mu(B)} = \prod_{N=DE} \prod_{M=AH} (W_{AD})^{\sum_{H=BC} \mu(B)}, \tag{3.12}$$

but

$$\sum_{B|H} \mu(B) = \begin{cases} 1 \text{ for } H = 1, \\ 0 \text{ otherwise}, \end{cases}$$

so that $M = AG$ reduces to $M = A$. Therefore by (3.10) and (3.12) we have

$$W_M(\omega_N) = \prod_{D|N} W_{DM} \quad \text{for } (M, N) = 1. \tag{3.13}$$

Interchanging M and N, (3.13) becomes

$$W_N(\omega_M) = \prod_{A|M} W_{AN}. \tag{3.14}$$

By (3.6) the greatest common divisor of $W_M(\omega_N)$ and $W_N(\omega_M)$ may be found by picking out the equal terms in the right member of (3.13) and (3.14). But $AN = DM$ together with $(M, N) = 1$ implies $N \mid D$, whence $D = N$ and $A = M$. Thus for $(M, N) = 1$,

$$(W_M(\omega_N), W_N(\omega_M)) = W_{MN}. \tag{3.15}$$

Suppose next that the irreducible $P \mid M$; then from (3.3) follows

$$W_M(\omega_{P^e}) = \prod_{M=AB} (\omega_{P^eA})^{\mu(B)} = W_{P^eM}.$$

More generally if every irreducible divisor of A is also a divisor of M, we have similarly

---

* For the proof compare Netto, Archiv der Mathematik und Physik, (3), vol. 4 (1902), pp. 65–67.

$$W_M(\omega_A) = W_{AM}. \tag{3.16}$$

If now $M = \prod P^e$, $N = \prod P^f$ are arbitrary, put

$$M = M_0M_1, \quad M_0 = \prod P^e \ (P \mid N), \quad M_1 = \prod P^e \ (P \nmid N),$$
$$N = N_0N_1, \quad N_0 = \prod P^f \ (P \mid N), \quad N_1 = \prod P^f \ (P \nmid N),$$

so that

$$(M_0, M_1) = (N_0, N_1) = (M_1, N_1) = 1,$$

while M_0, N_0 have precisely the same irreducible divisors. Then by (3.16),

$$W_M(\omega_N) = W_{M_0M_1}(\omega_{N_0N_1}) = W_{N_0M_0M_1}(\omega_{N_1}),$$

and this in turn, by (3.13), implies

$$W_M(\omega_N) = \prod_{D \mid N_1} W_{DN_0M_0M_1}.$$

Interchanging M and N in this equation, we have

$$W_N(\omega_M) = \prod_{A \mid M_1} W_{AM_0N_0N_1}.$$

As above the condition for common factors in the right members is $DN_0M_0M_1 = AM_0N_0N_1$, that is, $DM_1 = AN_1$, whence $D = N$ and $A = M$, and therefore (3.15) holds generally. The case $M = N$ is included, for by (3.16), $W_M(\omega_M) = W_{M^2}$.

THEOREM 6. *For arbitrary M, N, the greatest common divisor*

$$(W_M(\omega_N), W_N(\omega_M)) = W_{MN}.$$

4. **Irreducibility of $W_M(u)$.** Let β be a root of $W_M(u) = 0$ in a properly chosen $F_1 \supset F(x, p^n)$. If $(M, A) = 1$, the identity (3.11) implies

$$W_M\{\omega_A(\beta)\} = \prod_{D \mid A} W_{DM}(\beta) = 0,$$

so that $\omega_A(\beta)$ is also a root of $W_M(u)$. Assume $\omega_A(\beta) = \beta$. Then the polynomial $\omega_A(u) - u = \omega_{A-1}(u)$ has a root in common with $W_M(u)$, from which it follows that $A \equiv 1 \pmod{M}$. Similarly for $(M, A) = (M, B) = 1$, $\omega_A(\beta) = \omega_B(\beta)$ implies $A \equiv B \pmod{M}$. Thus it is clear that if β is any root of $W_M(u) = 0$, then the quantities $\omega_A(\beta)$, where A ranges over a reduced residue system (mod M), are distinct roots of $W_M(u) = 0$; by calculating the degree of $W_M(u)$ it is easily seen that the $\omega_A(\beta)$ furnish all the roots.

We shall now show* that $W_M(u)$ is irreducible in $F[u]$ or what amounts

* Cf. Weber, *Algebra*, 2d edition, vol. 1, 1898, pp. 596–600.

to the same thing (by Theorems 2) in $R[u]$. Assume the factorization

$$W_M(u) = f(u)g(u), \tag{4.1}$$

where $f(u)$ is irreducible in $R[u]$. Let β be a root of $f(u)=0$ (in a field $F_1 \supset F$). By the above paragraph, if we can show that $\omega_A(\beta)$ is also a root of $f(u)=0$ for all $(A, M)=1$, it will follow that $f(u)$ coincides with $W_M(u)$, and therefore that $W_M(u)$ is irreducible in $R[u]$. Clearly it suffices to show that $\omega_P(\beta)$ is a root of $f(u)=0$ for all irreducible P not dividing M. Assume therefore that $f(\omega_P(\beta)) \neq 0$, so that necessarily $g(\omega_P(\beta))=0$. Thus we see that the polynomial $g(\omega_P(u))$ has a root in common with the irreducible $f(u)$, and therefore

$$f(u) \mid g(\omega_P(u)). \tag{4.2}$$

On the other hand, by (2.9), for P of degree k,

$$\omega_P(u) \equiv u^{p^{nk}} \pmod{P},$$

which implies

$$g(\omega_P(u)) \equiv g(u^{p^{nk}}) \equiv g^{p^{nk}}(u) \pmod{P}.$$

Comparison with (4.2) shows that

$$(f(u), g(u))_P \equiv h(u) \pmod{P},$$

where $h(u)$ is of positive degree in u. Thus (4.1) implies that $W_M(u)$ has a repeated factor (mod P); since $P \nmid M$, this contradicts Theorem 5. We may state the following:

THEOREM 7. *For arbitrary M, the polynomial $W_M(u)$ is irreducible in $F[u]$, the ring of polynomials in u with coefficients in the field $F(x, p^n)$ of rational functions of x in $GF(p^n)$.*

This theorem may be extended somewhat.* For $(M, N)=1$, let β be a root of $W_M(u)=0$, γ a root of $W_N(u)=0$. Then

$$\omega_{MN}(\beta+\gamma) = \omega_{MN}(\beta) + \omega_{MN}(\gamma) = \omega_N(\omega_M(\beta)) + \omega_M(\omega_N(\gamma)) = 0,$$

so that $\beta+\gamma$ is a root of $\omega_{MN}(u)=0$; indeed we shall now show that it is a root of $W_{MN}(u)=0$. For assume $W_D(\beta+\gamma)=0$, where D is a proper divisor of MN, from which follows $\omega_D(\beta+\gamma)=0$. Now $D=AB$, where $A \mid M$, $B \mid N$; we may suppose that A is a proper divisor of M. Then by (2.5), $\omega_{AB}(\beta+\gamma)=0$ implies $\omega_{AN}(\beta+\gamma)=0$; but as above

$$\omega_{AN}(\beta+\gamma) = \omega_A(\omega_N(\beta)) + \omega_A(\omega_N(\gamma)) = \omega_A(\omega_N(\beta)).$$

* Cf. Weber, loc. cit., pp. 600–601.

Since $(N, M)=1$, $\omega_N(\beta)$ is a root of $W_M(u)=0$ and therefore not of $\omega_A(u)=0$. This proves

$$W_{MN}(\beta+\gamma)=0 \qquad \text{(for } (M, N)=1\text{)}. \tag{4.3}$$

Under the hypothesis $(M, N)=1$ we may choose A, B such that $AM+BN=1$. Put $\alpha=\beta+\gamma$, then

$$\begin{aligned}\omega_{AM}(\alpha) &= \omega_{AM}(\beta)+\omega_{AM}(\gamma)\\ &= \omega_{AM}(\beta)+\gamma-\omega_{BN}(\gamma)\\ &= \omega_A(\omega_M(\beta))+\gamma-\omega_B(\omega_N(\gamma)),\end{aligned}$$

so that we have

$$\omega_{AM}(\alpha)=\gamma, \qquad \omega_{BN}(\alpha)=\beta. \tag{4.4}$$

Let us now assume that $W_M(u)$ factors in $F_1[u]$, where $F_1=F(\gamma)$ is the field obtained by adjoining γ to F: put

$$W_M(u)=f(u, \gamma)g(u, \gamma),$$

where $f(u, v)$, $g(u, v)$ are polynomials with coefficients in F. Let β be a root of $f(u, \gamma)=0$, then by (4.4)

$$f\{\omega_{BN}(\alpha), \omega_{AM}(\alpha)\}=0.$$

But since $W_{MN}(u)$ is irreducible in $F[u]$, it follows from the first paragraph in this section that

$$f\{\omega_{BN}(\omega_H(\alpha)), \omega_{AM}(\omega_H(\alpha))\}=0 \tag{4.5}$$

for all $(H, MN)=1$. Now for arbitrary $(D, M)=1$, we may choose H so that

$$H\equiv D \pmod{M}, \qquad H\equiv 1 \pmod{N}.$$

Since by (4.4),

$$\begin{aligned}\omega_{BN}(\omega_H(\alpha)) &= \omega_H(\omega_{BN}(\alpha))=\omega_H(\beta)=\omega_D(\beta),\\ \omega_{AM}(\omega_H(\alpha)) &= \omega_H(\omega_{AM}(\alpha))=\omega_H(\gamma)=\gamma,\end{aligned}$$

we have after substitution in (4.5),

$$f\{\omega_D(\beta), \gamma\}=0,$$

so that $f(u, \gamma)$ has all the roots of $W_M(u)=0$.

THEOREM 8. *Let $(M, N)=1$, γ a root of $W_N(u)=0$, $F_1=F(\gamma)$ the field obtained by adjoining γ to F; then the polynomial $W_M(u)$ is irreducible in $F_1[u]$.*

As an application of Theorem 7 we state the following theorems:

THEOREM 9. *The group for the field F of the equation $W_M(u)=0$ is abelian; indeed it is simply isomorphic with the group (with respect to multiplication) of the reduced residue system* (mod M).

THEOREM 10. *If β is a root of $W_M(u)$, and t is an indeterminate, then the group for the field $F(\beta, t)$ of the equation $W_M(u)=t$ is abelian; indeed it is simply isomorphic with the additive group of residues* (mod M).

5. **Irreducibility proofs for the case $M=P^e$.** In the case $M=P^e$, where P, is irreducible, Theorem 7 may be proved very quickly in the following way. Assume the factorization

$$W_{P^e}(u) = f(u)g(u),$$

where $f(u)$ and $g(u)$ are in $R[u]$. By (3.5) $W_{P^e}(0)=\pm P$, so that $f(0)g(0)=\pm P$. We may therefore suppose that $f(0)=c$, an element of $GF(p^n)$. Construct the polynomial

$$h(u) = \prod_A f(\omega_A(u)), \tag{5.1}$$

where A ranges over a reduced residue system (mod P^e). Let β be an arbitrary root of $f(u)=0$. For fixed A, $P\nmid A$, determine B such that $AB=1+DP^e$. Thus

$$\omega_B(\omega_A(\beta)) = \omega_{BA}(\beta) = \beta + \omega_{DP^e}(\beta) + \beta + \omega_D(\omega_{P^e}(\beta)) = \beta,$$

$$f[\omega_B\{\omega_A(\beta)\}] = f(\beta) = 0,$$

from which it follows that

$$h(\omega_A(\beta)) = 0,$$

so that $h(u)=0$ is satisfied by every root of $W_M(u)=0$. Therefore $W_M(u)\mid h(u)$, and $W_M(0)\mid h(0)$. But $W_{P^e}(0)=\pm P$ and from (5.1) it follows at once that $h(0)=1$. This evidently proves our theorem.

It is clear from (1.6) that except for the coefficient of the highest power of u, all coefficients of $W_P(u)$ are divisible by P, while the last coefficient is $\pm P$. Let k be the degree of P; then by (2.5) and the last sentence, we have

$$W_{P^s}(u) = \frac{\omega_{P^s}(u)}{\omega_P(u)} = \frac{\omega_P(\omega_P(u))}{\omega_P(u)} = \{\omega_P(u)\}^{p^{nk-1}} + P\cdot g(u),$$

so that except for the leading term every coefficient is a multiple of P. The last term (that is, the one free of u) is precisely $(-1)^k P$. Clearly we may continue in this way and prove that in $W_{P^e}(u)$ every coefficient after the first is divisible by P, while by (3.5) the last term is $(-1)^k P$. Then the irreducibility of $W_{P^e}(u)$ in $R[u]$ follows as a special case of the following theorem:

THEOREM 11. *If in* $f(u)=u^k+A_1u^{k-1}+\cdots+A_k$, *all the* A_i *are divisible by some irreducible* P, *while* $P^2\nmid A_k$, *then* $f(u)$ *is irreducible in* $R[u]$.

Clearly this is an analogue of Eisenstein's well-known criterion for irreducibility. To prove the theorem, assume the factorization

$$f(u) = (u^r + M_1u^{r-1} + \cdots + M_r)(u^s + N_1u^{s-1} + \cdots + N_s).$$

We may suppose that $P \mid M_r$ while $P \nmid N_s$. Then

$$A_{k-1} = N_sM_{r-1} + N_{s-1}M_r;$$

since $P \mid A_{k-1}$, $P \mid M_r$, $P \nmid N_s$, it follows that $P \mid M_{r-1}$. Similarly from

$$A_{k-2} = N_sM_{r-2} + N_{s-1}M_{r-1} + N_{s-2}M_r,$$

it follows that $P \mid M_{r-2}$. Thus we prove that all the M_i are divisible by P. Consider now the coefficient of u^r:

$$A_s = N_s + N_{s-1}M_1 + N_{s-2}M_2 + \cdots.$$

Since $P \mid A_s$ this equation is certainly impossible. Hence $f(u)$ is irreducible.

6. **Factorization of W_M (mod P).** Assume first that $P \nmid M$. As usual let k be the degree of P. Let $e>0$ be the smallest exponent such that

$$P^e \equiv 1 \pmod{M}. \tag{6.1}$$

Then $e \mid \phi(M)$, where $\phi(M)$ is the Euler function for polynomials in R, and is evaluated by (3.4). We recall for later use that $\phi(M)$ is the degree of $W_M(u)$.

To begin with, we have

$$\omega_M(u) = \prod_{A \mid M} W_A(u); \tag{6.2}$$

secondly since $M \mid (P^e-1)$ it follows that

$$\omega_M(u) \mid \omega_{P^e-1}(u). \tag{6.3}$$

Next by (2.1) and (2.10),

$$\omega_{P^e-1}(u) = \omega_{P^e}(u) - \omega_1(u) \equiv u^{p^{nk}e} - u \pmod{P}. \tag{6.4}$$

Now since P is irreducible, the complete set of residues (mod P) form a finite field, which is indeed a concrete representation of the $GF(p^{nk})$. Then by a well-known theorem, we have the identity

$$u^{p^{nk}e} - u \equiv \prod_{\deg f \mid e} f(u) \pmod{P}, \tag{6.5}$$

the product extending over all $f(u)$ irreducible (mod P) and of degree a divisor of e. Then by (6.2), (6.3), (6.4), (6.5), it follows that $W_M(u)$ is con-

gruent (mod P) to the product of a certain number of the $f(u)$ occurring in the right member of (6.5). We shall now prove that in this factorization a polynomial $f(u)$ of degree $<e$ cannot appear. For suppose

$$f(u) \mid W_M(u) \pmod{P}, \tag{6.6}$$

where $f(u)$ is of degree $s<e$. By (6.5) we have also

$$f(u) \mid u^{p^{nk_s}} - u \pmod{P}. \tag{6.7}$$

Then (6.6) and (6.7) together imply

$$f(u) \mid (W_M(u), \omega_{P^s-1}(u))_P \pmod{P}, \tag{6.8}$$

since by (2.10)

$$u^{p^{nk_s}} - u \equiv \omega_{P^s-1}(u) \pmod{P}.$$

Using (3.2), it follows from (6.8) that for some $A \mid (P^s-1)$

$$f(u) \mid (W_M(u), W_A(u)) \pmod{P}.$$

Since e is the smallest exponent for which (6.1) holds, $M \neq A$; and since $P \nmid MA$, we have a contradiction with (3.7). Therefore we conclude that all the irreducible divisors (mod P) of $W_M(u)$ are of degree e. Comparing with the degree of $W_M(u)$, we have the following:

THEOREM 12. *For irreducible $P \nmid M$, let $e>0$ be the least exponent for which $P^e \equiv 1 \pmod{M}$. Then*

$$W_M(u) \equiv f_1(u)f_2(u) \cdots f_r(u) \pmod{P}, \tag{6.9}$$

where the $f_i(u)$ are irreducible (mod P) *of degree e, and $er=\phi(M)$, as defined by* (3.4).

To remove the restriction on P we use (3.8). Then we have the more general theorem:

THEOREM 13. *For irreducible P, let $M=P^sM_1$, where $P \nmid M$. Let $e>0$ be the least exponent for which $P^e \equiv 1 \pmod{M_1}$. Then*

$$W_M(u) \equiv \{f_1(u) \cdots f_r(u)\}^{p^s-p^{s-1}} \pmod{P}, \tag{6.10}$$

where the $f_i(u)$ are irreducible (mod P) *of degree e, and $er=\phi(M_1)$.*

As an application we consider certain congruences. We take first

$$W_M(u) \equiv 0 \pmod{P}, \tag{6.11}$$

where $P \nmid M$. Since solutions occur only when $W_M(u)$ has linear factors (mod P), it is clear that P must be $\equiv 1$ (mod M). In that case there are precisely $\phi(M)$ solutions; if β is a particular solution, all solutions are furnished by $\omega_A(\beta)$, where A ranges over a reduced residue system (mod M).

Next consider the congruence

$$\omega_M(u) \equiv 0 \pmod{P}, \tag{6.12}$$

where $P \nmid M$. Let $D=(M, P-1)$, so that (as in deriving (2.7)) $D=AM+B(P-1)$, for properly chosen A, B. Then by (2.1)

$$\begin{aligned} \omega_D(u) &= g(u)\omega_M(u) + h(u)\omega_{P-1}(u) \\ &\equiv g(u)\omega_M(u) + H(u)(u^{p^{nk}} - u) \pmod{P}. \end{aligned} \tag{6.13}$$

Thus all solutions of (6.12) are also solutions of $\omega_D(u)\equiv 0 \pmod{P}$. We may therefore suppose in (6.11) that $P\equiv 1 \pmod{M}$. In this case we may show that (6.12) has $|M|$ solutions (where as above $|M|=p^{nm}$, $m=\deg M$). Indeed if we put $P-1=MD$, (2.9) and (2.5) imply

$$u^{p^{nk}} - u \equiv \omega_D(\omega_M(u)) \pmod{P}, \tag{6.14}$$

so that $\omega_M(u)$ divides $u^{p^{nk}}-u \pmod{P}$, and therefore the congruence (6.12) has the maximum number of solutions. Again a solution of (6.11) is also a solution of (6.12). Let β be a solution of $W_M(u)\equiv 0$. Then for arbitrary A we have

$$\omega_M(\omega_A(\beta)) \equiv \omega_A(\omega_M(\beta)) \equiv 0 \pmod{P},$$

so that $\omega_A(\beta)$ is a solution of $\omega_M(u)\equiv 0$. Assume next that $\omega_A(\beta)\equiv\omega_B(\beta)$, whence $\omega_{A-B}(\beta)\equiv 0$. But this implies

$$\omega_{A-B}(\omega_H(\beta)) \equiv \omega_H(\omega_{A-B}(\beta)),$$

and therefore $W_M(u)\,|\,\omega_{A-B}(u)$, so that $M\,|\,A-B$. Thus the $|M|$ roots of (6.12) are furnished by $\omega_A(\beta)$, where A ranges over a *complete* residue system (mod M). It is clear from the above that the roots of (6.11) may be described as the *primitive* roots of (6.12).

If as above $P-1=MD$, (6.14) holds and we see that

$$u^{p^{nk}} - u \equiv \prod_{\delta} \{\omega_M(u) - \delta\} \pmod{P}, \tag{6.15}$$

where δ ranges over the roots of $\omega_D(u)\equiv 0$. Since $u^{p^{nk}}-u$ is completely factorable (mod P) it follows that for fixed δ, the congruence

$$\omega_M(u) \equiv \delta \pmod{P} \tag{6.16}$$

has $|M|$ roots. If u_0 is a particular solution of (6.16), then $u_0+\mu$ is also a solution of (6.16), where μ is any solution of the congruence $\omega_M(u)\equiv 0 \pmod{P}$. Clearly if δ is not a root of $\omega_D(u)\equiv 0$, the congruence (6.16) has no solutions. This follows from

$$\omega_D\{\omega_M(u) - \delta\} \equiv \omega_{P-1}(u) - \omega_D(\delta) \equiv u^{p^{nk}} - u - \omega_D(\delta) \equiv -\omega_D(\delta),$$

for all $u \pmod P$. We may now state the following two theorems.*

THEOREM 14. *The congruence* (6.12) *is completely solvable if and only if* $P \equiv 1 \pmod M$ *similarly for* (6.11). *If* β *is any root of* (6.11), *the general solution of* (6.11) *is* $\omega_A(\beta)$, *where* A *ranges over a reduced residue system* $\pmod M$; *the general solution of* (6.12) *is* $\omega_B(\beta)$ *where* B *ranges over a complete residue system* $\pmod M$.

THEOREM 15. *Let* $P-1=MD$. *The congruence* (6.16) *is solvable if and only if* δ *is a root of* $\omega_D(\delta) \equiv 0 \pmod P$. *If* u_0 *is a particular solution of* (6.16), *then the general solution is furnished by* $u_0+\mu$, *where* μ *ranges over the roots of* $\omega_M(\mu) \equiv 0 \pmod P$.

Finally we generalize the last theorem by removing the restriction $M \mid P-1$. Let $(P-1, M)=H$, so that $M=AH$, $P-1=BH$. Then if (6.16) is assumed solvable, we have

$$\omega_B(\delta) \equiv \omega_{BHA}(u) \equiv \omega_{P-1}(\omega_A(u)) \equiv 0,$$

so that a necessary condition is

$$\omega_B(\delta) \equiv 0 \pmod P. \tag{6.17}$$

Again for $A_1M+B_1(P-1)=H$, it follows readily that

$$\omega_H(u) \equiv \omega_{A_1}(\delta) \pmod P. \tag{6.18}$$

By Theorem 15, (6.17) is a sufficient condition for the solvability of (6.18). But if (6.18) holds, it is clear that

$$\omega_M(u) \equiv \omega_{AH}(u) \equiv \omega_{AA_1}(\delta) \equiv \omega_1(\delta) - \omega_{BB_1}(\delta) \equiv \delta,$$

so that (6.16) is indeed satisfied. Thus (6.17) is both necessary and sufficient for the solvability of (6.16). Also it is evident from the above that (6.16) has exactly the same solutions as (6.18). We have therefore the following:

THEOREM 16. *For arbitrary* M, *let* $(M, P-1)=H$, $M=AH$, $P-1=BH$, $AA_1+BB_1=1$. *Then the congruence* (6.16) *is solvable if and only if* (6.17) *holds*; *the congruences* (6.16) *and* (6.18) *are equivalent.*

THEOREM 17. *Let* $(M, P-1)=1$. *Then for arbitrary* δ, *the congruence* (6.16) *has a unique solution. Thus* (6.16) *defines a* (1, 1) *transformation of the residues* $\pmod P$; *the inverse of the transformation is* $\omega_{A_1}(\delta) \equiv u \pmod P$, *where* $A_1M \equiv 1 \pmod{P-1}$.

For in this case $B=P-1$, and (6.17) is automatically satisfied.

* Analogues of well known results on binomial congruences, modulo p.

DUKE UNIVERSITY,
DURHAM, N. C.