PACIFIC JOURNAL OF MATHEMATICS
Vol. 35, No. 3, 1970

CONGRUENCE FORMULAS OBTAINED BY COUNTING IRREDUCIBLES

MICHAEL L. FREDMAN

This paper shows how a class of congruence formulas can be generated by generalizing the process of counting irreducibles in polynomial rings. Among the specific applications of the methods in this paper are a solution to the necklace problem, as well as an enumeration of the solutions to certain Diophantine equations.

Let F denote the finite field with q elements and let $F[x]$ denote the polynomial ring over F. Let $\psi(n)$ denote the number of monic irreducible polynomials of degree n in $F[x]$. It is known that

$$(1) \qquad \sum_{d|n} \mu(n/d)q^d = n\psi(n) \quad \text{when} \quad n \geqq 1 ,$$

where μ denotes the Möbius function. Since ψ is integer valued it follows that

$$(2) \qquad \sum_{d|n} \mu(n/d)q^d \equiv 0 \bmod n ,$$

whenever q is the power of a prime. This paper shows that the process of counting irreducible in polynomials rings generalizes, and that this generalization leads to a generalized congruence formula.

Let G be any commutative multiplicative semigroup with cancellation, with an identity element, 1, and with no other unit elements. Suppose that all elements in G can be factored into irreducibles and that the factorization is unique. The positive integers and the monic polynomials in the above discussion provide examples of such a structure. Now assume that G has a valuation function v with the following properties:

(a) v is integer valued.

(b) $v(1) = 0$ and $v(s) > 0$ if $s \neq 1$.

(c) $v(st) = v(s) + v(t)$.

(d) $D(k) = \sum_{s \in G,\, v(s)=k} 1$ is finite. In other words v assumes a particular value no more than a finite number of times.

The monic polynomials are an example of this kind of structure where $v(Q(x)) =$ the degree of Q. Throughout this paper we reserve the use of the letter p to denote irreducibles. Now let

(e) $\psi(n) = \sum_{p \in G,\, v(p)=n} 1$.

In the case of the monic polynomials, $D(n) = q^n$ and ψ is given by equation (1). In this paper we show that ψ is uniquely determined

by D without regard to the specific structure G to which the functions pertain as described by (d) and (e). A particular formula for arriving at ψ given D is derived, and it is shown that given any integer valued function D, the formula leads to an integer valued function ψ which has the form $n\psi(n) = \sum_{d|n} \mu(n/d)E(d)$ where E is determined by D and is integer valued. Therefore, a congruence property similar to (2) is established. It is shown that the existence of a structure G which gives rise to D by formula (d) does not affect the validity of the derived congruence property. For example, if D assumes negative values it is obvious that the derived congruence cannot be given a structural interpretation as described by (a)-(e). Convolution products play a fundamental role throughout the arguments.

1. **Definitions and lemmas.** In this section we develop the definitions and lemmas which are used in this paper. Let G be a structure with a valuation function as described in the introduction. A complex valued function over G is called an arithmetical function. We define the Dirichlet product in the usual way. Given arithmetical functions f and g, we define h by $h(t) = \sum_{rs=t} f(r)g(s)$. We write $h = f*g$ and call h the Dirichlet product of f and g. Since G satisfies (a)-(e), it is clear that the sum in the definition is finite. We note that $*$ is commutative and associative. Now let J be the function such that $J(1) = 0$ and $J(s) = 1$ when $s \neq 1$. We define the function L as follows:

$$L(s) = (J - J^2/2 + J^3/3 - J^4/4 + \cdots)(s) \tag{3}$$

where J^n denotes the n-fold Dirichlet convolution of J. For fixed s, we note that (a)-(d) and the definition of J imply that the series on the right side of equation (3) reduces to a finite sum. The following lemma expresses L explicitly.

LEMMA A. *$L(p^n) = 1/n$ when p is irreducible and $n \geqq 1$. $L(s) = 0$ if s is not a positive power of an irreducible.*

We do not prove Lemma A but remark that it can be proven by noting that equation (3) can be regarded as a formal logarithmic series, and by expressing J by using a device analogous to an Euler product. For a particular case of the lemma, see [4].

Next, we define a function over the positive integers as follows:

$$E(n) = n \sum_{\substack{s \in G \\ v(s)=n}} L(s) .$$

Now letting ψ be defined as in (e), and using (a)-(d) and Lemma A we have that

$$E(n) = n \sum_{\substack{s \in G \\ v(s)=n}} L(s) = \sum_{d|n} d\psi(d) . \tag{4}$$

Hence, $E(n)$ is integer valued and

$$n\psi(n) = \sum_{d|n} \mu(n/d)E(d) . \tag{5}$$

Now we introduce the Cauchy product. Given two complex valued functions over the nonnegative integers, f and g, we define the Cauchy product, $h = f \circ g$ in the usual way: $h(n) = \sum_{i+j=n} f(i)g(j)$. Now let D be any function over the nonnegative integers such that $D(0) = 1$. Let $\bar{D}(n) = D(n)$ when $n \geqq 1$ and $\bar{D}(0) = 0$. We define a new function $\log D$ as follows:

$$\log D(n) = (\bar{D} - \bar{D}^2/2 + \bar{D}^3/3 - \cdots)(n) \tag{6}$$

where $\bar{D}^j$ denotes the j-fold Cauchy product of $\bar{D}$. Since $\bar{D}(0) = 0$, for fixed n it is clear that the right side of equation (6) reduces to a finite sum.

Let I be the function defined by $I(0) = 1$ and $I(n) = 0$ when $n > 0$. With respect to the Cauchy product, I acts as an identity element, $f \circ I = I \circ f = f$. Now given a function C such that $C(0) = 0$, we define a new function $\exp C$ as follows:

$$\exp C(n) = (I + C/1! + C^2/2! + \cdots)(n) . \tag{7}$$

Again we note that for fixed n this definition reduces to a finite sum. The properties of the exp and log operators are summarized in the following lemmas.

LEMMA B. *Let D_1 and D_2 be two functions with $D_1(0) = D_2(0) = 1$, and C_1 and C_2 be functions with $C_1(0) = C_2(0) = 0$. Then*

(a) $\log (D_1 \circ D_2) = \log D_1 + \log D_2$.

(b) $\exp (C_1 + C_2) = (\exp C_1) \circ (\exp C_2)$.

(c) $\exp (\log D_1) = D_1$, $\log (\exp C_1) = C_1$.

LEMMA C. *Let d be a positive integer and N be an integer (positive or negative), and assume f_N is defined as follows:*

$$f_N(n) = \begin{cases} Nd/n & \text{if } d|n \\ 0 & \text{if } d \nmid n . \end{cases}$$

Then $\exp f_N$ is integer valued.

We leave that proof of Lemma B as an exercise. Lemma C can be proven as follows. Define $j(n)$ and $j^{-1}(n)$ as below:

$$j(n) = \begin{cases} 1 \text{ if } d \mid n \\ 0 \text{ if } d \nmid n \end{cases} \qquad j^{-1}(n) = \begin{cases} 1 \text{ if } n = 0 \\ -1 \text{ if } n = d \\ 0 \text{ if } n \neq 0 \text{ or } d \,. \end{cases}$$

It is easy to verify that $j^{-1} \circ j = I$ and that $\log j^{-1} = f_{-1}$. Since $\log I(n) = 0$ for all n, it follows from (a) of Lemma B that $\log j = f_1$. From (b) of Lemma B it follows that

$$\exp f_N = \begin{cases} I & \text{if } N = 0 \\ j^N & \text{if } N > 0 \\ (j^{-1})^{-N} & \text{if } N < 0 \,. \end{cases}$$

Since I, j and j^{-1} are integer valued, it follows that $\exp f_N$ is integer valued, completing the proof.

The following lemma provides another expression for the log operator.

LEMMA D. *Let f be a function such that $f(0) = 1$ and let f^{-1} denote the unique function such that $f^{-1} \circ f = I$. Then*

$$n \log f(n) = \sum_{i+j=n} i f(i) f^{-1}(j).$$

Proof. Let $\bar{f} = f - I$. It is easy to verify that $f^{-1}(n) = (I - \bar{f} + \bar{f}^2 - \bar{f}^3 + \cdots)(n)$, where for fixed n, the series reduces to a finite sum. Hence,

$$\sum_{i+j=n} i f(i) f^{-1}(j) = n\bar{f}(n) - n\bar{f}^2(n)/2 + n\bar{f}^3(n)/3 - \cdots = n \log f(n) \,.$$

2. **Theorems.** The first theorem expresses $E(n)$, defined in equation (4), in terms of the function D defined in the introduction.

THEOREM 1. *Let G be a structure of the type described in the introduction and let $D(n) = \sum_{s \in G,\, v(s)=n} 1$ and $E(n) = n \sum_{s \in G,\, v(s)=n} L(s)$. Then*

$$E(n)/n = \log D(n) \,. \tag{8}$$

Assuming Theorem 1, equation (5) implies that

$$n\psi(n) = \sum_{d \mid n} \mu(n/d) d \log D(d) = \sum_{d \mid n} \mu(n/d) E(d) \,. \tag{9}$$

Proof of Theorem 1. From the definition of L given by equation (3), $\sum_{s\in G,\, v(s)=n} L(s) = \sum_{i\geqq 1} (-1)^{i+1}/i \sum_{s\in G,\, v(s)=n} J^i(s)$. But $\sum_{v(s)=n} J^i(s) = \sum_{t_1\cdots t_i=s,\, v(s)=n} J(t_1)\cdots J(t_i) =$ (using the definition of J and properties (b) and (c) of G) $\sum_{v(t_1)+\cdots+v(t_i)=n,\, v(t_k)>0,\, 1\leqq k\leqq i} 1 =$ (using (d))

$$\sum_{\substack{m_1+\cdots+m_i=n\\ m_k>0,\ 1\leqq k\leqq i}} D(m_1)\cdots D(m_i) = \bar{D}^i(n)\ .$$

Hence by equation (6), $E(n)/n = \sum_{s\in G,\, v(s)=n} L(s) = \log D(n)$, and this proves the theorem.

Theorem 1 provides a purely arithmetical link between the functions D and ψ. Hence, the relationship between D and ψ is independent of the particular structure to which they pertain. Now $E(n)$ is integer valued as shown by equation (4), and equation (9) implies that

$$\sum_{d\mid n} \mu(n/d)E(d) \equiv 0 \bmod n\ . \tag{10}$$

This suggests the following problem. What integer valued functions D have the property that the function E defined by equation (8) is integer valued and satisfies the congruence formula in (10)? The following theorem gives the complete answer.

THEOREM 2. *Let D be an integer valued function with $D(1)=0$ and let $E(n) = n\log D(n)$. Then $E(n)$ is integer valued and $\sum_{d\mid n} \mu(n/d)E(d) \equiv 0 \bmod n$.*

Before proving Theorem 2 we return to our structural model of the problem which suggests a method of proof. If $s\in G$ and $v(s) = n$, let us say that s has degree n. Then $D(n)$ is the number of elements in G of degree n, and $\psi(n)$ is the number of those which are irreducible. Now it is obvious that all elements of degree 1 are irreducible, and so $D(1) = \psi(1)$. When $n > 1$, $\psi(n)$ is the difference between $D(n)$ and the number of elements of degree n which are reducible. But the reducible elements can be factored into irreducibles, each factor having lower degree than n. Now given ψ, equations (4), (8), and Lemma B imply that if we let $E(m) = \sum_{d\mid m} d\psi(d)$ and let $E'(m) = E(m)/m$, then $D(m) = \exp E'(m)$. Now for $n > 1$, let $\psi_n(m) = \psi(m)$ when $m < n$ and $\psi_n(m) = 0$ when $m \geqq n$. Let $E_n(m) = \sum_{d\mid m} d\psi_n(d)$, let $E_n'(m) = E_n(m)/m$, and let $D_n(m) = \exp E_n'(m)$. If we consider the subset of G generated by the irreducibles of degree $< n$, it follows that the number of elements of degree m in this subset in $D_n(m)$. Hence, $\psi(n) = D(n) - D_n(n)$. We prove Theorem 2 by letting $\psi(n)$ be defined by

equation (9), showing that $\psi(n) = D(n) - D_n(n)$ when $n > 1$, and then showing that $D_n(n)$ is integer valued.

Proof of Theorem 2. Let ψ be given by equation (9). We prove by induction on n that $\psi(n)$ is integer valued. Equation (9) then implies that E is integer valued.

From equation (6) we see that $\log D(1) = D(1)$, and from equation (9) it follows that $\psi(1) = D(1)$. Now for $n > 1$, define $E_n(m)$, $E'_n(m)$ and $D_n(m)$ as in the above discussion. Clearly $E_n(m) = E(m)$ when $m < n$ and $E(n) - E_n(n) = n\psi(n)$. Hence, by equation (7) $D(n) - D_n(n) = \psi(n)$. We complete the proof by showing that $D_n(m)$ is integer valued for all m. When $n = 2$, $E'_n(m) = \psi(1)/m$. Since $\psi(1)$ is an integer, Lemma C implies that $D_n(m)$ is integer valued. Thus $\psi(2)$ is an integer. Now for $n > 2$ assume that $\psi(k)$ is integer valued when $k = n - 1$ and that $D_k(m)$ is integer valued. By Lemma B and the definition of D_k, $D_n = D_k \circ \exp(E'_n - E'_k)$. But

$$E'_n(m) - E'_k(m) = \begin{cases} k\psi(k)/m & \text{when } k \mid m \\ 0 & \text{when } k \nmid m \text{ since } k = n - 1 . \end{cases}$$

Hence, by Lemma C, $\exp(E'_n - E'_k)$ is integer valued and since D_k is integer valued, it follows that D_n is integer valued. Therefore, $\psi(n)$ is an integer. The theorem now follows by the principle of induction.

By repeated application of Lemmas B and C in much the same manner used to prove that D_n is integer valued, we can prove the following corollary.

COROLLARY. *Assume $E(n)$ is integer valued and satisfies* (10). *Let $E'(n) = E(n)/n$. Then* $\exp E'$ *is integer valued.*

It is appropriate at this point to show that if $\psi(n)$ is nonnegative for all n then a structural interpretation of the type defined in the introduction can be constructed. The nonnegative condition on ψ is obviously necessary for the existence of such a structure.

Now given $\psi(n) \geqq 0$, we define a function v on a subset of the rational primes as follows. Let $v(p) = 1$ when p is any one of the first $\psi(1)$ primes. Let $v(p) = 2$ when p is any one of the next $\psi(2)$ primes. We continue in this manner defining v on a subset of the primes (possibly the entire set of primes). We denote this subset by Q. Next, we define v over the subset of positive integers multiplicatively generated by Q. $v(1) = 0$ and

$$v(p_1^{a_1} \cdots p_r^{a_r}) = a_1 v(p_1) + \cdots + a_r v(p_r)$$

if each $p_i \in Q$. It is clear that this subset of the positive integers along with the function v is the desired structure.

By making somewhat more general the structural axioms stated in the introduction, we can create a structural model for the cases where ψ assumes negative values. We state without proof the following theorem.

THEOREM 3. *Let G be a commutative multiplicative semi-group with cancellation, with an identity element 1, with no other unit elements, and which has unique factorization. Let v be a valuation function over G such that*

(a) *v is integer valued.*

(b) *$v(1) = 0$ and $v(s) > 0$ when $s \neq 1$.*

(c) *$v(st) = v(s) + v(t)$.*

(d) *$\sum_{s \in G,\, v(s)=n} 1$ is finite for all n.*

Assume there exists a function λ over G such that

(e) *$\lambda(1) = 1$.*

(f) *If p is irreducible, $\lambda(p) = 1$ or $\lambda(p) = -1$.*

(g) *If p is irreducible and $\lambda(p) = 1$, then $\lambda(p^n) = 1$ for all $n > 1$. If $\lambda(p) = -1$, then $\lambda(p^n) = 0$ for all $n > 1$.*

(h) *If $p_1, \cdots, p_r$ are all distinct irreducibles, then $\lambda(p_1^{a_1} \cdots p_r^{a_r}) = \lambda(p_1^{a_1}) \cdots \lambda(p_r^{a_r})$. Let $D(n) = \sum_{s \in G,\, v(s)=n} \lambda(s)$ and $\psi(n) = \sum_{p \in G,\, v(p)=n} \lambda(p)$. Then $n\psi(n) = \sum_{d|n} \mu(n/d) d \log D(d)$.*

Now given ψ we define as before a function v on a subset Q of the rational primes, but instead of defining $v(p) = n$ for $\psi(n)$ primes, we define $v(p) = n$ for $|\psi(n)|$ primes. Then using (b) and (c) we induce v on the subset G of positive integers multiplicatively generated by the primes in Q. Next, if $\psi(n) < 0$ and $v(p) = n$, define $\lambda(p) = -1$, and if $\psi(m) > 0$ and $v(p) = m$, define $\lambda(p) = 1$. Then using (e), (f), (g) and (h), we induce λ on the remaining numbers in G. It is easy to verify that G, v and λ satisfy the structural properties of Theorem 3 with $\psi(n) = \sum_{v(p)=n} \lambda(p)$.

It is convenient to recast Theorem 2 and its corollary in the language of power series. First, we observe that the ring of complex valued functions over the nonnegative integers with the operations of addition and the Cauchy product is isomorphic to the ring of power series with complex coefficients under the mapping

$$f(n) \longleftrightarrow F(x) = \sum_{n \geqq 0} f(n) x^n .$$

Next we observe that the operator, $\delta f(n) = n f(n)$ corresponds to $x(\partial/\partial x)F(x)$ under the above isomorphism. $((\partial/\partial x)$ is the formal derivative).

THEOREM 4. *Let* $\mathscr{D}(x) = 1 + \sum_{n\geq 1} D(n)x^n$ *where* $D(n)$ *is integer valued. Let* $\mathscr{E}(x) = x(\partial/\partial x)\mathscr{D}(x)/\mathscr{D}(x) = \sum_{n\geq 1} E(n)x^n$. *Then* $E(n)$ *is integer valued and* $\sum_{d|n} \mu(n/d)E(d) \equiv 0 \bmod n$. *Conversely, assume* E *is integer valued and satisfies the above congruence property. Let* $\mathscr{E}(x) = \sum_{n\geq 1} E(n)x^n$. *Then there exists a series*

$$\mathscr{D}(x) = 1 + \sum_{n\geq 1} D(n)x^n ,$$

where $D(n)$ *is integer valued, such that* $\mathscr{E}(x) = x(\partial/\partial x)\mathscr{D}(x)/\mathscr{D}(x)$.

Proof. Lemma D implies that $n \log D(n) \leftrightarrow x(\partial/\partial x)\mathscr{D}(x)/\mathscr{D}(x)$. The theorem now follows from Theorem 2 and its corollary.

Next, we consider some consequences of the above theorems.

THEOREM 5. *Assume* $E(n)$ *is an integer valued function and satisfies* (10). *For any integer* k, *let* $E_k(n) = k^n E(n)$. *Then* E_k *satisfies* (10).

Proof. Using the notation in Theorem 4, let $\mathscr{D}(x)$ be the power series such that $x(\partial/\partial x)\mathscr{D}(x)/\mathscr{D}(x) = \mathscr{E}(x)$. Let $\mathscr{D}_k(x) = \mathscr{D}(kx)$. The theorem follows when we observe that $x(\partial/\partial x)\mathscr{D}_k(x)/\mathscr{D}_k(x) = \mathscr{E}(kx)$.

THEOREM 6. *Assume* $k(n)$ *and* $E(n)$ *are integer valued functions and that* $E(n)$ *satisfies* (10). *Let* $F(n) = \sum_{j|n} k(j)^{n/j} E(n/j)j$. *Then* F *satisfies* (10).

Proof. Using the notation in Theorems 4 and 5, let $\mathscr{D}_1(x) = \prod_{j\geq 1} \mathscr{D}(k(j)x^j)$. We complete the proof by observing that

$$x\frac{\partial}{\partial x}\mathscr{D}_1(x)/\mathscr{D}_1(x) = \sum_{j\geq 1} j\mathscr{E}(k(j)x^j) = \sum_{n\geq 1} F(n)x^n .$$

Now we show an example of the use of these theorems. Let $k(j) = j^j$ and $E(j) = 1$ for all j. E satisfies (10), and therefore, by Theorem 6, $F(n) = \sigma_{n+1}(n) = \sum_{d|n} d^{n+1}$ satisfies (10). Finally, by Theorem 5, $F_k(n) = k^n\sigma_{n+1}(n)$ satisfies (10).

3. Extensions. The power series interpretation of Theorem 2 suggests the possibility of similar theorems for power series in several indeterminates. The structural interpretation in Theorem 3 would be modified to allow for vector valued valuation functions and the Cauchy product would be modified to apply to functions of several variables. For example, let G be the set of normalized

polynomials with two indeterminates over a finite field and let $Q(x, y) \in G$. Then define $v(Q(x, y)) = (m, n)$ where $m =$ the degree of Q in x and $n =$ the degree of Q in y. We state without proof the following generalization of Theorem 4.

THEOREM 7. *Let*

$$\mathscr{D}(x_1, \cdots, x_N) = 1 + \sum_{n_1+\cdots+n_N>0} D(n_1, \cdots, n_N)x_1^{n_1} \cdots x_N^{n_N}$$

where D is integer valued. Let

$$\begin{aligned}\mathscr{E}(x_1, \cdots, x_N) &= \left(x_1\frac{\partial}{\partial x_1} + \cdots + x_N\frac{\partial}{\partial x_N}\right)\mathscr{D}(x_1, \cdots, x_N)/\mathscr{D}(x_1, \cdots, x_N) \\ &= \sum_{n_1+\cdots n_N>0} E(n_1, \cdots, n_N)x_1^{n_1} \cdots x_N^{n_N} .\end{aligned}$$

Then E is integer valued and

$$\sum_{d|gcd(n_1,\cdots,n_N)} \mu(d)E(n_1/d, \cdots, n_N/d) \equiv 0 \bmod n_1 + \cdots + n_N .$$

Conversely, assume E is integer valued and satisfies the above congruence property. Let

$$\mathscr{E}(x_1, \cdots, x_N) = \sum_{n_1+\cdots+n_N>0} E(n_1, \cdots, n_N)x_1^{n_1} \cdots x_N^{n_N} .$$

Then there exists a series

$$\mathscr{D}(x_1, \cdots, x_N) = 1 + \sum_{n_1+\cdots+n_N>0} D(n_1, \cdots, n_N)x_1^{n_1} \cdots x_N^{n_N} ,$$

where D is integer valued, such that

$$\mathscr{E}(x_1, \cdots, x_N) = \left(x_1\frac{\partial}{\partial x_1} + \cdots + x_N\frac{\partial}{\partial x_N}\right)\mathscr{D}(x_1, \cdots, x_N)/\mathscr{D}(x_1, \cdots, x_N) .$$

As an example of this theorem, when D is a finite polynomial or the reciprocal of a finite polynomial, E is an N dimensional array which satisfies linear recurrence properties. Specifically, if we let $\mathscr{D}(x_1, x_2) = 1 - x_1 - x_2$, we obtain the congruence formula

$$\sum_{\substack{d|m \\ d|n}} \mu(d)\binom{\frac{m+n}{d}}{\frac{m}{d}} \equiv 0 \bmod m + n$$

where $\binom{j}{k}$ denotes the binomial coefficient.

4. **Some applications.** We conclude this paper with some

applications of these theorems to particular semigroups. As a consequence of the first application, we obtain some formulas regarding the number of solutions to certain Diophantine equations.

Let V and W be vector spaces over the rationals with bases $v_1, \cdots, v_m$, and $w_1, \cdots, w_n$ respectively. Let M be a linear map from V into W with the following properties: $M: v_i \to \sum_{j=1}^{n} a_{ij} w_j$ $1 \leqq i \leqq m$ where all a_{ij} are nonnegative integers and $M(v_i) \neq 0$ for all i.

Let $G = \{\sum_{i=1}^{m} b_i v_i \mid b_i$ are nonnegative integers$\}$. With the operation of addition, G becomes a semigroup. Using multiplicative terminology, G has unique factorization, and the irreducibles in G are $v_1, \cdots, v_m$. The map M serves as a vector valued valuation function over G. We can now apply our theorems (generalized where appropriate) to G.

Given $\omega \in W$, we define $D(\omega) = \sum_{g \in G, M(g)=\omega} 1$ and $\psi(\omega) = \sum_{p \in G, M(p)=\omega} 1$. Since we know the irreducibles in G, we can easily determine ψ. Now let $g = \sum_{i=1}^{m} c_i v_i$. Then $M(g) = \sum_{j=1}^{n} (\sum_{i=1}^{m} c_i a_{ij}) w_j$. Hence, if $\omega = \sum_{j=1}^{n} d_j w_j$ then $D(\omega) =$ the number of solutions $(c_1, \cdots, c_m)$ to the system

$$\sum_{i=1}^{m} c_i a_{ij} = d_j \qquad 1 \leqq j \leqq n ,$$

where the c_i are nonnegative integers. Using our theorems, we can express D in terms of ψ. Let $E'(\omega) = \sum_{d \mid (d_1, \cdots, d_n)} \psi(\omega/d)/d$ and let $\mathscr{E}'(z_1, \cdots, z_n) = \sum_{d_1 + \cdots + d_n > 0} E'(d_1 w_1 + \cdots + d_n w_n) z_1^{d_1} \cdots z_n^{d_n}$. Then

$$\begin{aligned} \mathscr{D}(z_1, \cdots, z_n) &= 1 + \sum_{d_1 + \cdots + d_n > 0} D(d_1 w_1 + \cdots + d_n w_n) z_1^{d_1} \cdots z_n^{d_n} \\ &= \exp(\mathscr{E}'(z_1, \cdots, z_n)) . \end{aligned}$$

As a consequence of the next application, we obtain an enumeration of irreducible polynomials over the field F of order 2 that equal their own reversals.

Let $F[x]$ denote the ring of binary polynomials and let $p(x) \in F[x]$. If $p(x)$ is of degree n, we define the reversal $\bar{p}(x)$ of $p(x)$ with the equation $\bar{p}(x) = x^n p(1/x)$, and $\bar{p}(x) \in F[x]$. It is easy to verify that $\bar{p}(x)\bar{q}(x) = \overline{p(x)q(x)}$. If the constant term of $p(x)$ is nonzero, then $\deg \bar{p}(x) = \deg p(x)$ and $\bar{\bar{p}}(x) = p(x)$. We say that $p(x)$ is self-reversible if $\bar{p}(x) = p(x)$. If $q(x)$ is a polynomial with a nonzero constant term, then $q(x)\bar{q}(x)$ is self-reversible. Finally, if $p(x)$ and $q(x)$ are self-reversible, then $p(x)q(x)$ is self-reversible; if $r(x) \mid p(x)$, then $\bar{r}(x) \mid p(x)$; and if $q(x) \mid p(x)$, then $p(x)/q(x)$ is self-reversible.

Now let G denote the subset of $F[x]$ consisting of all self-reversible polynomials. From the above we see that G is a semigroup. Now we show that factorization is unique within G. To distinguish between irreducibles in $F[x]$ and irreducibles in G (which may not

be irreducible as polynomials in $F[x]$), we refer to irreducibles as F-irreducibles or G-irreducibles accordingly. Let $q(x)$ be G-irreducible and suppose in $F[x]$ we have $p(x) \mid q(x)$ where $p(x)$ is F-irreducible. Then $\bar{p}(x) \mid q(x)$. If $\bar{p}(x) = p(x)$ then $p(x) \in G$ and $p(x) \mid q(x)$ in G. Hence $q(x) = p(x)$ since $q(x)$ is G-irreducible. If $\bar{p}(x) \neq p(x)$, then since $\bar{p}(x)$ is F-irreducible, $p(x)\bar{p}(x) \mid q(x)$ in $F[x]$. But $p(x)\bar{p}(x) \in G$ and therefore $p(x)\bar{p}(x) \mid q(x)$ in G. Hence, $q(x) = p(x)\bar{p}(x)$. Thus, G-irreducibles are characterized as being either self-reversible F-irreducible polynomials, or of the form $p(x)\bar{p}(x)$ where $p(x)$ is an F-irreducible and $p(x) \neq \bar{p}(x)$. From this it is easy to show that factorization in G is unique, and we can apply our theorems to G.

First, it is easy to see that

$$D(n) = \sum_{\substack{q(x) \in G \\ \deg q = n}} 1 = \begin{cases} 2^{n/2} & n \text{ even} \\ 2^{(n-1)/2} & n \text{ odd} \end{cases}$$

and therefore, that $\mathscr{D}(z) = 1 + \sum_{n>0} D(n)z^n = (1+z)/(1-2z^2)$. Using our previous notation, it follows that $E(n) = \begin{cases} 1 & n \text{ odd} \\ 2^{(n+2)/2} - 1 & n \text{ even} \end{cases}$. Now

$$\psi(n) = \sum_{\substack{p(x) \in G \\ \deg p = n \\ p\ G\text{-irreducible}}} 1 = (1/n) \sum_{d \mid n} \mu(d) E(n/d) .$$

Let $\psi_1(n) = \sum_{p(x) \in F[x],\ \deg p = n,\ p\ F\text{-irreducible}} 1$. We know that

$$\psi_1(n) = (1/n) \sum_{d \mid n} \mu(d) 2^{n/d} . \quad \text{It follows that}$$

$$\psi(n) = \begin{cases} 1 \text{ when } n = 1, 2 \\ 0 \text{ when } n > 1 \text{ and } n \text{ odd} \\ \psi_1(n/2) \text{ when } n \text{ is even and } > 2 . \end{cases} \tag{11}$$

Using this information, we can derive a formula for $\tau(n) =$ the number of irreducible self-reversible polynomials in $F[x]$. Clearly $\tau(n) \leqq \psi(n)$. Hence, $\tau(1) = 1$ and $\tau(n) = 0$ when n is odd and > 1. Now using our characterization of G-irreducibles, we have that $\psi(2n) = (1/2)(\psi_1(n) - \tau(n)) + \tau(2n)$ when $n > 1$. (The argument fails when $n = 1$ since x is irreducible but has a zero constant term). Now by (11), $\psi(2n) = \psi_1(n)$, and therefore,

$$\begin{aligned} \tau(2n) &= (1/2)(\psi_1(n) + \tau(n)) \text{ when } n > 1 \\ \tau(2n+1) &= 0 \text{ when } n \geqq 1 \\ \tau(1) &= \tau(2) = 1 . \end{aligned}$$

Using these formulas, τ can be determined recursively for all n. The problem of enumerating self-reversible irreducibles is sometimes

referred to as the necklace problem. In a similar manner we can solve the problem of enumerating irreducibles $p(x)$ such that $p(x) = p(x + 1)$. This time we have

$$\tau(n) = 0 \quad n \text{ odd}$$
$$\tau(n) = (1/2)(\psi_1(n/2) + \tau(n/2)) \quad n \text{ even}.$$

REFERENCES

1. L. Carlitz, *The distribution of irreducible polynomials in several indeterminates*, Illinois J. Math. **7** (1963), 371-375.
2. ———, *The distribution of irreducible polynomials in several indeterminates* II, Canad. J. Math. **17** (1965), 261-266.
3. Stephen D. Cohen, *The distribution of irreducible polynomials in several indeterminates over a finite field*, Proc. Edinburgh Math. Soc. (2) **16** (1968/69), 1-17.
4. Herbert S. Zuckerman, *On some formulas involving the divisor function*, Bull. Amer. Math. Soc. **49** (1943) 292-298.

Received January 30, 1970.

UNIVERSITY OF CALIFORNIA, BERKELEY