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

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

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

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

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