COUNTING POLYNOMIAL FUNCTIONS (mod p^n)

BY GORDON KELLER* AND F. R. OLSON

If Z is the ring of integers and Z_n is the ring of integers mod p^n, then to every polynomial F in $Z[x]$ there corresponds in a natural way (evaluation in Z_n) a function from Z_n into Z_n which we shall call F_n.

The total number of functions from Z_n into Z_n which can be realized as as polynomial functions has been computed [3]. We shall give a considerably shorter demonstration of this count.

We shall then use the same techniques to give a count of all permutations on Z_n which can be realized as polynomial functions. This count is the main result of the paper. (In the literature polynomials which yield permutations on Z_n are said to be uniformly distributed (mod p^n) [4].)

It is easily seen that for a fixed n the set of all F_n such that F is in $Z[x]$ form a finite ring under point-wise addition and multiplication. We designate this ring by R_n and denote its order by r_n. If two polynomials are being considered as functions in R_n then $f = g$ is used to designate the fact that the functions on Z_n given by f and g are the same. Whether or not a specific polynomial such as x is being considered as an element of $Z[x]$ or an element of R_n will not be mentioned unless the context is ambiguous.

Let $x^{[j]} = x(x-1)(x-2)\cdots(x-j+1)$ for j any integer greater than 0 and let $x^{[0]} = 1$. Obviously $x^{[j]}$ is in $Z[x]$ for every $j \geq 0$. Since x^m appears with coefficient 0 in $x^{[j]}$ for $j < m$ and with coefficient 1 in $x^{[m]}$ it is clear that x^m is an integer combination of the $x^{[j]}$ for $j \leq m$. Thus we see easily that the $x^{[j]}$ for $j \geq 0$ form a Z-basis for $Z[x]$. (Actually it is well known that $x^m = \sum_{i=1}^{m} s_i^m x^{[i]}$ for $m > 0$, where the s_i^m are Stirling numbers of the second kind.)

We shall now give the reason for using the polynomials $x^{[j]}$. Since the product of any t consecutive integers is divisible by $t!$, the value of $x^{[t]}$ at any integer is divisible by the highest power of p dividing $t!$. Let $\alpha(t)$ be the largest integer s such that $p^s \mid t!$. If $\alpha(j) \geq n$, $x^{[j]}$ vanishes (mod p^n). Therefore, if $f \in R_n$, there exists a polynomial $F = \sum_{\alpha(j)<n} b_j x^{[j]}$ such that $f = F_n$. In fact, since our only concern is evaluation on Z_n, we may take $b_j \geq 0$. Let $b_j = \sum a_{ij} p^i$ with $0 \leq a_{ij} \leq p-1$. If $i + \alpha(j) \geq n$, $p^i x^{[j]}$ vanishes (mod p^n). Therefore F can be chosen in the form $\sum_{i+\alpha(j)<n} a_{ij} p^i x^{[j]}$ with $F_n = F$.

THEOREM 1. *If $f \in R_n$, there exists one and only one polynomial F in $Z[x]$ with $f = F_n$, with $F = \sum_{i+\alpha(j)<n} a_{ij} p^i x^{[j]}$ such that $0 \leq i, j$ and the a_{ij} integers with $0 \leq a_{ij} \leq p-1$.*

Proof. Let $f \in R_n$. We have just seen that a polynomial F of the form

Received June 28, 1967.
*The first author was supported in part by NSF GP-5434.