Europ. J. Combinatorics (1997) **18,** 601–606

Roots of Polynomials Modulo Prime Powers

BRUCE DEARDEN AND JERRY METZGER

In general, not every set of values modulo n will be the set of roots modulo n of some polynomial. In this note, some characteristics of those sets which are root sets modulo a prime power are developed, and these characteristics are used to determine the number of different sets of integers which are root sets of polynomials modulo some prime powers.

1. INTRODUCTION

To say that R is a root set modulo n means that R is a subset of $\mathbf{Z}_n$, the ring of integers modulo n, and there is a polynomial the roots of which modulo n are exactly the elements of R. Note that $\varnothing$ and $\mathbf{Z}_n$ are always root sets modulo n.

It seems that only two papers have appeared which mention the nature of root sets modulo n, and then only at a very basic level: Sierpiński [3] and Chojnacka-Pniewska [1] noted that not every subset of $\mathbf{Z}_6$ is a root set modulo 6. Of course, for a prime p, every subset of $\mathbf{Z}_p$ is a root set modulo p, but, in general, it appears that the property of being a root set modulo n is rare. The theorems of the next section provide tools that permit the efficient computation of the number of root sets modulo a prime power.

Throughout this note, p is a prime and k is a positive integer.

For an integer j and an integer $m \geqslant 1$, $j^{\underline{m}}$, read j to the m falling, is defined by

$$j^{\underline{m}} = j(j-1)(j-2)\cdots(j-m+1).$$

Also $j^{\underline{0}}$ is defined to be 1.

For an integer $n \geqslant 1$, and a prime p, $\varepsilon_p(n)$ will denote the highest power of p that divides n. It is well known (see Graham, Knuth and Patashnik [2], for example), that for an integer $n \geqslant 1$, $\varepsilon_p(n!) = \sum_{i\geqslant 1}\left\lfloor \frac{n}{p^i}\right\rfloor$. Finally, $\varepsilon_p(0)$ is taken to be $+\infty$.

LEMMA 1. *For integers $j, m \geqslant 0$, $\varepsilon_p(j^{\underline{m}}) \geqslant \varepsilon_p(m!)$.*

PROOF. For $0 \leqslant j < m$, $j^{\underline{m}} = 0$, and the inequality is clear.
For $j \geqslant m$,

$$\begin{aligned}\varepsilon_p(j^{\underline{m}}) &= \varepsilon_p\left(\frac{j!}{(j-m)!}\right)\\ &= \varepsilon_p(j!) - \varepsilon_p((j-m)!)\\ &= \sum_{i\geqslant 1}\left(\left\lfloor \frac{j}{p^i}\right\rfloor - \left\lfloor \frac{j-m}{p^i}\right\rfloor\right)\\ &\geqslant \sum_{i\geqslant 1}\left\lfloor \frac{m}{p^i}\right\rfloor \qquad (\text{since } \lfloor a+b\rfloor \geqslant \lfloor a\rfloor + \lfloor b\rfloor)\\ &= \varepsilon_p(m!).\end{aligned}$$

□

LEMMA 2. *If $j(m!) \equiv 0 (\text{mod } p^k)$, then, for every $t \in \mathbf{Z}_{p^k}$, $j(t^{\underline{m}}) \equiv 0 (\text{mod } p^k)$.*

0195-6698/97/060601 + 06 $25.00/0 ej960124

Proof. For $0 \leqslant t < m$, $j(t^{\underline{m}}) = 0$, and so certainly $j(t^{\underline{m}}) \equiv 0 (\bmod p^k)$ in that case. On the other hand, if $t \geqslant m$, then, by Lemma 1, $\varepsilon_p(j(t^{\underline{m}})) \geqslant \varepsilon_p(j(m!))$. By hypothesis, the last quantity is at least k, and so $j(t^{\underline{m}}) \equiv 0 (\bmod p^k)$. □

2. The Main Results

Theorem 1. *Let R be a root set modulo p^k. For each $j = 0, 1, 2, \ldots, p-1$, there is a polynomial f_j the root set modulo p^k of which is exactly $R_j = \{r \in R \mid r \equiv j (\bmod p)\}$.*

Proof. For each $0 \leqslant j \leqslant p-1$, form two polynomials by splitting the factors, $(x-t)$, of $x^{\underline{p^k}}$ into two groups: $K_j(x)$ is the product of those factor for which $t \equiv j (\bmod p)$, and $L_j(x)$ is the product of those factors for which $t \not\equiv j (\bmod p)$. Note that for $r \equiv j (\bmod p)$, $K_j(r) \equiv 0 (\bmod p^k)$ and $L_j(r)$ is not a zero divisor modulo p^k, while if $r \not\equiv j (\bmod p^k)$, then $K_j(r)$ is not a zero divisor modulo p^k and $L_j(r) \equiv 0 (\bmod p^k)$.

Now, let f be any polynomial with root set R modulo p^k, and define $f_j(x) = L_j(x)f(x) + K_j(x)$. For $r \not\equiv j (\bmod p)$, we have $f_j(r) \equiv K_j(r) \not\equiv 0 (\bmod p^k)$. And for $r \equiv j (\bmod p)$, we have $f_j(r) \equiv 0 \ (\bmod p^k)$ iff $L_j(r)f(r) \equiv 0 \ (\bmod p^k)$. Since $L_j(r)$ is not a zero divisor modulo p^k, we see that the root set of f_j is exactly R_j. □

Theorem 1 says when a root set modulo p^k is decomposed into p segments, each of a fixed value modulo p, then each segment is itself a root set modulo p^k. The next theorem shows that such segments can always be reassembled into a root set modulo p^k.

Theorem 2. *Let $R_0, R_1, R_2, \ldots, R_{p-1}$ be a collection of root sets modulo p^k such that for $0 \leqslant j \leqslant p-1$, the elements of R_j are all congruent to j modulo p. Then $R_0 \cup R_1 \cup R_2 \cup \cdots \cup R_{p-1}$ is a root set modulo p^k.*

Proof. For each $j = 0, 1, \ldots, p-1$, let f_j be a polynomial with root set R_j modulo p^k. Using the polynomials $L_j(x)$ defined in the proof of Theorem 1, let

$$f(x) = \sum_{0 \leqslant j < p} L_j(x) f_j(x).$$

Note that if $r \in \mathbf{Z}_{p^k}$ and $r \equiv t (\bmod p)$, then

$$f(r) \equiv \sum_{0 \leqslant j < p} L_j(r) f_j(r) \equiv L_t(r) f_t(r) (\bmod p^k),$$

since $L_j(r) = 0$ if $j \not\equiv t (\bmod p)$. It follows that if r is a root of $f(x)$ modulo p^k, then $f_t(r) \equiv 0 (\bmod p^k)$, since $L_t(r)$ is not a zero divisor modulo p^k. Thus every root of f modulo p^k appears among the roots of the $f_0, f_1, \ldots, f_{p-1}$ modulo p^k. Conversely, if r is a root of some f_j, then it is also a root of f. □

For $S \subseteq \mathbf{Z}_n$ and $j \in \mathbf{Z}_n$, the notation $j + S$ will mean $\{j + s \mid s \in S\}$. If $S = \varnothing$, then $j + S = \varnothing$. Since r is a root modulo n of $f(x)$ iff $r + j$ is a root of $f(x - j)$ modulo n, the following theorem is evident.

Theorem 3. *If R is a root set modulo n, then, for every $j \in \mathbf{Z}_n$, $j + R$ is also a root set modulo n.* □

Corollary. *R is a root set modulo p^k iff R can be written in the form $R = (0 + S_0) \cup (1 + S_1) \cup (2 + S_2) \cup \cdots \cup ((p-1) + S_{p-1})$, where each S_j is a root set modulo p^k*

containing only integers congruent to 0 *modulo p.* (*Note that some of the* S_j's *might be empty.*)

PROOF. Suppose that R is a root set modulo p^k. By Theorem 1, $R = R_0 \cup R_1 \cup \cdots \cup R_{p-1}$, where the elements of each R_j are congruent to j modulo p. Let $S_j = (-j) + R_j$ for $j = 0, 1, \ldots, p-1$, so that $R_j = j + S_j$. Then, by Theorem 3, S_j is a root set modulo p^k for each $j = 0, 1, \ldots, p-1$, and, moreover, every element of S_j is congruent to 0 modulo p. Conversely, if, for each $j = 0, 1, \ldots, p-1$, S_j is a root set modulo p^k containing only integers congruent to 0 modulo p, then, by Theorems 2 and 3, $R = (0 + S_0) \cup (1 + S_1) \cup \cdots \cup ((p-1) + S_{p-1})$ is a root set modulo p^k. □

The following is an immediate consequence of the previous corollary.

COROLLARY. *Let* N_{p^k} *be the number of root sets modulo* p^k *which contain only multiples of p. Then the total number of different root sets modulo* p^k *is* $N_{p^k}^p$, *a perfect* p^{th} *power.*

To count the number of distinct root sets modulo p^k, we need only count the number of root sets modulo p^k containing only multiples of p. The following theorems make feasible a computer search for such root sets, and hence the determination of specific values of N_{p^k}. Let d_{p^k} be the smallest positive integer d such that p^k divides $d!$. Note that d_{p^k} will always be a multiple of p.

THEOREM 4. *If R is a root set modulo* p^k, *then there is a polynomial with degree less than* d_{p^k} *with root set exactly R.*

PROOF. Let $K(x) = x^{\underline{d_{p^k}}}$. For $j \in \mathbf{Z}_{p^k}$, Lemma 1 shows $\varepsilon_p(K(j)) = \varepsilon_p(j^{\underline{d_{p^k}}}) \geqslant \varepsilon_p(d_{p^k}!)$, and that last quantity is at least k by the definition of d_{p^k}. Thus $K(x) \equiv 0 (\text{mod}\, p^k)$ for all $x \in \mathbf{Z}_{p^k}$. Now, let f let a polynomial with root set R modulo p^k. Write f as $f(x) = q(x)K(x) + r(x)$, where either the degree of $r(x)$ is less than d_{p^k}, or $r(x)$ is identically 0. Since $K(x)$ is identically 0 modulo p^k, it follows that $f(x) \equiv r(x)\ (\text{mod}\, p^k)$, for all $x \in \mathbf{Z}_{p^k}$, and thus the root set of $r(x)$ is R. □

There is a root set modulo p^k produced by a polynomial of degree $d_{p^k} - 1$, but by no polynomial of smaller degree, so when searching for root sets modulo p^k, the bound of Theorem 4 cannot be reduced.

EXAMPLE. Let $m = d_{p^k} - 1$, and consider $h(x) = x^{\underline{m}}$. Then $h(j) = 0$ for $j = 0, 1, \ldots, m-1$, while $h(m) = m! \not\equiv 0 (\text{mod}\, p^k)$ by the definition of d_{p^k}. Suppose that $f(x)$ is any polynomial of degree less than m such that $f(j) \equiv 0 (\text{mod}\, p^k)$ for every $j = 0, 1, \ldots, m-1$. By the division algorithm, we may write $f(x)$ in the form

$$f(x) = a_0 + a_1 x^{\underline{1}} + a_2 x^{\underline{2}} + \cdots + a_{m-1} x^{\underline{m-1}}.$$

By successively considering $f(0), f(1), \ldots, f(m-1) \equiv 0 (\text{mod}\, p^k)$, while applying Lemma 2, we see that $f(x)$ is identically 0 modulo p^k. In particular, $f(m) \equiv 0 (\text{mod}\, p^k)$. Hence, no polynomial of degree less than m has the same root set as $h(x)$ modulo p^k. □

THEOREM 5. *If R is a root set modulo* p^k *which contains only multiples of p, then* *there is a polynomial with degree less than d_{p^k}/p the set of roots of which congruent to* 0 *modulo p is R.*

Proof. Let $m = d_{p^k}/p$ and let $K(x) = \prod_{0 \leqslant l < m} (x - pl)$. If $t \not\equiv 0 (\operatorname{mod} p)$, then $K(t)$ is not a zero divisor modulo p^k. Note that if $d = pe$, then $\varepsilon_p(d!) = \varepsilon_p(p^e(e!)) = \mathrm{e} + \varepsilon_p(e!)$. Hence, for $j \geqslant 0$,

$$\begin{aligned}\varepsilon_p(K(pj + d_{p^k})) &= \varepsilon_p\left(p^m \frac{(j+m)!}{j!}\right)\\ &\geqslant m + \varepsilon_p(m!)\\ &= \varepsilon_p(d_{p^k}!)\\ &\geqslant k.\end{aligned}$$

Thus it follows that $K(t) \equiv 0 (\operatorname{mod} p^k)$, for every $t \equiv 0 (\operatorname{mod} p)$. Now any polynomial f can be written as $f(x) = q(x)K(x) + r(x)$, where $r(x) = 0$ or $r(x)$ has degree less than m. It follows that, for every $t \equiv 0 (\operatorname{mod} p)$, $f(t) \equiv r(t) (\operatorname{mod} p^k)$. Hence, the roots of f which are congruent to 0 modulo p coincide with the roots of $r(x)$ that are congruent to 0 modulo p. □

Theorem 6. *If $R \neq \varnothing$ is a root set modulo p^k which contains only multiples of p, and $j \in R$, then $(-j) + R$ is a root set modulo p^k containing* 0 *and only multiples of p.*

Proof. Modulo p^k, if $f(x)$ has root set R, then $g(x) = f(x + j)$ has root set $S = (-j) + R$. Since the difference of multiples of p is a multiple of p, and since $(-j) + j = 0 \in S$, we are done. □

Thus the non-empty root sets containing only multiples of p are all the possible translates by multiples of p of the root sets containing 0 and only multiples of p. The next theorem allows us to count the number of such translates.

Theorem 7. *Let R be a root set modulo p^k containing* 0 *and only multiples of p. Let $T = \{t \in \mathbf{Z} \mid t + R = R\}$,* and let *$t_0$ be the smallest positive integer in T. Then $t_0 = p^e$ for some $e \leqslant k$ and R will have p^e distinct translates.*

Proof. T is an ideal in $\mathbb{Z}$, and $p^k \in T$. Since every non-zero ideal in $\mathbf{Z}$ is generated by its smallest positive member, letting the smallest positive element of T be t_0, we have $T = (t_0)$. Since $p^k \in T$, it follows that t_0 divides p^k, and thus $t_0 = p^e$ for some $e \leqslant k$. Thus R is periodic with minimum period t_0. Hence there are exactly t_0 distinct translates of R. □

The final theorem shows the coefficients of a polynomial can be reduced in certain ways without changing the root set.

Theorem 8. *Every root set modulo p^k containing* 0 *and only multiples of p is produced by a polynomial*

$$\begin{aligned}f(x) = a_0 + a_1 x + a_2 x(x-p) + a_3 x(x-p)(x-2p) + \cdots\\ + a_m x(x-p)(x-2p)\cdots(x-(m-1)p),\end{aligned}$$

where $m = d_{p^k}/p - 1$, $a_0 = 0$, $a_1 = 0, 1, p, p^2, \ldots, p^{k-1}$ and, for $j = 2, 3, \ldots, m$, $0 \leqslant a_j < p^{k-e_j}$, where $e_j = \varepsilon_p((pj)!)$.

PROOF. Let R be a root set modulo p^k containing 0 and only multiples of p. By Theorem 5, there is a polynomial $f(x)$ of degree no more than m such that $r \in R$ iff $r \equiv 0 (\mathrm{mod}\, p)$ and $f(r) \equiv 0 (\mathrm{mod}\, p^k)$. By the division algorithm, $f(x)$ may be expressed in the form given in the statement of the theorem. Since $0 \in R$, we have $a_0 \equiv 0 (\mathrm{mod}\, p^k)$. Next, if a_1 is written in the form $p^t s$ with p not dividing s, then s will have a multiplicative inverse, s^{-1}, modulo p^k and $s^{-1} f(x)$ has the same roots as $f(x)$ modulo p^k. It follows that only the values $0, 1, p, \ldots, p^{k-1}$ need be considered for the coefficient a_1. Finally, for each $x \in \mathbf{Z}_{p^k}$, $\varepsilon_p(x(x-p)\cdots(x-(j-1)p)) \geqslant \varepsilon_p((pj)(pj-p)\cdots(p)) = \varepsilon_p((pj)!) = e_j$. Hence $(a_j + p^{k-e_j} l) x(x-p)\cdots(x-(j-1)p) \equiv a_j x(x-p)\cdots(x-(j-1)p)\ (\mathrm{mod}\, p^k)$. It follows that we may reduce a_j modulo p^{k-e_j} without changing the root set modulo p^k of the polynomial. □

3. NUMERICAL RESULTS

Based on the theorems of the last section, only a small portion of all possible polynomials modulo p^k need be solved to determine the total number of root sets modulo p^k. In particular, only the number of root sets modulo p^k containing only multiples of p—that is, N_{p^k}—needs to be determined. At least for small values of p and k, these can be found by a computer search. The polynomials are generated, and the root sets consisting of 0 and multiples of p are recorded. Each such root set discovered is compared to a list of such root sets already computed and to their translates. A program to implement this search was written by Stroth [4]. In each case, the total number of root sets modulo p^k is given by $N_{p^k}^p$.

The values of N_{p^k} for some small values of p and k are presented in Table 1. Some of the entries in the table are easy to understand. For example, modulo p, $\{0\}$ is the only root set containing 0 and multiples of p. Hence $\{0\}$ and the empty root set are the only two basic root sets modulo p. Consequently, the first column in the table will be all 2's. As for the second column, recall that if t is a root of a polynomial modulo p, then t yields either no roots modulo p^2, or a single root $t + kp$ modulo $p^2 (k = 0, 1, \ldots, p-1)$, or else the roots $\{t + kp \mid k = 0, 1, \ldots, p-1\}$ modulo p^2. As $\{0\}$ is the only non-empty root set modulo p made up of 0 and multiples of p, it follows that there are $p+2$ root sets modulo p^2 containing only 0 and multiples of p. Thus $N_{p^2} = p + 2$, and so there are $(p+2)^p$ root sets modulo p^2. Somewhat more complicated reasoning explains the third column.

TABLE 1. A small table of N_{p^k} values.

p \ k	1	2	3	4	5	6	7	8	9	10	11
2	2	4	8	20	56	184	632	2 752	13 464	80 840	577 000
3	2	5	17	71	449	4 040	51 353				
5	2	7	42	427	8 707	336 957					
7	2	9	79	1 486	66 740	6 825 968					
11	2	13	189	8 340							
13	2	15	262	15 927							
17	2	19	444	45 341							
19	2	21	553	70 112							
23	2	25	807	148 582							
29	2	31	1 278	370 767							

References

1. M. M. Chojnacka-Pniewska, Sur les congruences aux racines données, *Ann. Pol. Math.,* **3** (1956), 9–12.
2. R. Graham, D. Knuth and O. Patashnik, *Concrete Mathematics,* 2nd edn, Addison-Wesley, Reading, Mass., 1995.
3. W. Sierpiński, Remarques sur les racines d'une congruence, *Ann. Pol. Math.,* **1** (1954), 89–90.
4. T. R. Stroth, Root sets of polynomials $(\mathrm{mod}\, 2^k)$, Masters independent study, University of North Dakota, May 1995.

Received 2 May 1995 and accepted 15 October 1996

Bruce Dearden and Jerry Metzger
Department of Mathematics,
University of North Dakota,
P.O. Box 8376, Grand Forks,
North Dakota 58202–8376, U.S.A.