ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 22, Number 3, Summer 1992

ON THE POWER POLYNOMIAL x^d OVER GALOIS RINGS

JAVIER GOMEZ-CALDERON

ABSTRACT. Let p denote a prime. Let $\mathrm{GR}(p^n, m)$ denote the Galois ring of order p^{nm}. Let $P_d(x)$ denote the power polynomial $P_d(x) = x^d$ over the ring $\mathrm{GR}(p^n, m)$. In this paper we determine two cardinalities: the cardinality of the value set $\{P_d(x) : x \in \mathrm{GR}(p^n, m)\}$, and the cardinality of the preimage $P_d^{-1}(P_d(x))$ for each x in $\mathrm{GR}(p^n, m)$.

1. Introduction. For a prime p, let $\mathrm{GR}(p^n, m)$ denote the Galois ring of order p^{nm} which can be obtained as a Galois extension of Z_{p^n} of degree m. Thus $\mathrm{GR}(p^n, 1) = Z_{p^n}$ and $\mathrm{GR}(p, m) = K_{p^m}$, the finite field of order p^m. The reader can find further details concerning Galois rings in the excellent reference [**1**].

Now, for $d \geq 1$, let $P_d(x) = x^d$ denote the power polynomial of degree d over $\mathrm{GR}(p^n, m)$. Then it is easy to check that the cardinality of the value set of $P_d(x)$ over the field $\mathrm{GR}(p, m) = K_p m = K_q$ depends only upon $(d, q-1)$, the greatest common divisor of d and $q-1$. To be more specific,

$$|\{P_d(x) : x \in \mathrm{GR}(p, m) = K_q\}| = \frac{q-1}{(q-1, d)} + 1$$

where $q = p^m$.

In this paper we not only determine the cardinality of the value set $\{P_d(x) : x \in \mathrm{GR}(p^n, m)\}$ for $n \geq 1$, but if $x_0 \in \mathrm{GR}(p^n, m)$, we also determine the cardinality of the preimage of $P_d(x_0)$.

2. p odd. Throughout this section we assume that p is odd. Let $\mathrm{GR}^*(p^n, m)$ denote the group of units of $\mathrm{GR}(p^n, m)$. Then, see [**1**, Theorem XVI.9], $\mathrm{GR}^*(p^n, m)$ is a direct product of two groups G_1 and

Received by the editors on September 8, 1989 and in revised form on June 15, 1990.

G_2 where G_1 denotes a cyclic group of order $p^m - 1 = q - 1$, and G_2 denotes a direct product of m cyclic groups each of order p^{n-1}. Thus,

$$\text{(1)} \qquad \mathrm{GR}^*(p^n, m) = G_1 \times G_2 = G_1 \times H_1 \times H_2 \times \cdots \times H_m$$

where H_i denotes a cyclic group of order p^{n-1} for $i = 1, 2, \ldots, m$.

Lemma 1. *Let d denote a positive integer and write $d = p^t e$ with $(e, p) = 1$. Then*

$$|\{x \in \mathrm{GR}(p^n, m) : x^d = 1\}| = (d, q-1)q^k$$

where $k = \min\{n-1, t\}$ and $q = p^m$.

Proof. Let $A(d)$ denote the set of elements x in $\mathrm{GR}(p^n, m)$ so that $x^d = 1$. Thus, $A(d)$ is a multiplicative subgroup of $\mathrm{GR}^*(p^n, m)$, the group of units of $\mathrm{GR}(p^n, m)$.

Now, by (1),

$$A(d) = A^* \times H_1^* \times H_2^* \times \cdots \times H_m^*$$

where A^* denotes the subgroup of G_1 of order $(d, q-1)$ and H_i^* denotes the subgroup of H_i of order (p^t, p^{n-1}) for $i \geq 1$. Therefore,

$$|A(d)| = (d, q-1)(p^k)^m = (d, q-1)q^k$$

where $k = \min\{t, n-1\}$. □

Theorem 2. *Let d denote a positive integer and write $d = p^t e$ with $(e, p) = 1$. Let $x_0 \in \mathrm{GR}(p^n, m)$ and write $x_0 = p^i A$ with A a unit of $\mathrm{GR}(p^n, m)$. Let $P_d^{-1}(P_d(x_0))$ be the preimage of $P_d(x_0)$. Then*

$$|P_d^{-1}(P_d(x_0))| = \begin{cases} (d, q-1)q^{i(d-1)+k} & \text{if } i \leq [(n-1)/d] \\ q^{n-[(n-1)/d]-1} & \text{if } i > [(n-1)/d] \end{cases}$$

where $k = \min\{t, n - id - 1\}$ and $q = p^m$.

Proof. Let $x_0 \in \mathrm{GR}(p^n, m)$ and write $x_0 = p^i A$ with A a unit of $\mathrm{GR}(p^n, m)$. Let $d = p^t e \geq 1$ with $(e, p) = 1$. Then we consider two cases.

Case 1. $i \le [(n-1)/d]$. Then, $x^d = x_0^d$ if and only if $x = p^i B$ for some B in $\mathrm{GR}(p^n, m)$ with $B^d \equiv A^d \pmod{p^{n-id}}$. Thus, $B \equiv wA \pmod{p^{n-id}}$ for some w in $\mathrm{GR}(p^{n-id}, m)$ with $w^d = 1$. Hence, by Lemma 1, there are $(d, q-1)q^k$ distinct values B over $\mathrm{GR}(p^{n-id}, m)$ where $k = \min\{t, n-id-1\}$ and $q = p^m$. Therefore, there are $(d, q-1)q^{k+(n-1)-(n-id-1)-i} = (d, q-1)q^{i(d-1)+k}$ distinct values x over $\mathrm{GR}(p^n, m)$ satisfying $x^d = x_0^d$.

Case 2. $n \ge i \ge [(n-1)/d] + 1$. $x^d = x_0^d = p^{id}A = 0$ if and only if $x = Bp^{[(n-1)/d]+1}$ for some B in $\mathrm{GR}(p^n, m)$. Therefore, there are $q^{n-1-[(n-1)/d]}$ distinct values x in $\mathrm{GR}(p^n, m)$ so that $x^d = 0$. This completes the proof of the theorem. □

Theorem 3. *Let d denote a positive integer and write $d = p^t e$ with $(e, p) = 1$. Then*

$$|\{P_d(x) : x \in \mathrm{GR}(p^n, m)\}| = \frac{q-1}{(q-1, d)} \sum_{i=0}^{[\frac{n-1}{d}]} q^{n-1-id-k_i} + 1$$

where $k_i = \min\{t, n-id-1\}$ for $0 \le i \le [(n-1)/d]$.

Proof. We partition $\mathrm{GR}(p^n, m)$ as follows:

$$\mathrm{GR}(p^n, m) = \left(\bigcup_{i=0}^{[\frac{n-1}{d}]} p^i \mathrm{GR}^*(p^n, m) \right) \cup \left(\bigcup_{i > [\frac{n-1}{d}]} p^i \mathrm{GR}^*(p^n, m) \right).$$

Therefore, by Theorem 2,

$$\begin{aligned} |\{P_d(x) : x \in \mathrm{GR}(p^n, m)\}| &= \sum_{i=0}^{[\frac{n-1}{d}]} \frac{(q-1)q^{n-1-i}}{(q-1, d)q^{i(d-1)+k_i}} + 1 \\ &= \frac{q-1}{(q-1, d)} \sum_{i=0}^{[\frac{n-1}{d}]} q^{n-1-id-k_i} + 1 \end{aligned}$$

where $k_i = \min\{t, n-id-1\}$. □

Corollary. *$P_d(x) = x^d$ permutes $\mathrm{GR}\,(p^n, m)$ if and only if $d = 1$ or $n = 1$ and $(d, p^m - 1) = 1$.*

3. p even. Throughout this section we assume that $p = 2$. Then, the group of units $\mathrm{GR}^*(p^n, m)$, see [**1**, Theorem XVI.9], is a direct product of two groups G_1 and G_2, where G_1 denotes a cyclic group of order $p^m - 1 = q - 1$, and G_2 denotes a group with two possible structures depending on the value of n. If $n \leq 2$, G_2 is a direct product of m cyclic groups of order p^{n-1}. Thus,

$$\mathrm{GR}^*(p^n, m) = G_1 \times G_2 = G_1 \times H_1 \times H_2 \times \cdots \times H_m \tag{2}$$

where H_i denotes a cyclic group of order p^{n-1} for $i \geq 1$. On the other hand, if $n \geq 3$, G_2 is a direct product of a group of order 2, a cyclic group of order 2^{n-2} and $m-1$ cyclic groups each of order 2^{n-1}. Thus,

$$\mathrm{GR}^*(p^n, m) = G_1 \times G_2 = G_1 \times E_1 \times E_2 \times H_1 \times H_2 \times \cdots \times H_{m-1} \tag{3}$$

where E_1, E_2 and H_i, $i \geq 1$ are cyclic groups of orders 2, 2^{n-2} and 2^{n-1}, respectively.

Corresponding to Lemma 1 and Theorems 2 and 3 for odd p, we can prove the following results when $p = 2$. As the proofs are analogous to those given for odd p, we omit the details for the $p = 2$ case.

Lemma 1′. *Let d denote a positive integer and write $d = p^t e$ with $(p, e) = 1$. Then*

$$|\{x \in \mathrm{GR}\,(p^n, m) : x^d = 1\}| = \begin{cases} (d, q-1) & \text{if } t = 0 \\ 2(d, q-1)q^t & \text{if } 1 \leq t \leq n-2 \\ (d, q-1)q^{n-1} & \text{if } n-1 \leq t \end{cases}$$

where $q = p^m$.

Theorem 2′. *Let d denote a positive integer and write $d = p^t e$ with $(e, p) = 1$. Let $x_0 \in \mathrm{GR}\,(p^n, m)$ and write $x_0 = p^i A$ with A a unit of*

$\mathrm{GR}(p^n, m)$. *Let* $P_d^{-1}(P_d(x_0))$ *be the preimage of* $P_d(x_0)$. *Then,*

$$|P_d^{-1}(P_d(x_0))| = \begin{cases} (d, q-1)q^{i(d-1)} & \text{if } t = 0 \text{ and } id \le n-1 \\ 2(d, q-1)q^{t+i(d-1)} & \text{if } 1 \le t,\ t < n-1-id, \\ & \text{and } id \le n-1 \\ (d, q-1)q^{n-1-i} & \text{if } 1 \le t,\ t \ge n-1-id, \\ & \text{and } id \le n-1 \\ (d, q-1)q^{n-[(n-1)/d]-1} & \text{if } id \ge n. \end{cases}$$

Theorem 3′. *Let* d, n *and* m *denote three positive integers and write* $d = p^t e$ *with* $(e, p) = 1$. *Let* V *denote the value set*

$$V = \{P_d(x) : x \in \mathrm{GR}(p^n, m)\}.$$

a) *Assume* $t = 0$. *Then,*

$$|V| = \frac{q-1}{(q-1, d)} \sum_{i=0}^{[\frac{n-1}{d}]} q^{n-1-id} + 1$$

b) *Assume* $1 \le t$ *and* $n-1-(j+1)d \le t < n-1-jd$ *for some* j, $0 \le j \le [(n-1)/d]$. *Then,*

$$|V| = \frac{q-1}{(d, q-1)} \left([(n-1)/d] - j + (1/2) \sum_{i=0}^{j} q^{n-1-id+t} \right) + 1$$

c) *Assume* $t \ge n-1$. *Then,*

$$|V| = \frac{q-1}{(d, q-1)} ([(n-1)/d] + 1) + 1$$

Acknowledgment. The author thanks the referee for his suggestions which improved the final version of the paper.

REFERENCES

1. B.R. MacDonald, *Finite rings with identity*, Marcel Dekker, New York, 1974.

Department of Mathematics, New Kensington Campus, Pennsylvania State University, New Kensington, PA 15068