Mathematical Journal of Okayama University

Volume 33, *Issue* 1 1991 *Article* 1

JANUARY 1991

Cycle structure of dickson permutation polynomials

Rudolf Lidl* Gary L. Mullen†

*University Of Tasmania
†Pennsylvania State University

Math. J. Okayama Univ. 33 (1991), 1−11

CYCLE STRUCTURE OF DICKSON PERMUTATION POLYNOMIALS

RUDOLF LIDL* and GARY L. MULLEN**

1. If R is a commutative ring with identity and $a \in R$, then the Dickson polynomial $D_n(x, a)$ of degree n is defined by

$$D_n(x, a) = \sum_{j=0}^{\lfloor n/2 \rfloor} \frac{n}{n-j} \binom{n-j}{j} (-a)^j x^{n-2j},$$

where $\lfloor \ \rfloor$ denotes the greatest integer function. Dickson polynomials have been extensively studied over finite fields and over residue class rings of integers as well as over various other rings. For a survey of many properties of Dickson polynomials including applications to cryptography and number theory, see Lidl [3] and for results related to finite fields, see Lidl and Niederreiter [4] and Mullen [6].

If F_q denotes the finite field of order q a prime power, it is well known that $D_n(x, 0) = x^n$ permutes F_q if and only if n and $q-1$ are relatively prime, i.e. if and only if $(n, q-1) = 1$, and for $a \neq 0$, $D_n(x, a)$ permutes F_q if and only if $(n, q^2-1) = 1$. Moreover the Dickson permutation polynomials are closed under composition of polynomials if and only if $a = 0, 1$, or -1, see [4, Thm. 7.22] for details.

In section 2 we determine the cycle structure of the Dickson permutation polynomials over F_q and in section 3 we consider the analogous problem in the setting of a Galois ring.

2. **Finite Fields.** We will make use of the following properties. First for $a, x \in F_q$, let $\mu \in F_{q^2}$ be such that $x = \mu + a/\mu$. Then the functional equation for Dickson polynomials indicates that

$$D_n(x, a) = \mu^n + a^n/\mu^n, \tag{1}$$

see [4, Equation (7.8)]. Use will also be made of the easy to prove fact

* This author acknowledges support from the Australian Research Council, grant A69031913.

** This author would like to thank the Mathematics Department of the University of Tasmania for its hospitality during a stay as part of his sabbatical. Thanks are also due NSA for partial support under grant agreement ♯MDA 904-87-H-2023.

that for $a \in F_q$, if $M(a)$ is the subset of F_{q^2} consisting of all solutions of the q equations of the form $x^2 - rx + a = 0$ with $r \in F_q$, then

$$M(a) = \{\mu \in F_{q^2} \mid \mu^{q-1} = 1 \text{ or } \mu^{q+1} = a\}. \tag{2}$$

We now consider the cycle structure of the Dickson permutation polynomials. While the cycle structure for the power polynomial x^n on F_q^* was determined in Ahmad [1], for the sake of completeness we restate the result here. Recall that n belongs to the exponent m mod t if m is the smallest positive integer such that $n^m \equiv 1 \bmod t$. Throughout this paper we let $(a, b) = \gcd(a, b)$.

Theorem 1. *Let m be a positive integer. Then x^n has a cycle of length m over F_q^* if and only if $q-1$ has a divisor t such that n belongs to the exponent m mod t. Moreover the number N_m of such cycles is*

$$mN_m = (q-1, n^m - 1) - \sum_{i \mid m,\, i<m} iN_i. \tag{3}$$

Proof. We have $x^{n^m} = x$ if and only if $n^m - 1 \equiv 0 \bmod t$ where t is the multiplicative order of x so the first part follows. There are mN_m elements that belong to cycles of length m and $(n^m - 1, q-1)$ elements of F_q^* which belong to cycles of length i where $i \mid m$.

From (3) with $m = 1$ we can easily deduce that x^n has $(q-1, n-1)+1$ fixed points over F_q where by a fixed point is meant an element x so that $x^n = x$.

Theorem 2. *Let m be a positive integer and let $D_n(x, 1)$ permute F_q. Then $D_n(x, 1)$ has a cycle of length m if and only if $q-1$ or $q+1$ has a divisor t such that $n^m \equiv \pm 1 \bmod t$. Moreover the number M_m of such cycles is*

$$\begin{aligned} mM_m = {} & [(q+1, n^m+1) + (q-1, n^m+1) + (q+1, n^m-1) \\ & + (q-1, n^m-1)]/2 - \varepsilon_1 - \sum_{i \mid m,\, i<m} iM_i, \end{aligned} \tag{4}$$

where

$$\varepsilon_1 = \begin{cases} 1 & \text{if } p = 2 \text{ or } p \text{ is odd and } n \text{ is even} \\ 2 & \text{if } p \text{ is odd and } n \text{ is odd.} \end{cases}$$

Proof. From (2) let

$$M_1(a) = \{\mu \in F_{q^2} \mid \mu^{q+1} = a\},\ M_2(a) = \{\mu \in F_{q^2} \mid \mu^{q-1} = 1\}.$$

If w is a primitive element of F_{q^2} then

$$M_1(1) = \{w^{(q-1)r} \mid r = 0, 1, \ldots, q\}, \; M_2(1) = \{w^{(q+1)s} \mid s = 0, 1, \ldots, q-2\}.$$

We note that $\mu \in M_1(1) \cap M_2(1)$ if and only if $\mu = \pm 1$. Let $N_3(1) = \{1\}$ if $p = 2$ and $N_3(1) = \{\pm 1\}$ if p is odd and let $N_1(1) = M_1(1) \backslash N_3(1)$ and $N_2(1) = M_2(1) \backslash N_3(1)$. We note that $M(1)$ is the disjoint union $N_1(1) \cup N_2(1) \cup N_3(1)$. Finally if μ is a solution of $z^2 - \rho z + 1 = 0$, so is μ^{-1}, and $\mu = \mu^{-1}$ if and only if $\mu^2 = 1$ so that $\mu \in N_3(1)$.

Let $D_n^{(m)}(x, 1)$ denote the m-th iterate of $D_n(x, 1)$ under composition. Using the functional equation (1), an element $x = \mu + \mu^{-1}$ has the property that $D_n^{(m)}(\mu + \mu^{-1}, 1) = \mu + \mu^{-1}$ if and only if $\mu^{n^m} + \mu^{-n^m} = \mu + \mu^{-1}$, i.e. if and only if

$$(\mu^{n^m+1} - 1)(\mu^{n^m-1} - 1) = 0. \tag{5}$$

Since a solution ν of (5) is a solution of both $\mu^{n^m+1} = 1$ and $\mu^{n^m-1} = 1$ if and only if $\nu \in N_3(1)$, the number of solutions to (5) on $M(1)$ is the sum of the number of solutions of $\mu^{n^m+1} = 1$ and $\mu^{n^m-1} = 1$ on $N_1(1)$ and $N_2(1)$ plus the number of solutions of (5) on $N_3(1)$.

Now $\nu \in M_1(1)$ is a solution of $\mu^{n^m+1} = 1$ if and only if $r(n^m+1) \equiv 0 \bmod (q+1)$. This congruence has $(q+1, n^m+1)$ solutions. Similarly $\mu^{n^m+1} = 1$ has exactly $(q-1, n^m+1)$ solutions on $M_2(1)$, $\mu^{n^m-1} = 1$ has exactly $(q+1, n^m-1)$ solutions on $M_1(1)$ and $\mu^{n^m-1} = 1$ has exactly $(q-1, n^m-1)$ solutions on $M_2(1)$. We also note that (5) has exactly one solution if $p = 2$ or p is odd and n is even and it has exactly two solutions when p is odd and n is odd. Thus (5) has exactly ε_1 solutions on $N_3(1)$. Noting that μ is a solution to (5) if and only if μ^{-1} is a solution, the proof is complete.

It is worth remarking that for $m = 1$ Theorem 2 holds for any $n \geq 1$, not just those for which $D_n(x, 1)$ permutes F_q. Theorem 2 thus determines the number of fixed points of $D_n(x, 1)$ over F_q.

We now consider the case where $a = -1$, n is odd, and since $D_n(x, -1) = D_n(x, 1)$ if $p = 2$, we may assume the characteristic p of F_q is odd. Let $\nu_p(m)$ denote the highest power of p dividing m for $m \neq 0$ and set $\nu_p(0) = \infty$. Then clearly $\nu_p((a, b)) = \min\{\nu_p(a), \nu_p(b)\}$, $\nu_p(ab) = \nu_p(a) + \nu_p(b)$ and if $a \mid b$, then $\nu_p(b/a) = \nu_p(b) - \nu_p(a)$ for integers a and b. We can now prove

Theorem 3. *Let m be a positive integer. If n and q are odd then*

$D_n(x, -1)$ has a cycle of length m if and only if $q-1$ or $q+1$ has a divisor t such that $n^m \equiv 1 \bmod t$ or $2(n^m+1) \equiv 0 \bmod t$. Moreover the number K_m of such cycles is

$$mK_m = [(a_1(n^m+1, 2(q+1))+a_2(n^m+1, q-1)+a_3((n^m-1)/2, q+1) \\ +(n^m-1, q-1)]/2-\varepsilon_{-1}-\sum_{i\mid m,\, i<m} iK_i,$$

where

$$a_1 = \begin{cases} 1 & \text{if } \nu_2(n^m+1) = \nu_2(q+1) \\ 0 & \text{otherwise}, \end{cases}$$
$$a_2 = \begin{cases} 1 & \text{if } \nu_2(n^m+1) < \nu_2(q+1) \\ 0 & \text{otherwise}, \end{cases}$$
$$a_3 = \begin{cases} 1 & \text{if } \nu_2(n^m-1) > \nu_2(q+1) \\ 0 & \text{otherwise}, \end{cases}$$
$$\varepsilon_{-1} = \begin{cases} 2 & \text{if } n^m \equiv 1 \bmod 4 \text{ and } q \equiv 1 \bmod 4 \\ 0 & \text{otherwise}. \end{cases}$$

Proof. We first note that if w is a primitive element of F_{q^2}, then

$$M_1(-1) = \{w^{(q-1)r/2} \mid r = 1, 3, \dots, 2q+1\},$$
$$M_2(-1) = \{w^{(q+1)s} \mid s = 0, 1, \dots, q-2\}.$$

For $i = 0, 1$ let $\mu_i = w^{(q^2-1)(1+2i)/4}$. For $\mu \in M_1(-1) \cap M_2(-1)$ we have $\mu^{q+1} = -1$ and $\mu^{q-1} = 1$ so that $\mu^2 = -1$ and $\mu \in \{\mu_0, \mu_1\}$. If $q = 4t+1$, then for $i = 0, 1$, $\mu_i^{q+1} = w^{(q^2-1)/2} = -1$ and $\mu_i^{q-1} = 1$ for $i = 0, 1$ so $\mu_i \in M_1(-1) \cap M_2(-1)$. If $q = 4t+3$ then $\mu_i^{q+1} = 1$ and $\mu_i^{q-1} = -1$ and so $\mu_i \notin M_j(-1)$ for $i = 0, 1$ and $j = 1, 2$ and hence $\mu_i \notin M_1(-1) \cap M_2(-1)$.

Let $N_3(-1) = \{\mu_0, \mu_1\}$ if $q \equiv 1 \bmod 4$ and let $N_3(-1) = \phi$ if $q \equiv 3 \bmod 4$ and for $j = 1, 2$ let $N_j(-1) = M_j(-1)\backslash N_3(-1)$. Then $M(-1)$ is the disjoint union $N_1(-1) \cup N_2(-1) \cup N_3(-1)$. Finally note that $z^2-\rho z -1$ has solutions μ and μ^{-1} and $\mu = \mu^{-1}$ only when $\mu^2 = -1$ so that $\mu \in N_3(-1)$.

If $x = \mu-\mu^{-1}$ satisfies $D_n^{(m)}(x, -1) = x$ then by (1) we have

$$(\mu^{n^m+1}+1)(\mu^{n^m-1}-1) = 0. \tag{6}$$

Since a solution μ of (6) is a solution of both $\mu^{n^m+1} = -1$ and $\mu^{n^m-1} = 1$ if and only if $\mu \in N_3(-1)$, the number of solutions of (6) which are in $M(-1)$ is the sum of the number of solutions of the equations in the sets

$N_1(-1)$ and $N_2(-1)$ plus the number of solutions of (6) which are in $N_3(-1)$.

An element $v \in M_1(-1)$ is a solution of $\mu^{n^m+1} = -1$ if and only if

$$r(n^m+1) \equiv q+1 \bmod (2(q+1)). \tag{7}$$

This is solvable if and only if $\nu_2(n^m+1) \leq \nu_2(q+1)$. Let $d = (n^m+1, 2(q+1))$ so that $\nu_2(d) = \min\{\nu_2(n^m+1), \nu_2(q+1)+1\} = \nu_2(n^m+1)$. If α and β are integers with

$$\alpha(n^m+1)+2\beta(q+1) = d, \tag{8}$$

then all solutions of (7) are given by

$$\frac{\alpha(q+1)}{d}+\frac{2(q+1)i}{d},\ i = 0, 1, \ldots, d-1.$$

If α is even, $\nu_2(d) \geq \min\{\nu_2(n^m+1)+1, \nu_2(q+1)+1\} > \nu_2(n^m+1)$ so that by considering the highest power of 2 in (8), we have a contradiction so that α must be odd. Now $\nu_2((q+1)/d) = \nu_2(q+1)-\nu_2(n^m+1)$ so that $(q+1)/d$ is odd if and only if $\nu_2(q+1) = \nu_2(n^m+1)$. Since $d|(q+1)$, $2(q+1)/d$ is even. Finally (7) has a solution r with r odd if and only if $\nu_2(n^m+1) = \nu_2(q+1)$ and in this case it has $(n^m+1, 2(q+1))$ solutions each of which is odd.

Now $v \in M_2(-1)$ is a solution of $\mu^{n^m+1} = -1$ if and only if $w^{(q+1)s(n^m+1)} = -1$, i.e. if and only if $s(n^m+1) \equiv (q-1)/2 \bmod (q-1)$ which is solvable if and only if $\nu_2(n^m+1) < \nu_2(q-1)$ in which case it has $(n^m+1, q-1)$ solutions. Similarly $v \in M_1(-1)$ is a solution of $\mu^{n^m-1} = 1$ if and only if

$$r(n^m-1) \equiv 0 \bmod (2(q+1)). \tag{9}$$

Let $d = (n^m-1, 2(q+1))$ so that all solutions of (9) are given by $2(q+1)i/d$ for $i = 0, 1, \ldots, d-1$. Moreover $2(q+1)/d$ is odd if and only if $\nu_2(n^m-1) > \nu_2(q+1)$. Hence (9) is solvable if and only if $\nu_2(n^m-1) > \nu_2(q+1)$ and then it has $((n^m-1)/2, q+1)$ odd solutions.

We note that $\mu^{n^m-1} = 1$ has exactly $(n^m-1, q-1)$ solutions in $M_2(-1)$. The set of all solutions of (9) on $N_3(-1)$ is the set of all solutions of $\mu^{n^m-1} = 1$ on $N_3(-1)$ which is empty if $q \equiv 3 \bmod 4$. It is also empty if $q \equiv 1 \bmod 4$ and $n^m \equiv 3 \bmod 4$ and it is equal to $\{\mu_0, \mu_1\}$ if $q \equiv n^m \equiv 1 \bmod 4$. Hence ε_{-1} is determined. To complete the proof we note that μ is a solution of $\mu^{n^m+1} = -1$ (resp. $\mu^{n^m-1} = 1$) if and only if $-\mu^{-1}$ is also a solution.

We note that if $m = 1$, the above results reduce to those of Nöbauer

[7] for the number of fixed points of $D_n(x, a)$ where by a fixed point is meant an element $x \in F_q$ with the property that $D_n(x, a) = x$.

3. Galois Rings. If p is a prime and $r, s \geq 1$ are integers $GR(p^r, s)$ will denote the Galois ring of order p^{rs} which can be obtained as a degree s Galois extension of $Z/(p^r)$, the residue class ring of integers mod p^r. Thus as special cases we have $GR(p^r, 1) = Z/(p^r)$ and $GR(p, s) = F_{q^s}$, the finite field of order p^s. Numerous properties of Galois rings can be found in Chapter XVI of McDonald [5].

In Gomez-Calderon and Mullen [2, Thm.3] it was shown that if $a \in GR(p^r, s)$ is a unit, then $D_n(x, a)$ permutes $GR(p^r, s)$ with $r > 1$ if and only if $(n, p^{2s}-1) = (n, p) = 1$ while in Theorem 4 of that same paper, it was shown that the Dickson permutation polynomials with a unit, are closed under composition if and only if $a = \pm 1$. It is thus sufficient to consider the cycle structure of $D_n(x, a)$ over $GR(p^r, s)$ for $a = 0, \pm 1$. We consider only those cases where $(n, p) = 1$.

For $a = 0$ we have by [2, Cor. 15(a)] that $D_n(x, a) = x^n$ permutes $GR(p^r, s)$ if and only if $n = 1$ or $r = 1$ and $(n, p^s-1) = 1$. For $a = \pm 1$ we make use of the following results of [2]. The first result generalizes the well known result concerning lifting solutions over $Z/(p^r)$.

Lemma 5. *Let $f(x)$ be a monic polynomial with coefficients in $GR(p^r, s)$. Assume $r \geq 2$ and let t be a solution of the equation $f(x) = 0$ in the Galois ring $GR(p^{r-1}, s)$.*

(a) *Assume $f'(t) \neq 0$ over the field $GR(p, s)$. Then t can be lifted in a unique way from $GR(p^{r-1}, s)$ to $GR(p^r, s)$.*

(b) *Assume $f'(t) = 0$ over the field $GR(p, s)$. Then we have two possibilities:*

  (b.1) *If $f(t) = 0$ over $GR(p^r, s)$, t can be lifted from $GR(p^{r-1}, s)$ to $GR(p^r, s)$ in p^s distinct ways.*

  (b.2) *If $f(t) \neq 0$ over $GR(p^r, s)$, t cannot be lifted from $GR(p^{r-1}, s)$ to $GR(p^r, s)$.*

The next technical lemma is proved as Corollary 6 of Gomez-Calderon and Mullen [2]. The structure of the group $U(p^r, s)$ of units of $GR(p^r, s)$ is given in McDonald [5, p.322–323].

Lemma 6. *For p odd and $q = p^s$, let $w = fp^t$ denote a positive integer* *with* $(f, p) = 1$. *The group* $U(p^r, 2s)$ *of units can be written as a product of a cyclic group* G *of order* q^2-1 *and* $2s$ *cyclic groups* H_i *each of order* p^{r-1}. *Let* H_i' *denote the subgroup of* H_i *of order* (p^t, p^{r-1}) *for* $i = 1, \ldots, 2s$. *Let* C_1 *and* C_2 *denote the groups* $C_1 = H_1' \times \cdots \times H_s'$ *and* $C_2 = H_{s+1}' \times \cdots \times H_{2s}'$ *where* $H_i = \langle \beta_i \rangle$ *and*

$$\sigma(\beta_i) = \begin{cases} \beta_i & \text{if } 1 \le i \le s \\ \beta_i^{-1} & \text{if } s < i \le 2s, \end{cases}$$

where σ *denotes a generator of the Galois group for* $GR(p^r, 2s)/GR(p^r, s)$. *Then*

(a) *Assume* $\mu \in GR(p^r, s)$. *Then*

(a.1) $\{\mu \mid \mu^w = 1\} = A_1 \times C_1$ *where* A_1 *denotes the group of* G *of order* $(w, q-1)$.

(a.2) $\{\mu \mid \mu^w = -1\}$
$$= \begin{cases} \phi & \text{if } w/(w, (q-1)/2) \text{ is even} \\ \{ac \mid a \in G,\ a^{(w, q-1)/2)} = -1,\ c \in C_1\} & \text{otherwise.} \end{cases}$$

(b) *Assume* $\mu \in GR(p^r, 2s)$. *Then*

(b.1) $\{\mu \mid \mu^w = 1,\ \mu\sigma(\mu) = 1\} = A_2 \times C_2$ *where* A_2 *denotes the subgroup of* G *of order* $(w, q+1)$.

(b.2) $\{\mu \mid \mu^w = -1,\ \mu\sigma(\mu) = -1\}$
$$= \begin{cases} \phi & \text{if } w/(w, q+1) \text{ or } (q+1)/(w, q+1) \text{ is even} \\ \{ac \mid a \in G,\ a^{(w, q+1)} = -1,\ c \in C_2\} & \text{otherwise.} \end{cases}$$

(c) *Assume* w *is even and* $\mu \in GR(p^r, 2s)$. *Then*
$\{\mu \mid \mu^w = 1,\ \mu\sigma(\mu) = -1\}$
$$= \begin{cases} \phi & \text{if } (q+1)/(w/2, q+1) \text{ is even} \\ \{ac \mid a \in G,\ a^{(w/2, q+1)} = -1,\ c \in C_2\} & \text{otherwise.} \end{cases}$$

(d) *Assume* w *is odd and* $\mu \in GR(p^r, 2s)$. *Then*
$\{\mu \mid \mu^w = 1,\ \mu\sigma(\mu) = -1\} = \phi$.

We are now ready to prove

Theorem 7. *Let* $r, s, m \ge 1$, p *be an odd prime and* $q = p^s$. *Let* e, E, k, K *denote nonnegative integers such that* $n^m - 1 = ep^k$ *and* $n^m + 1 = Ep^K$ *with* $(e, p) = (E, p) = 1$. *Let* $C_{\pm 2, m}$ *denote the number of cycles of* $D_n(x, 1)$ *of length* m *over* $GR(p^r, s)$ *consisting of elements* $x \not\equiv \pm 2 \bmod p$. *Then*

$$mC_{\pm 2, m} = [A(e, q) - \beta]q^{\min(r-1, k)} + [B(E, q) - \beta]q^{\min(r-1, K)} - \sum_{i \mid m,\, i < m} iC_{\pm 2, i}, \tag{10}$$

where $A(e, q) = [(e, q-1)+(e, q+1)]/2$ *and* $B(E, q) = [(E, q-1)+(E, q+1)]/2$ *and* $\beta = 1$ *if* n *is even and* $\beta = 2$ *if* n *is odd.*

Proof. Let $D_n^{(m)}(x, 1)$ denote the m-th iterate of $D_n(x, 1)$ under composition. Let $x \in GR(p^r, s)$ with $x \not\equiv \pm 2 \bmod p$. Then $x = \mu + 1/\mu$ for some $\mu \in GR(p^r, 2s)$. Then

$$D_n^{(m)}(\mu+1/\mu, 1) = \mu^{n^m}+1/\mu^{n^m} = \mu+1/\mu$$

if and only if $(\mu^{n^m-1}-1)(\mu^{n^m+1}-1) = 0$.
If $\mu^{n^m-1}-1 \equiv \mu^{n^m+1}-1 \equiv 0 \bmod p$, then $\mu \equiv \pm 1 \bmod p$ so that $x \equiv \pm 2 \bmod p$, a contradiction. Hence $D_n^{(m)}(\mu+1/\mu, 1) = \mu+1/\mu$ if and only if

$$\mu^{n^m-1} = 1 \text{ or } \mu^{n^m+1} = 1. \tag{11}$$

Moreover by Lemma 5, $x = \mu_1+1/\mu_1 = \mu_2+1/\mu_2$ with $\mu_1, \mu_2 \in GR(p^r, 2s)$ if and only if $\mu_1 = \mu_2$ or $\mu_1\mu_2 = 1$.

By Lemma 6 the number of elements $x \not\equiv \pm 2 \bmod p$ with $D_n^{(m)}(x, 1) = x$ is given by

$$(1/2)[(e, q-1)+(e, q+1)-\alpha]q^{\min(r-1, k)} + (1/2)[(E, q-1)+(E, q+1)-\alpha]q^{\min(r-1, K)}$$

where $\alpha = 2$ if n is even and $\alpha = 4$ if n is odd. By subtracting the number of elements whose cycle length divides m, we complete the proof.

Let C_m be the number of cycles of $D_n(x, 1)$ of length m.

Corollary 8. *Let* $r, s, m \geq 1$, p *be an odd prime and* $q = p^s$. *If* $n^{2m} \not\equiv \pm 1$ *mod* p *then*

$$mC_m = [(n^m-1, q-1)+(n^m-1, q+1)+(n^m+1, q-1)+(n^m+1, q+1)]/2 - \varepsilon - \sum_{i|m, i<m} iC_i,$$

where $\varepsilon = 1$ *if* n *is even and* $\varepsilon = 2$ *if* n *is odd.*

Proof. Let $f(x) = D_n^{(m)}(x, 1)-x$ so that $f(2) \equiv 0 \bmod p$ and

$$f(-2) \equiv \begin{cases} 0 \bmod p & \text{if } n \text{ is odd} \\ 4 \bmod p & \text{if } n \text{ is even.} \end{cases}$$

Also $f'(\pm 2) = D_n^{(m)'}(\pm 2, 1)-1 = (\pm 1)^{n^m-1}n^{2m}-1 \not\equiv 0 \bmod p$ by hypothesis. There are ε fixed points x with $x \equiv \pm 2 \bmod p$.

In an analogous way for $a = -1$ we may prove

Theorem 9. *Let $r, s, m \geq 1$, p be an odd prime and $q = p^s$. Let e, E, k, K denote nonnegative integers with $n^m - 1 = ep^k$ and $n^m + 1 = Ep^K$ where $(e, p) = (E, p) = 1$. Let $E_{\pm 2, m}$ denote the number of cycles of $D_n(x, -1)$ of length m over $GR(p^r, s)$ consisting of elements x with $x^2 \not\equiv -4 \bmod p$. Assume n is odd. Then*

$$mE_{\pm 2, m} = A - \sum_{i \mid m, i < m} iE_{\pm 2, i},$$

where A

$$= \frac{(n^m-1, q-1) + ((n^m-1)/2, q+1) - 4}{2} q^{\min(r-1, k)} + \frac{(n^m+1, (q-1)/2) + (n^m+1, q+1) - 4}{2} q^{\min(r-1, K)}$$

if $n^m - 1 \equiv q - 1 \equiv 0 \bmod 4$,

$$= \frac{(n^m-1, q-1) + \varepsilon_1}{2} q^{\min(r-1, k)} \qquad \text{if } n^m - 1 \equiv q + 1 \equiv 0 \bmod 4,$$

where

$$\varepsilon_1 = \begin{cases} 0 & \text{if } (q+1)/((n^m-1)/2, q+1) \text{ is even} \\ ((n^m-1)/2, q+1) & \text{if } (q+1)/((n^m-1)/2, q+1) \text{ is odd} \end{cases}$$

$$= \frac{(n^m+1, q-1) - 2}{2} q^{\min(r-1, k)} + \frac{\varepsilon_2}{2} q^{\min(r-1, K)}$$

if $n^m + 1 \equiv q - 1 \equiv 0 \bmod 4$,

where

$$\varepsilon_2 = \begin{cases} 0 & \text{if } (n^m+1)/(n^m+1, (q-1)/2) \text{ is even} \\ (n^m+1, (q-1)/2) & \text{if } (n^m+1)/(n^m+1, (q-1)/2) \text{ is odd} \end{cases}$$

$$= \frac{(n^m+1, q-1)}{2} q^{\min(r-1, k)} \qquad \text{if } n^m + 1 \equiv q + 1 \equiv 0 \bmod 4,$$

Corollary 10. *Let $r, s, m \geq 1$, p be an odd prime and $q = p^s$. Let n be an odd positive integer with $n^{2m} \not\equiv \pm 1 \bmod p$. If E_m denotes the number of cycles of $D_n(x, -1)$ of length m, then*

$$mE_m = B - \sum_{i \mid m, i < m} iE_i,$$

where B

$$= \frac{(n^m-1, q-1)+((n^m-1)/2, q+1)+(n^m+1, (q-1)/2)+(n^m+1, q+1)-4}{2}$$

$$\text{if } n^m-1 \equiv q-1 \equiv 0 \text{ mod } 4,$$

$$= \frac{(n^m-1, q-1)+\varepsilon_1}{2} \qquad \text{if } n^m-1 \equiv q+1 \equiv 0 \text{ mod } 4,$$

$$= \frac{(n^m+1, q-1)-2+\varepsilon_1}{2} \qquad \text{if } n^m+1 \equiv q-1 \equiv 0 \text{ mod } 4,$$

$$= \frac{(n^m+1, q-1)}{2} \qquad \text{if } n^m+1 \equiv q+1 \equiv 0 \text{ mod } 4.$$

If $x^2 \not\equiv 4a \bmod p$ then $x \in GR(p^r, s)$ can be written as $x = \mu + a/\mu$ for some $\mu \in GR(p^r, 2s)$. However if $x^2 \equiv 4a \bmod p$, then it may not be possible to write x in the above form. In this case the above argument becomes much more complicated and so to keep this paper to a reasonable length, we omit discussion of this more complicated case.

REFERENCES

[1] S. AHMAD: Cycle structure of automorphisms of finite cyclic groups, J. Comb. Thy. 6 (1969), 370–374.

[2] J. GOMEZ-CALDERON and G. L. MULLEN: Galois rings and algebraic cryptography, Acta Arith., to appear.

[3] R. LIDL: Theory and applications of Dickson polynomials, in Topics in Polynomials of One and Several Variables and Their Applications: A Mathematical Legacy of P. L. Chebyshev (1821–1894), (eds. T. M. Rassias, H. M. Srivastava, A. Yanushauskas), World Scientific, 1991.

[4] R. LIDL and H. NIEDERREITER: Finite Fields, Encyclo. Math. and Appls. Vol. 20, Addison-Wesley, Reading, MA 1983; Now distributed by Camb. Univ. Press.

[5] B. R. McDONALD: Finite Rings with Identity, Marcel Dekker, Inc., New York, 1974.

[6] G. L. MULLEN: Dickson polynomials over finite fields, Proc. First Internat. Symp. Alg. Structures and No. Thy., Hong Kong 1988, World Scientific, 1991, 190–207.

[7] R. NÖBAUER: Über die Fixpunkte von durch Dicksonpolynome dargestellten Permutationen, Acta Arithmetica, 45 (1985), 173–181.

R. LIDL
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF TASMANIA
HOBART, TASMANIA 7001, AUSTRALIA

G. L. MULLEN
MATHEMATICS DEPARTMENT
THE PENNSYLVANIA STATE UNIVERSITY
UNIVERSITY PARK, PA 16802, USA

(Received May 17, 1991)