ACTA ARITHMETICA
LIX.4 (1991)

Galois rings and algebraic cryptography

by

JAVIER GOMEZ-CALDERON (New Kensington, Pa.) and
GARY L. MULLEN* (University Park, Pa.)

1. Introduction. It is well known that many cryptographic systems can be constructed based on polynomials and functions over finite fields and residue class rings of integers. As stated by McDonald [11, p. 307] "it is classically accepted that the researcher handles separately the finite field $GF(p^n)$ and the prime ring $\mathbf{Z}/\mathbf{Z}_{p^m}$. It is our belief that both cases should be treated simultaneously in the setting of a Galois ring." Following the lead of McDonald, in this paper we study a number of properties of Dickson polynomials over Galois rings. As a result, we show that a number of cryptographic systems constructed using polynomials over finite fields and residue class rings of integers can be generalized by considering Dickson polynomials over Galois rings.

2. Basic properties of Galois rings. If R is a finite local commutative ring with maximal ideal M and residue field $k = R/M$, by a *monic basic irreducible* $f \in R[x]$ is meant a monic irreducible polynomial f with the property that μf is irreducible in $k[x]$ where μ denotes the natural projection $\mu\colon R[x] \to k[x]$.

Galois rings are finite extensions of the residue class ring $\mathbf{Z}/\mathbf{Z}_{p^n}$ of integers. In particular, if p is a prime and $n, m \geqslant 1$ are integers, $GR(p^n, m)$ will denote the Galois ring of order p^{nm} which can be obtained as a Galois extension of $\mathbf{Z}/\mathbf{Z}_{p^n}$ of degree m. Hence $GR(p^n, m)$ can be viewed as $(\mathbf{Z}/\mathbf{Z}_{p^n})[x]/(f)$ where f is a monic basic irreducible in $(\mathbf{Z}/\mathbf{Z}_{p^n})[x]$ of degree m. Thus $GR(p^n, 1) = \mathbf{Z}/\mathbf{Z}_{p^n}$ and $GR(p, m) = GF(p^m)$, the finite field of order p^m.

For purposes of construction and ease of implementation of Galois rings, one can construct $GR(p^n, m)$ by considering $(\mathbf{Z}/\mathbf{Z}_{p^n})[x]/(f)$ where f is a monic irreducible polynomial of degree $m \geqslant 1$ over the finite field $GF(p)$ with p prime. Tables of such irreducibles are readily available, see for example Tables C–F and the references in Lidl and Niederreiter [10]. Further details concerning properties of Galois rings can be found in Chapter XVI of McDonald [11].

* This author would like to thank the National Security Agency for partial support under grant agreement # MDA904-87-H-2023.

The following lemma, proved in McDonald [11, pp. 269–271], provides a generalization of the well known result concerning lifting solutions over $\mathbf{Z}/\mathbf{Z}_{p^n}$, see for example Apostol [1, Thm. 5.30].

LEMMA 1. *Let $f(x)$ be a monic polynomial with coefficients in $\mathrm{GR}(p^n, m)$. Assume $n \geq 2$ and let T be a solution of the equation $f(x) = 0$ in the Galois ring $\mathrm{GR}(p^{n-1}, m)$.*

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

(b) *Assume $f'(T) = 0$ over the field $\mathrm{GR}(p, m)$. Then we have two possibilities:*

(b.1) *If $f(T) = 0$ over $\mathrm{GR}(p^n, m)$, T can be lifted from $\mathrm{GR}(p^{n-1}, m)$ to $\mathrm{GR}(p^n, m)$ in p^m distinct ways.*

(b.2) *If $f(T) \neq 0$ over $\mathrm{GR}(p^n, m)$, T can not be lifted from $\mathrm{GR}(p^{n-1}, m)$ to $\mathrm{GR}(p^n, m)$.*

3. Dickson polynomials. Let R be a commutative ring with identity. If $a \in R$ and $d \geq 1$ is an integer, the Dickson polynomial $g_d(x, a)$ of degree d over R is defined by

$$g_d(x, a) = \sum_{t=0}^{[d/2]} \frac{d}{d-t}\binom{d-t}{t}(-a)^t x^{d-2t} \tag{1}$$

where [ ] denotes the greatest integer function. Since $g_d(x, 0) = x^d$ the Dickson polynomial $g_d(x, a)$ may be viewed as a generalization of the power polynomial x^d on R. Many papers have been written concerning various properties of Dickson polynomials over finite fields and residue class rings of integers, see for example the references in Chou, Gomez-Calderon, and Mullen [3], Nöbauer [13], and Lidl and Niederreiter [10].

In Lausch and Nöbauer [6, Thm. 9.43] the following useful result is proven.

LEMMA 2. *Suppose $(d, p^{2m}-1) = 1$ and $0 \neq a \in \mathrm{GR}(p, m)$. Then the derivative $g_d'(x, a)$ does not vanish on the field $\mathrm{GR}(p, m)$ if and only if $(d, p) = 1$.*

It is well known [10, Thm. 7.16] that if $0 \neq a \in \mathrm{GF}(p^m)$, then $g_d(x, a)$ permutes $\mathrm{GF}(p^m)$ if and only if $(d, p^{2m}-1) = 1$. This result has been extended to the setting of Galois rings, see Bremser and Gomez-Calderon [2, Thm. 3]. The Galois ring result also follows from Lausch and Nöbauer [6, Prop. 4.31]. However, because of the importance of this result for our purposes, we include a proof here:

THEOREM 3. *Let a be a unit in $\mathrm{GR}(p^n, m)$. Then $g_d(x, a)$ permutes $\mathrm{GR}(p^n, m)$ with $n > 1$ if and only if $(d, p^{2m}-1) = (d, p) = 1$.*

Proof. Suppose $g_d(x, a)$, a a unit, permutes the ring $\mathrm{GR}(p^n, m)$ with $n > 1$. Then $\bar{g}_d(x, a)$, the reduction of $g_d(x, a)$ modulo p, permutes the field $\mathrm{GR}(p, m)$ and each preimage of $\bar{g}_d(x, a)$ can be lifted in a unique way from $\mathrm{GR}(p, m)$ to $\mathrm{GR}(p^n, m)$. Therefore, $(d, p^{2m}-1) = 1$ and, by Lemmas 1 and 2, $(d, p) = 1$. Now, suppose $(d, p^{2m}-1) = (d, p) = 1$ and $n > 1$. Then by Lemma 2, $\bar{g}_d'(x, a)$ does not vanish on $\mathrm{GR}(p, m)$ for all units a in $\mathrm{GR}(p, m)$. Hence, each preimage of $\bar{g}_d(x, a)$ can be lifted in a unique way. Therefore, $g_d(x, a)$ permutes $\mathrm{GR}(p^n, m)$.

We now consider the question of when the Dickson polynomials over Galois rings are closed under composition, extending the corresponding finite field result, see [10, Thm. 7.22]. To this end, for a unit $a \in \mathrm{GR}(p^n, m)$ let

$$P(a) = \{g_d(x, a) : g_d(x, a) \text{ permutes } \mathrm{GR}(p^n, m)\}.$$

THEOREM 4. *Let a be a unit in $\mathrm{GR}(p^n, m)$ with p odd. Then $P(a)$ is closed under composition if and only if $a = \pm 1$.*

Proof. If $n = 1$, the result follows from [10, Thm. 7.22]. We make use of the functional equation for Dickson polynomials. If $x \in \mathrm{GR}(p^n, m)$ then x can be written as $x = y + a/y$ for some $y \in \mathrm{GR}(p^n, 2m)$ if $x^2 \not\equiv 4a \pmod p$ and for some $y \in \mathrm{GR}(p^n, 2m)$ $[\sqrt{p}]$ if $x^2 \equiv 4a \pmod p$. Then

$$g_d(x, a) = y^d + (a/y)^d. \tag{2}$$

Analogous to the argument of Lidl and Niederreiter [10, Thm. 7.22], for a unit $a \in \mathrm{GR}(p^n, m)$ we have

$$g_k(g_r(y + a/y, a), a^r) = g_k(y^r + (a/y)^r, a^r) = y^{kr} + (a/y)^{kr} = g_{kr}(y + a/y, a). \tag{3}$$

Thus,

$$g_{kr}(x, a) = g_k(g_r(x, a), a^r). \tag{4}$$

Suppose $P(a)$ is closed. Then $g_k(g_r(x, a), a) = g_{kr}(x, a)$. Hence, by (4),

$$g_k(g_r(x, a), a) = g_k(g_r(x, a), a^r).$$

Therefore, since g_r is a permutation,

$$g_k(x, a) = g_k(x, a^r).$$

Considering $k = p^m \pm 2$, we compare coefficients of x^{k-2} to obtain $a^r = a$ for all r, $(r, p^{2m}-1) = (r, p) = 1$. Thus, we can take $r = (p^m+1)e - 1$ where $e = (p^m-1)p^{n-1}$ denotes the exponent of the group $U(p^n, m)$ of units of $\mathrm{GR}(p^n, m)$. Therefore, $a^r = a^{-1} = a$. Hence, since p is odd, $a = \pm 1$.

Now, if $a = \pm 1$, then it is easy to see, from (4), that $P(a)$ is closed under composition. This completes the proof of the theorem.

LEMMA 5. *Let S denote a generator of the Galois group for $\mathrm{GR}(p^n, 2m)/\mathrm{GR}(p^n, m)$ with p odd. Let $q = p^m$. Then*

(a) *The group of units $U(p^n, 2m)$ can be written as a product of a cyclic group G of order q^2-1 and $2m$ cyclic groups $H_i = \langle \beta_i \rangle$ where*

$$S(\beta_i) = \begin{cases} \beta_i & \text{if } 1 \leqslant i \leqslant m, \\ \beta_i^{-1} & \text{if } m < i \leqslant 2m. \end{cases}$$

(b) *If G_1 and G_2 denote the subgroups of G of order $q-1$ and $q+1$, respectively, and $y \in G$, then $y \in G_1$ if and only if $S(y) = y$ and $y \in G_2$ if and only if $S(y) = 1/y$.*

(c) $\{y \in U(p^n, 2m)\colon yS(y) = -1\} = \{ab\colon a \in A, b \in H_{m+1} \times \ldots \times H_{2m}\}$ *where A denotes the set $A = \{a \in G\colon a^{q+1} = -1\}$.*

Proof. By [11, Thm. XVI.9], the group $U(p^n, 2m)$ of units is the direct product of a cyclic group G of order q^2-1 and $2m$ cyclic groups H_i of order p^{n-1}. Further, without loss of generality, we assume that

$$U(p^n, 2m) \cap \mathrm{GR}(p^n, m) = G_1 \times H_1 \times \ldots \times H_m$$

where G_1 denotes the subgroup of G of order $q-1$. Now, let G_2 denote the subgroup of G of order $q+1$. Then $bS(b) \in G_1 \cap G_2 = \{\pm 1\}$ for all b in G_2. Therefore, since $bS(b) \equiv 1 \pmod p$, $bS(b) = 1$ for all b in G_2. On the other hand, wif $b \in G$ and $bS(b) = 1$ then it is easy to see that $b \in G_2$.

Now, for $i > m$ we have

$$S(\beta_i)\beta_i = \prod_{j=1}^{m} \beta_i^{a_j} \in \mathrm{GR}(p^n, m) \tag{5}$$

for some integers a_j, $1 \leqslant j \leqslant m$. We also note, since p is odd, that $\langle \beta_i^2 \rangle = \langle \beta_i \rangle$ for all $i \geqslant 1$. Therefore, equation (5) can be rewritten as

$$S(\beta_i)\beta_i = \prod_{j=1}^{m} \beta_j^{2a_j}$$

or

$$S\Big(\beta_i / \prod_{j=1}^{m} \beta_j^{a_j}\Big) = \Big(\prod_{j=1}^{m} \beta_j^{a_j}\Big)/\beta_i$$

for some integers a_j', $j \geqslant 1$. Hence, we can rearrange, if necessary, the generators β_i for $i > m$ to obtain $S(\beta_i) = 1/\beta_i$ for all $i > m$.

This completes the proof of parts (a) and (b). Now, to prove part (c), assume that $b \in G$ with $b \neq \pm 1$. Then $b^{q+1} = -1$ if and only if $b^2 \in G_2$ but $b \notin G_2$. Therefore, $b^{q+1} = -1$ if and only if $bS(b) = -1$, which completes the proof of the lemma.

COROLLARY 6. *With notation as in Lemma 5, let w denote a positive integer and write $w = fp^t$ with $(f, p) = 1$. Let H_i' denote the subgroup of H_i of order (p^t, p^{n-1}) for $i = 1, 2, \ldots, 2m$. Let C_1 and C_2 denote the groups $C_1 = H_1' \times \ldots \times H_m'$ and $C_2 = H_{m+1}' \times \ldots \times H_{2m}'$.*

(a) *Assume $y \in \mathrm{GR}(p^n, m)$. Then*

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

(a.2)

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

(b) *Assume $y \in \mathrm{GR}(p^n, 2m)$. Then*

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

(b.2)

$$\{y\colon y^w = -1, yS(y) = -1\} = \begin{cases} \emptyset & \text{if } w/(w, q+1) \text{ or } (q+1)/(w, q+1) \text{ are even}, \\ \{ac\colon a \in G, a^{(w,q+1)} = -1, c \in C_2\} & \text{otherwise}. \end{cases}$$

(c) *Assume w is even and $y \in \mathrm{GR}(p^n, 2m)$. Then*

$$\{y\colon y^w = 1, yS(y) = -1\} = \begin{cases} \emptyset & \text{if } (q+1)/(w/2, q+1) \text{ is even}, \\ \{ac\colon a \in G, a^{(w/2,q+1)} = -1, c \in C_2\} & \text{otherwise}. \end{cases}$$

(d) *Assume w is odd and $y \in \mathrm{GR}(p^n, 2m)$. Then*

$$\{y\colon y^w = 1, yS(y) = -1\} = \emptyset.$$

Because of Theorem 4 we restrict our attention to Dickson polynomials $g_d(x, \pm 1)$. A straightforward calculation yields

LEMMA 7. *Let $g_d(x, \pm 1)$ denote the Dickson polynomial of degree d over the complex numbers C. Then*

(a) $g_d'(\pm 2, 1) = (\pm 1)^{d-1} d^2$,

(b) $g_d'(\pm 2i, -1) = (\pm i)^{d-1} d^2$.

THEOREM 8. *Let $n, m \geqslant 1$, p be an odd prime and $q = p^m$. Let e, E, k, and K denote nonnegative integers so that $d-1 = ep^k$ and $d+1 = Ep^K$ with $(e, p) = (E, p) = 1$. If $F_{\pm 2} = F_{\pm 2}(g, d, 1)$ denotes the number of fixed points x of $g_d(x, 1)$ with $x \not\equiv \pm 2 \pmod p$ then*

$$F_{\pm 2} = \begin{cases} [A(e, q)-1]q^{\min\{n-1,k\}} + [B(E, q)-1]q^{\min\{n-1,K\}} & \text{if } d \text{ is even}, \\ [A(e, q)-2]q^{\min\{n-1,k\}} + [B(E, q)-2]q^{\min\{n-1,K\}} & \text{if } d \text{ is odd}, \end{cases}$$

where

$$A(e, q) = [(e, q-1)+(e, q+1)]/2 \quad \text{and} \quad B(E, q) = [(E, q-1)+(E, q+1)]/2.$$

Proof. Let x denote an element of $GR(p^n, m)$ with $x \not\equiv \pm 2 \pmod p$. Then $x = y + 1/y \in GR(p^n, m)$ for some y in $GR(p^n, 2m)$. Hence,

$$g_d(y+1/y, 1) = y^d + (1/y)^d = y + 1/y$$

if and only if

$$(y^{d-1}-1)(y^{d+1}-1) = 0.$$

Further, if $y^{d-1}-1 \equiv y^{d+1}-1 \equiv 0 \pmod p$, then $y \equiv \pm 1 \pmod p$ and so $x \equiv \pm 2 \pmod p$, a contradiction. Therefore,

$$g_d(y+1/y, 1) = y + 1/y$$

if and only if

$$y^{d-1} = 1 \quad \text{or} \quad y^{d+1} = 1.$$

We also see, by Lemma 1 and since $x \not\equiv \pm 2 \pmod p$, that

$$x = y_1 + 1/y_1 = y_2 + 1/y_2 \in GR(p^n, m)$$

with $y_1, y_2 \in GR(p^n, 2m)$ if and only if

$$y_1 = y_2 \quad \text{or} \quad y_1 y_2 = 1.$$

Therefore, combining with Corollary 6, the number of fixed points x so that $x \not\equiv \pm 2 \pmod p$ is given by

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

if d is even, and

$$\tfrac{1}{2}[(e, q-1)+(e, q+1)-4]q^{\min\{n-1,k\}} + \tfrac{1}{2}[(E, q-1)+(E, q+1)-4]q^{\min\{n-1,K\}}$$

if d is odd.

This completes the proof of the theorem.

For cryptographic applications where one would like to have a small number of fixed points, we now determine the number $F(g, d, 1)$ of fixed points of the Dickson polynomial $g_d(x, 1)$ over $GR(p^n, m)$ when $d^2 \not\equiv \pm 1 \pmod p$ so that $k = K = 0$, $e = d-1$ and $E = d+1$.

COROLLARY 9. *Let $n, m \geq 1$, p be an odd prime and $q = p^m$. Assume $d^2 \not\equiv \pm 1 \pmod p$. Then*

$$F(g, d, 1) = [(d-1, q-1)+(d-1, q+1)+(d+1, q-1)+(d+1, q+1)]/2 - \varepsilon$$

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

Proof. Let $f(x)$ be the difference $f(x) = g_d(x, 1) - x$. Thus, $f(2) \equiv 0 \pmod p$ and

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

We also have, by Lemma 7,

$$f'(\pm 2) \equiv g_d'(\pm 2, 1) - 1 \equiv \pm d^2 - 1 \not\equiv 0 \pmod p$$

for all positive integers d. Therefore, by Lemma 1, the number of fixed points x with $x \equiv \pm 2 \pmod p$ of $g_d(x, 1)$ is 2 if d is odd and 1 if d is even. This result combined with Theorem 8 completes the proof of the corollary.

We note that this result is independent of n and so agrees with Nöbauer [13, Thm. 1] in the finite field case.

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

THEOREM 10. *Let $n, m \geq 1$, p be an odd prime and $q = p^m$. Let e, E, k, and K denote nonnegative integers so that $d-1 = ep^k$ and $d+1 = Ep^K$ with $(e, p) = (E, p) = 1$. Let $F_{\pm 2i} = F_{\pm 2i}(g, d, -1)$ denote the number of fixed points x of $g_d(x, -1)$ with $x^2+4 \not\equiv 0 \pmod p$. Assume d is odd. If*

(a) $d-1 \equiv q-1 \equiv 0 \pmod 4$, *then*

$$F_{\pm 2i} = \frac{(d-1, q-1)+((d-1)/2, q+1)-4}{2} q^{\min\{n-1,k\}} + \frac{(d+1, (q-1)/2)+(d+1, q+1)-4}{2} q^{\min\{n-1,K\}};$$

(b) $d-1 \equiv q+1 \equiv 0 \pmod 4$, *then*

$$F_{\pm 2i} = \frac{(d-1, q-1)+\varepsilon_1}{2} q^{\min\{n-1,k\}}$$

where

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

(c) $d+1 \equiv q-1 \equiv 0 \pmod 4$, *then*

$$F_{\pm 2i} = \frac{(d+1, q-1)-2}{2} q^{\min\{n-1,k\}} + \frac{\varepsilon_2}{2} q^{\min\{n-1,K\}}$$

where

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

(d) $d+1 \equiv q+1 \equiv 0 \pmod 4$, *then*

$$F_{\pm 2i} = \frac{(d+1, q-1)}{2} q^{\min\{n-1,k\}}.$$

COROLLARY 11. *Let $n, m \geq 1$, p be an odd prime and $q = p^m$. Let d be a positive odd integer and assume $d^2 \not\equiv \pm 1 \pmod p$. Let $F = F(g, d, -1)$ denote the number of fixed points of $g_d(x, -1)$ over $GR(p^n, m)$. If*

(a) $d-1 \equiv q-1 \equiv 0 \pmod 4$ *then*

$$F = \frac{(d-1, q-1)+((d-1)/2, q+1)+(d+1, (q-1)/2)+(d+1, q+1)-4}{2};$$

(b) $d-1 \equiv q+1 \equiv 0 \pmod 4$, *then*

$$F = \frac{(d-1, q-1)+\varepsilon_1}{2}$$

where

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

(c) $d+1 \equiv q-1 \equiv 0 \pmod 4$, *then*

$$F = \frac{(d+1, q-1)-2+\varepsilon_2}{2}$$

where

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

(d) $d+1 \equiv q+1 \equiv 0 \pmod 4$, *then*

$$F = \frac{(d+1, q-1)}{2}.$$

Let $G(\pm 1)$ be the group of permutations represented by the polynomials in $P(\pm 1)$. Further, let $G'(\pm 1)$ denote the subgroup of $G(\pm 1)$ defined by

$$G'(\pm 1) = \{g_d(x, \pm 1)\colon\ g_d(x, \pm 1) = x \text{ for all } x \in \mathrm{GR}(p^n, m),\ x^2 \not\equiv \pm 4 \pmod p\}.$$

Finally, define the quotient group $Q(\pm 1) = G(\pm 1)/G'(\pm 1)$.

Extending [10, Thm. 7.23] for finite fields to the setting of Galois rings, we now study the structure of the groups $Q(1)$ and $Q(-1)$. To this end we first prove

LEMMA 12. *Let* $\mathrm{GR}(p^n, m)$, $n > 1$, *denote the Galois ring of order* p^{mn} *with* p *odd. Let* $Q(\pm 1)$ *denote the associated quotient group. Let* $\mathrm{Red}((q^2-1)p^{n-1})$ *denote the reduced residue system for the integers modulo* $(q^2-1)p^{n-1}$ *where* $q = p^m$. *Define* h: $\mathrm{Red}((q^2-1)p^{n-1}) \to Q(\pm 1)$ *by* $h(d) = g_d(x, \pm 1)$. *Then*

(a) h *is well defined,*

(b) h *is a group homomorphism,*

(c) h *is onto.*

Proof. Suppose $d_1 \equiv d_2 \pmod{(q^2-1)p^{n-1}}$. Let x be in $\mathrm{GR}(p^n, m)$ and assume $x^2 \not\equiv \pm 4 \pmod p$. Then, by Lemma 1, $x = y \pm 1/y$ for some y in $U(p^n, 2m)$. Therefore,

$$g_{d_1}(x, \pm 1) = y^{d_1} + (\pm 1)^{d_1}/y^{d_1} = y^{d_2} + (\pm 1)^{d_2}/y^{d_2} = g_{d_2}(x, \pm 1)$$

for all $x \in \mathrm{GR}(p^n, m)$, $x^2 \not\equiv \pm 4 \pmod p$ which proves (a).

Now, parts (b) and (c) follow directly from Theorems 4 and 3 respectively.

We are ready to prove

THEOREM 13. *Let* $\mathrm{GR}(p^n, m)$, $n > 1$, *denote the Galois ring of order* p^{nm} *with* p *odd. Let* $Q(\pm 1)$ *denote the associated quotient group. Let* $q = p^m$. *Then*

$$Q(1) \cong \frac{\mathrm{Red}((q^2-1)p^{n-1})}{\{\pm 1, \pm 1 + (q^2-1)p^{n-1}/2\}}, \tag{6}$$

$$Q(-1) \cong \begin{cases} \mathrm{Red}((q^2-1)p^{n-1}) & \text{if } q \equiv 3 \pmod 4, \\ \dfrac{\mathrm{Red}((q^2-1)p^{n-1})}{\{1, 1+(q^2-1)p^{n-1}/2\}} & \text{if } q \equiv 1 \pmod 4. \end{cases} \tag{7}$$

Proof. By Lemma 12, it suffices to determine the kernel of the homomorphism h.

Let $a = \pm 1$ and assume $d \in \ker(h)$. Then $g_d(x, a) = x$ for all x in $\mathrm{GR}(p^n, m)$ with $x^2 \not\equiv \pm 4 \pmod p$. Thus,

$$y^d + (a/y)^d = y + a/y \tag{8}$$

for all $y \in U(p^n, 2m)$ with $y^2 \not\equiv \pm 1 \pmod p$. Hence $yS(y) = a$ or $S(y) = y$, where S denotes a generator of the Galois group of the extension $\mathrm{GR}(p^n, 2m)/\mathrm{GR}(p^n, m)$. Therefore, combining (8) and Lemma 1,

$$y^{d-1} = 1 \quad \text{or} \quad y^{d+1} = a. \tag{9}$$

This is also sufficient for d to be in $\ker(h)$. Let $a = 1$. Then, combining with Lemma 5, $d \in \ker(h)$ if and only if d is a solution of one of the following two systems of congruences:

$$\begin{cases} d \equiv 1 \pmod{(q-1)p^{n-1}}, \\ d \equiv 1 \pmod{(q+1)p^{n-1}}; \end{cases} \qquad \begin{cases} d \equiv -1 \pmod{(q-1)p^{n-1}}, \\ d \equiv -1 \pmod{(q+1)p^{n-1}}. \end{cases}$$

By solving these systems $\bmod (q^2-1)p^{n-1}$, we obtain

$$\ker(h) = \{\pm 1, \pm 1 + (q^2-1)p^{n-1}/2\}.$$

We now assume $a = -1$. Then $d \in \ker(h)$ if and only if d is a solution of one of the following two systems

$$\begin{cases} d \equiv 1 \pmod{(q-1)p^{n-1}}, \\ d \equiv 1 \pmod{2(q+1)p^{n-1}}; \end{cases} \qquad \begin{cases} d \equiv -1 + (q-1)p^{n-1}/2 \pmod{(q-1)p^{n-1}}, \\ d \equiv -1 + (q+1)p^{n-1} \pmod{2(q+1)p^{n-1}}. \end{cases}$$

By solving these systems $\bmod (q^2-1)p^{n-1}$, we obtain

$$\ker(h) = \begin{cases} \{1\} & \text{if } q \equiv 3 \pmod 4, \\ \{1,\ 1+(q^2-1)p^{n-1}/2\} & \text{if } q \equiv 1 \pmod 4. \end{cases}$$

This completes the proof of the theorem.

For the sake of completeness we now mention several analogous results for the power polynomials $g_d(x, 0) = x^d$ over $\mathrm{GR}(p^n, m)$. These results are corollaries of the following theorem given by Gomez-Calderon in [5].

THEOREM 14. *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*

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

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

COROLLARY 15. *With notation as in Theorem 14,*

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

(b) *$P_d(x) = x^d$ permutes the group $U(p^n, m)$ of units if and only if $(d, p^{n-1}(p^m-1)) = 1$.*

COROLLARY 16. *Let F_d denote the number of fixed points of x^d over $\mathrm{GR}(p^n, m)$. Then*

$$F_d = (d-1, q-1)q^k + 1$$

where $k = \min\{n-1, t\}$, $q = p^m$ and $d-1 = ep^t$ with $(e, p) = 1$.

4. Cryptographic applications. Suppose that M is a message (an element of $\mathrm{GR}(p^n, m)$) which is to be sent securely from A to B. If $P(x)$ is a permutation of $\mathrm{GR}(p^n, m)$, then A sends to B the element $N = P(M)$. Since $P(x)$ is a bijection, B can obtain the original message M by calculating $P^{-1}(N) = P^{-1}(P(M)) = M$. Hence $P(x)$ should have a simple form so that $N = P(M)$ can be easily computed. Also $P(x)$ must have the property that without some secret information (the key) that only A and B know, $P^{-1}(x)$ will be hard or impossible to get, so that an unauthorized receiver cannot calculate $P^{-1}(N)$. At the same time with knowledge of the key, $P^{-1}(x)$ is easily obtained by B so that $P^{-1}(N) = M$ can be recovered by B.

In this section we briefly indicate how one can use Dickson polynomials over Galois rings to generalize a number of cryptographic systems based on finite fields and residue class rings of integers. Dickson polynomials $g_d(x, a)$ with $a = 0, \pm 1$ have been extensively studied for cryptographic purposes, see for example [8, 9, 12, 14, 17]. The usefulness of Dickson polynomials in public key

cryptography is based upon the fact that given a Dickson permutation polynomial, one can easily compute the inverse permutation if one knows the factorization of the modulus but without knowledge of this factorization, one cannot easily obtain the inverse permutation.

To be more specific, suppose m is square free and R denotes the ring of reduced residues modulo m. If $(d, \varphi(m)) = 1$ where φ is the Euler function, then as indicated in [7], $g_d(x, 0) = x^d$ permutes R, and moreover, if $de \equiv 1 \pmod{\varphi(m)}$, then x^e is the inverse permutation of x^d. Of course e is easy to calculate if $\varphi(m)$ is known. However, without the prime factorization of m, it is difficult to determine $\varphi(m)$. If m is carefully chosen and sufficiently large, the problem of determining the prime factorization of m, and hence the value $\varphi(m)$, is at the moment generally believed to be intractable.

The Dickson polynomials $g_d(x, \pm 1)$ can be used in an analogous manner. As shown in [15] if $m = p_1^{e_1} \dots p_r^{e_r}$ is the prime factorization of m and $v = \varphi(m)(p_1+1)\dots(p_r+1)$ then $g_d(x, \pm 1)$ permutes the integers modulo m if and only if $(d, v) = 1$. Choose e so that $de \equiv 1 \pmod v$. Then $g_e(x, \pm 1)$ is the inverse of $g_d(x, \pm 1)$. As in the previous case, the inverse is intractable without the prime factorization of m.

Both of the above cryptographic systems are examples of RSA-type cryptosystems, see [16]. See also the survey paper [4] for a discussion of public key cryptography. If one works over the finite field $\mathrm{GF}(q)$ then x^d permutes $\mathrm{GF}(q)$ if and only if $(d, q-1) = 1$ and the inverse permutation is given by x^e where $de \equiv 1 \pmod{q-1}$. For $0 \neq a \in \mathrm{GF}(q)$, $g_d(x, a)$ permutes $\mathrm{GF}(q)$ if and only if $(d, q^2-1) = 1$, see [10, Thm. 7.16]. From [10, Thm. 7.22] for $a \neq 0$ the Dickson polynomials are closed under composition if and only if $a = \pm 1$, and hence the inverse permutation is given by $g_e(x, \pm 1)$ where $de \equiv 1 \pmod{q^2-1}$.

We now briefly illustrate how one can employ the Galois ring $R = \mathrm{GR}(p^n, m)$ with $n > 1$ for the construction of public key cryptosystems. Theorem 3 shows that if a is a unit in R then $g_d(x, a)$ permutes R if and only if $(d, p^{2m}-1) = (d, p) = 1$. Our Theorem 4 shows that if a is a unit then the set of Dickson polynomials over R is closed under composition if and only if $a = \pm 1$. Moreover, Theorem 13 shows that if $g_d(x, \pm 1)$ permutes R, then the inverse permutation is given by $g_e(x, \pm 1)$ where $de \equiv 1 \pmod{(p^{2m}-1)p^{n-1}}$. Similarly using results of Theorem 14 and Corollaries 15 and 16, one can use the power polynomial x^d over R to construct cryptographic systems.

Because the number of fixed points of a polynomial increases upon iteration under composition, one would like to have polynomials with a small number of fixed points. For the Dickson polynomials $g_d(x, a)$ over R with $a = 0, \pm 1$, the numbers of fixed points are given in Corollaries 9, 11, and 16. These facts provide the necessary tools to construct public key and public key distribution systems over $\mathrm{GR}(p^n, m)$.

In order to work in non-prime power settings, by an application of the Chinese Remainder Theorem, we can consider the direct product of Galois

rings. For example if $m = p_1^{n_1} \dots p_r^{n_r}$ is the prime factorization of m, let $GR(p_i^{n_i}, m_i)$ be the Galois ring of order $p_i^{n_i m_i}$, $m_i \geq 1$ for $i = 1, \dots, r$. Let S denote the direct product of the Galois rings $GR(p_i^{n_i}, m_i)$, $i = 1, \dots, r$. Using the ring S one can construct various cryptographic systems generalizing those constructed over the residue class ring of integers modulo m. We shall not, however, go into these details here.

Acknowledgement. The authors would like to thank the referee for a number of suggestions that improved an earlier version of the paper.

References

[1] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer, New York 1976.
[2] P. S. Bremser and J. Gomez-Calderon, *Value sets of Dickson polynomials over Galois rings*, J. Number Theory 38 (1991), 240–250.
[3] W.-S. Chou, J. Gomez-Calderon and G. L. Mullen, *Value sets of Dickson polynomials over finite fields*, J. Number Theory 30 (1988), 334–344.
[4] W. Diffie and M. Hellman, *New directions in cryptography*, IEEE Trans. Inform. Theory IT-22 (1976), 644–654.
[5] J. Gomez-Calderon, *On the power polynomial x^d over Galois rings*, Rocky Mountain J. Math., to appear.
[6] H. Lausch and W. Nöbauer, *Algebra of Polynomials*, North-Holland, Amsterdam 1973.
[7] H. Lausch, W. Nöbauer und F. Schweiger, *Polynompermutationen auf Gruppen*, Monatsh. Math. 69 (1965), 410–423.
[8] R. Lidl and W. B. Müller, *Permutation polynomials in RSA-cryptosystems*, in *Advances in Cryptology* (ed. D. Chaum), Plenum Publ. Corp., New York 1984, 293–301.
[9] –, –, *A note on polynomials and functions in algebraic cryptography*, Ars Combin. 17 (1984), 223–229.
[10] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl., Vol. 20, Addison-Wesley, Reading, Mass., 1983 (now distributed by Cambridge Univ. Press).
[11] B. R. McDonald, *Finite Rings with Identity*, Marcel Dekker, New York 1974.
[12] W. B. Müller and W. Nöbauer, *Some remarks on public-key cryptosystems*, Studia Sci. Math. Hungar. 16 (1981), 71–76.
[13] R. Nöbauer, *Über die Fixpunkte von durch Dicksonpolynome dargestellten Permutationen*, Acta Arith. 45 (1985), 173–181.
[14] –, *Key distribution systems based on polynomial functions and on Rédei functions*, Problems Control Inform. Theory 15 (1) (1986), 91–100.
[15] –, *Über Permutationspolynome und Permutationsfunktionen für Primzahlpotenzen*, Monatsh. Math. 69 (1965), 230–238.
[16] R. L. Rivest, A. Shamir and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Comm. ACM 21 (1978), 120–126.
[17] V. Varadharajan, *Cryptosystems based on permutation polynomials*, J. Comput. Math. 23 (1988), 237–250.

DEPARTMENT OF MATHEMATICS
NEW KENSINGTON CAMPUS
THE PENNSYLVANIA STATE UNIVERSITY
New Kensington, PA 15068
U.S.A.
DEPARTMENT OF MATHEMATICS
THE PENNSYLVANIA STATE UNIVERSITY
University Park, PA 16802
U.S.A.

Received on 2.5.1990
and in revised form on 23.11.1990 (2039)

ACTA ARITHMETICA
LIX.4 (1991)

Lattice points in ellipsoids

by

SUKUMAR DAS ADHIKARI (Madras) and Y.-F. S. PÉTERMANN (Genève)

1. Introduction. The main object of this paper is to prove two-sided Omega estimates for the error terms in the classical lattice-points problem for the three- and four-dimensional spheres.

If $A_l(x)$ is the number of integer lattice-points in an l-dimensional sphere of radius $\sqrt{x}$, then as $x \to \infty$ $A_l(x) \sim V_l(x)$, where $V_l(x)$ is the volume of the sphere. We denote the corresponding error term by

$$P_l(x) = A_l(x) - V_l(x). \tag{1.1}$$

For every $l > 4$ it is known that [14, Satz 2.2.2]

$$P_l(x) = O(x^{l/2-1}) \tag{1.2}$$

and that [14, Sätze 4.4.8 and 4.4.9]

$$P_l(x) = \Omega_{\pm}(x^{l/2-1}). \tag{1.3}$$

In fact, a large part of Walfisz' book [14] (Chapters III through VII) is dedicated to the study of the lim inf and lim sup as $x \to \infty$ of the bounded function $P_l(x)x^{1-l/2}$, which in some cases are determined explicitly or sharply approximated. The main results gathered in that book are due to Landau, Lursmanaschwili, Petersson and Walfisz. When $2 \leqslant l \leqslant 4$, however, the exact order of magnitude of $P_l(x)$ (in the sense of (1.2) and (1.3)) is not even known. The case $l = 2$ is the famous circle problem; to date, the best Ω_+, Ω_-, and O-estimates are due respectively to Corrádi and Kátai [4], Hafner [5], and Huxley [6].

We first consider the case $l = 4$. Walfisz [15] proved that

$$P_4(x) = O(x(\log x)^{2/3}). \tag{1.4}$$

On the other hand, Adhikari, Balasubramanian and Sankaranarayanan [1] recently obtained the one-sided

$$P_4(x) = \Omega_+(x \log\log x) \tag{1.5}$$