EXTRACTA MATHEMATICAE 5, n.3, 124-126 (1990)

LIFTING SOLUTIONS OVER GALOIS RINGS

J. GOMEZ-CALDERON, Penn State University, New Kensington, PA 15068 U.S.A.

Let F_q denote the finite field of order q where q is an odd prime power. Let N denote the number of solutions of the equation

$$b_1 x_1^2 + b_2 x_2^2 + \dots + b_n x_n^2 = e$$

in the field F_q. Then, see [1, Thms.6.26 and 6.27],

$$N = \begin{cases} q^{n-1} + v(e)\, q^{\frac{n-2}{2}} C\left((-1)^{\frac{n}{2}} b_1 b_2 \dots b_n\right) & \text{if n is even} \\ q^{n-1} + q^{\frac{n-1}{2}} C\left((-1)^{\frac{n-1}{2}} e b_1 b_2 \dots b_n\right) & \text{if n is odd,} \end{cases} \qquad (1)$$

where C is the quadratic character of F_q and V is the integer - valued function on F_q defined by $V(x) = -1$ for $x \in F_q^*$ and $V(0) = q-1$.

In this note we generalize above result from finite fields to Galois rings which are finite extensions of the ring Z_{p^m} of integers modulo p^m where p is a prime and $m \geq 1$. In particular, $GR(p^m, r)$ will denote the Galois ring of order p^{mr} which can be obtained as a Galois extension of Z_{p^m} of degree r. Thus, $GR(p^m, 1) = Z_{p^m}$ and $GR(p, r) = F_{p^r}$, the finite field of order p^r. The reader can find further details concerning Galois rings in the reference [2].

LEMMA: Let $F(\vec{x}) = F(x_1, x_2, \dots, x_n)$ be a polynomial with coefficients in $GR(p^m, r)$. Assume $\vec{a} = (a_1, a_2, \dots, a_n)$ is a solution of the equation $F(\vec{x}) = 0$ in $GR(p^m, r)$. Let $L = L(\vec{a})$ denote the set of vectors $\vec{A} = (A_1, A_2, \dots, A_n)$ in $GR^n(p^{m+1}, r)$ such that $F(\vec{A}) = 0$ over $GR(p^{m+1}, r)$ and $A_i = a_i \bmod (p^m)$ for $i = 1, 2, \dots, n$. Then

(a) Assume $\nabla F(\vec{a}) = (D_{x1}F(\vec{a}), D_{x2}F(\vec{a}), \dots, D_{xn}F(\vec{a})) \neq 0 \pmod p$. Then $|L| = (p^r)^{n-1} = q^{n-1}$

(b) Assume $\nabla F(\vec{a}) = 0 \pmod p$. Then we have two possibilities:

(b.1) If $F(a) = 0$ over $GR(p^{m+1}, r)$ then $|L| = (p^r)^n = q^n$

(b.2) If $F(a) \neq 0$ over $GR(p^{m+1}, r)$ then $|L| = 0$.

PROOF: Assume $F(\vec{a}) = F(a_1, a_2, \dots, a_n) = 0$ over $GR(p^m, r)$ and let $\vec{A} = \vec{a} + (w_1, w_2, \dots, w_n)\, p^m$ where $w_i \in GR(p, r)$ for $i = 1, 2, \dots, n$. Then by Taylor's formula

$$F(\vec{A}) = F(\vec{a}) + \sum_{i=1}^{n} D_{xi}(\vec{a})\, w_i\, p^m$$

over GR (p^{m+1},r). Further, since $F(\vec{a}) = 0$ over GR (p^m,r),

$$F(\vec{A}) = [k + \sum_{i=1}^{n} D_{xi} F(\vec{a})\, w_i]\, p^m$$

for some k in GR (p^{m+1}, r). Therefore, $F(\vec{A}) = 0$ over GR (p^{m+1},r) if and only if $k + \sum_{i=1}^{n} D_{xi}F(\vec{a})\, w_i = 0$ over the field GR (p, r). If $\nabla F(\vec{a}) \neq 0 \pmod p$ then the number of distinct vectors $(w_1, w_2,\ldots,w_n)$ in GR ^{n} (p,r) is $(p^r)^{n-1} = q^{n-1}$.

On the other hand, if $\nabla F(\vec{a}) = 0 \pmod p$ then there are no solutions if $k \neq o$ and q^n solutions if $k = 0$.

THEOREM: Let $b_1, b_2, \ldots, b_n$ and e denote n+1 units in GR (p^m,r). Let N' denote the number of solutions of the equation

$$b_1 x_1{}^2, + b_2 x_2{}^2 + \ldots + b_n x^2{}_n = e$$

in the ring GR (p^m,r). Let $q = p^r$. Then

$$N' = \begin{cases} [q^{n-1} - q^{\frac{n-2}{2}} C'((-1)^{\frac{n}{2}} b_1 b_2 \ldots b_n)]\, q^{(n-1)(m-1)} & \text{if n is even} \\ [q^{n-1} + q^{\frac{n-1}{2}} C'((-1)^{\frac{n-1}{2}} e\, b_1 b_2 \ldots b_n)]\, q^{(n-1)(m-1)} & \text{if n is odd} \end{cases}$$

where C' is the quadratic character on GR (p^m,r) defined by

$$C'(a) = \begin{cases} 0 \text{ if } a = 0 \bmod p \\ 1 \text{ if a is a square unit} \\ -1 \text{ if a is a nonsquare unit} \end{cases}$$

PROOF: Let $f(\vec{x})$ denote the polynomial

$$f(\vec{x}) = b_1 x_1{}^2 + b_2 x_2{}^2 + \ldots + b_n x^2{}_n - e$$

where $b_1, b_2, \ldots, b_n$ and e denote n + 1 units of GR (p^m,r). Let $\vec{a} = (a_1, \ldots, a_n)$ denote a solution of the congruence $f(\vec{x}) = 0 \pmod p$. Then $\nabla F(\vec{a}) = 2(b_1 a_1, b_2 a_2, \ldots, b_n a_n) \neq 0 \pmod p$. Therefore, by the Lemma, the number of vectors $\vec{A} = (a_1, a_2, \ldots, a_n)$ in GR^n (p^m,r)

so that $f(\vec{A}) = 0$ and $A_i = a_i \pmod p$, $i = 1, 2, \ldots n$, is $q^{(n-1)(m-1)}$. We also apply the Lemma, with n=1, to see that b_i is a quadratic residue of GR (p^m,r) if and only if $\bar{b}_i$, the reduction of b_i modulo p, is a quadratic residue of the field GR (p,r). Therefore, combining with (1), we have completed the proof of the theorem.

REFERENCES

1. R. Lidl and H. Niederreiter, Finite Fields, Encyclo. Math. and Apps., Vol. 20, Addison-Wesley, Reading, Mass. 1983. (Now distributed by Cambridge University Press).

2. B. R. McDonald, Finite Rings With Identity, Marcel Dekker, Ind., New York, 1974.

AMS Classification 12 CO5, 10C02 and 10J05