EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
Vol. 5, No. 2, 2012, 250-259
ISSN 1307-5543 – www.ejpam.com

Generalized Gaussian Numbers Related to Linear Codes over Galois Rings

Esengül Saltürk*, İrfan Şiap

Department of Mathematics, Yildiz Technical University, Istanbul, Turkey

Abstract. In this paper, we define a family of Generalized Gaussian Numbers that gives the number of linear codes over Galois rings directly. Also, we study some of their properties and obtain some relations between them.

2010 Mathematics Subject Classifications: 11T71, 94B05, 05A10

Key Words and Phrases: Gaussian binomial coefficients, linear codes over rings

1. Introduction

Binomial coefficients and Gaussian binomial coefficients are two fundamental classes of numbers arising in enumerative combinatorics. Binomial coefficients give the number of subsets of a finite set. On the other hand, Gaussian binomial coefficients give the number of linear codes over finite fields of a particular dimension. Since the theory of linear codes over fields has been extended linear codes over rings recently, the problems that had found answers for field cases remain open for the ring cases. One of such problems is establishing a formula for the number of linear codes of a particular type similar to Gaussian Number formula. In this paper, the authors provide such a formula that directly gives the number of linear codes over Galois rings of a particular type.

Linear codes over finite rings have been a very important field of coding theory due to Hammons et al [4]. The enumeration problems over rings are studied by many researchers. Some of them are [1, 2, 3, 5, 10, 11, 14]. The enumeration in all of these works are based on recursive formulae.

In this work, we give a direct calculation of the number of linear codes over an important family of finite rings which is Galois rings. As a result of this, we define Generalized Gaussian Numbers as a further generalization of the previous works [10, 11] and give some of their properties similar to Gaussian binomial coefficients. Finally, some number sequences are also

*Corresponding author.

Email addresses: esalturk@yildiz.edu.tr (E. Saltürk), isiap@yildiz.edu.tr (İ. Şiap)

presented.

In the sequel, we present some well known concepts and results in both coding theory and algebra. F_q will denote the finite field with q elements where q is a prime power. A linear code C of length n over $\mathbb{F}_q$ is a subspace of $\mathbb{F}_q^n$.

Definition 1. *[8] For positive integers $b \neq 1$ and n, and all nonnegative integers k, the b-ary Gaussian binomial coefficients $\left[\begin{array}{c} n \\ k \end{array} \right]_b$ are defined by*

$$\left[\begin{array}{c} n \\ 0 \end{array} \right]_b = 1, \text{ and}$$

$$\left[\begin{array}{c} n \\ k \end{array} \right]_b = \frac{(b^n-1)(b^{n-1}-1)\dots(b^{n-k+1}-1)}{(b^k-1)(b^{k-1}-1)\dots(b-1)}, \qquad k = 1,2,\dots$$

Theorem 1. *[8] The number of distinct (although not necessarily inequivalent) $[n,k]$-codes over F_q is the q-ary Gaussian binomial coefficient $\left[\begin{array}{c} n \\ k \end{array} \right]_q$ where q is a prime.*

For the proof of this theorem and some more details the reader is kindly directed to [8].

Definition 2. *[13] A Galois ring is defined to be a finite ring with identity 1 such that the set of its zero divisors including 0 forms a principal ideal $(p1)$ for some prime p where*

$$p1 = \underbrace{1+1+\dots+1}_{p}.$$

It is well known that the characteristic a finite Galois ring is a prime power number. A finite Galois ring of characteristic p^m and cardinality p^{mt} where p is a prime number and m,t are positive integers is denoted by $R = GR(p^m,t)$. Besides some further remarks which will be given in the next section, more detailed and further information regarding Galois rings can be found in [9, 13].

Definition 3. *An R submodule of R^n is called an R-linear code.*

Theorem 2. *[6] A generator matrix of an $GR(p^m,t)$-linear code C is equivalent to a linear code generated by*

$$\begin{pmatrix} I_{k_1} & A_{11} & A_{12} & \cdots & A_{1m} \\ 0 & pI_{k_2} & pA_{22} & \cdots & pA_{2m} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & p^{m-1}I_{k_{m-1}} & p^{m-1}A_{mm} \end{pmatrix} \tag{1}$$

where A_{ij}'s denote matrices whose entries are from R and $I_{k_1}, I_{k_2}, \dots, I_{k_m}$ are identity matrices of sizes $k_1, k_2, \dots, k_m$ respectively.

A linear code C generated by a matrix (1) is called a $(k_1, k_2, \dots, k_m)$-type code.

2. Codes over Galois rings

A definition in a closed form for Galois rings is given in the previous section (Definition 2). Here, first we give an alternative description of a Galois ring which is constructive and it will be referred frequently. Define the following map [13] from polynomial ring $\mathbb{Z}_{p^m}[x]$ over $\mathbb{Z}_{p^m}$ to the polynomial $\mathbb{F}_p[x]$ over $\mathbb{F}_p$:

$$\begin{gathered} - : \mathbb{Z}_{p^m}[x] \to \mathbb{F}_p[x] \\ a_0 + a_1 x + \ldots + a_n x^n \mapsto \bar{a}_0 + \bar{a}_1 x + \ldots + \bar{a}_n x^n \end{gathered}$$

where x is an indeterminate over $\mathbb{Z}_{p^m}$ and also over $\mathbb{F}_p$, $\bar{a}_i \in \mathbb{Z}_p$ is the residue of $a_i \in \mathbb{Z}_{p^m}$ and $i = 0, 1, \ldots, n$.

Definition 4. *[9] Let $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ be monic polynomial of degree $d \geqslant 1$ in $\mathbb{Z}_{p^m}[x]$. If $\bar{f}(x) = \bar{a}_0 + \bar{a}_1 x + \ldots + \bar{a}_n x^n$ is irreducible in $\mathbb{F}_p[x]$, $f(x)$ is called a monic basic irreducible polynomial in $\mathbb{Z}_{p^m}[x]$.*

Let $R = \mathbb{Z}_{p^m}[\xi]$ where p is a prime and m is an integer. A Galois ring of characteristic p^m and cardinality p^{mr} is a ring isomorphic to R, where ξ is a primitive root of a basic irreducible polynomial $f(x)$ of degree n.

Obviously, $R = \mathbb{Z}_{p^m}[x]/\langle f(x)\rangle$ and $R = GR(p^m, d)$, where $\langle f(x)\rangle$ means the ideal generated by $f(x)$ and d is the degree of $f(x)$. In the remaining part of the paper, R will be always referred as the ring $GR(p^m, d)$. Although R is not a vector space, we will nevertheless call its elements as "vectors" . The Galois ring R has elements of orders $(p^m)^d, (p^{m-1})^d, (p^{m-2})^d, \ldots, p^d$ and the element zero is of order 1.

Here, we give a formula for the number of distinct (not necessarily inequivalent) linear codes over R. We do the enumeration by constructing the generator matrices of those codes.

Theorem 3. *The number of distinct (not necessarily inequivalent) linear codes over R is*

$$N^R_{k_1,k_2,\ldots,k_s}(n) = \left[\begin{array}{c} n \\ k_1, k_2, \ldots, k_s \end{array} \right]_R = \frac{A}{B}, \tag{2}$$

where $A = \prod_{t=1}^{m} \prod_{i=0}^{k_t - 1} ((p^{m-(t-1)})^{dn} - (p^{m-1-(t-1)})^{dn} . d^{\sum_{j=0}^{t-1} k_j} \cdot p^{di})$, and

$$\begin{aligned} B = \prod_{s=1}^{m} \prod_{r=0}^{k_s - 1} \Bigg(& \prod_{z=1}^{s} (p^{m-(s-1)})^{dk_z} \prod_{j=s+1}^{m} (p^{m-(j-1)})^{dk_j} \\ & - (\prod_{z=1}^{s} (p^{m-s})^{dk_z})(p^{m-(s+1)})^{dk_{s+1}} \cdot \prod_{t=s+2}^{m} (p^{m-(t-1)})^{dk_t} \cdot p^r \Bigg) \end{aligned}$$

Proof. In order to enumerate linear codes of length n and type $(k_1, k_2, \ldots, k_m)$ over R, we construct their generator matrices by choosing ordered k_i R-linearly independent elements of order $(p^{m-i+1})^d$, $i \in \{1, 2, \ldots, m\}$ respectively. Let

$$S = (v_1^{(p^m)^d}, v_2^{(p^m)^d}, \ldots, v_{k_1}^{(p^m)^d}, v_1^{(p^{m-1})^d}, \ldots, v_{k_2}^{(p^{m-1})^d}, \ldots, v_1^{(p^2)^d}, \ldots, v_{k_{m-1}}^{(p^2)^d}, v_1^{(p)^d}, \ldots, v_{k_m}^{(p)^d})$$

be the ordered set of such elements where $v_i^{(j)^d}$ denote the i^{th} element of order $(j)^d$, $p \leq j \leq p^m$, $1 \leq i \leq k_w$ and $w = 1, 2, \ldots, m$.

There are $((p^m)^d)^n$ elements in R^n. In order to choose the first free vector, $v_1^{(p^m)^d}$, we subtract the number of elements which are not of order $(p^m)^d$ from the whole group R^n. The elements of order $(p^m)^d$ have at least one unit element of R in any of n components. The number of the unit elements of R is $(p^m)^d - (p^{m-1})^d$ since the number of elements which are not of order $(p^m)^d$ in R is $(p^{m-1})^d$.

Since there are n choices for a unit in order to get an element of order $(p^{m-1})^d$, we obtain the number $(p^{(m-1)^d})^n$ as the number of elements of R^n which are not of order $(p^m)^d$. We have

$$((p^m)^d)^n - ((p^{m-1})^d)^n$$

possibilities.

For the second vector, $v_2^{(p^m)^d}$, we can take all vectors of order p^m except the vectors which are linearly dependent with the first taken into account. Hence, we choose the second one such that $\langle v_1^{(p^m)^d}, v_2^{(p^m)^d} \rangle = C_2$ and $|C_2| = ((p^m)^d)^2$. The set of vectors that cannot be taken for the second vector is the following:

$$K_2 = \{\alpha_1 {v_1}^{(p^m)^d} + w | w \text{ is not of order } (p^m)^d \text{ and } \alpha_1 \in \mathbb{Z}_p[\xi]\}.$$

Since $|K_2| = ((p^{m-1})^d)^n p^d$, we have

$$(((p^m)^d)^n - ((p^{m-1})^d)^n p^d)$$

possibilities for the second vector.

Next, we choose $v_3^{(p^m)^d}$ from R^n such that $C_3 = \langle C_2 \cup \{v_3^{(p^m)^d}\} \rangle$ and $|C_3| = ((p^m)^d)^3$. While making this choice, again we exclude the set

$$K_3 = \{\alpha_1 {v_1}^{(p^m)^d} + \alpha_2 {v_2}^{(p^m)^d} + w | o(w) \neq p^m \text{ and } \alpha_1, \alpha_2 \in \mathbb{Z}_p[\xi]\}.$$

Hence, we have

$$(((p^m)^d)^n - ((p^{m-1})^d)^n p^{2d})$$

ways to choose $v_3^{(p^m)^d}$ since $|K_3| = ((p^{m-1})^d)^n (p^d)^2$ possibilities.

The same calculation for the remaining $k_1 - 3$ vectors yields the following number (by considering all possibilities)

$$(p^{mdn} - p^{(m-1)dn})(p^{mdn} - p^{(m-1)dn} p^d)(p^{mdn} - p^{(m-1)dn} p^{2d}) \ldots ((p^m)^n - (p^{m-1})^n p^{d(k_1-1)}) = \prod_{j=0}^{k_1-1} p^{mdn} - p^{(m-1)dn} p^{dj}.$$

Now, we choose k_2 elements of order $p^{(m-1)d}$ and the first one is $v_1^{(p^{(m-1)d})}$ such that $C_{k_1+1} = \langle C_{k_1} \cup \{v_1^{(p^{(m-1)d})}\} \rangle$ and $|C_{k_1+1}| = (p^{md})^{k_1} . (p^{(m-1)d})^1$. Here, we have to take into

account the k_1 elements which have been already considered of order p^m that will contribute to the set of elements of order $p^{(m-1)d}$.

We consider the elements of the following set:

$$K_{k_1+1} = \{\alpha_1 v_1{}^{p^{md}} + \alpha_2 v_2{}^{p^{md}} + \ldots + \alpha_{k_1} v_{k_1}{}^{p^{md}} + w | w \text{ is of order less or equal to } p^{(m-1)d} \text{ and } \alpha_i \in \mathbb{Z}_p[\xi], i = 1,2,\ldots,k_1\}$$

which has elements of order less or equal to $p^{(m-1)d}$.

Since $|K_{k_1+1}| = (p^{(m-2)d})^n p^{dk_1}$ and there are $p^{(m-1)dn}$ elements of order $\leq p^{(m-1)d}$ in R, we have $v_1^{(p^{(m-1)dn})}$ is

$$(p^{(m-1)dn} - p^{(m-2)dn} p^{dk_1})$$

possibilities.

The same calculation for the remaining $k_2 - 1$ vectors yields the number

$$\{(p^{(m-1)d})^n - (p^{(m-2)d})^n p^{dk_1}\}\{(p^{(m-1)d})^n - (p^{(m-2)d})^n p^{dk_1} p^d\}\{(p^{(m-1)d})^n - (p^{(m-2)d})^n p^{dk_1} p^{2d}\}\ldots$$
$$\{(p^{(m-1)d})^n - (p^{(m-2)d})^n p^{dk_1} p^{d(k_2-1)}\} = \prod_{j=0}^{k_2-1} \{(p^{(m-1)d})^n - (p^{(m-2)d})^n p^{dk_1} p^d j\}.$$

Inductively, if the remaining k_i, $(i = 3,4,\ldots,m)$, linearly independent vectors of orders $(p^{m-i+1})^d$ are chosen in a similar way, the we get

$$A = \prod_{t=1}^{m} \prod_{i=0}^{k_t-1} ((p^{(m-(t-1))d})^n - (p^{(m-1-(t-1))d})^n p^{\sum_{j=0}^{t-1} dk_j} p^d i).$$

possibilities.

Analogously, the term

$$B = \prod_{s=1}^{m} \prod_{r=0}^{k_s-1} \left(\prod_{z=1}^{s} (p^{m-(s-1)})^{dk_z} \prod_{j=s+1}^{m} (p^{m-(j-1)})^{dk_j} - (\prod_{z=1}^{s} (p^{m-s})^{dk_z})(p^{m-(s+1)})^{dk_{s+1}} \cdot \prod_{t=s+2}^{m} (p^{m-(t-1)})^{dk_t} . p^r \right)$$

describes the number of bases determining linear codes of length n and type $(k_1, k_2, \ldots, k_m)$ over R. Here, the choices are taken from inside a linear code of length n and type $(k_1, k_2, \ldots, k_m)$. Such a code has $(p^{md})^{k_1} . (p^{(m-1)d})^{k_2} \ldots (p^{2d})^{k_{m-1}} (p)^{dk_m}$ vectors. Hence the following ratio gives the result

$$N = \frac{A}{B}.$$

Now we give a corollary for counting the linear codes over the first non trivial Galois ring $\mathbb{Z}_4[\xi]$ of 16 elements.

Corollary 1. *The number of distinct linear codes of type* (k_1, k_2) *over* $\mathbb{Z}_4[\xi]$ *is*

$$\left[\begin{array}{c} n \\ k_1, k_2 \end{array}\right]_{\mathbb{Z}_4[\xi]} = N^R_{k_1,k_2}(n) = \frac{\prod_{i=0}^{k_1-1}(16^n - 4^{n+i})\prod_{j=0}^{k_2-1}(4^n - 4^{k_1+j})}{\prod_{t=0}^{k_1-1}(16^{k_1}.4^{k_2} - 4^{k_1+k_2+t})\prod_{l=0}^{k_2-1}(4^{k_1+k_2} - 4^{k_1+l})}$$

where ξ *is a root of the basic irreducible polynomial* $1 + x + x^2 \in \mathbb{Z}_4[x]$.

Example 1. *The number of distinct linear codes of length* 3 *and type* $(k_1, k_2) = (2, 1)$ *over* $\mathbb{Z}_4[\xi]$ *is*

$$\frac{(16^3 - 4^3)(16^3 - 4^4)(4^3 - 4^2)}{(16^2 4 - 4^2 4)(16^2 4 - 4^2 4^2)(4^2 4^1 - 4^2)} = 21.$$

These linear codes are given by the following generator matrices:

$$\left(\begin{array}{ccc} 1 & 0 & x \\ 0 & 1 & x \\ 0 & 0 & 2 \end{array}\right)\left(\begin{array}{ccc} 1 & x & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{array}\right)\left(\begin{array}{ccc} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right)$$

where $x \in \{0, 1, \xi, 1 + \xi\}$ *and* ξ *is a root of the polynomial* $1 + x + x^2$.

Definition 5. *Let R be a Galois ring. An additive code of length n over R is subgroup of* R^n.

Here we emphasize that an additive code is actually a $\mathbb{Z}$- submodule of R^n. On the other hand, a linear code is an R- submodule of R^n. Now we give the number of additive codes of a particular type over Galois rings.

Theorem 4. *The number of distinct (not necessarily inequivalent) additive codes over R is*

$$N^{+R}_{k_1,k_2,\ldots,k_s}(n) = \left[\begin{array}{c} n \\ k_1, k_2, \ldots, k_s \end{array}\right]^+_R = \frac{A}{B}, \tag{3}$$

where $A = \prod_{t=1}^{m}\prod_{i=0}^{k_t-1}((p^{m-(t-1)})^{dn} - (p^{m-1-(t-1)})^{dn}.p^{\sum_{j=0}^{t-1}k_j}.p^i)$, *and*

$$B = \prod_{s=1}^{m}\prod_{r=0}^{k_s-1}\left(\prod_{z=1}^{s}(p^{m-(s-1)})^{k_z}\prod_{j=s+1}^{m}(p^{m-(j-1)})^{k_j}\right.$$
$$\left.-(\prod_{z=1}^{s}(p^{m-s})^{k_z})(p^{m-(s+1)})^{k_{s+1}}\cdot\prod_{t=s+2}^{m}(p^{m-(t-1)})^{k_t}\cdot p^r\right)$$

Proof. We prove the theorem similar to the proof of the Theorem 3. Here, we will take the additive orders of the elements of $\mathbb{Z}_{p^m}[\xi]$.

Corollary 2. *The number of distinct additive codes of type* (k_1, k_2) *over* $\mathbb{Z}_4[\xi]$ *is*

$$\left[\begin{array}{c} n \\ k_1, k_2 \end{array}\right]^+_{\mathbb{Z}_4[\xi]} = N^{+R}_{k_1,k_2}(n) = \frac{\prod_{i=0}^{k_1-1}(16^n - 4^n 2^i)\prod_{j=0}^{k_2-1}(4^n - 2^{k_1+j})}{\prod_{t=0}^{k_1-1}(4^{k_1}\cdot 2^{k_2} - 2^{k_1+k_2+t})\prod_{l=0}^{k_2-1}(2^{k_1+k_2} - 2^{k_1+l})}$$

where ξ *is a root of the polynomial* $1 + x + x^2$.

3. Generalized Gaussian Numbers

In this section, we are interested in the properties of the numbers $N^R_{k_1,k_2,\ldots,k_m}(n)$. Since they resemble in some sense the Gaussian numbers we call these numbers Generalized Gaussian Numbers. Hence, we study some properties of these numbers.

Some of the well known properties of the classical Gaussian binomial coefficients are as follows:

Theorem 5. *Assume the notations in Definition 1. Then,*

(i) $\left[\begin{array}{c} n \\ k \end{array}\right]_q = \left[\begin{array}{c} n \\ n-k \end{array}\right]_q,$

(ii) $\left[\begin{array}{c} n \\ 0 \end{array}\right]_q = \left[\begin{array}{c} n \\ n \end{array}\right]_q = 1,$

(iii) $\left[\begin{array}{c} n \\ k \end{array}\right]_q = \left[\begin{array}{c} n-1 \\ k-1 \end{array}\right]_q + q^k \left[\begin{array}{c} n-1 \\ k \end{array}\right]_q,$

(iv) $\left[\begin{array}{c} n \\ k \end{array}\right]_q = \left[\begin{array}{c} n-1 \\ k \end{array}\right]_q + q^{n-k} \left[\begin{array}{c} n-1 \\ k-1 \end{array}\right]_q,$

(v) $\lim_{q\to 1} \left[\begin{array}{c} n \\ k \end{array}\right]_q = \binom{n}{k}$ *(binomial coefficient).*

Now we present some properties of Generalized Gaussian Numbers in the following theorem:

Theorem 6. *Let n be a positive integer,* $R = \mathbb{Z}_{p^m}$, $(k \le n)$ *and* $(k_i \le n)$. *Then,*

(i) If $\sum_{i=1}^m k_i = n$, *then* $\left[\begin{array}{c} n \\ k_1, k_2, \ldots, k_m \end{array}\right]_R = \left[\begin{array}{c} n \\ k_m, k_{m-1}, \ldots, k_1 \end{array}\right]_R,$

(ii) $\left[\begin{array}{c} n \\ k_1, k_2, \ldots, k_m \end{array}\right]_R = \left[\begin{array}{c} n \\ n-\sum_{i=1}^m k_i, k_m, k_{m-1}, \ldots, k_2 \end{array}\right]_R,$

(iii) $\left[\begin{array}{c} n+1 \\ n-(k-1), k, \ldots, 0 \end{array}\right]_R = \left[\begin{array}{c} n \\ n-(k-1), k-1, 0, 0 \ldots, 0 \end{array}\right]_R + p^k \left[\begin{array}{c} n \\ n-k, k, 0, 0 \ldots, 0 \end{array}\right]_R,$

(iv) $(p-1)\left[\begin{array}{c} n \\ 0, 0, \ldots, k, 1 \end{array}\right]_R = (p^n - 1)\left[\begin{array}{c} n-1 \\ 0, 0, \ldots, k, 0 \end{array}\right]_R,$

(v) $\left[\begin{array}{c} n \\ n, 0, 0, \ldots, 0 \end{array}\right]_R = \left[\begin{array}{c} n \\ 0, n, 0, \ldots, 0 \end{array}\right]_R = \ldots = \left[\begin{array}{c} n \\ 0, 0, 0, \ldots, n \end{array}\right]_R = 1.$

(vi) The followings hold:

$$\textit{(vi).(1).}\quad \left[\begin{array}{c} n \\ k,0,0,\ldots,0 \end{array}\right]_R = \left[\begin{array}{c} n \\ n-k,0,0,\ldots,0 \end{array}\right]_R,$$

$$\textit{(vi).(2).}\quad \left[\begin{array}{c} n \\ 0,k,0,\ldots,0 \end{array}\right]_R = \left[\begin{array}{c} n \\ 0,n-k,0,\ldots,0 \end{array}\right]_R,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\textit{(iv).(m).}\quad \left[\begin{array}{c} n \\ 0,0,0,\ldots,k \end{array}\right]_R = \left[\begin{array}{c} n \\ 0,0,0,\ldots,n-k \end{array}\right]_R.$$

(vii) For $m=2,3,\ldots$, *we have* $\left[\begin{array}{c} n \\ 0,k_1,k_2,\ldots,k_{m-1} \end{array}\right]_{\mathbb{Z}_{p^m}} = \left[\begin{array}{c} n \\ k_1,k_2,\ldots,k_{m-1} \end{array}\right]_{\mathbb{Z}_{p^{m-1}}}.$

$$\textit{(viii)}\quad \left[\begin{array}{c} n \\ k,0,0,\ldots,0 \end{array}\right]_R = (p^k)^{n-k}\left[\begin{array}{c} n \\ 0,k,0,\ldots,0 \end{array}\right]_R = ((p^k)^{n-k})^2\left[\begin{array}{c} n \\ 0,0,k,\ldots,0 \end{array}\right]_R =$$
$$((p^k)^{n-k})^3\left[\begin{array}{c} n \\ 0,0,0,k,0,\ldots,0 \end{array}\right]_R = \cdots = ((p^k)^{n-k})^{m-1}\left[\begin{array}{c} n \\ 0,0,0,\ldots,0,k \end{array}\right]_R.$$

Proof. The proof follows by applying the definitions carefully.

The properties given above are generalizations of the given properties in [10]. Also very recently some similar studies are also done over different rings in [11]. In a similar approach to those works, there may be obtained some new and existing number sequences. Here we only give a few examples of number sequences.

Table 1: Number of linear codes over $\mathbb{Z}_4[\xi]$ for $n=2$, $n=3$ and $n=4$.

n (length)	$(k_1,\ k_2)$	Number	n (length)	$(k_1,\ k_2)$	Number
n=2	(0,1)	5	n	(0,1)	85
	(0,2)	1		(0,2)	357
	(1,0)	20		(0,3)	85
	(1,1)	5		(0,4)	31
	(2,0)	1		(1,0)	5440
n=3	(0,1)	21	n=4	(1,1)	28560
	(0,2)	21		(1,2)	7140
	(0,3)	1		(1,3)	85
	(1,0)	336		(2,0)	91392
	(1,1)	420		(2,1)	85680
	(1,2)	21		(2,2)	357
	(2,0)	336		(3,0)	5440
	(2,1)	21		(3,1)	85
	(3,0)	1		(4,0)	1

Table 1 is given as a special example of Theorem 6 for $p^m = 4$. Here, for $k_1 = 0, k_2 = 1$, for the values of n, we obtain a sequence: $5, 21, 85, 341, 1365, \ldots$. This sequence exists in OEIS [12] by reference number A002450 and it is given by the formula $\frac{4n-1}{3}$. For $k_1 = 1, k_2 = 0$, we obtain a sequence: $20, 336, 5440, \ldots$ which exists as A166984 in OEIS [12]. Moreover some new number sequences may be obtained by further examining the numbers obtained by fixing (k_1, k_2) and changing n. For instance, if we take $k_1 = 1, k_2 = 1$, then sequence: $5, 420, 28560, 1855040 \ldots$ does not exist in the literature [12].

4. Conclusion

In this paper, we have developed and proved a direct formula for the number of linear codes over the Galois Ring $\mathbb{Z}_{p^m}[\xi]$. As an application of this formula, we generalize the properties given in [10] and name them Generalized Gaussian Numbers. A new number sequence is also presented. It is believed that the properties of Generalized Gaussian Numbers can be further explored. Also some more new sequences can be obtained from these numbers.

ACKNOWLEDGEMENTS We would like to thank the referees for their remarks and suggestions. This research is supported by Yildiz Technical University Research Support Unit (2011-03-DOP01).

References

[1] G. Calugareanu. The total number of subgroups of a finite Abelian group. *Scientiae Mathematicae Japonicae*, 60:157-167, 2004.

[2] S. Delsarte. Fonctions de Möbius sur les groupes abeliens finis, *Annals of Math.* 49:600-609, 1948.

[3] P.E. Djubjuk. On the number of subgroups of a finite abelian group, *Izv. Akad. Nauk SSSR Ser. Mat.*, 12:351-378, 1948.

[4] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane and P. Sole. The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes. *IEEE Transactions on Information Theory,* 40:301-319, 1994.

[5] T. Honold and I. Landjev. Linear codes over finite chain rings, *The Electronic Journal of Combinatorics* 7, 2000.

[6] W.C. Huffman. Decompositions and extremal type II codes over Z4. *IEEE Trans. Inf. Theory* 44:800-809, 1998.

[7] M. Ozen and I. Siap. Codes over Galois rings with respect to the Rosenbloom-Tsfasman metric. *Special issue for ICMSAOŠ05 First International Conference On Modeling, Simulation and Applied Optimization, The Franklin Institute Journal,* 5:790-799, 2007.

[8] F.J. MacWilliams and N.J.A Sloane. The theory of error correcting codes. *North-Holland Pub. Co.*, 1977.

[9] B.R. McDonald, Finite rings with identity, *Pure and Applied Mathematics*. Marcel Dekker. 1974.

[10] E. Saltürk and İ. Şiap. On the number of linear codes over $\mathbb{Z}_{p^m}$, submitted.

[11] E. Saltürk and İ. Şiap. The total number of linear codes over $\mathbb{F}_q + u\mathbb{F}_q$, submitted.

[12] N.J.A. Sloane. On-line encyclopedia of integer sequences. Published electronically at `http://www.research.att.com/njas/sequences`.

[13] Z.X. Wan. Quaternary codes. *Series on Applied Mathematics,* World Scientific Publisher Co., Singapore, 1997.

[14] Y. Yeh. On prime power abelian groups. *Bull. AMS*, 54:323-327, 1948.