Acta Mathematica Academiae Paedagogicae Nyíregyháziensis
24 (2008), 221–225
www.emis.de/journals
ISSN 1786-0091

THE SPECIAL CIRCULANT MATRIX AND UNITS IN GROUP RINGS

JOE GILDEA

Abstract. We introduce a new $n \times n$ circulant matrix over $\mathbb{F}_{p^k}$. Under certain conditions, we show that this matrix generates a copy of C_{p^k-1}. We conclude with determining the element of $\mathcal{U}(\mathbb{F}_{p^k}C_n)$ that corresponds to this matrix and providing explicit generators for $\mathcal{U}(\mathbb{F}_{p^k}C_2)$ when $p \neq 2$.

1. Introduction

Let $\mathbb{F}_{p^k}$ be the Galois field of p^k elements where p is a prime. To begin we define a special $n \times n$ circulant matrix over $\mathbb{F}_{p^k}$. We show that this matrix generates a copy of C_{p^k-1} when p does not divide n.

The set of all the invertible elements of a ring S form a group called the unit group of S, denoted by $\mathcal{U}(S)$. Let RG denote the group ring G of the group G over the ring R. In [3], an explicit isomorphism between RG and a certain ring of $n \times n$ matrices is given. Using this isomorphism we determine the element of $\mathcal{U}(\mathbb{F}_{p^k}C_n)$ that correspond to the above mentioned matrix when p does not divide n.

We provide explicit generators for $\mathcal{U}(\mathbb{F}_{p^k}C_2)$ when $p \neq 2$, using the special circulant matrix and another matrix. The description of our method allows its straightforward implementation using the LAGUNA package [1] for the GAP system [4].

Definition 1. A circulant matrix over a ring R is a square $n \times n$ matrix, which takes the form

$$\operatorname{circ}(a_1, a_2, \dots, a_n) = \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_n & a_1 & a_2 & \dots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \dots & a_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & a_4 & \dots & a_1 \end{pmatrix}$$

2000 *Mathematics Subject Classification.* 15A33, 20C05, 16S34.
Key words and phrases. special circulant matrix, group ring, group algebra, unit group.

where $a_i \in R$.

For further details on circulant matrices see Davis [2].

Let R be a ring and C_n be the cyclic group of order n. There exists an isomorphism between RC_n and a certain ring of $n \times n$ matrices over R given by $\sigma : \sum_{i=0}^{n-1} a_i x^i \mapsto \mathrm{circ}(a_0, a_1, \ldots, a_{n-1})$. See [3] for further details.

2. The Special Circulant Matrix

Definition 2. Let $a \in \mathbb{F}_{p^k}$ where a generates $\mathcal{U}(\mathbb{F}_{p^k})$ and p is a prime. Define the *special circulant matrix* of order n over $\mathbb{F}_{p^k}$ by

$$\mathcal{G}_n = \mathrm{circ}(1 + (n-1)a, \underbrace{1-a, \ldots, 1-a}_{(n-1)-\text{times}}).$$

Example 3. $\mathcal{G}_2 = \mathrm{circ}(1+a, 1-a)$ and $\mathcal{G}_3 = \mathrm{circ}(1+2a, 1-a, 1-a)$.

Proposition 4. *Let* $A = \mathrm{circ}(\gamma, \underbrace{\delta, \ldots, \delta}_{(n-1)-times})$, *where* A *is a* $n \times n$ *matrix and* $\gamma, \delta \in \mathbb{F}_{p^k}$ *and* p *is a prime. Then* $|A| = (\gamma + (n-1)\delta)(\gamma - \delta)^{n-1}$.

Proof. Let $A = \mathrm{circ}(\gamma, \delta, \ldots, \delta)$, where A is a $n \times n$ matrix and $\gamma, \delta \in \mathbb{F}_{p^k}$. Then

$$\begin{aligned}
|A| &= (\gamma + (n-1)\delta) \begin{vmatrix} 1 & 1 & \ldots & 1 \\ \delta & \gamma & \ldots & \delta \\ \vdots & \vdots & \ddots & \vdots \\ \delta & \delta & \ldots & \gamma \end{vmatrix} \\
&= (\gamma + (n-1)\delta) \begin{vmatrix} 1 & 0 & \ldots & 0 \\ \delta & \gamma - \delta & \ldots & 0 \\ \delta & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \delta & 0 & \ldots & \gamma - \delta \end{vmatrix} \\
&= (\gamma + (n-1)\delta)(\gamma - \delta)^{n-1}.
\end{aligned}$$

∎

Proposition 5. *Suppose that* p *does not divide* n. *Then*

(i) $\mathcal{G}_n$ *is invertible.*
(ii) ${\mathcal{G}_n}^N = n^{N-1}\,\mathrm{circ}(1 + (n-1)a^N, \underbrace{1 - a^N, \ldots, 1 - a^N}_{(n-1)-times})$.

Proof. (i)

$$\begin{aligned}|\mathcal{G}_n| &= (1+(n-1)a+(n-1)(1-a))(1+(n-1)a-(1-a))^{n-1}\\ &= (1+na-a+n-na-1+a)(1+na-a-1+a)^{n-1}\\ &= (n)(na)^{n-1}\\ &= n^n a^{n-1}.\end{aligned}$$

Therefore $\mathcal{G}_n$ is invertible if p does not divide n.

(ii) We prove this by induction on N. Let $N=1$, clearly ${\mathcal{G}_n}^1 = \mathcal{G}_n$. Now let's assume that it holds for $N=k$. i.e.

$${\mathcal{G}_n}^k = n^{k-1}\ \mathrm{circ}(1+(n-1)a^k, \underbrace{1-a^k, \dots, 1-a^k}_{(n-1)-\text{times}}).$$

We must show that

$${\mathcal{G}_n}^{k+1} = n^k\ \mathrm{circ}(1+(n-1)a^{k+1}, \underbrace{1-a^{k+1}, \dots, 1-a^{k+1}}_{(n-1)-\text{times}}).$$

$${\mathcal{G}_n}^{k+1} = {\mathcal{G}_n}^k \times {\mathcal{G}_n}^1 =$$

$$= n^{k-1}\begin{pmatrix} 1+(n-1)a^k & 1-a^k & 1-a^k & \dots & 1-a^k\\ 1-a^k & 1+(n-1)a^k & 1-a^k & \dots & 1-a^k\\ 1-a^k & 1-a^k & 1+(n-1)a^k & \dots & 1-a^k\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 1-a^k & 1-a^k & 1-a^k & \dots & 1+(n-1)a^k\end{pmatrix}$$

$$\times\begin{pmatrix} 1+(n-1)a & 1-a & 1-a & \dots & 1-a\\ 1-a & 1+(n-1)a & 1-a & \dots & 1-a\\ 1-a & 1-a & 1+(n-1)a & \dots & 1-a\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 1-a & 1-a & 1-a & \dots & 1+(n-1)a\end{pmatrix}.$$

When we multiply these matrices every diagonal entry will be of the form

$$(\dagger)\qquad (1+(n-1)a^k)(1+(n-1)a)+(n-1)(1-a^k)(1-a)$$

and every off diagonal entry has the form

$$(\ddagger)\quad (1+(n-1)a^k)(1-a)+(1-a^k)(1+(n-1)a)+(n-2)(1-a^k)(1-a).$$

$$\begin{aligned}&(1+(n-1)a^k)(1+(n-1)a)+(n-1)(1-a^k)(1-a)\\ &\quad= 1+(n-1)a+(n-1)a^k+(n-1)^2a^{k+1}+(n-1)(1-a-a^k+a^{k+1})\\ &\quad= n+(n-1)^2a^{k+1}+(n-1)a^{k+1}\\ &\quad= n+(n^2-2n+1+n-1)a^{k+1}\\ &\quad= n+(n^2-n)a^{k+1}\\ &\quad= n(1+(n-1)a^{k+1}).\end{aligned}$$

$$\begin{aligned}
&(1+(n-1)a^k)(1-a)+(1-a^k)(1+(n-1)a)+(n-2)(1-a^k)(1-a)\\
&\quad= 1-a+(n-1)a^k-(n-1)a^{k+1}+1+(n-1)a-a^k-(n-1)a^{k+1}\\
&\qquad+(n-2)-(n-2)a-(n-2)a^k+(n-2)a^{k+1}\\
&\quad= n+(-2(n-1)+(n-2))a^{k+1}\\
&\quad= n+(-2n+2+n-2)a^{k+1}\\
&\quad= n-na^{k+1}\\
&\quad= n(1-a^{k+1}).
\end{aligned}$$

Therefore ${\mathcal{G}_n}^k \times {\mathcal{G}_n}^1 = n^k\ \mathrm{circ}(1+(n-1)a^{k+1}, \underbrace{1-a^{k+1},\dots,1-a^{k+1}}_{(n-1)-\text{times}}) = {\mathcal{G}_n}^{k+1}$.

□

Theorem 6. *For a prime p which does not divide n, $\langle \mathcal{G}_n \rangle \cong C_{p^k-1}$.*

Proof.

$$\begin{aligned}
{\mathcal{G}_n}^{p^k-1} &= n^{p^k-2}\ \mathrm{circ}(1+(n-1)a^{p^k-1}, \underbrace{1-a^{p^k-1},\dots,1-a^{p^k-1}}_{(n-1)-\text{times}})\\
&= n^{p^k-2}\ \mathrm{circ}(1+(n-1).1, 1-1,\dots,1-1)\\
&= n^{p^k-1} I_n\\
&= I_n \quad \text{since } a \text{ generates } \mathcal{U}(\mathbb{F}_{p^k}) \text{ and } n \in \mathcal{U}(\mathbb{F}_{p^k}).
\end{aligned}$$

Consider $n^{N-1}(1-a^N)$, which is an off diagonal entry of ${\mathcal{G}_n}^N$. Now $n^{N-1}(1-a^N) = 0 \iff 1-a^N = 0 \iff a^N = 1 \iff N = p^k-1$ since a generates $\mathcal{U}(\mathbb{F}_{p^k})$ and $n \in \mathcal{U}(\mathbb{F}_{p^k})$. Therefore $\langle \mathcal{G}_n \rangle \cong C_{p^k-1}$. □

Let $\mathcal{A}_n = \mathrm{diag}_n(a)$ where a generates $\mathcal{U}(\mathbb{F}_{p^k})$ and p is a prime. Clearly $\langle \mathcal{A}_n \rangle \cong C_{p^k-1}$. Also $\langle \mathcal{A}_n \rangle \cap \langle \mathcal{G}_n \rangle = I_n$ since $1-a^N = 0$ iff $N = p^k-1$.

Corollary 7. *Let $\alpha_n = (1+(n-1)a)+(1-a)\left(\sum_{i=1}^{n-1} x^i\right) \in \mathbb{F}_{p^k}C_n$ where a generates $\mathcal{U}(\mathbb{F}_{p^k})$, p is a prime and $C_n = \langle x \mid x^n = 1\rangle$. Suppose $p \nmid n$, then*

(i) $\langle \alpha_n \rangle \cong C_{p^k-1}$.
(ii) *α_2 and a generate $\mathcal{U}(\mathbb{F}_{p^k}C_2)$.*

Proof. (i) $\sigma(\alpha) = \mathcal{G}_n$.
(ii) $\sigma(a) = \mathcal{A}_2$, $\sigma(\alpha_2) = \mathcal{G}_2$ and $\langle \mathcal{A}_2, \mathcal{G}_2 \rangle \cong C_{p^k-1} \times C_{p^k-1}$. □

References

[1] V. Bovdi, A. Konovalov, R. Rossmanith, and C. Schneider. Laguna – lie algebras and units of group algebras. http://www.cs.st-andrews.ac.uk/ alexk/laguna.htm, 2007. Version 3.4.

[2] P. J. Davis. *Circulant matrices*. John Wiley & Sons, New York-Chichester-Brisbane, 1979. A Wiley-Interscience Publication, Pure and Applied Mathematics.

[3] T. Hurley. Group rings and rings of matrices. *Int. J. Pure Appl. Math.*, 31(3):319–335, 2006.
[4] The GAP Group. Gap – groups, algorithms, and programming. http://www.gap-system.org, 2007. Version 4.4.10.

Received February 28, 2008.

Department of Mathematics,
National University of Ireland,
Galway,
IRELAND
E-mail address: gildeajoe@gmail.com