# Orders of Diamond Alternating Sign Matrices 

Sean Janson<br>Supervised by: Rachel Quinlan

## Contents

1 Introduction ..... 2
2 Dodgson's Condensation Method ..... 2
3 Diamond ASM's ..... 3
4 Group Theory ..... 5
5 The Coding ..... 5
6 Results ..... 8
6.1 Initial Analysis ..... 8
6.2 Powers of 3 ..... 9
7 Analysis ..... 9
7.1 Rows and Columns ..... 10
8 Conclusions and Continuations ..... 11


#### Abstract

An Alternating Sign Matrix (ASM) of order n , is an $n \mathrm{x} n$ matrix whose entries are either $+1,0$ or -1 . The first and last non-zero entries of each row and column must be +1 , and each successive non-zero entry must alternate in sign. For instance the 7 ASM's of order 3 are:


$$
\begin{gathered}
\left(\begin{array}{lll}
1 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 1
\end{array}\right)\left(\begin{array}{lll}
1 & 0 & 0 \\
0 & 0 & 1 \\
0 & 1 & 0
\end{array}\right)\left(\begin{array}{lll}
0 & 1 & 0 \\
1 & 0 & 0 \\
0 & 0 & 1
\end{array}\right)\left(\begin{array}{ccc}
0 & 1 & 0 \\
1 & -1 & 1 \\
0 & 1 & 0
\end{array}\right) \\
\left(\begin{array}{lll}
0 & 1 & 0 \\
0 & 0 & 1 \\
1 & 0 & 0
\end{array}\right)\left(\begin{array}{lll}
0 & 0 & 1 \\
1 & 0 & 0 \\
0 & 1 & 0
\end{array}\right)\left(\begin{array}{lll}
0 & 0 & 1 \\
0 & 1 & 0 \\
1 & 0 & 0
\end{array}\right)
\end{gathered}
$$

It was first conjectured by Mills, Robbins and Rumsey, and later proven by Zeilberger [1], that the number of ASM's of order n was

$$
\frac{1!4!7!\ldots(3 n-2)!}{n!(n+1)!(n+2)!\ldots(2 n-1)!}
$$

## 1 Introduction

The aim of my internship was to familiarise myself with these ASM's, and the various surprising areas they're found. This developed into studying the more 'well-behaved' Diamond ASM's. The even-ordered versions of these diamonds have finite order, when looked at as a subgroup of $S L\left(2, \mathbb{Z}_{3}\right)$ [2]. Working over the integers modulo 3 makes sense as the elements of an ASM must be 1 of 3 possible integers. However for convention I will still write -1 instead of 2 as they are congruent to each other modulo 3 . The remainder of the research project was centered around finding these orders, before this I'd like to explore the origins of ASM's, to give context for the rest of the paper.

## 2 Dodgson's Condensation Method

ASM's first were studied by Mills et al [3] using their definition of a ' $\lambda$ determinant'. Consider a square 2-by-2 matrix:

$$
A=\left(\begin{array}{ll}
a & b \\
c & d
\end{array}\right)
$$

Then

$$
\lambda_{D e t}=a d+\lambda b c \quad \text { with } \lambda \in \mathbb{R}
$$

In order to extend this idea to matrices larger than 2-by-2, one could use

Dodgson's Condensation Method for computing determinants [4]. However Robbins and Rumsey chose a variant of this method utilising the aforementioned lambda-determinant [5]. Ultimately this boiled down to an algebraic recurrence relation:

$$
f_{i, j, k+1}=\frac{\left(f_{i+1, j, k} f_{i-1, j, k}+\lambda f_{i, j+1, k} f_{i, j-1, k}\right)}{f_{i, j, k-1}}
$$

with $(i, j)$ ranging over $\mathbb{Z}^{2}$
It was found that letting $\lambda=1$ always obtained Laurent polynomials, and that the coefficients of these polynomials actually encoded ASM's [6].

## 3 Diamond ASM's

A Diamond ASM of order n , which I will denote $D_{n}$, is the ASM of that order that contains the largest number of non-zero entries. ASM's of even order contain two diamonds, while those of odd order only have one. The diamond ASM's of order 3,4 and 5 can be seen below.

$$
\left(\begin{array}{ccc}
0 & 1 & 0 \\
1 & -1 & 1 \\
0 & 1 & 0
\end{array}\right)\left(\begin{array}{cccc}
0 & 1 & 0 & 0 \\
1 & -1 & 1 & 0 \\
0 & 1 & -1 & 1 \\
0 & 0 & 1 & 0
\end{array}\right)\left(\begin{array}{cccc}
0 & 0 & 1 & 0 \\
0 & 1 & -1 & 1 \\
1 & -1 & 1 & 0 \\
0 & 1 & 0 & 0
\end{array}\right)\left(\begin{array}{ccccc}
0 & 0 & 1 & 0 & 0 \\
0 & 1 & -1 & 1 & 0 \\
1 & -1 & 1 & -1 & 1 \\
0 & 1 & -1 & 1 & 0 \\
0 & 0 & 1 & 0 & 0
\end{array}\right)
$$

Note how both $D_{4}$ 's are just reflections of the other about the vertical axis. The reason the diamond ASM's are studied in particular is due to the evenordered diamond ASM's having full rank. In fact they're determinant is always 1 [7].
To see this consider a diamond ASM of even order n, now apply the following row operations:

1. Consider rows 1 through $\frac{n}{2}$ of the matrix. Reflect this half of the matrix about the horizontal axis. One can do this by first swapping rows 1 and $\frac{n}{2}$, then rows 2 and $\frac{n}{2}-1$, and so on (Recalling that $n$ must be even here as we are only considering diamond ASM's of even order). The sign of the determinant is changed each time two rows are swapped, so the determinant is changed $\left\lfloor\frac{n}{4}\right\rfloor$ times. This also leaves the upper half of the matrix in upper-triangular form.
2. Subtract row 2 from row $\frac{n}{2}+1$, row 3 from row $\frac{n}{2}+2$, up until reaching row $n$ (This will take $\frac{n}{2}-1$ operations).
3. Swap rows $\frac{n}{2}+1$ and $n-1$, rows $\frac{n}{2}+2$ and $n-2$, until all these outer pairs are swapped, excluding row $n$. This will once again change the sign of the determinant $\lfloor n-1 / 4\rfloor$ times, leaving all but the bottom row of the matrix in upper-triangular form.
4. Finally adding row $\frac{n}{2}+1$ to row $n$, row $\frac{n}{2}+2$ to row $n$, until after adding row $n-1$ to row $n$, the matrix will be in upper-triangular form. I will denote it $U_{n}$.

Then it's determinant is computed as follows: (The fourth row of the below matrix is the $\frac{n}{2}$ th row of the matrix in question.)

$$
(-1)^{\left(\left\lfloor\frac{n}{4}\right\rfloor\right)+\left(\left\lfloor\frac{n-1}{4}\right\rfloor\right)}\left|\begin{array}{ccccccccc}
1 & -1 & 1 & \ldots & 1 & \ldots & -1 & 1 & 0 \\
0 & 1 & -1 & \ldots & -1 & \ldots & 1 & 0 & 0 \\
0 & 0 & 1 & \ldots & 1 & \ldots & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \ldots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \ldots & 1 & \ddots & 0 & 0 & 0 \\
0 & 0 & 0 & \ldots & 0 & \ldots & -1 & 1 & 0 \\
0 & 0 & 0 & \ldots & 0 & \ldots & 0 & -1 & 1 \\
0 & 0 & 0 & \ldots & 0 & \ldots & 0 & 0 & 1
\end{array}\right|
$$

This means the determinant can only be 1 or -1 , as -1 raised to any integer power will always be 1 or -1 and because the product of the diagonals of the above matrix can only be one of the two as well.
More specifically, the left term becomes

$$
(-1)^{\left(\left\lfloor\frac{n}{4}\right\rfloor\right)+\left(\left\lfloor\frac{n-1}{4}\right\rfloor\right)}= \begin{cases}1 & \text { if }\left\lfloor\frac{n}{4}\right\rfloor+\left\lfloor\frac{n-1}{4}\right\rfloor \text { is even } \\ -1 & \text { if }\left\lfloor\frac{n}{4}\right\rfloor+\left\lfloor\frac{n-1}{4}\right\rfloor \text { is odd }\end{cases}
$$

While the right becomes

$$
\left|U_{n}\right|= \begin{cases}1 & \text { if } \frac{n}{2}-1 \text { is even } \\ -1 & \text { if } \frac{n}{2}-1 \text { is odd }\end{cases}
$$

If $\frac{n}{2}-1$ is even, then $\left\lfloor\frac{n}{4}\right\rfloor=\frac{n}{4}-\frac{1}{2}$, while $\left\lfloor\frac{n-1}{4}\right\rfloor=\frac{n-1}{4}-\frac{1}{4}$. So $\left\lfloor\frac{n}{4}\right\rfloor+\left\lfloor\frac{n-1}{4}\right\rfloor=$ $\frac{n}{2}-1$, which is even by assertion. This means if $\frac{n}{2}-1$ is even, then $\left|A_{n}\right|=1$.

Now if $\frac{n}{2}-1$ is odd, then $\left\lfloor\frac{n}{4}\right\rfloor=\frac{n}{4}$, and $\left\lfloor\frac{n-1}{4}\right\rfloor=\frac{n-1}{4}-\frac{3}{4}$. So $\left\lfloor\frac{n}{4}\right\rfloor+\left\lfloor\frac{n-1}{4}\right\rfloor=$ $\frac{n}{2}-1$, which is odd by assertion. So finally if $\frac{n}{2}-1$ is odd, then $\left|A_{n}\right|=1$, and so the determinant of an even-ordered diamond ASM must be equal to 1.

## 4 Group Theory

Since these even-ordered diamond ASM's have non-zero determinant, they are invertible, and so generates a group under multiplication modulo 3. This is a subgroup of $S L\left(n, \mathbb{Z}_{3}\right)$.
Since $S L\left(n, \mathbb{Z}_{3}\right)$ is a finite group, so too is $\left\langle D_{n}\right\rangle$ by Lagrange's Theorem [8]. The remainder of the paper will be about finding the orders of the groups generated by these $D_{n}$ 's, or $\left|\left\langle D_{n}\right\rangle\right|$.

Figure 1: 'Cayley Table for the group $\left\langle D_{4}\right\rangle$


## 5 The Coding

To begin answering this question, I sought experimental answers in MATLAB. I wrote a program that would generate $D_{n}$ for a given order n .

```
//Two inputs, n is an integer and varargin is either 1,2 or 3
function m=Diamonds(n, varargin)
    h=n / 2;
    c=ceil(n/2);
    f=floor(n/2);
    A=zeros(n);
    C=ones(1,n);
    //Creates alternating 1's and - 1's.
    C(2:2: end )=-1;
    //Checks if Diamond is even-ordered.
    if mod}(\textrm{n},2)==
    //Creates ASM, it does the top and the bottom rows at the same time
        for i=1:h
                        ind}=(2*i)-1
                        A(i,:)=[zeros(1,h-1),C(1: ind ), zeros(1,h)];
                A(n+1-i,:)=[zeros(1,h),C(1:ind),zeros(1,h-1)];
                h=h-1;
            end
            if isequal(varargin,{2})
                A=flip (A,2);
            elseif isequal(varargin,{3})
                A={A,flip (A,2) };
            end
    //For odd-ordered diamond ASM's
        else
            for i=1:c
                ind}=(2*i)-1
            A(i,:)=[zeros(1,f),C(1:ind ),zeros(1,f)];
            A(n+1-i,:)=[zeros(1,f),C(1:ind), zeros(1,f)];
                f=f -1;
            end
    end
    m=A;
end
```

Here the function takes optional input arguments to be used if the order of the diamond ASM is even. It is either 1,2 or 3 . 1 is the default and gives the leftward slanting diamond, 2 gives the rightward slanting diamond, and

3 gives them both.
I then wrote a program that takes in a Diamond ASM, and computes $\left|\left\langle D_{n}\right\rangle\right|$ using brute force. It takes a second tolerance argument, which is the maximum number of iterations allowed in the for loop.

```
function m=Order(A, tol)
s=size(A);
k=s(1);
n=2;
B=A;
    while n<tol
        B}=\textrm{B}*\textrm{A}
        B}=\operatorname{mod}(\textrm{B},3)
        B(B==2)=-1;
        if isequal(B, eye(k))
                %fprintf('Matrix has order %d',n+2)
                m=n;
                n=tol +1;
        elseif n= tol-1
            m=NaN;
            n=n+1;
        else
            n=n+1;
        end
    end
end
```

The results from this were limited, it was a shame that I could only work over the even numbers.
Despite only having half-rank, and determinant zero, knowing more about the odd-ordered diamond ASM's would still be informative. Since I'm working over a finite field, $Z_{3}$, raising odd-ordered diamond ASM's to incrementally increasing powers, would eventually form repeating periods.
If a diamond ASM of even order $D_{n}$, has order $k$, then $D_{n}^{(k+1)}=D_{n} \bmod 3$. Moreover, we know for an odd-ordered diamond ASM, say $B_{2 n-1}$, there exists a $p$ such that $B_{2 n-1}^{p}=B_{2 n-1}$. For the remainder of the paper I will let the order of $B_{2 n-1}=p-1$.

## 6 Results

This table contains orders of diamond ASM's of order 2 through 100, using my above definition for orders of odd-ordered diamond ASM's.

| $1-20$ | Order | $21-40$ | Order | $41-60$ | Order | $61-80$ | Order | $81-100$ | Order |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 1 | N/A | 21 | 78 | 41 | 80 | 61 | 242 | 81 | 81 |
| 2 | 2 | 22 | 122 | 42 | 78 | 62 | unknown | 82 | 82 |
| 3 | 3 | 23 | 177146 | 43 | unknown | 63 | 234 | 83 | unknown |
| 4 | 8 | 24 | 60 | 44 | 59048 | 64 | unknown | 84 | 168 |
| 5 | 8 | 25 | 59048 | 45 | 72 | 65 | unknown | 85 | unknown |
| 6 | 6 | 26 | 28 | 46 | 177148 | 66 | 366 | 86 | unknown |
| 7 | 26 | 27 | 27 | 47 | unknown | 67 | 177146 | 87 | 14348904 |
| 8 | 20 | 28 | 56 | 48 | 492 | 68 | unknown | 88 | unknown |
| 9 | 9 | 29 | 4782968 | 49 | unknown | 69 | 131438 | 89 | unknown |
| 10 | 10 | 30 | 30 | 50 | 59050 | 70 | unknown | 90 | 90 |
| 11 | 121 | 31 | 1103762 | 51 | 4920 | 71 | unknown | 91 | 728 |
| 12 | 24 | 32 | 13124 | 52 | 728 | 72 | 180 | 92 | unknown |
| 13 | 26 | 33 | 363 | 53 | unknown | 73 | 728 | 93 | 3581286 |
| 14 | 26 | 34 | 6562 | 54 | 54 | 74 | 19682 | 94 | unknown |
| 15 | 24 | 35 | 265720 | 55 | unknown | 75 | 177144 | 95 | unknown |
| 16 | 164 | 36 | 72 | 56 | 1460 | 76 | 39368 | 96 | unknown |
| 17 | 164 | 37 | 19682 | 57 | 29523 | 77 | unknown | 97 | unknown |
| 18 | 18 | 38 | 19682 | 58 | unknown | 78 | 84 | 98 | unknown |
| 19 | 9841 | 39 | 78 | 59 | unknown | 79 | unknown | 99 | 1089 |
| 20 | 80 | 40 | 80 | 60 | 240 | 80 | 164 | 100 | unknown |

The unknowns arise as a result of computing the order taking too long. This makes sense as these computations get more expensive the larger the order of the ASM, which would account for the unknowns being more frequent the larger the order of the ASM becomes.

### 6.1 Initial Analysis

There are a number of trends I noticed all pertaining to the number of elements in the field, 3 .

1. The order of any power of 3 is its order, $n$.
2. If $\left|\left\langle D_{n}\right\rangle\right|=k$, then $A_{3 n}=3 k$.
3. After examining the prime-ordered ASM's, I noticed all of them divided $3^{d}-1$ evenly, for various $d \in \mathbb{Z}$

### 6.2 Powers of 3

Upon further examining these powers of 3 , I noticed that one could write most of the orders I found as $\left(3^{d}+a\right)$, where $d \in \mathbb{Z}_{+}$and $a \in 1,0,-1$. However the rest of them required an extra multiplicative constant $c$, with $\frac{1}{c} \in \mathbb{Z}_{+}$to fit the pattern. For simplicity, I will write $O_{i}$ for $\mid\left\langle D_{n}\right\rangle$.
For example:

| $1-10$ | Order | $11-20$ | Order | $21-30$ | Order | $31-40$ | Order |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 1 | $3^{0}$ | 11 | $.5\left(3^{5}-1\right)$ | 21 | $3 * O_{7}$ | 41 | $3^{4}-1$ |
| 2 | $3^{1}-1$ | 12 | $3 * O_{4}$ | 22 | $.5\left(3^{5}+1\right)$ | 32 | $2\left(3^{8}+1\right)$ |
| 3 | $3^{1}$ | 14 | $3^{3}-1$ | 23 | $3^{11}-1$ | 33 | $3 * O_{11}$ |
| 4 | $2\left(3^{1}+1\right)$ | 14 | $3^{3}-1$ | 24 | $3 * O_{8}$ | 34 | $3^{8}+1$ |
| 5 | $3^{2}-1$ | 15 | $3 * O_{5}$ | 25 | $3^{10}-1$ | 35 | $.5\left(3^{12}-1\right)$ |
| 6 | $3 * O_{2}$ | 16 | $2\left(3^{4}+1\right)$ | 26 | $3^{3}+1$ | 36 | $3 * O_{12}$ |
| 7 | $3^{3}-1$ | 17 | $2\left(3^{4}+1\right)$ | 27 | $.5\left(3^{5}+1\right)$ | 37 | $3^{9}-1$ |
| 8 | $2\left(3^{2}+1\right)$ | 18 | $3 * O_{6}$ | 28 | $2\left(3^{3}+1\right)$ | 38 | $3^{9}-1$ |
| 9 | $3^{2}$ | 19 | $.5\left(3^{9}-1\right)$ | 29 | $3^{14}-1$ | 39 | $3 * O_{13}$ |
| 10 | $3^{2}+1$ | 20 | $3^{4}-1$ | 30 | $3 * O_{10}$ | 40 | $3^{4}-1$ |

I find these patterns very intriguing, and they lead me to believe that the answer to my question may lie somewhere in combinatorics, one of the areas in mathematics where ASM's have garnered most fame. I think this because each entry can only be 1 of 3 numbers. So without alternating sign or row sum constraints, the number of unique rows of length $n$ modulo 3 , would be $3^{n}$.

## 7 Analysis

My next step was to look 'under the hood' a little bit, and see what kinds of matrices arise when a diamond ASM is raised to any non-negative integer
power modulo 3. These are figures $2-4^{[2]}$. For the sake of clarity I have once again used the colour-mapping from the Cayley Tabel ${ }^{[1]}$.

Figure 2: The very left and very right most matrix is the original diamond ASM of order $3, A_{3}$. The middle two are then $A_{3}^{2}$ and $A_{3}^{3} \bmod 3$


Figure 3: This is the same again but for $A_{4}$. Notice how $A_{4}^{4}$ and $A_{4}^{8}$ are the horizontally reflected identity and identity matrix of order 4


Figure 4: This is the same again but for $A_{5}$. Notice how its pattern is more like it's odd-ordered counter part $A_{3}$


### 7.1 Rows and Columns

Usually with ASM's, the row and column sums must each be 1, due to the alternating sign condition. However for these powers of diamond ASM's, the
$D_{n}^{i}$ 's, seem to have rows and columns whose entries must be congruent to 1 modulo 3.
Moreover, many of the symmetries of the diamond ASM's are also shared by these intermediate matrices. For powers of odd-ordered diamond ASM's, they are both symmetric over the vertical. horizontal and both diagonal axes. For the powers of even-ordered diamond ASM's then, they are only symmetric over the two diagonal axes. This gives two constraints for these powers of diamond ASM's. For one, each column and row must have their entries sum to 1 modulo 3 . For two, the matrices must be symmetric over the two diagonal axes, and powers of odd-ordered diamond ASM's must also be symmetric over the vertical and horizontal axes.
Another trait possessed by the powers of even-ordered diamond ASM's, is half of the unique powers are horizontally reflected of the other half. For example in the $\mathrm{n}=4$ case, the first bottom four matrices in Figure 2, are the top ones horizontally reflected.

I decided to examine these rows and columns. My plan is to find a link between the orders, and the number of unique rows and columns seen in the intermediate matrices. For instance, in the $\mathrm{n}=3$ case, only three unique rows and columns are used. Namely: 010,1-11 and 10-1. The $n=4$ case uses 8 unique rows and columns, however for each row, that row read in reverse is also another unique row. These unique rows and columns are: 0100,0010,1-$110,01-11,-1011,110-1,1000$, and 0001.
The $\mathrm{n}=5,6$ and 7 cases can be seen in figure $5^{[5]}$.
For the $\mathrm{n}=3,4,5$ and 7 cases, the number of these unique rows and columns is exactly $O_{n}$. The exception is 6 , a power of 3 that is greater than 3 . It has 18 unique rows and columns, which is $3^{*} 6$. Many rows in the $n=5$ case have analogues in the $n=7$ case. The same is also true for the $n=4$ and $n=6$ cases. I believe computing the number of these unique rows present in $\left\langle D_{n}\right\rangle$ would lead to being able to compute $O_{n}$

## 8 Conclusions and Continuations

Unfortunately I was not able to research much more into these matrices and their fascinating properties. I do fully plan on continuing this research however. My main goal is to create a formula for each $O_{n}$, and prove it. I'd also like to explain some more of these phenomena, such as the link between
$O_{n}$ and the number of unique rows of each $\left\langle D_{n}\right\rangle$.

Figure 5: Unique rows and columns for $\mathrm{n}=5,6$ and 7 cases.
Here I've put the $\mathrm{n}=6$ case on the right, as to make it easier to compare some of the similarities in the rows of the $\mathrm{n}=5$ and 7 cases.

|  | $\mathrm{n}=7$ | $\mathrm{n}=7$ continued |  |  |
| :---: | :---: | :---: | :---: | :---: |
|  | 0110110 | 1-1-11-1-11 |  |  |
|  | 01-11-110 | -11-10-11-1 | $\mathrm{n}=6$ | $\mathrm{n}=6$ (reflected) |
| n=5 | 0001000 | -1-10-10-1-1 | 100000 | 000001 |
| 001-110 | 001-1100 | -110101-1 | 010000 | 000010 |
| 01-11-11 | 1-11-11-11 | -1-1101-1-1 | 001000 | 000100 |
| -1-1000-1 | -100000-1 | 0-1-1-1-1-10 | 01-1100 | 001-110 |
| -1000-1 | 1100011 | -1-1-11-1-1-1 | 1-11-110 | 01-11-11 |
| 10-101 | 100-1001 | 1010101 | -100011 | 11000-1 |
| -1111-1 | -101110-1 | 0-1111-10 | 10-1-10-1 | -10-1-101 |
| -111-1 | 00-10-100 | 1-1-10-1-11 | -101-10-1 | -10-110-1 |
| 0-10-10 | 10-11-101 | 010-1010 | 1110-1-1 | -1-10111 |
|  | -10-1-1-10-1 | 1-1010-11 |  |  |
|  | -111-11-1 | 11-1-1-111 |  |  |

## References

[1] Doron Zeilberger (1994) Proof of the Alternating Sign Matrix Conjecture, Temple University.
[2] Oliver King(1990) Subgroups of the Special Linear Group Containing the Diagonal Subgroup,Department of Mathematics and Statistics, The University of Newcastle upon Tyne.
[3] James Propp (2018) The many faces of alternating-sign matrices, University of Wisconsin.
[4] A.N.W Hone(2006) Dodgson condensation, alternating signs and square ice,Philosophical Transactions: Mathematical, Physical and Engineering Sciences.
[5] Greg Kuperberg(2002) Symmetry Classes of Alternating-Sign Matrices under One Roof.
[6] Ilse Fischer and Lukas Riegler(2014) Vertically symmetric alternating sign matrices and a multivariate Laurent polynomial identity.
[7] David P. Robbins and Howard Rumsey Jr. (1986) Determinants and alternating sign matrices, Institute for Defense Analyses.
[8] M.R Darafsheh(2005) Order of elements in the groups related to the general linear group, Finite Fields and their Applications.

