International Journal of Mathematics And its Applications
Volume 5, Issue 1–A (2017), 13–15.
ISSN: 2347-1557
Available Online: http://ijmaa.in/

International Journal of Mathematics And its Applications

A Note on Construction of Finite Field of Order p and p^2

Research Article

S.K.Pandey[1]*

1 Department of Mathematics, Sardar Patel University of Police, Security and Criminal Justice, Daijar, Jodhpur, Rajasthan, India.

Abstract: In this note we construct finite field of order p (here p is a positive prime) and p^2 for $p > 2$ through even square elements of Z_{2p}. It has been already noticed that a finite field of order p^2, $p > 2$ can be directly constructed without using the concept of quotient rings. We utilize the same technique to yield a finite field of order p^2 for $p > 2$ however here we use the notion of even square elements of a ring R. It is noticed that for all the finite fields constructed in this article the reducing modulo m is a composite integer.

MSC: 12E20.

Keywords: Finite field, matrix field, matrix, even square element.

1. Introduction

In the mathematical literature [4–6], the most common example of a finite field of order p is Z_p. Generally one does not find any other example in the textbooks. Though all finite fields of a given order are algebraically equivalent however it is interesting to yield various examples of a finite field of a given order. Conventionally a finite field of order p^2 is constructed by using the concept of quotient rings. However in this article we follow the approach given in [2] and we do not use the well known conventional technique to get a finite field of order p^2.

In [1] we have given a technique to yield finite matrix fields of order p for each positive prime p. [2] gives a technique to yield a finite field of order p^2 for each $p > 2$. Here we provide some other representations and we utilize the concept of even square elements and the techniques introduced in [1] and [2].

In [3] we have introduced the notion of even square elements and even square rings. It may be noted that an element a of a ring R is called an even square element if $a^2 \in 2R$ and a ring R is called an even square ring if every element of R is an even square element. For more details one may refer [3].

It may also be noted that in the case of Z_p the reducing modulo p is a prime integer however here in the case of F, F_1, F_2 and F_3 described in the next section the reducing modulo m is a composite integer. Similarly in the case of finite field of order p^2 given below the reducing modulo m is a composite integer. It is worth to note that the construction of a finite field of order p^2 described in [2] is different from the conventional technique. We follow the same approach as described in [2] but here we use the even square elements of Z_{2p}.

* E-mail: skpandey12@gmail.com

2. Finite Fields of Order p

In [1] we have given the following three representations for Z_p.

a). $M_1 = \left\{ \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} : x \in Z_p \right\}$,

b). $M_2 = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in Z_p \right\}$,

c). $M_3 = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} : a \in Z_p \right\}$.

It may be noted that M_3 works for $p > 2$. Here we consider some other representations of Z_p for $p > 2$ based on the notion of even square elements of a ring R. First of all we consider the set F consisting of all even square elements of Z_m where $m = 2p$ and $p > 2$ is a prime integer.

d). $F = \{x : x \in D\}$. Here D is the set of all even square elements of Z_m.

It is easy to verify that F gives a finite field of order p under addition and multiplication modulo m. It is noticed that if we replace Z_p by F in M_1, M_2 and M_3 then we shall obtain F_1, F_2 and F_3 respectively which are given by

e). $F_1 = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in F \right\}$,

f). $F_2 = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} : a \in F \right\}$,

g). $F_3 = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in F \right\}$.

One may easily verify that F_1, F_2 and F_3 all give a finite field of order p under addition and multiplication of matrices modulo m. Clearly the reducing modulo m is a composite integer.

Thus this article gives four distinct finite fields of order p for each $p > 2$. These four representations of Z_p are distinct from those given in [1] however all representations are algebraically same for a given prime p.

3. Finite Fields of Order p^2

In [2] we have noticed that $M = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in Z_p, p > 2 \right\}$ gives a finite field of order p^2 under addition and multiplication of matrices modulo p. Here we provide another representation of M using even square elements of Z_{2p}. Let $M' = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in F \right\}$. It is easy to see that M' gives a finite field of order p^2 under addition and multiplication of matrices modulo m. Though M and M' are algebraically equivalent however both provide two distinct representations of a finite field of order p^2 for each $p > 2$. Here the reducing modulo m is a composite number. Taking $p = 3$ we obtain a finite field of order 9 as under.

$$M'_9 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}, \begin{pmatrix} 0 & 4 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 4 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 4 \\ 2 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 4 & 2 \end{pmatrix}, \begin{pmatrix} 4 & 2 \\ 4 & 4 \end{pmatrix}, \begin{pmatrix} 4 & 4 \\ 2 & 4 \end{pmatrix} \right\}.$$

One may verify that M'_9 is a finite field of characteristic 3 under addition and multiplication of matrices modulo 6. This representation of a finite field of order 9 is obtained using M' and it is distinct from those given in [2]. Similarly if we take $F = \{0, 2, 4, 6, 8\}$ then M' shall yield a finite field of order 25 as under.

$$M'_{25} = \left\{ \begin{matrix} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}, \begin{pmatrix} 6 & 0 \\ 0 & 6 \end{pmatrix}, \begin{pmatrix} 8 & 0 \\ 0 & 8 \end{pmatrix}, \begin{pmatrix} 0 & 8 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 8 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 6 \\ 4 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 4 \\ 6 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 4 \\ 6 & 2 \end{pmatrix}, \\ \begin{pmatrix} 2 & 6 \\ 4 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 8 \\ 2 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 8 & 2 \end{pmatrix}, \begin{pmatrix} 4 & 4 \\ 6 & 4 \end{pmatrix}, \begin{pmatrix} 4 & 6 \\ 4 & 4 \end{pmatrix}, \begin{pmatrix} 4 & 8 \\ 2 & 4 \end{pmatrix}, \begin{pmatrix} 4 & 2 \\ 8 & 4 \end{pmatrix}, \begin{pmatrix} 6 & 4 \\ 6 & 6 \end{pmatrix}, \begin{pmatrix} 6 & 6 \\ 4 & 6 \end{pmatrix}, \begin{pmatrix} 6 & 8 \\ 2 & 6 \end{pmatrix}, \\ \begin{pmatrix} 6 & 2 \\ 8 & 6 \end{pmatrix}, \begin{pmatrix} 8 & 8 \\ 2 & 8 \end{pmatrix}, \begin{pmatrix} 8 & 2 \\ 8 & 8 \end{pmatrix}, \begin{pmatrix} 8 & 4 \\ 6 & 8 \end{pmatrix}, \begin{pmatrix} 8 & 6 \\ 4 & 8 \end{pmatrix} \end{matrix} \right\}$$

M'_{25} is a finite field of order 25 under addition and multiplication of matrices modulo 10. Similarly M' easily yields a finite field of order 49, 121, 169 and so on.

References

[1] S.K.Pandey, *Matrix Field of Finite and Infinite Order*, International Research Journal of Pure Algebra, 5(12)(2015), 214-216.

[2] S.K.Pandey, *Visualizing Finite Field of Order p^2 through Matrices*, Global Journal of Science Frontier Research (F), XVI(1-1)(2016).

[3] S.K.Pandey, *Nil Elements and Even Square Rings*, (communicated).

[4] I.N.Herstein, *Topics in Algebra*, Wiley-India, New Delhi, (2011).

[5] T.W.Hungerford, *Algebra*, Springer-India, New Delhi, (2005).

[6] W.J.Wickless, *A First Graduate Course in Abstract Algebra*, Marcel Dekker Inc., New York, (2004).