Irreducible Polynomial on Finite Field

Poonam[#1],Shilpa Aggrwal[#2]
[#1] *Department of Mathematics, Govt. College,Hisar .*
[#2] *Department of Mathematics, Govt. College,Hisar .*

Abstract

The aim of this paper is to study about irreducible polynomials over finite field and to find irreducible polynomials of degree 2 and 3 over the field Z_2 and Z_3.

Key Words: *Irreducible, Polynomial, Reducible, Field.*

Introduction

Irreducible polynomial plays very important role in field theory. An irreducible polynomial is a non-constant polynomial that can't factorised into the product of two non constant polynomials. A polynomial that is irreducible over any field containing coefficients is absolutely irreducible.

Notations

$Z_2 = \{0, 1\}$ is field under addition modulo 2 and multiplication modulo 2.

$Z_2 [x]$ is a polynomial ring.

$Z_3 = \{0, 1, 2\}$ is a field under addition modulo 3 and multiplication modulo 3.

$Z_3 [x]$ is polynomial ring.

Irreducible Polynomial

Let F be a field. Let $f(x) \epsilon F[x]$ be a non zero, non-constant polynomial. Then f(x) is said to be irreducible if it can not be factorised into the product of two non-constant polynomial with coefficients in F.

Theorem - Reducibility test for degree 2 and 3.

Let f be a field. If $f(x) \epsilon F[x]$ and deg f(x) = 2 or 3, then f(x) is reducible over F if and only if f(x) has a zero in field F.

Now we calculate number of irreducible polynomials of degree 2 over Z_2

$ax^2 + bx + C$ over Z_2

Clearly $a \neq 0$, so a = 1,equation becomes

$x^2 + bx + C$

Now we have two choice for c and two for b.

Case – I If C = 0 , then polynomial $x^2 + bx$ is reducible over Z_2.

Case – II If C = 1 then polynomial becomes

$x^2 + bx + 1$ Now we have two choice for b

If b = 0 , then polynomial $x^2 + 1$ is reducible over Z_2.

If b = 1, then polynomial $x^2 + x + 1$ is irreducible over Z_2.

Now we calculate number of irreducible polynomials of degree 2 over Z_3

Now $ax^2 + bx + C$ over Z_3

Clearly $a \neq 1$, so a have two choices.

Case – I If a = 1, then polynomial becomes $x^2 + bx + C$, here C have three choices.

Sub Case-(i) If C = 0, then polynomial x^2+bx is reducible over Z3.

Sub Case-(ii) If C = 1, then polynomial becomes $x^2 + bx + 1$

Now b has three choices.

If b = 0, then polynomial $x^2 + 1$ is irreducible over Z_3.

If b = 1, then polynomial $x^2 + x + 1$ is reducible over Z_3.

If b = 2, then polynomial $x^2+2x + 1$ is reducible over Z_3.

Sub Case-(iii) If C = 2, then polynomial becomes $x^2 + bx + 2$ Now b has three choices.

If b = 0, then polynomial $x^2 +bx+ 2$ is reducible Over Z_3.

If b = 1, then polynomial $x^2+x+ 2$ is irreducible over Z_3.

If b = 2, then polynomial x^2+2x+1 is irreducible over Z_3.

Case – II If a = 2, then the polynomial becomes $2x^2 + bx + C$. Now C have again three choices.

Sub Case-(i) If C = 0, then polynomial $2x^2 + bx$, is reducible over Z_3.

Sub Case-(ii) C = 1, then polynomial becomes $2x^2 + bx + 1$, here b has three choices.

If b = 0, then polynomial $2x^2 + 1$ is reducible over Z_3.

If b = 1, then polynomial $2x^2+x + 1$ is irreducible over Z_3.

If b = 2, then polynomial $2x^2 + 2x + 1$ is irreducible over Z_3.

Sub Case-(iii) C = 2, then polynomial becomes $2x^2 + bx + 2 = 0$, here b has three choices.

If b = 0, then polynomial $2x^2 + 2$ is irreducible over Z_3.

If b = 1, then polynomial $2x^2 + x + 2$ is reducible over Z_3.

If b = 2, then polynomial $2x^2 + 2x + 2$ is reducible over Z_3.

Now we calculate irreducible polynomials of degree 3 over Z_2.

Now $ax^3 + bx^2 + cx + d$ over Z_2

Clearly a≠0, so a = 1, then the polynomial becomes $x^3 + bx^2 + cn + d$. Here d have two choices.

Case – I If d = 0, then polynomial $x^3 + bx^2 + cx$, is reducible over Z_2.

Case – II If d = 1, then polynomial becomes $x^3 + bx^2 + cx + 1$ here C has two choices.

Sub Case (i) If C = 0, then polynomial becomes $x^3 + bx^2 + 1$, here b has two choices.
If b = 0, then polynomial $x^3 + 1$ is reducible over Z_2.

If b = 1, then polynomial $x^3 + x + 1$ is irreducible over Z_2.

Sub Case (ii) If C =1, then polynomial $x^3 + bx^2 + x + 1$, here b has two choices.

If b = 0, then polynomial $x^3 + x +1$ is reducible over Z_2.

If b = 1, then polynomial $x^3+ x^2 + x + 1$ is irreducible over Z_2.

Now we calculate irreducible polynomials of degree 3 over Z_3.

Now $ax^3 + bx^2 + cx + d = 0$ over Z_3

Clearly a≠0 clearly a has two choices.

Case – I If a = 1, then polynomial becomes $x^3 + bx^2 + cx + d$, here d has three choices.

Sub Case (i) If d = 0, then polynomial becomes $x^3 + bx^2 + cx$ reducible over Z_3

Sub Case (ii) If d = 1, then polynomial becomes $x^3 + bx^2+cx+1$ here C has three choices.

(A)

If C = 0, then polynomial becomes $x^3 + bx^2 + 1$, here b has three choices.

If b = 0, then polynomial $x^3 + 1$ is reducible over Z_3.

If b = 1, then polynomial $x^3 + x^2 + 1$ is reducible over Z_3.
If b = 2, then polynomial $x^3 + 2x^2 + 1$ is irreducible over Z_3

(B)

If C = 1, then polynomial becomes $x^3 + bx^2 + x + 1$, here b has three choices.
If b = 0, then polynomial x^3+x+1 is reducible over Z_3.
If b = 1, then polynomial $x^3 + x^2 + x + 1$ is reducible over Z_3.
If b = 2, then polynomial $x^3 + 2x^2 + x + 1$ is irreducible over Z_3.

(C)

If C = 2, then polynomial becomes $x^3 + bx^2 + 2x + 1$, here b has three choices.
If b = 0, then polynomial $x^3 + x^2 + 2x + 1$ is irreducible over Z_3.
If b = 1, then polynomial $x^3 + x^2 + 2x + 1$ is irreducible over Z_3.
If b = 2, then polynomial $x^3 + 2x^2 +2x + 1$ is reducible over Z_3.

Sub Case (iii) If d = 2, then polynomial
$x^3 + bx^2 + cx + 2$ here C has three choices.

(A)

If C = 0, then polynomial $x^3 + bx^2 + 2$, here b has three choices.
If b = 0, then polynomial $x^3 + 2$ is reducible over Z_3.
If b = 1, then polynomial $x^3 + x^2 + 2$ is irreducible over Z_3.
If b = 2, then polynomial $x^3 + 2x^2 + 2$ is reducible over Z_3.

(B)

If C = 1, then polynomial $x^3 + bx^2 + x + 2$, here b has three choices.
If b = 0, then polynomial $x^3 + x + 2$ is reducible over Z_3.
If b = 1, then polynomial $x^3 + x^2 + x + 2$ is irreducible over Z_3.
If b = 2, then polynomial $x^3 + 2x^2 + x + 2$ is reducible over Z_3.

(C)

If C = 2, then polynomial becomes $x^3 + bx^2 + 2x +2$ here b has three choices.
If b = 0, then polynomial $x^3 + 2x + 2$ is irreducible over Z_3.
If b = 1, then polynomial $x^3 + x^2 + 2x + 2$ is reducible over Z_3.
If b = 2, then polynomial $x^3 + 2x^2 + 2x + 2$ is irreducible over Z_3.

Case – II If a = 2, then poly. becomes $2x^3 + bx^2 + cx + d = 0$, here d has three choices.

Sub Case (i) If d = 0 , then polynomial $2x^3 + bx^2 + cx$ is reducible over Z_3

Sub Case (ii) If d = 1, then polynomial becomes $2x^3+bx^2+cx+1$ here C has three choices.

(A)

If C = 0, then polynomial becomes $2x^3 + bx^2 + 1$, here b has three choices.
If b = 0, then polynomial $2x^3 + 1$ is reducible over Z_3.
If b = 1, then polynomial $2x^3 + x^2 + 1$ is reducible over Z_3.
If b = 2, then polynomial $2x^3 + 2x^2 + 1$ is irreducible over Z_3.

(B)

If C = 1, then polynomial $2x^3 + bx^2 + x +1$, here b has three choices.
If b = 0, then polynomial $2x^3 + x + 1$ is irreducible over Z_3.
If b = 1, then polynomial $2x^3 + x^2 + x +1$ is irreducible over Z_3.
If b = 2, then polynomial $2x^3 + 2x^2 + x +1$ is reducible over Z_3

(C)

If C = 2, then polynomial $2x^3 + bx^2 + 2x +1$, here b has 3 choices.
If b = 0, then polynomial $2x^3 + 2x + 1$ is reducible over Z_3.
If b = 1, then polynomial $2x^3 + x^2 + 2x + 1$ is reducible over Z_3.
If b = 2, then polynomial $2x^3 + 2x^2 + 2x+ 1$ is irreducible over Z_3.

Sub Case (iii) If d = 2, then polynomial becomes
$2x^3 + bx^2 + cx + 2$, here C has 3 choices.

(A)

If C = 0, then polynomial becomes $2x^3 + bx^2 + 2$, here b has three choices.
If b = 0, then polynomial $2x^3 + 2$ is reducible over Z_3.
If b = 1, then polynomial $2x^3 + x^2 + 2$ is reducible over Z_3.
If b = 2, then polynomial $2x^3 + 2x^2 + 2$ is irreducible over Z_3.

(B)

If C =1,then polynomial becomes $2x^3 + bx^2 + x + 2$, here b has three choices.
If b = 0,then polynomial $2x^3 + x + 2$ is irreducible over Z_3.
If b = 1,then polynomial $2x^3 + x^2 + x + 2$ is reducible over Z_3.
If b = 2,then polynomial $2x^3+2x^2+x + 2$ is irreducible over Z_3.

(C)

If C = 2, then polynomial becomes $2x^3 + bx^2 + 2x +2$, here b has 3 choices.
If b = 0, then polynomial $2x^3 + 2x + 2$ is reducible over Z_3.
If b = 1, then polynomial $2x^3 + x^2 + 2x + 2$ is reducible over Z_3.
If b = 2, then polynomial $2x^3 + 2x^2 + 2x+ 2$ is irreducible over Z_3.

CONCLUSION

Irreducible polynomial of degree 2 over Z_2 is
$x^2 + x +1$
Irreducible polynomials of degree 2 over Z_3 are
$x^2 + 1$, $x^2 + x + 2$, $x^2 + 2x + 2$, $2x^2 + x + 1$, $2x^2 + 2x +1$
Irreducible polynomials of degree 3 over Z_2 are
$x^3 + x^2 + 1$, $x^3 + x + 1$
Irreducible polynomials of degree 3 over Z_3 are
$x^3 + 2x^2 + 1$, $x^3 + 2x^2 + x + 1$, $x^3 + 2x + 1$, $x^3 + x^2 + 1$, $x^3 + x^2 + 2$, $x^3 + x^2 + x + 2$, $x^3 + 2x + 2$, $x^3 + 2x^2 + 2x +1$, $2x^3 + 2x^2 + 1$, $2x^3 + x + 1$, $2x^3 + x^2 + x + 1$, $2x^3 + 2x^2 + 2x + 1$, $2x^3 + x^2 + 2$, $2x^3 + x + 2$, $x^3 + 2x^3\ 2x^2+ x + 2$, $x^3 + 2x^3 + x^2 + 2x + 2$,

Reference

1) "Contemporary Abstract Algebra" by Joseph A. Gallian. ISBN - 1305887859, 9781305887855
2) "A Course in Abstract Algebra" by V.K. Khanna & S.K. Bhambri, Second Edition,Vikas Publication House Pvt Limmited,1999,070698675X, 9780706986754.
3) "A first Court in Abstract Algebra" (7th Edition) by – J.B. Fraleigh. ISBN - 13:9780201763904
4) "Abstract Algebra" (3rd Edition) by David S. Dummit, Richard M.Foote,ISBN - 9780471433347
5) "Abstract Algebra" by I.N. Hersterin. ISBN-10:0471368792