Finite Fields

Temi Owoeye

March 3, 2020

Finite Fields can be considered by taking integers mod a prime number.

$F_p \rightarrow$ polynomials F_2 modulo an irreducable polynomial of degree n give the field.

Irreducible Polynomial $\rightarrow$a polynomial evenly divisible only by itself and 1

<u>GOAL</u> : Find $\mathrm{F}_4 = F_{2^2}$

We need an irreducible polynomial in $F_2[x]$ of degree 2.

<u>CLAIM</u> : $x^2 + x + 1$ is irreducible in $F_2[x]$

What smaller polynomials are there?

- x
- $x + 1$

Check that $x^2 + x + 1$ *is not divisible by either*

- $$\begin{array}{rl} & \phantom{x^2+{}}x+1 \\ x\big) & \overline{\;x^2+x+1} \\ & \underline{-x^2} \\ & \phantom{x^2+{}}x \\ & \underline{-x} \\ & \phantom{x^2+x+{}}1 \end{array}$$

- $$\begin{array}{rl} & \phantom{x^2+x+{}}x \\ x+1\big) & \overline{\;x^2+x+1} \\ & \underline{-x^2-x} \\ & \phantom{x^2+x+{}}1 \end{array}$$

Because there are remainders, $x^2 + x + 1$ is irreducible. So the polynomials (mod $x^2 + x + 1$) form a field

Addition table for $\mathbf{F}_4$

+	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

Multiplication table table for $\mathbf{F}_4$

*	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	x+1	1
x+1	0	x+1	1	x

$x^{-1} \equiv x + 1 \pmod{x^2 + x + 1}$

How do we find the inverse of polynomials without computing the whole multiplication table?

<u>**Example**</u> Compute $(x^3 + x_{-1}) \pmod{x^4 + x + 1}$

$*use Euclid's Algorithm*$

1) Compute the gcd $(x^3 + x, x^4 + x + 1)$

$$
\begin{array}{r|l}
 & \quad\quad\quad\quad x \\
\hline
x^3 + x & x^4 \quad\quad\quad + x + 1 \\
 & -x^4 - x^2 \\
\hline
 & \quad\quad -x^2 + x + 1
\end{array}
$$

remainder = x^2+x+1 **quotient = x**

$(x^4+x+1) = x(x^3+x)+(x^2+x+1)$

$(x^3+x) = (x+1)(x^2+x+1)+(x+1)$

$(x^2+x+1) = x(x+1)+1$

Now work backwards - Euclid's Algorithm

$1 = 1(x^2+x+1)+x(x+1)$

$x+1 = (x^3+x)+(x+1)(x^2+x+1)$

2) Substitute the equation

$1 = 1\ (x^2+x+1)+x((x^3+x)+(x+1)(x^2+x+1))$

3) Distribute the x

$1 = 1(x^2+x+1)\ +\ x(x^3+x)+(x^2+x)(x^2+x+1)$

Combine the terms in* $1(x^2+x+1)$ *and* $(x^2+x)(x^2+x+1)$ *and add their coefficients

$1 = x(x^3+x)+(x^2+x+1)(x^2+x+1)$

Go back to computing the inverse

$(x^3+x)^{-1} \equiv x^3+x^2 (\mathrm{mod}\ x^2+x+1)$

4) Check your solution

$(x^3+x^2)(x^3+x) = x^6+x^5+x^4+x^3\ (\mathrm{mod}\ x^4+x+1)$

$$
\begin{array}{r|rrrrrrr}
 & & & & & x^2 & +x & +1 \\
\hline
x^4+x+1 & x^6 & +x^5 & +x^4 & +x^3 & & & \\
 & -x^6 & & & -x^3 & -x^2 & & \\
\hline
 & & x^5 & +x^4 & & -x^2 & & \\
 & & -x^5 & & & -x^2 & -x & \\
\hline
 & & & x^4 & & -2x^2 & -x & \\
 & & & -x^4 & & & -x & -1 \\
\hline
 & & & & & -2x^2 & -2x & -1
\end{array}
$$