Fields and Finite Fields

If we have a collection of things we can add,subtract,multiply and divide(everything besides 0)
and the usual math rules apply
Then we call this collection a <u>Field</u>

Fields.
Real numbers$\mathbb{R}$
Complex numbers $\mathbb{C}$
Rational Numbers $\mathbb{Q}$
If p is prime integers((mod)p) form a field $\mathbb{F}_p$

Finite Field. is a field with a finite number of things in it

useful fact. For any integer n there is at most one finite field with n elements
If p is prime then $\mathbb{F}_p$ is the integers modulo p
If n is composite and $\mathbb{F}_n$ exists it is <u>not</u> the integers ((mod)n)
n=4 Integers(mod4)

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
⊛2	0	2	0	2⊛
3	0	3	2	1

not a field because 2 has no inverse

Polynomials over Finite Fields. Take polynomials with coefficients (mod(2))
0 and 1 are the only coefficients $\mathbb{F}_2[x]$

$g(x) = x^3 + x + 1 \qquad f(x) = x^4 + x$

$f(x) + g(x)$

$$\begin{array}{ccccc} & x^4 & & +x & \\ + & & x^3 & +x & +1 \\ \hline & x^4 & +x^3 & +0x & +1 \\ = & x^4 & +x^3 & & +1 \end{array}$$

$f(x) + g(x) = x^4 + x^3 + 1$

$f(x) - g(x)$

$$\begin{array}{ccccc} & x^4 & & +x & \\ - & & x^3 & +x & +1 \\ \hline & x^4 & +x^3 & +0x & +1 \\ = & x^4 & +x^3 & & +1 \end{array}$$

$f(x) - g(x) = x^4 + x^3 + 1$

Nifty fact for $\mathbb{F}_2[x]$ Addition and subtraction are the same thing!
$f(x)\cdot g(x) = (x^4+x)(x^3+x+1) = x^4(x^3+x+1)+x(x^3+x+1) = (x^7+x^5+x^4)+(x^4+x^2+x) = x^7 + x^5 + x^2 + x$
we can do division with remainder
$f(x) \div g(x)$
$(x^4 + x) \div (x^3 + x + 1) = x(x^3 + x + 1) + x^2$
$R(x^2)$

A ring is a collection of things you can add, subtract, multiply but not necessary divide
Exs: All Fields, Integers, Polynomials, Matrices

Since we can do division with remainder we can do modular arithmetic with polynomials what is:
$(x^2+1)\cdot(x+1)(\pmod x)^3+x+1)$?
$\equiv(x^3+x^2)+(x+1)(\pmod x)^3+x+1)\equiv x^3+x^2+x+1(\pmod x)^3+x+1)$
do division with remainder
$x^3+x^2+x+1\div x^3+x+1=1(x^3+x+1)+x^2 \quad R(x^2)$

note. Always reduce to get a polynomial smaller(degree) than the modulus!

A polynomial that cant be factored into smaller polynomials is called <u>irreducible</u>

Suppose g(x) is an irreducible polynomial in $\mathbb{F}_2[x]$ of degree n
Then the polynomials mod g(x) form a field with 2^n many things in it

Claim: x^2+x+1 is irreducible
smaller degree polynomials: x, 1, x+1
$x^2+x+1\div x=x+1(x)+1\ R(1)$
$x^2+x+1\div x+1=x(x+1)+1\ R(1)$
x^2+x+1 is irreducible
Possible remainders mod x^2+x+1
0, 1, x, x+1

+	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

$\cdot$	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

$\{0,1,x,x+1\}$ Form a field $\mathbb{F}_4$
x^4+x+1 is irreducible
$\mathbb{F}_16$ is the polynomials $(\pmod x)^4+x+1)$
x^2 is one such element, compute $(x^2)^{-1}$
Euclid's Algorithm
Division with remainder