AN INTRODUCTION TO FINITE FIELDS.

A Field f is a set with two operations denoted $+$ and $\cdot$ such that:

1. $\forall a, b \in F$, $a+b \in F$, $a \cdot b \in F$
2. $a+b = b+a$ $\quad ab = ba$
3. $(a+b)+c = a+(b+c)$
   $(ab)c = (ab)c$
4. $a(b+c) = ab+ac$
5. $\exists\, 0 \in F$, $1 \in F$: $\forall a \in F$
   $a+0 = a$
   $1 \cdot a = a$

6. $\forall a \in F \quad \exists (-a) \in F :$

$$a + (-a) = 0$$

$$\forall a \in F, \; a \neq 0$$

$$\exists a^{-1} \in F :$$

$$a \cdot a^{-1} = 1.$$

Theorem

$$a \cdot 0 = 0$$

$$ab = 0 \Rightarrow a = 0 \text{ or } b = 0$$

Finite Field ~~is~~ is a field with a finite number of elements (Galois fields)

Examples of fields

1. Z_3 with addition and multiplication mod 3

2. Z_6 is <u>not</u> a field mod 6

   since $2 \cdot 3 = 0 \mod 6$

T: Z_p is a field mod p iff p is prime

(p cannot be represented as $p = r \cdot s$ where $r > 1, s > 1$)

T. Finite fields with q elements exist only if. $q = p^n$ where p is a prime

This is a field of all p-ary vectors of length n

Addition is component wise addition mod p

We will define multiplication for p-ary vectors later

PRIMITIVE ELEMENTS IN FINITE FIELDS

Let $GF(q)$ is a finite field with q elements and $\alpha \in GF(q)$ $\alpha \neq 0$

Consider

$$\alpha^0 = 1 \;, \alpha^2 = \alpha \cdot \alpha \;, \alpha^3 = \alpha \cdot \alpha \cdot \alpha \ldots$$

$$\alpha^{q-2} = \underbrace{\alpha \cdot \alpha \ldots \alpha}_{q-2}$$

If $\alpha^i \neq \alpha^j$ $(i \neq j \;;\; i,j = 0,1,\ldots,q-2$

then α is primitive

Logarithms

Let $\alpha \in GF(q)$ is primitive

then $GF(q) = \{0, 1=\alpha^0, \alpha, \alpha^2, \alpha^3, \ldots \alpha^{q-2}\}$

$\alpha^{q-1} = 1$

or for any $a \in GF(q)$ $\exists i$

$a = \alpha^i$

Then $i = \log_\alpha a$

EXAMPLES

$GF(9) = GF(7)$ $\alpha = 3$ primitive

$\log_3 6 = 3$ $\log_3 2 = 2$

$\log_3 4 = 4$ etc.

$\log_3 1 = 0$ $\log_3$

$$\boxed{\log 1 = 0}$$ FOR ANY FIELD

T. Every finite field contains at least one primitive element α

Example GF(7)

1) Take $\alpha = 2$

$\alpha^0 = 1$, $\alpha = 2$, $\alpha^2 = 4$, $\alpha^3 = 1 \Rightarrow$

2 is not primitive in GF(7)

2) Take $\alpha = 3$

$\alpha^0 = 1$, $\alpha^1 = 3$, $\alpha^2 = 2$, $\alpha^3 = 6$,

$\alpha^4 = 4$, $\alpha^5 = 5 \Rightarrow$

3 is primitive in GF(7)

MULTIPLICATION BY ADDITION OF LOGARITHMS

$a, b, c \in GF(q)$

$$a\,b = c \iff \log a \oplus \log b = \log c \pmod{(q-1)}$$

Examples

$q = 7$ 1) $a = 2$, $b = 3$, $\alpha = 3$

$\log 2 = 2$ $\log 3 = 1$ $\Rightarrow \log 6 = 3$

$a\,b = 6$

2) $a = 4$, $b = 3$, $\alpha = 3$

$4 \cdot 3 = 5$ $\log 4 = 4$, $\log 3 = 1$ $\log 5 = 5$

Binomial Formula in GF(q)

① Let q is prime $a, b \in GF(q)$

Then $\boxed{(a+b)^q = a^q + b^q} \pmod q$

Proof

$$(a+b)^q = a^q + \binom{q}{1} a^{q-1} b +$$

$$\binom{q}{2} a^{q-2} b^2 + \ldots +$$

$$\binom{q}{q-1} a b^{q-1} + \binom{q}{q} b^q =$$

$$\boxed{\binom{q}{i} = \frac{q!}{i!\,(q-i)!}} \qquad \boxed{\text{Ind}} \; a^q + b^q$$

but $q! = 1 \cdot 2 \cdot 3 \cdots (q-1)\, q = 0 \pmod q$

Thus $\binom{q}{i} = 0 \pmod q$

Example: 1) $q=5$

$GF(5)=\{0,1,2,3,4\}$

$a=2$, $b=3$

$(2+3)^5 = 5^5 = 0 \pmod 5$

$2^5+3^5 = 32+243 = 275 = 0 \pmod 5$

2) $q=3$ $\quad a=b=2$

$(2+2)^3 = 4^3 = 2^6 = 64 = 1 \pmod 3$

$2^3+2^3 = 8+8 = 16 = 1 \pmod 3$

Generalisation of the Binomial Formula

let $a_1, a_2, \ldots, a_s \in GF(q)$

then

$$(a_1 + a_2 + \ldots + a_s)^q =$$

$$a_1^q + a_2^q + \ldots + a_s^q \pmod{q}$$