Introduction to Coding Theory Assignment 15

Divij Singh

14/04/19

1 Q1

As p is prime, and $gcd(a, p = 1)$, $a \bmod p \in \{1, 2...p-1\}$
This holds true for $2a, ...(p-1)a$

Let us suppose there exists an x and y where $1 \leq x < y \leq (p-1)$
Such that $xa \equiv ya(p)$
$\therefore p|a(x-y)$ which means that $p|a(x-y)$ (As $gcd(a, p) = 1$)

But the fact that $x, y < p$ and $x < y$, meaning that $0 < s - t < p$ which gives us a contradiction.

Thus, mod p gives us a bijective map between $\{a, 2a...(p-1)a\}$ and $\{1, 2...(p-1)\}$
$\therefore a^{p-1} \equiv 1 \bmod p$

2 Q2

$d = gcd(a, b)$
Let us assume that the above is false, such that $d \neq ax' + by'$
Then let $c = \min\{ax' + by' : ax' + by' > 0\} = ax + by$ for some x, y
Say $a = ci + j, 0 < j < a$
Then $ci = a - j$
$\therefore i(ax + by) = a - j$
$\therefore j \in \{ax' + by' : ax' + by' > 0\}, j < c$
But as c is the smallest positive integer, this is a contradiction.

Say $c|a$, and similarly $c|b$.
Let $a = dk, b = dl$
$c = ax + by = d(kx + jy) =$ d
But d is the gcd, and $c = ax + by$

$\therefore d = ax + by$ for integers x and y.

3 Q3

We know that F is a field.
So, the additive axioms of vector spaces hold in F, as do the multiplicative axioms.
As $K \subset F$ the multiplicative axioms hold for any $x \in K$ as well.
Thus, F is a vector space over K.