Information Theory & Error Correcting Codes

Written by HADIOUCHE Azouaou.

Disclaimer

This document contains the lectures given by Dr.Seffah.

> To separate the contents of the course to actual additions or out of context information, a black band will be added by its side like the globing this comment.

Contents

Chapter 0

Remainders

1. Congruences & $\mathbb{Z}/m\mathbb{Z}$ Arithmetic

Definition 1.1 (Congruence Of Integers / Congruence Class): *Let $a, b, m \in \mathbb{Z}$ with $m > 0$, we say that a is congruent to b modulo m and we write $a \equiv b \bmod m$ if $m \mid a - b$ which gives an equivalence relation. The class of a in the congruence relation by m is called the congruence class of a modulo m, which is $\overline{a} = a + m\mathbb{Z}$.*

Theorem 1.2: *Let $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{N}$, with $a \equiv b \bmod m$ and $c \equiv d \bmod m$ then we have the following statements are true:*

1. $a + c \equiv b + d \bmod m$.
2. $a - c \equiv b - d \bmod m$.
3. $ac \equiv bd \bmod m$.

We denote $\mathbb{Z}/m\mathbb{Z}$, the set of all congruence classes modulo m.

2. Euler Φ Function

Definition 2.3 (Φ Function): *The Euler Φ function is defined as $\Phi : \mathbb{Z} \to \mathbb{N}$, where $\Phi(n) = \#\{x \in [\![0, m-1]\!] \mid \gcd(x, m) = 1\}$.*

Proposition 2.4: *Let p be a prime number, then $\Phi(p) = p - 1$ and $\varphi(p^r) = p^r - p^{r-1} = p^r\left(1 - \frac{1}{p}\right)$.*

Theorem 2.5 (Euler): *Let m be a positive integer modulo a be an integer relatively prime to m then $a^{\Phi(m)} \equiv 1 \bmod m$.*

Theorem 2.6 (Fermat): *Let p be a prime, if the integer a is not divisible by p then $a^p \equiv a \bmod p$.*

Theorem 2.7 (Lagrange): *Let G be a finite group and H a subgroup of G, then $\# H \mid \# G$.*

2.1. Quadratic Residues

Definition 2.1.8 (Quadratic Residue): *Let p be an odd prime and a an integer not divisible by p, we say that a is a quadratic residue modulo p if there exists $x \in \mathbb{Z}$, such that $x^2 \equiv a \bmod p$.*

Theorem 2.1.9: *An integer a is a quadratic residue modulo p if and only if $\gcd(a, p) = 1$ and a has a square rest modulo p.*

Definition 2.1.10 (Legendre Symbol): *Let p be an odd prime, define the Legendre symbol as:*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if} \gcd(a,p) = 1 \text{ and } a \text{ is a quadratic residue} \bmod p \\ -1 & \text{if} \gcd(a,p) = -1 \text{ and } a \text{ is not a quadratic residue} \\ 0 & \text{if } p \text{ divides } a \end{cases}$$

Theorem 2.1.11: *Let p be an odd prime for every integer a*

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \bmod p$$

Exercise 2.1.12:

1. *Decompose into partial fractions in* $\mathbb{R}[x]$ *the rational function*

$$\frac{x}{x^4 + x^2 + 1}$$

2. *Let* K *be a commutative field, and let* $p : x^2 + \lambda x + \mu$ *be a monic polynomial of degree* 2*, show that* p *is reducible over* K *if and only if it has a root in* K.
3. *Let* $K = \mathbb{Z}/5\mathbb{Z}$ *be the field of residue classes, factor the polynomial* $(x^2 + 4)(x^2 + 3)$ *into irreducible factors over* K.
4. *Still with* $K = \mathbb{Z}/5\mathbb{Z}$*, decompose into partial fractions the rational function*

$$\frac{x - 2}{(x^2 + 4)(x^2 + 3)}$$