

**MATH 482: HOMEWORK 12**

- (1) Let  $H$  be an Hadamard matrix of order  $n = 4m$  and suppose that every entry of the first row is one. Let  $H'$  denote the matrix obtained by replacing all the  $-1$ 's with zeros. Let  $R_1, \dots, R_n$  be the rows of  $H'$ . If  $k, l \geq 2$  and  $k \neq l$ , prove that

$$R_k \cdot R_l = m$$

- (2) Let  $p$  be a prime such that  $p \equiv 3 \pmod{4}$ . Let  $S$  denote the set of non-zero squares in  $\mathbb{Z}_p$ . For any  $k \in \mathbb{Z}_p$ , define the set:

$$B_k = \{k + s \mid s \in S\}$$

Prove that, for any  $k, l \in \mathbb{Z}_p$ , we have:

$$|B_k \cap B_l| = \frac{p-3}{4}$$

Conclude that the Paley digraph of order  $p$  is 2-paradoxical if and only if  $p \geq 7$ .

Hint: Use problem (1).

- (3) Let  $G$  be the graph of order 4 and size 5. Find the eigenvalues of the adjacency matrix and Laplacian matrix of  $G$ . Then find  $h(G)$  and  $\tau(G)$ .
- (4) Alice sends Bob a coded message in the following way. She chooses a monic cubic irreducible in  $\mathbb{Z}_3[x]$  with a root  $\mu$  that generates  $\mathbb{F}_{27}^\times$ . She uses the following cipher to encrypt the message:  $A = \mu, B = \mu^2, C = \mu^3, \dots, Z = \mu^{26}$ .

Here is the message she sends:  $\mu^2 + \mu, 2\mu^2 + 2\mu + 1, 2, 2\mu^2, 2\mu^2 + 2\mu, \mu^2 + \mu, 2\mu^2 + \mu + 1, 2\mu^2 + 2\mu + 1, \mu, \mu + 1, 2\mu + 2, \mu^2 + \mu, 2\mu^2, 2\mu^2 + 2\mu, 2\mu^2 + 2\mu, 2\mu^2 + 2\mu + 2, \mu + 1, \mu^2 + \mu, 2\mu^2 + 2, \mu^2 + \mu, 2\mu + 2, \mu^2 + \mu + 1, 2\mu + 2, 2\mu, \mu^2 + 2\mu + 2, 2\mu^2 + 2\mu + 2, \mu^2 + 1, 2\mu^2 + 2\mu + 2, 2\mu^2 + 2, \mu^2 + \mu, 2\mu^2, 2\mu^2 + 2\mu, 2\mu^2 + 1, 2\mu^2 + 2\mu + 2$

Find the number of monic cubic irreducibles in  $\mathbb{Z}_3[x]$  and the degree of  $\Phi_{26}(x)$ . Show that a root  $\mu$  of a monic cubic irreducible in  $\mathbb{Z}_3[x]$  will generate  $\mathbb{F}_{27}^\times$  if and only if  $\mu^{13} = 2$ . Now decode the message.

- (5) Let  $p$  be my favorite prime number. Find all  $x \in \mathbb{Z}_p$  such that  $x^2 = -1 \pmod{p}$ . Write  $p = a^2 + b^2$  for some positive integers  $a$  and  $b$  with  $a < b$ . Find the smallest positive integer  $c$  such that  $c \pmod{a} = 2$  and  $c \pmod{b} = 9$ . Finally, find  $n$  such that  $p(n) = c$ .