

MATH 482: EXTRA CREDIT PROBLEMS

- (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 tournament of order p is 2-paradoxical if and only if $p \geq 7$.

Hint: Use problem (1).

- (3) Alice sends Bob a coded message in the following way. She uses a monic cubic irreducible in $\mathbb{Z}_3[x]$ to construct \mathbb{F}_{27}^\times . She uses the following cipher to encrypt the message: $A = x, B = x^2, C = x^3, \dots, Z = x^{26}$.

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

What is my favorite prime number?