Coding Theory: Problems 2

1. In $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$, calculate

   (a) $2^{20} + 3^{33}$ (b) $2^{20}3^{33}$ (c) $2^{20} - 3^{33}$ (d) $2^{20} \div 3^{33}$.

2. Show that every square integer is either 0 or 1 mod 4. Hence prove that $x^2 + y^2 = 1839$ has no integer solutions.

3. Construct a table of multiplicative inverses for $\mathbb{Z}_7$ and $\mathbb{Z}_{13}$.

4. Find the missing digit x in the ISBN $0679x60806$.

5. Let C be the 10-ary analogue of the ISBN code, that is,

   $$C = \{x \in \mathbb{Z}_{10}^9 \mid \sum_{i=1}^{9} ix_i = 0\}.$$

   What is the minimum distance $d(C)$ of this code? Give a counterexample which demonstrates that C cannot detect transposition errors like the ISBN code can.

6. According to Galois' Theorem, there *does* exist a field of order 4, F_4, although $\mathbb{Z}_4$ is *not* a field. Let $0, 1$ denote the additive and multiplicative identity elements in F_4, and denote the other two elements a, b. Deduce the addition and multiplication tables for F_4. What is the characteristic of F_4?

7. Does there exists a finite field of order 254? What about 256?

8. Let F be a finite field of characteristic 2. Show that every element is a square, that is, for all $a \in F$ there exists $b \in F$ such that $a = b^2 = b \times b$.

9. Let E_n be the set of all even weight vectors in F_2^n. (Recall the weight of a vector is the number of non-zero entries it has.) Show that E_n is a subspace of F_2^n. What is $\dim E_n$? What is $|E_n|$? Write down a basis for E_n.

10. Let C be a subspace of F_3^4 having $\{(0, 1, 2, 1), (1, 0, 2, 2), (1, 2, 0, 1)\}$ as a spanning set. Find a basis for C. What is $\dim C$?