Homework #2. Due Wednesday, January 29th, in class

All reading assignments and references to exercises, definitions etc. are from our main book 'Coding Theory: A First Course' by Ling and Xing

Reading:

1. For this homework assignment: 3.1, 3.2 and 4.1

2. For the classes next week: 4.2-4.6. It is very unlikely that we will cover all the material from those sections in 2 classes, but I might touch on at least one topic from each section.

Problems:

1. Problem 3.1, page 36

2. Problem 3.2, page 36

3.

(a) Use the Euclidean algorithm to find integers u and v such that $127u+35v = 1$. If you have not studied this before, see Lecture 4 of my 3354 notes.

(b) Use your answer in (a) to compute 35^{-1} in $\mathbb{Z}_{127}$. Make sure to explain your logic.

4. Problem 3.4, page 36. **Hint:** (a) can be proved directly from the standard formula for binomial coefficients and basic divisibility properties. Then use (a) to solve both (b) and (c).

5. Problem 3.5, page 36

6. Let F be a finite field, and let Q be the set of all nonzero squares in F, that is, all nonzero elements of F representable as a^2 for some $a \in F$.

(a) Assume that F has odd characteristic (for the definition of characteristic see Definition 3.1.10 on page 21). Prove that $|Q| = \frac{|F|-1}{2}$. **Hint:** Prove that for every nonzero $b \in F$ the equation $x^2 = b$ has either no solutions (for x) in F or exactly two solutions.

(b) Now assume that F has characteristic 2. Prove that $|Q| = |F| - 1$, that is, every nonzero element of F is a square. **Hint:** Since F is finite, it suffices to prove that the map $x \mapsto x^2$ from $F \setminus \{0\}$ to $F \setminus \{0\}$ is injective (one-to-one). The latter is not hard to prove directly (using the assumption $\mathrm{char}F = 2$).

For both parts you will likely need to use the fact that fields have no zero divisors (Lemma 3.1.3(ii) from the book).

7. Problem 4.2, page 66. Ignore the question about the number of bases, but make sure to prove your answer whether the given set is a subspace or not. If the set in question is a subspace, compute its dimension (also with proof).