Homework #2. Summary of common mistakes

4(a) A common mistake was to say that $\binom{p}{j} = p \cdot \frac{(p-1)!}{j!(p-j)!}$, whence $\binom{p}{j}$ is a multiple of p and therefore an integer. The problem with this argument is that it is not clear at all why $\frac{(p-1)!}{j!(p-j)!}$ is an integer.

4(b) Several solutions involved expressions like $\frac{a}{b} \equiv c \mod p$ where $a, b, c \in \mathbb{Z}$ and $\frac{a}{b}$ is not necessarily an integer. While one can make sense out of such congruences, you have to explain what you mean by that (the standard definition of congruences assumes that you have integers on both sides).

4(c) Many of you correctly figured out that in view of the binomial theorem, 4(c) is equivalent to the statement that $\binom{p^k}{j} \equiv 0 \mod p$ for any prime p and any $1 \leq j \leq p^k - 1$. You know this is true for $k = 1$ by part (a). While it is possible to establish this congruence directly for arbitrary k, it is technically much harder and is not the point of this problem. The idea of 4(c) is to first prove it for $k = 1$ (using (a)) and then do something else for $k > 1$.

6. Very few people explained how the hypothesis $charF \neq 2$ is used. Note that you clearly have to use this assumption somewhere for otherwise what you prove in (a) contradicts the assertion of (b).

7. Two comments about this problem. First, if you tried to prove that the set in question is a vector space using the definition of a vector space, please redo it, instead proving that the set is a subspace of F^n (for suitable F and n), using **the definition of a subspace** (as you will see this is both shorter and cleaner).

However, the main issue in 7 was computing the dimension. The default way to compute the dimension of a subspace in an explicit problem with numbers is to find a basis for that subspace (and take its cardinality). Many of you correctly identified a basis B, but did not prove that B is indeed a basis. To do the latter, by definition you have to show that B is both spanning and linearly independent. In practice, it is often easier to first show that B is spanning and then show that every proper subset of B is not spanning (this will imply that B is a basis since every spanning set contains a basis); of course, for the second part it suffices to consider subsets of B of cardinality $|B| - 1$.

There are many other ways to compute the dimension which may work well or not depending on how the subspace is defined. For instance, if the subspace is defined as the set of solutions to a system of linear equations, the simplest way to compute its dimension is by using the rank-nullity theorem.