Problem Set 3, Part D – Solutions

Corina Pătraşcu

Solution

(a) Using the same arguments as for part C of Problem Set 2, we get that the number of one-dimensional subspaces is $\frac{p^n-1}{p-1}$ because we group all non-zero vectors with their scalar multiples.

(b) A basis for a 2-dimensional subspace contains 2 linearly independent vectors. Reasoning similarly as in part C of Problem Set 2, we get that each of those two linearly independent vectors generates a 1-dimensional subspace. So, to obtain a 2-dim subspaces, we just take two 1-dim subspaces, get one non-zero vector from each and use those two vectors as a basis. We use the following property:

P/1 Given two 1-dim subspaces, each combination of two non-zero vectors, one from the first and the other from the second gives us the same 2-dim subspace.

Proof Each of the two 1-dim subspaces is generated by one non-zero vector, and the others are just scalar multiples of this one. So say $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ are the two generators and taken together as a basis, they give the 2-dim subspace U.

Now take two scalar multiples of these two vectors, ax and by and let W be the 2-dim subspace generated by them $\Rightarrow$ all scalar multiples of ax and by are in W. Since we are in the field Z/pZ, all elements are invertible $\Rightarrow a^{-1}$ and b^{-1} exist and are scalars in this field $\Rightarrow a^{-1}ax \in W, b^{-1}bx \in W \Rightarrow x, y \in W$, which implies that in fact, $W = V$.

So now to find 2-dim subspaces, we just choose two 1-dim subspaces so we get $\binom{\frac{p^n-1}{p-1}}{2}$ possibilities.

But we clearly overcount because a 2-dim subspace can be obtained from several different pairs of 1-dim subspaces. But these 1-dim subspaces of V are also subspaces of the 2-dim subspace that they form. So we only need to count the number of 1-dim subspaces of a given 2-dim subspaces and if we choose two of them, their direct sum will give the entire 2-dim subspace.

By part (a), we get that regarless of the subspace, the number of its 1-dim subspaces is $\frac{p^2-1}{p-1}$ (the reasoning is the same).

So now, the number of ways in which we can obtain a 2-dim subspace from two 1-dim subspaces is $\binom{\frac{p^2-1}{p-1}}{2}$.

In conclusion, the number of two dimensional subspaces is $\frac{\binom{\frac{p^n-1}{p-1}}{2}}{\binom{\frac{p^2-1}{p-1}}{2}}$.