Matematiska Institutionen
KTH

Solutions of homework number 1 to SF2736, fall 2013.

Please, deliver this homework at latest on Monday, November 18.

The homework must be delivered individually, and, in general, just handwritten notes are accepted. You are allowed to discuss the problems with your classmates, but you are not allowed to deliver a copy of the solution of another student.

1. (0.1p) The integer $x = 92$ solves the two congruences $x \equiv 12 (\text{mod } 20)$ and $x \equiv -4 (\text{mod } 24)$. Find all other solutions.

   Solution. If x' is another solution then

   $$\begin{cases} x' & = & 92 & + & 20s \\ x' & = & 92 & + & 24t \end{cases}$$

   for some integers s and t, and vice versa. From the system above we get that

   $$20s = 24t.$$

   Necessary is thus that $s = 6k$ and $t = 5k$. It is also sufficient as then

   $$x' = 92 + 120k$$

   will be a solution.

2. (0.2p) Find necessary and sufficient conditions for the integers a_1 and a_2 such that the two congruences $x \equiv a_1 (\text{mod } q_1)$ and $x \equiv a_2 (\text{mod } q_2)$ are simultaneously solvable.

   Solution. An integer x solves the first congruence if and only if

   $$x = a_1 + sq_1$$

   for some integer s. For some such integer $s = s_0$ we get that $x = a_1 + s_0 q_1$ also will solve the second congruence if and only if

   $$a_1 + s_0 q_1 = a_2 + t_0 q_2$$

   for some integer t_0, or equivalently

   $$a_2 - a_1 = s_0 q_1 - t_0 q_2.$$

   This Diophantine equation has a solution if and only if $\gcd(q_1, q_2)$ divides $a_2 - a_1$, which thus is our answer.

3. Let p be a prime number. The elements in the direct product

$$Z_p{}^n = Z_p \times Z_p \times \cdots \times Z_p,$$

can be regarded as vectors with scalars in Z_p (instead of the real numbers as scalars). Defining addition of vectors and multiplication with scalars in the traditional way, Z_p^n becomes a vector space, that we denote by $V(n, p)$. These so called finite vector spaces are important in many applications used in real world. Linear independence, subspace and dimension are concepts that can be defined in the same way as they are defined in real vector space.

(a) (0.1p) Find the number of 1-dimensional subspaces of $V(7, 2)$.

Solution. A 1-dimensional space L is spanned by one single vector $\bar{e}$ and consists of the vectors in the set

$$L = \{\lambda\bar{e} \mid \lambda \in Z_p\},$$

a set with $p - 1$ non-zero vectors. Any two distinct 1-dimensional subspaces of a vector space intersects in the zero vector, and any vector $\bar{v}$ belongs to at least one 1-dimensional subspace. Hence the number of 1-dimensional subspaces in the finite vector space $V(n, p)$ is equal to

$$\frac{p^n - 1}{p - 1}.$$

In the case under consideration, i.e., $n = 7$ and $p = 2$, the number of 1-dimensional subspaces thus is 127.

(b) (0.2p) Find the number of 2-dimensional subspaces of $V(n, p)$.

Solution. We count the number of candidates for ordered basis of a 2-dimensional subspace L. So the basis

$$\bar{e}_1 = (1, 0, 0, \ldots, 0) \qquad \bar{e}_2 = (0, 1, 0, \ldots, 0)$$

and the basis

$$\bar{f}_1 = (0, 1, 0, \ldots, 0) \qquad \bar{f}_2 = (1, 0, 0, \ldots, 0)$$

for L will be counted as two distinct ordered basis in this enumeration.

We can choose the first basis vector $\bar{v}$ in $p^n - 1$ ways as we can take any non-zero vector. The next vector $\bar{w}$ can be chosen to be any vector not belonging to the linear span of $\bar{v}$. Thus $\bar{w}$ can be chosen in $(p^n - 1) - (p - 1)$ distinct ways. So in total there are

$$(p^n - 1)(p^n - p)$$

distinct ordered selection of two linearly independent vectors in $V(n,p)$. Now the number of distinct ordered basis for any 2-dimensional subspace L, is, by reasoning as above, equal to

$$(p^2-1)(p^2-p)$$

Each ordered set of two linearly independent vectors span a unique two dimensional space. If N denotes the number of 2-dimensional spaces we thus get

$$(p^2-1)(p^2-p)N = (p^n-1)(p^n-p).$$

which simplifies to

Answer:

$$N = \frac{(p^n-1)(p^{n-1}-1)}{(p^2-1)(p-1)}.$$

(c) (0.2) Consider the space $V(4,5)$. Find the dimension of the kernel of the linear map represented by the matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 1 & 2 \\ 0 & 1 & 3 & 2 \\ 2 & 4 & 3 & 3 \end{bmatrix}$$

in the "standard" basis.

Solution. We denote the matrix above by $\mathbf{A}$. A vector $\bar{x} = (x_1, x_2, x_3, x_4)$ belongs to the kernel of the given linear map if and only if $\mathbf{A}\bar{x}^T = \bar{0}^T$. To find the kernel we thus can solve the corresponding linear system of equations, by using the traditional Gauss elimination:

$$\left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 0 \\ 0 & 2 & 1 & 2 & 0 \\ 0 & 1 & 3 & 2 & 0 \\ 2 & 4 & 3 & 3 & 0 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 0 \\ 0 & 2 & 1 & 2 & 0 \\ 0 & 1 & 3 & 2 & 0 \\ 0 & 2 & 1 & 1 & 0 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 3 & 2 & 0 \\ 0 & 2 & 1 & 1 & 0 \end{array}\right)$$

and continuing, to bring it to a row echelon form (which is not necessary at all)

$$\left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 3 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right)$$

The kernel is thus the linear span

$$\ker(A) = \operatorname{span}\{(2,2,1,0)\}.$$

So the dimension of the kernel is equal to one. (Alternatively: The elementary row operations above give that the matrix has rank 3. Thus its null-space has dimension $4-3$.)

(d) (0.2p) Find the number of 3×3-matrices $\mathbf{A}$ with elements in Z_p, such that the determinant of $\mathbf{A}$ is non-zero, (that is, p divides $\det(\mathbf{A})$).

Solution. Elementary row operations do not change the linear span of the rows of a matrix, as in the real case. We may thus conclude, as in the real case, that the determinant is non-zero if and only if the rows of the matrix are linear independent. We now count the number of ordered sets of three linear independent vectors, row no 1, row no. 2 and row no 3, in $V(3,p)$.

Row no 1 can be chosen in $p^3 - 1$ ways, just take any of the non-zero vectors, denote it by $\bar{r}_1$. Row no. 2 cannot belong to the linear span $\text{span}\{\bar{r}_1\}$, which contains $p-1$ non-zero vectors, but can be equal to any of the remaining $(p^3 - 1) - (p - 1)$ vectors. So $\bar{r}_2$ can be chosen in $p^3 - p$ distinct ways. For the third row we can just takevectors $\bar{r}_3$ such that

$$\bar{r}_3 \notin \text{span}\{\bar{r}_1, \bar{r}_2\},$$

a subspace of dimension 2, which contains $p^2 - 1$ non-zero vectors. Any such $\bar{r}_3$ will accomplish the set of rows to a set of three linearly independent vectors. Thus

Answer: $(p^3 - 1)(p^3 - p)(p^3 - p^2)$, that is,

$$p^{1+2}(p^3 - 1)(p^2 - 1)(p - 1).$$

(It is thus easy to generalize this formula. (An extra voluntary homework!)