Matematiska Institutionen
KTH

Solutions to homework number 1 to SF2736, fall 2011.

1. (0.2p) Find all solutions to the equation

$$6x + 9y = 15$$

in the ring Z_{18}.

Solution: Evidently $(x, y) = (1, 1)$ is a solution. Assume that (x', y') is another solution. Then

$$6x + 9y = 6x' + 9y' \qquad \Longleftrightarrow \qquad 6(x - x') = 9(y' - y)$$

in the ring Z_{18}. However in Z_{18} the set $\{6z \mid z \in Z_{18}\}$ is equal to the set $\{0, 6, 12\}$ and the set $\{9w \mid w \in Z_{18}\}$ is the set $\{0, 9\}$. As the intersection of these sets just consists of the element 0, we get that (x', y') is a solution if and only if $6(x - x') = 0$ and $9(y' - y) = 0$, that is,

$$x - x' \in \{3, 6, 9, 12, 15\} \qquad \text{and} \qquad y' - y \in \{0, 2, 4, 6, 8, 10, 12, 14, 16\},$$

or equivalently

$$x' \in 1 - \{3, 6, 9, 12, 15\} = \{1, 4, 7, 10, 13, 16\}$$

and

$$y' \in 1 + \{0, 2, 4, 6, 8, 10, 12, 14, 16\} = \{1, 3, 5, 7, 9, 11, 13, 15, 17\}$$

So in total there are $6 \cdot 9 = 54$ distinct solutions to the given equation.

2. (0.1p) Find all solutions to the equation

$$6x + 9y = 15$$

in the ring Z_{19}.

Solution: As $6 \cdot 3 = -1$ we get that $6 \cdot (-3) = 1$ and hence 6 has the invers $-3 = 16$ in the ring Z_{19}. The given equation is thus equivalent to the equation

$$x = (-3) \cdot (-4) - (-3) \cdot 9y,$$

that can be simplified to

$$x = 12 + 8y.$$

To each element y in Z_{19} we can find an element $x \in Z_{19}$ so that the pair (x, y) satisfies the equation above, namely

Answer: $(x, y) \in \{(12 + 8t, t) \in Z_{19} \times Z_{19} \mid t \in Z_{19}\}$.

3. (0.2) Find the number of solutions to an equation

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b \ ,$$

in a ring Z_p, where p is a prime number.

Solution: In case all elements a_1, a_2, ..., a_n are equal to zero and $b \neq 0$ then there is no solution, and in case $b = 0$ any n-tuple of values $(a_1, a_2, \ldots, a_n)$ will give a solution. In the latter case the number of solutions is equal to p^n.

If one of the elements a_i is non zero, than it has an inverse $c = a_i^{-1}$ and we get the equivalent equation

$$x_i = c \cdot b - \sum_{k \neq i} ca_kx_k$$

For every possible choice of value to each of the variables x_k, for $k \neq i$, we can find a value to x_i that satisfies the equation above. Hence

Answer: p^{n-1} possible solutions in case some a_i is non zero. For the other cases see above.

4. (0.2p) Give, and discuss, i.e., and sketch a proof of a more general result from which your answer to the previous problem follows.

Solution: We consider the theory for systems of linear equations

$$\mathbf{A}\bar{x} = \bar{b},$$

where $\mathbf{A}$ is a $n \times m$-matrix and $\bar{x}$ and $\bar{b}$ are column vectors.

Linear independence can be defined similarly in Z_p^n as in the real vector space R^n. Furthermore, any theorem in the theory for vector spaces that can be proven by just using ordinary calculations, addition, subtraction, multiplication and dividing with the non zero elements from Z_p can be proven to be true also in Z_p^n. So we can define the rank, rank($\mathbf{A}$), of the $n \times m$-matrix $\mathbf{A}$, the null space, $N(\mathbf{A})$, of a matrix, as well as we can prove the dimension theorem

$$\text{rank}(\mathbf{A}) + \text{dim}(\mathbf{N}(\mathbf{A})) = \mathbf{m}.$$

Thus, also from linear algebra, if $\bar{b}$ is in the column space of $\mathbf{A}$, then we get a solution with $m - \text{rank}(\mathbf{A})$ parameters. Each of these parameters can be chosen arbitrarily in p distinct ways. Hence

Answer: The number of solutions to the linear system $\mathbf{A}\bar{x} = \bar{b}$ is zero if $\bar{b}$ is not in the column space of $\mathbf{A}$. Else the number of solutions is

$$p^{m - \text{rank}(\mathbf{A})}$$

(where m is the number of indeterminates).

5. (0.2p) Let p be a prime number. The set of all n-tuples $\bar{x} = (x_1, x_2, \dots, x_n)$, where $x_i \in Z_p$, can be regarded as a vector space, denoted Z_p^n, with the elements $\bar{x}$ as vectors and the elements of Z_p as scalars. You do not need to verify this. However, explain why the following dotproduct

$$\bar{x} \cdot \bar{y} = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n$$

is not suitable for defining length of vectors, as it is done in real vector spaces.

Solution: Just the zero vector should have length 0. In Z_2^2 the vector $(1,1)$ gives with the definition above the dot product with itself

$$(1,1) \cdot (1,1) = 1 \cdot 1 + 1 \cdot 1 = 0,$$

so the normal way to define length, i.e.

$$||\bar{u}|| = \sqrt{\bar{u} \cdot \bar{u}}$$

is not good here.

6. (0.1p) Consider the vector space Z_p^n and the dotproduct defined as in the previous problem. To every subspace U of Z_p^n define $U^\perp$ to be the following set

$$U^\perp = \{\bar{y} \in Z_p^n \ \mid \ \bar{y} \cdot \bar{x} = 0 \text{ for all } \bar{x} \in U\} \ .$$

Find and describe an example, i.e., find p, n and U, such that

$$U = U^\perp \ .$$

Solution: Take $p = 2$, $n = 2$ and $U = \{(0,0), (1,1)\}$, that is, a 1-dimensional subspace of Z_2^2 with basis $(1,1)$. By the dimension theorem discussed above, the solution space to

$$1 \cdot x + 1 \cdot y = 0$$

has dimension $2 - 1 = 1$. As easily verified the solution space is $U^\perp$ and is equal to U.