Solution for HW2, part B
Geoff Anderson
granders@fas.harvard.edu

Problem 5(a) *Let p be a fixed prime number, and let $V = (\mathbb{Z}/p\mathbb{Z})^n$. How many vectors are there in V?*

Solution:

V is the collection of ordered $n-$tuples $(v_1, \ldots, v_n)$, where each $v_i \in \mathbb{Z}/p\mathbb{Z}$. Each v_i $(i = 1 \ldots n)$ can take any of p possible values, so there are a total of p^n vectors in V. $\square$

We can look at a more general situation without too much trouble. Let A and B be finite sets with n_A and n_B elements, respectively. Then the cartesian product $A \times B = \{(a, b) | a \in A, b \in B\}$ has a total of $n_A \cdot n_B$ elements. That is, the *cardinality* of $A \times B$ is $n_A \cdot n_B$. Suppose now that $S_1, \ldots, S_n$ are finite sets of cardinality $m_1, \ldots, m_n$, respectively. We can use the above observation to give an inductive proof of the fact that the set

$$\Pi_{i=1}^n S_i = S_1 \times S_2 \times \ldots S_n = \{(s_1, \ldots, s_n) | s_i \in S_i \text{ for } i = 1 \ldots n\}$$

has a total of $m_1 \cdot m_2 \cdot \ldots \cdot m_n$ elements. Problem 5(a) is a special case of this, where $S_1 = \ldots = S_n = \mathbb{Z}/p\mathbb{Z}$.

Problem 5(b)

In the case of $n = 2$ and arbitrary $p > 2$, show that $(1, 1)$ and $(1, 2)$ span V.

Solution

We must show that given $(a, b) \in (\mathbb{Z}/p\mathbb{Z})^2 = V$, there exist some $s, t \in \mathbb{Z}/p\mathbb{Z}$ such that $(a, b) = s(1, 1) + t(1, 2)$. You can check $s = 2a - b$ and $t = b - a$ do the trick. $\square$

To reach this solution, note that we must have

$a = s + t$ and

$b = s + 2t$. Solve for s and t as you would with any system of two equations in two unkowns.

Some of you gave a different proof, which read something like: the dimension of V is 2. $(1, 1)$ and $(1, 2)$ are linearly independent (insert proof of linear independence), and hence must span the space. While this is correct, it relies on the notion of dimension and theorems which we had not yet proven in class, so I took off a few points. In general, don't use a result not proven in class without supplying the proof yourself.

Problem 5(c)

In the same case as in 5(b), show $(1, 4), (2, 6), (3, 3)$ are linearly dependent.

Solution

We must write $\overrightarrow{0}$ as a nontrivial linear combination of the three vectors.

$$(1, 4) + (2, 6) - (3, 3) = (0, 0) \square$$

Note that we're working modulo 7, which can make our life easy if we let it. E.g. $5 = -2$, so $5/2 = -1$ and $4 = -3$, so $4/3 = -1$. Also, division by a multiple of 7 is meaningless, because a multiple of 7 is 0 modulo 7, and 0 has no multiplicative inverse.