If you don't understand anything about any of the solutions here, or if you spot mistakes, feel free to e-mail me at `zeyliger@fas.harvard.edu`. Homework problems have a tendency to creep up on exams, so be sure you know how to do all the assigned homework.

Almost everyone didn't do problem 7 correctly.

6

We wish to find the inverse of the linear map $L : (\mathbb{Z}/7\mathbb{Z})^3 \to (\mathbb{Z}/7\mathbb{Z})^3$ given by $L(x, y, z) = (x + y + z, 2x + 3y + 4z, 3x + 4y + 6z)$.

It is notationally convenient to use matrices for this linear map and find its inverse by row reduction. Curtis describes this method in the reading. Note that it is equivalent to writing down the required linear system.

I'm using notation that I hope will suggest why this method works. At every step of the way, I am multiplying both sides (on the left) by an invertible 3×3 matrix representing one elementary row operation. It is worthwhile to work out the matrices that I'm using once or twice in your life.

We're working in $\mathbb{Z}/7\mathbb{Z}$, but, as we know, it doesn't matter which equivalence class representatives we use; I chose nice representatives at the end.

$$\begin{pmatrix} 1 & 1 & 1 \\ 2 & 3 & 4 \\ 3 & 4 & 6 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 2 & 3 & 4 \\ 3 & 4 & 6 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 3 & 4 & 6 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 1 & 3 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ -3 & 0 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & -2 \\ -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 & -3 & 2 \\ 0 & 3 & -2 \\ -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2 & -2 & 1 \\ 0 & 3 & -2 \\ -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} 2 & 5 & 1 \\ 0 & 3 & 5 \\ 6 & 6 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}.$$

We conclude that L^{-1} is the map defined by $L(x, y, z) = (2x + 5y + z, 3y + 5z, 6x + 6y + z)$.

7

Claim: $L : F^2 \to F^2$, where $L(x, y) = (ax + by, cx + dy)$ is invertible if and only if $ad - bc \neq 0$.

Proof: ($\Leftarrow$) Consider the linear map $M : F^2 \to F^2$ defined by $M(x, y) = (dx - by, -cx + ay)$. Then,

$$\begin{aligned} M \circ L(x, y) &= (d(ax + by) - b(cx + dy), c(dx - by) + d(-cx + ay)) \\ &= ((ad - bc)x, (ad - bc)y). \end{aligned}$$

Since, $ad-bc \neq 0$, we can define $M : F^2 \to F^2$ by $N(x, y) = (\frac{1}{ad-bc}x, \frac{1}{ad-bc}y)$ Then $(N \circ M) \circ L(x, y) = (x, y)$, which implies that $N \circ M$ is L^{-1}.

Notes: (1) A super complete answer would check that $N \circ M$ is a linear map. At this point, we should be able to recognize that it is. (2) People often skip the composition symbol and just write $NM = N \circ M$. That's because linear operators can be represented by matrices, and the matrix form of a composition of linear operators is the product of their matrix forms. (3) I found M by inspection, or by doing the row reduction. By coming up with a map that works, I didn't have to split anything up into cases ($a \neq 0$, etc.). I took off points if you divided by, for example, d without splitting into cases.

($\Rightarrow$) We prove the contrapositive: if $ad - bc = 0$, then L is not invertible. It is sufficient to show that L is not bijective. If $cd = 0$, then $L(x, y) = (ax + by, 0)$, so L is not surjective. Suppose that $cd \neq 0$. $L(d, -c) = (ad - bc, cd - dc) = (0, 0)$. $L(-d, c) = (-ad + bc, -cd + dc) = (0, 0)$. Since $(d, -c) \neq (-d, c)$, L is not injective.

Alternate Proof: We showed in class that L is invertable if and only if $\ker(L) = \{0\}$. Suppose $(x, y) \in \ker(L)$. Therefore, $ax + by = 0 = cx + dy$. Now,

$$\begin{aligned} ax &= -by \\ cx &= -dy \\ acx = -ady &= -bcy \\ 0 &= (ad - bc)y \\ bcx &= -bdy = adx \\ 0 &= (ad - bc)x. \end{aligned}$$

This implies that $x = y = 0$. If $ad-bc \neq 0$, then the kernel is trivial and L must be invertible. If $ad-bc = 0$, then the kernel is non-trivial (see above for specific elements of the kernel), so L is not invertible.

Grading Notes: *I haven't actually graded these, so this is subject to change.*

1. (-1 point, usually) You cannot divide by any of the variables because any one of them might be zero.
2. (-4 points) If you've found L^{-1} for the case when $ad-bc \neq 0$, you cannot just claim that L^{-1} does not exist when $ad - bc = 0$ because it is not well-defined. Your first calculation depended on $ad - bc \neq 0$, so you can't apply it to the other case. You have not shown the non-existance of an inverse.
3. (-4 points) It is true that multiplicative inverse are unique, but this does not imply that the inverse doesn't exist when $ad - bc = 0$.
4. (-x points) You should be wary of claiming your steps are reversible. This claim is often false and even more often confuses your argument.