Math 417 Problem Set 2

Starred (*) problems are due Friday, September 7.

(*) 9. Use the Euclidean algorithm to find the inverses of the elements 2, 5, and 7 in the group $G = (\mathbb{Z}_{141}^*, \cdot, 1)$.

We want to find, for $a = 2, 5, 7$, the element(s) $b \in \mathbb{Z}_{141}$ with $ab \equiv_{141} 1$, i.e., $ab = 1 + 141k$ for some k. So we want to solve $ab - 141k = 1$ for b (and k). We can use the Euclidean algorithm to do this:

$141 = 70 \cdot 2 + 1$, so $1 = 141 \cdot 1 + (-70) \cdot 2$, so $1 \equiv_{141} (-70) \cdot 2 \equiv_{141} 71 \cdot 2$. So $2^{-1} = 71$ in $\mathbb{Z}_{141}^*$.

$141 = 28 \cdot 5 + 1$, so $1 = 141 \cdot 1 + (-28) \cdot 5$, and so $5^{-1} = -28 = 113$ in $\mathbb{Z}_{141}^*$.

$141 = 20 \cdot 7 + 1$, so $1 = 141 \cdot 1 + (-20) \cdot 7$, and so $7^{-1} = -20 = 121$ in $\mathbb{Z}_{141}^*$.

OK, those went a lot faster than your instructor had intended.....

(*) 10. Find the inverse of the element $\begin{pmatrix} 2 & 6 \\ 3 & 5 \end{pmatrix}$ in $GL(2, \mathbb{Z}_7)$ and in $GL(2, \mathbb{Z}_{11})$.

[The answers are different!]

We can either use the (determinant) formula for the inverse of a 2-by-2 matrix, or use superaugmented forms and row reduction. Using the determinant,

$$\begin{pmatrix} 2 & 6 \\ 3 & 5 \end{pmatrix}^{-1} = (2{\cdot}5{-}6{\cdot}3)^{-1} \begin{pmatrix} 5 & -6 \\ -3 & 2 \end{pmatrix} = (-8)^{-1} \begin{pmatrix} 5 & -6 \\ -3 & 2 \end{pmatrix} = (-1)^{-1} \begin{pmatrix} 5 & -6 \\ -3 & 2 \end{pmatrix} = (-1) \begin{pmatrix} 5 & -6 \\ -3 & 2 \end{pmatrix} = \begin{pmatrix} -5 & 6 \\ 3 & -2 \end{pmatrix} = \begin{pmatrix} 2 & 6 \\ 3 & 5 \end{pmatrix}$$

in $GL(2, \mathbb{Z}_7)$. On the other hand,

$$\begin{pmatrix} 2 & 6 \\ 3 & 5 \end{pmatrix}^{-1} = (2{\cdot}5{-}6{\cdot}3)^{-1} \begin{pmatrix} 5 & -6 \\ -3 & 2 \end{pmatrix} = (-8)^{-1} \begin{pmatrix} 5 & -6 \\ -3 & 2 \end{pmatrix} = (3)^{-1} \begin{pmatrix} 5 & -6 \\ -3 & 2 \end{pmatrix} = 4 \begin{pmatrix} 5 & -6 \\ -3 & 2 \end{pmatrix} = \begin{pmatrix} 20 & -24 \\ -12 & 8 \end{pmatrix} = \begin{pmatrix} 9 & 9 \\ 10 & 8 \end{pmatrix}$$

in $GL(2, \mathbb{Z}_{11})$, since $3^{-1} = 4$ in $\mathbb{Z}_{11}^*$.

Using row reduction, for the second one (you should try the first one for practice!), working over $\mathbb{Z}_{11}$, this looks like

$$\left(\begin{array}{cc|cc} 2 & 6 & 1 & 0 \\ 3 & 5 & 0 & 1 \end{array}\right) \to \left(\begin{array}{cc|cc} 2 & 6 & 1 & 0 \\ 1 & -1 & -1 & 1 \end{array}\right) \to \left(\begin{array}{cc|cc} 1 & -1 & -1 & 1 \\ 2 & 6 & 1 & 0 \end{array}\right) \to \left(\begin{array}{cc|cc} 1 & -1 & -1 & 1 \\ 0 & 8 & 3 & -2 \end{array}\right) \to \left(\begin{array}{cc|cc} 1 & -1 & -1 & 1 \\ 0 & 56 & 21 & -14 \end{array}\right) \to \left(\begin{array}{cc|cc} 1 & -1 & -1 & 1 \\ 0 & 1 & 10 & 8 \end{array}\right) \to \left(\begin{array}{cc|cc} 1 & 0 & 9 & 9 \\ 0 & 1 & 10 & 8 \end{array}\right),$$

and so $\begin{pmatrix} 2 & 6 \\ 3 & 5 \end{pmatrix}^{-1} = \begin{pmatrix} 9 & 9 \\ 10 & 8 \end{pmatrix}$ in $GL(2, \mathbb{Z}_{11})$.

(*) 12. (Gallian, p.57, #34) Prove that if G is a group and $a, b \in G$ then $(ab)^2 = a^2b^2$ if and only if $ab = ba$.

By definition, $(ab)^2 = (ab)(ab) = abab$ and $a^2b^2 = (aa)(bb) = aabb$. If the two are equal, $abab = aabb$, then multiplying by a^{-1} on the left yields

$bab = (a^{-1}a)bab = a^{-1}(abab) = a^{-1}(aabb) = (a^{-1}a)abb = abb.$

Then multiplying by b^{-1} on the right yields

$ba = ba(bb^{-1}) = (bab)b^{-1} = (abb)b^{-1} = (ab)(bb^{-1}) = ab,$

and so $ba = ab$, as desired. On the other hand, if we know that $ba = ab$, then

$aba = a(ba) = a(ab) = aab$, and so

$(ab)^2 = abab = (aba)b = (aab)b = (aa)(bb) = a^2b^2.$

A selection of further solutions

11. (Gallian, p.57, #42) Suppose that $F_1 = M(\theta)$ and $F_2 = M(\psi)$ (in Gallian's/our notation) are reflections in lines through the origin of slope θ and ψ, with $\theta \neq \psi$, and $F_1 \circ F_2 = F_2 \circ F_1$. Show that then $F_1 \circ F_2 = R(\pi)$ is rotation by angle π.

[Your results from Problem #1 might help!]

From Problem #1 we know that $F_1 \circ F_2 = F(\theta) \circ F(\psi) = R(2\theta - 2\psi)$, and (so) $F_2 \circ F_1 = F(\psi) \circ F(\theta) = R(2\psi - 2\theta)$. If these two rotations are equal, then their rotation angles must be equal, up to a multiple of 2π. (That is, their difference is a multiple of 2π.) If we interpret the question as saying that θ and ψ are between 0 and 2π and unequal, then $0 < |(2\theta - 2\psi) - (2\psi - 2\theta)| < 4\pi$, so $|(2\theta - 2\psi) - (2\psi - 2\theta)| = |4(\theta - \psi)| = 2\pi$, and $2\theta - 2\psi = \pm\pi$. So $F_1 \circ F_2 = R(\pm\pi)$ is rotation by π (which is equal to rotation by $-\pi$).