MATH 210A

Name: Quin Darcy
Instructor: Dr. Shannon

Due Date: 9/4/19
Assignment: Homework 1

1. Assume that $(a, b) = g$ and that $d \mid a$ and $d \mid b$. Prove that $d \mid g$.

   Proof. Since d divides both a and b, then there exists $k_1, k_2 \in \mathbb{Z}$ such that $a = k_1 d$ and $b = k_2 d$. Additionally, since g is the greatest common factor of a and b, then there exists integers x and y such that $g = ax + by$, by result (b) on handout 1. Thus, substituting in our values from earlier we obtain

   $$\begin{aligned} g &= ax + by \\ &= (k_1 d)x + (k_2 d)y \\ &= (k_1 x + k_2 y)d. \end{aligned}$$

   Hence, there exists an integer $k = k_1 x + k_2 y$ such that $g = kd$. Therefore, $d \mid g$. □

2.

   (a) Prove that if $(a, c) = 1$ and $(b, c) = 1$, then $(ab, c) = 1$.

   Proof. By result (b) on handout 1, our two assumptions imply the existence of $x, y, w, z \in \mathbb{Z}$ such that $ax + cy = 1$ and $bw + cz = 1$. Multiplying both of these together we obtain

   $$\begin{aligned} (ax + cy)(bw + cz) &= (ab)xw + (ac)xz + (bc)yw + (c^2)yz \\ &= (ab)xw + (c)\big((a)xz + (b)yw + (c)yz\big) \\ &= 1. \end{aligned} \tag{1}$$

   Since the integers are closed under multiplication, we may write (1) as $(ab)m + (c)n = 1$, where $m, n \in \mathbb{Z}$. Thus, by (b) of handout 1, it follows that $(ab, c) = 1$. □

   (b) Assume that $(a, n) = 1$. Prove that there exists $x \in \mathbb{Z}$ such that $ax \equiv 1 (\text{mod } n)$ and $(x, n) = 1$.

   Proof. Since $(a, n) = 1$, then there exists $x, y \in \mathbb{Z}$ such that $ax + ny = 1$. Subtracting ax from both sides, we obtain $ny = 1 - ax$. Thus, $n \mid (1 - ax)$. Hence, $ax \equiv 1 (\text{mod } n)$. Additionally, since $a, y \in \mathbb{Z}$, then the equation $ax + ny = 1$ also implies that $(x, n) = 1$. □

(c) Let $\mathbb{Z}_{(n)} = \{[k] \in \mathbb{Z}_n \colon (k, n) = 1\}$. Prove that $(\mathbb{Z}_{(n)}, \odot)$ is a group, and find $\left|\mathbb{Z}_{(n)}\right|$.

Proof. Let $[a], [b] \in \mathbb{Z}_{(n)}$. Then it follows that $(a, n) = 1$ and $(b, n) = 1$. We want to show that $[a] \odot [b] \in \mathbb{Z}_{(n)}$. Thus, we need to show that $[ab] \in \mathbb{Z}_n$ such that $(ab, n) = 1$. Since the integers are closed under multiplication, we have that $[a] \odot [b] = [ab] \in \mathbb{Z}_n$. Next, we can use the result from part (a) of question 2 to confirm that $(ab, n) = 1$ since $(a, n) = 1$ and $(b, n) = 1$ by assumption. Thus, for all $[a], [b] \in \mathbb{Z}_{(n)}$, we have that $[a] \odot [b] \in \mathbb{Z}_{(n)}$. Thus, $\odot$ is an operation, i.e., $\odot \colon \mathbb{Z}_{(n)} \times \mathbb{Z}_{(n)} \to \mathbb{Z}_{(n)}$.

Next, we need to show that $\odot$ is an associative operation on $\mathbb{Z}_{(n)}$. This fact follows from multiplication being associative on $\mathbb{Z}$.

Now we need to show that there exists a unique identity with respect to $\odot$. Consider the element $[1] \in \mathbb{Z}_n$. We have that $(1, n) = 1$ which means that $[1] \in \mathbb{Z}_{(n)}$. Next, let $[a] \in \mathbb{Z}_{(n)}$. Then $[a] \odot [1] = [a \cdot 1] = [a]$. Similarly, since multiplication is commutative in $\mathbb{Z}$, it follows that $[a] \odot [1] = [1] \odot [a]$.

Finally, we must show that for each $[a] \in \mathbb{Z}_{(n)}$, there exists $[a]^{-1} \in \mathbb{Z}_{(n)}$ such that $[a] \odot [a]^{-1} = [1]$. By part (b) of question 2, since for each $[a] \in \mathbb{Z}_{(n)}$, we have that $(a, n) = 1$, then there exists some $x \in \mathbb{Z}$ such that $ax \equiv 1 (\text{mod } n)$. Thus, for all $[a]$, there is some $x \in \mathbb{Z}$ such that $[a] \odot [x] = [1]$. Therefore, $(\mathbb{Z}_{(n)}, \odot)$ is a group.

To determine the $\left|\mathbb{Z}_{(n)}\right|$ note that for each $[a] \in \mathbb{Z}_{(n)}$, $(a, n) = 1$ which means a and n are relatively prime. Thus, the order of this group should be equal to the number of integers $k \leq n$ which are relatively prime to n. Hence, $\left|\mathbb{Z}_{(n)}\right| = \varphi(n)$. □

3.

(a) Assume that $(c, n) = 1$. Prove that if $ca \equiv cb (\text{mod } n)$, then $a \equiv b (\text{mod } n)$.

Proof. Since $ca \equiv cb (\text{mod } n)$, then $n \mid (cb - ca)$. Thus, $n \mid c(b - a)$. Additionally, we have that $(c, n) = 1$ and so by Euclid's lemma, it follows that $n \mid (b - a)$. Therefore, $a \equiv b (\text{mod } n)$. □

(b) Assume that $c_1, c_2, \ldots, c_{\varphi(n)}$ is a RRS mod n, and that $(a, n) = 1$. Prove that $ac_1, ac_2, \ldots, ac_{\varphi(n)}$ is a RRS mod n.

Proof. Let ac_i be in the collection $ac_1, \ldots, ac_{\varphi(n)}$. We know that $(c_i, n) = 1$ and $(a, n) = 1$ both by assumption. Then by part (c) of question 3., it follows that $(ac_i, n) = 1$ for all i. Now let ac_i and ac_j be in the collection $ac_1, \ldots, ac_{\varphi(n)}$. Assume for contradiction that $ac_i \equiv ac_j (\text{mod } n)$. Then $n \mid a(c_j - c_i)$. Since $(a, n) = 1$, then by Euclid's lemma, it follows that $n \mid (c_j - c_i)$. Thus, $c_i \equiv c_j (\text{mod } n)$ which is a contradiction. Thus, for all i and j where $i \neq j$, we have that $ac_i \not\equiv ac_j (\text{mod } n)$. Therefore, $ac_1, \ldots, ac_{\varphi(n)}$ is a RRS mod n. □

$\circ$	μ_1	μ_2	μ_3	μ_4	μ_5	μ_6	μ_7	μ_8	μ_9	μ_{10}
μ_1	μ_1	μ_2	μ_3	μ_4	μ_5	μ_6	μ_7	μ_8	μ_9	μ_{10}
μ_2	μ_2	μ_3	μ_4	μ_5	μ_1	μ_9	μ_{10}	μ_6	μ_7	μ_8
μ_3	μ_3	μ_4	μ_5	μ_1	μ_2	μ_7	μ_8	μ_9	μ_{10}	μ_6
μ_4	μ_4	μ_5	μ_1	μ_2	μ_3	μ_{10}	μ_6	μ_7	μ_8	μ_9
μ_5	μ_5	μ_1	μ_2	μ_3	μ_4	μ_8	μ_9	μ_{10}	μ_6	μ_7
μ_6	μ_6	μ_8	μ_{10}	μ_7	μ_9	μ_1	μ_4	μ_2	μ_5	μ_3
μ_7	μ_7	μ_9	μ_6	μ_8	μ_{10}	μ_3	μ_1	μ_4	μ_2	μ_5
μ_8	μ_8	μ_{10}	μ_7	μ_9	μ_6	μ_5	μ_3	μ_1	μ_4	μ_2
μ_9	μ_9	μ_6	μ_8	μ_{10}	μ_7	μ_2	μ_5	μ_3	μ_1	μ_4
μ_{10}	μ_{10}	μ_7	μ_9	μ_6	μ_8	μ_4	μ_2	μ_5	μ_3	μ_1

4.

$$\begin{array}{llll}
\mu_1 = (a) & \mu_6 = (ac)(de) & (\mu_1)^{-1} = \mu_1 & (\mu_6)^{-1} = \mu_6 \\
\mu_2 = (abcde) & \mu_7 = (ae)(bd) & (\mu_2)^{-1} = \mu_5 & (\mu_7)^{-1} = \mu_7 \\
\mu_3 = (abcde)^2 & \mu_8 = (ab)(ce) & (\mu_3)^{-1} = \mu_4 & (\mu_8)^{-1} = \mu_8 \\
\mu_4 = (abcde)^3 & \mu_9 = (ad)(bc) & (\mu_4)^{-1} = \mu_3 & (\mu_9)^{-1} = \mu_9 \\
\mu_5 = (abcde)^4 & \mu_{10} = (be)(cd) & (\mu_5)^{-1} = \mu_2 & (\mu_{10})^{-1} = \mu_{10}
\end{array}$$

Consider the two rotations μ_2 and μ_3 and the two flips μ_6 and μ_8. Composing μ_2 and μ_6 we obtain

$$\mu_2 \circ \mu_6 = \mu_9.$$

Composing μ_6 with $(\mu_2)^{-1}$ we obtain

$$\mu_6 \circ (\mu_2)^{-1} = \mu_6 \circ \mu_5 = \mu_9.$$

Thus, $\mu_2 \circ \mu_6 = \mu_6 \circ (\mu_2)^{-1}$. Similarly, for elements μ_3 and μ_8, we find that

$$\mu_3 \circ \mu_8 = \mu_9 = \mu_8 \circ \mu_4 = \mu_8 \circ (\mu_3)^{-1}.$$

5. Assume that $(G, \star)$ is a finite group, and that $|G| = n$. Prove that if $g \in G$, then $o(g)$ is finite, and that if $g^t = e$, then $o(g) \mid t$.

Proof. Let G be a finite group with order n. Take $g \in G$ and assume $o(g)$ is not finite. Then there does not exist $k \in \mathbb{Z}$ with $k > 0$ such that $g^k = e$. Now let $k_1, k_2 \in \mathbb{Z}$ where $k_1, k_2 > 0$ and $k_1 \neq k_2$. Assume $g^{k_1} = g^{k_2}$. Then $g^{k_2 - k_1} = e$. Since $k_2 - k_1 \in \mathbb{Z}$, and $o(g) \leq k_2 - k_1$, then $o(g)$ is finite. Since this is a contradiction, then it is the case that for all $k_1, k_2 \in \mathbb{Z}$ where $k_1, k_2 > 0$ and $k_1 \neq k_2$, then $g^{k_1} \neq g^{k_2}$. Thus, there exists a one-to-one and onto correspondence between $\langle g \rangle$ and $\mathbb{Z}$. However, since $\langle g \rangle \subseteq G$ and $|G| = n$, then we a contradiction and $o(g)$ must be finite.

Let $t \in \mathbb{Z}$ such that $g^t = e$. Then $g^t = g^{o(g)}$ which implies $g^{t - o(g)} = e$. We now have that either $t = o(g)$, in which case $o(g) \mid t$, or $t \neq o(g)$. If $t \neq o(g)$, then either $o(g) \nmid t$ or $o(g) \mid t$. If $o(g) \nmid t$, then by the division algorithm, there exists $q, r \in \mathbb{Z}$ with $0 < o(g)$, such that $t = q(o(g)) + r$. Thus,

$$\begin{aligned} g^t &= g^{q(o(g))+r} \\ &= g^{q(o(g))} \star g^r \\ &= \left(g^{o(g)}\right)^q \star g^r \\ &= e^q \star g^r \\ &= g^r. \end{aligned}$$

However, since $g^t = e$ and $g^r = g^t$, then $g^r = e$. This is a contradiction since $r < o(g)$. Therefore, $o(g) \mid t$. □

6. Assume $(G, \star)$ is a group, $|G| = 2n$. Prove that there exists $a \in G$, $a \neq e$, such that $a^2 = e$.

Proof. Let $(G, \star)$ be a group with $|G| = 2n$. Assume for contradiction that for all $a \in G$, if $a \neq e$, then $a^2 \neq e$. Denote $G = \{e, a_1, a_2, \ldots, a_{2n-1}\}$. Now take the subset H of G containing all the elements not equal to the identity. Since G is a group, each element of G must have a unique inverse. Thus, for every $a \in H$, it must be the case that $a^{-1} \in H$. Consider the element $a_1 \in H$. By assumption, it follows that $a_1^{-1} \neq a_1$. Without loss of generality, let $a_1^{-1} = a_2$. Similarly, let $a_2^{-1} = a_3$. Continuing in this fashion, we let $a_i^{-1} = a_{i+1}$, for all $1 \leq i < 2n - 1$. Thus, for the element a_{2n-1} it follows that $a_{2n-1}^{-1} = a_1$ is the only choice left. However, since $a_1^{-1} = a_2$ and $a_1 = a_{2n-1}^{-1}$, then $a_{2n-1} = a_1^{-1}$ and $a_1 = a_2^{-1}$, but $a_2^{-1} = a_3$. Thus, $a_1 = a_3$ which implies $|G| < 2n$ which is a contradiction. Therefore, there must exist some $a \in G$ such that $a \neq e$ and $a^2 = e$. □

7. Assume that $(G, \star)$ is a group. Prove in each of the three cases: $o(G) = 3$, $o(G) = 4$, and $o(G) = 5$.

Proof. Let $G = \{e, a_1, a_2\}$. Suppose we let $a_1^2 = e$. Then if $a_2 \star a_1 = e$ this would mean a_2 is the inverse of a_1 which cannot be the case since $a_1^2 = e$. Thus, if we let $a_2 \star a_1$ equal to either a_1 or a_2, then that would imply the other is equal to the identity which cannot be the case. Thus, $a_1^2 \neq e$. Moreover, we see that $a_1^2 \neq a_1$ since this would also imply that $a_1 = e$. Thus, $a_1^2 = a_2$. This forces $a_2^2 = a_1$. Lastly, using the fact that each row and column of a Cayley table must contain one of each element means that $a_1 \star a_2 = e = a_2 \star a_1$. Therefore, if $o(G) = 3$, G is abelian.

Considering the case where $o(G) = 4$, and letting $G = \{e, a_1, a_2, a_3\}$ then we can ask what $a_1 \star a_2$ must equal. It cannot equal either a_1 or a_2 since this would imply the other is the identity. Thus, we have that $a_1 \star a_2 = e$ or $a_1 \star a_2 = a_3$. If $a_1 \star a_2 = e$, then considering what $a_2 \star a_1$ must equal, we can choose either e or a_3. If we choose a_3, then using the fact that each column of the Cayley table must contain one of each element, this means that $a_3 \star a_1 = e$ and $a_1^2 = a_2$. On the other hand, if we had let $a_2 \star a_1 = e$. Did not have enough time to finish this problem. My apologies! $\square$