Chris Hayduk
Math B4900
Homework 1
9/11/2020

1. Recall that $\mathbb{Z}/n\mathbb{Z} = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z}\}$ is the set of congruence classes modulo n. Define $(\mathbb{Z}/n\mathbb{Z})^\times$ to be the subset of $\mathbb{Z}/n\mathbb{Z}$ that have multiplicative inverses, i.e.

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \text{ there is some } \bar{c} \in \mathbb{Z}/n\mathbb{Z} \text{ such that } \bar{c}\bar{a} = 1 \}.$$

   (a) Compute $(\mathbb{Z}/n\mathbb{Z})^\times$ for $n = 1, 2, 3, 4, 5$, and 6.

   Answer. **Case 1** $(\mathbb{Z}/1\mathbb{Z})$: note that every integer is divisible by 1. This is true because, for any integer $x \in \mathbb{Z}$, we have that $x = 1 \cdot x$. Hence, every integer belongs to $\overline{0}$ when $n = 1$.

   By the definition of modular multiplication on p. 9 of the text, if we have $\overline{a}, \overline{b} \in (\mathbb{Z}/1\mathbb{Z})$, we can take $\overline{a} \cdot \overline{b} = \overline{ab}$.

   Since we just showed that every integer in $(\mathbb{Z}/1\mathbb{Z})$ belongs to the congruence class $\overline{0}$, we have $\overline{0} \cdot \overline{0} = \overline{0 \cdot 0} = \overline{0}$ $\forall\ z \in \mathbb{Z}$.

   Hence, there are no elements $\overline{a} \in \mathbb{Z}/1\mathbb{Z}$ such that $\exists \overline{c} \in \mathbb{Z}/1\mathbb{Z}$ with the property that $\overline{ca} = 1$.

   Thus, $(\mathbb{Z}/n\mathbb{Z})^\times = \varnothing$

   Case 2 $(\mathbb{Z}/2\mathbb{Z})$: note that there are two congruence classes, $\overline{0}$ and $\overline{1}$.

   We have $\overline{0} \cdot \overline{0} = \overline{0} \cdot \overline{1} = \overline{1} \cdot \overline{0} = \overline{0}$.

   However, we have $\overline{1} \cdot \overline{1} = \overline{1}$. Hence, for $\overline{1} \in (\mathbb{Z}/2\mathbb{Z})$, $\exists \overline{c} \in (\mathbb{Z}/2\mathbb{Z})$ such that $\overline{c} \cdot \overline{1} = \overline{1}$. In this case, $\overline{c} = \overline{1}$.

   Hence, $(\mathbb{Z}/2\mathbb{Z})^\times = \{\overline{1}\}$

   Case 3 $(\mathbb{Z}/3\mathbb{Z})$: note that there are three congruence classes, $\overline{0}$, $\overline{1}$, $\overline{2}$.

   We know that $\overline{0} \cdot \overline{c} = \overline{0}$ $\forall\ \overline{c} \in (\mathbb{Z}/3\mathbb{Z})$, so we don't need to consider it.

   For the other two congruence classes, we have $\overline{1} \cdot \overline{1} = \overline{1}$, $\overline{1} \cdot \overline{2} = \overline{2} = \overline{2} \cdot \overline{1}$, and $\overline{2} \cdot \overline{2} = \overline{4} = \overline{1}$.

   So we have that $(\mathbb{Z}/3\mathbb{Z})^\times = \{\overline{1}, \overline{2}\}$

Case 4 ($\mathbb{Z}/4\mathbb{Z}$): note that there are four congruence classes, $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$.

From here I will assume the commutativity of multiplication of congruence classes and as such will only show one direction.

Once again, we do not need to consider $\overline{0}$ since multiplying it by any other congruence class yields $\overline{0}$.

We have,

$$\begin{aligned}
\overline{1} \cdot \overline{1} &= \overline{1} \\
\overline{1} \cdot \overline{2} &= \overline{2} \\
\overline{2} \cdot \overline{2} &= \overline{4} = \overline{0} \\
\overline{1} \cdot \overline{3} &= \overline{3} \\
\overline{2} \cdot \overline{3} &= \overline{6} = \overline{2} \\
\overline{3} \cdot \overline{3} &= \overline{9} = \overline{1}
\end{aligned}$$

So we have that $(\mathbb{Z}/4\mathbb{Z})^\times = \{\overline{1}, \overline{3}\}$

Case 5 ($\mathbb{Z}/5\mathbb{Z}$): note that there are five congruence classes, $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$.

We have,

$$\begin{aligned}
\overline{1} \cdot \overline{1} &= \overline{1} \\
\overline{1} \cdot \overline{2} &= \overline{2} \\
\overline{1} \cdot \overline{3} &= \overline{3} \\
\overline{1} \cdot \overline{4} &= \overline{4} \\
\overline{2} \cdot \overline{2} &= \overline{4} \\
\overline{2} \cdot \overline{3} &= \overline{6} = \overline{1} \\
\overline{2} \cdot \overline{4} &= \overline{8} = \overline{3} \\
\overline{3} \cdot \overline{3} &= \overline{9} = \overline{4} \\
\overline{3} \cdot \overline{4} &= \overline{12} = \overline{2} \\
\overline{4} \cdot \overline{4} &= \overline{16} = \overline{1}
\end{aligned}$$

So we have that $(\mathbb{Z}/5\mathbb{Z})^\times = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$

Case 6 $(\mathbb{Z}/6\mathbb{Z})$: note that there are six congruence classes, $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{5}$.

We have,

$$\begin{aligned}
\overline{1}\cdot\overline{1} &= \overline{1}\\
\overline{1}\cdot\overline{2} &= \overline{2}\\
\overline{1}\cdot\overline{3} &= \overline{3}\\
\overline{1}\cdot\overline{4} &= \overline{4}\\
\overline{1}\cdot\overline{5} &= \overline{5}\\
\overline{2}\cdot\overline{2} &= \overline{4}\\
\overline{2}\cdot\overline{3} &= \overline{6} = \overline{0}\\
\overline{2}\cdot\overline{4} &= \overline{8} = \overline{2}\\
\overline{2}\cdot\overline{5} &= \overline{10} = \overline{4}\\
\overline{3}\cdot\overline{3} &= \overline{9} = \overline{3}\\
\overline{3}\cdot\overline{4} &= \overline{12} = \overline{0}\\
\overline{3}\cdot\overline{5} &= \overline{15} = \overline{3}\\
\overline{4}\cdot\overline{4} &= \overline{16} = \overline{4}\\
\overline{4}\cdot\overline{5} &= \overline{20} = \overline{2}
\end{aligned}$$

So we have that $(\mathbb{Z}/6\mathbb{Z})^\times = \{\overline{1}\}$

. . . . . .

(b) Prove that if $\bar{a}, \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$, then $\bar{a}\cdot\bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. Suppose $\bar{a}, \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Then $\exists \overline{c_1}, \overline{c_2} \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that

$$\begin{aligned}
\bar{a}\cdot\overline{c_1} &= \overline{1}\\
\bar{b}\cdot\overline{c_2} &= \overline{1}
\end{aligned}$$

Thus we have that,

$$\begin{aligned}
\overline{ab}\cdot\overline{c_1c_2} &= \overline{(a\cdot b)\cdot(c_1\cdot c_2)} \qquad (1)\\
&= \overline{a\cdot c_1\cdot b\cdot c_2}\\
&= (\bar{a}\cdot\overline{c_1})\cdot(\bar{b}\cdot\overline{c_2})\\
&= \overline{1}\cdot\overline{1}\\
&= \overline{1}
\end{aligned}$$

The first three equalities come from the properties of modular multiplication described on p. 9 in the text.

Since multiplication in $(\mathbb{Z}/n\mathbb{Z})^\times$ is well-defined and both $\overline{c_1}, \overline{c_2} \in (\mathbb{Z}/n\mathbb{Z})^\times$, we have that $\overline{c_3} = \overline{c_1 c_2} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Similarly, $\overline{ab} \in (\mathbb{Z}/n\mathbb{Z})^\times$

Hence by (1) and the above statements, we have that $\bar{a} \cdot \bar{b} = \overline{ab} \in (\mathbb{Z}/n\mathbb{Z})^\times$. □

(c) Let $a \in \mathbb{Z}$. Show that if $(a, n) \neq 1$, then there is some $1 \leqslant b \leqslant n-1$ for which $n \mid ab$. Conclude that if $(a, n) \neq 1$, there is some $1 \leqslant b \leqslant n-1$ for which $\bar{a} \cdot \bar{b} = \bar{0}$.

Proof. Let $a \in \mathbb{Z}$ and suppose $(a, n) \neq 1$. Since the gcd is a positive integer, we know that $(a, n) > 1$.

Hence, $\exists d \in \mathbb{Z}$ such that $d > 1$, $d|a$, and $d|n$.

Let $b = n/d$ and $c = a/d$. We know that $d|n$ and $d|a$, so $b, c \in \mathbb{Z}$.

Then we have,

$$\begin{aligned} ab &= a \cdot \frac{n}{d} \\ &= \frac{a}{d} \cdot n \\ &= cn \end{aligned} \tag{2}$$

Thus, we clearly have that $n|ab$.

We know that $d > 1$ and also that $n \geqslant 1$. Hence, it is clear that $b \geqslant 1$.

Now suppose that $b \geqslant n$. Since $d > 1$, it is clear that,

$$bd > n$$

However, we defined $b = n/d$. Hence, the above statement is a contradiction and thus $b < n$.

We already established that $b \geqslant 1$, so we have $1 \leqslant b < n$, or equivalently since $b, n \in \mathbb{Z}$, $1 \leqslant b \leqslant n-1$.

Now note that $\overline{0} = \{0 + kn | k \in \mathbb{Z}\}$. We have from (2) that $ab = cn$.

Since $c \in \mathbb{Z}$, cn satisfies the condition defined for the set $\bar{0}$ and so $cn = ab \in \bar{0}$.

Hence, we have

$$\overline{ab} = \bar{0} = \bar{a} \cdot \bar{b}$$

□

(d) Let $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$. Show that if there is some non-zero $\bar{b} \in \mathbb{Z}/n\mathbb{Z}$ such that $\bar{a} \cdot \bar{b} = \bar{0}$, then $\bar{a} \notin (\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. Let $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ and suppose there is some non-zero $\bar{b} \in \mathbb{Z}/n\mathbb{Z}$ such that $\bar{a} \cdot \bar{b} = \bar{0}$.

We have that,

$$\bar{a} \cdot \bar{b} = \bar{0} \implies ab = 0 + kn$$

for some $k \in \mathbb{Z}$

Now assume $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Then there exists $\bar{c} \in \mathbb{Z}/n\mathbb{Z}$ such that $\bar{a} \cdot \bar{c} = \bar{1}$. That is,

$$ac = 1 + mn$$

for some $m \in \mathbb{Z}$. □

(e) Prove that if a and n are relatively prime then there is an integer c such that $ac \equiv_n 1$. [Hint: use the fact that the g.c.d. of two integers is a $\mathbb{Z}$-linear combination of the integers]

(f) Conclude from the previous exercises that $(\mathbb{Z}/n\mathbb{Z})^\times$ is the set of elements $\bar{a}$ of $\mathbb{Z}/n\mathbb{Z}$ with $(a, n) = 1$ and hence prove Proposition 0.3.4. Verify this directly in the case $n = 6$.

2. Determine (prove positive, or give a reason why not) which of the following sets are groups under addition:

(a) the set of polynomials $\mathbb{Z}[x]$;

Tip: Start with "Yes, this is a group. First..." or "No, this is not a group. For example...". You do not have to prove that addition is associative—you may take that for granted.

(b) the set of rational numbers (including $0 = 0/1$) in lowest terms whose denominators are even;

(c) the set of rational numbers of absolute value < 1;

3. Let $x, y \in G$. Prove that $xy = yx$ if and only if $y^{-1}xy = x$ if and only if $x^{-1}y^{-1}xy = 1$.

4. Let G be a group and let $x \in G$.

(a) If $g \in G$, show $|g^{-1}xg| = |x|$.

(b) Prove that if $|x| \leqslant 2$ for all $x \in G$ then G is abelian.

(c) If $|x| = n < \infty$, prove that the elements $e, x, x^2, \ldots, x^{n-1}$ are all distinct. Deduce that $|x| \leqslant |G|$.

5. **The dihedral group.** The dihedral group D_{2n} has the usual presentation

$$D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle.$$

LaTeX Tip: There is a difference between the symbols < (meaning less than) and ⟨ (meaning left angle bracket). As you can see above, I made a shortcut to use of \< in place of \langle: ⟨ (and similar for \> in place of \rangle: ⟩.

(a) Compute the order of each of the elements in D_8.

(b) Use the generators and relations above to show that if x is any element of D_{2n} which is not a power of r, then

$$rx = xr^{-1} \qquad \text{and} \qquad |x| = 2.$$

(c) Show that if $s_1 = s$ and $s_2 = sr$, then those together with the relations

$$s_1^2 = s_2^2 = (s_1 s_2)^n = 1$$

forms and alternative presentation of D_{2n} (you have to show that $S = \{s_1, s_2\}$ generates the whole group and that you can derive these relations from the old ones and vice versa).

6. **The symmetric group.**

(a) Let

$$\alpha = (1\ 2\ 3\ 4\ 5\ 6\ 7), \quad \beta = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12), \quad \text{and} \quad \gamma = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8).$$

(i) Compute α^2, β^2, and γ^2.

(ii) For which i between 1 and 7 is α^i still a 7-cycle? ... between 1 and 12 is β^i still a 12-cycle? ... between 1 and 8 is γ^i still an 8-cycle?

(iii) What's the theorem in general?

If σ is an m-cycle, then σ^i is also an m-cycle if and only if ...

(Just state, don't prove it.)

(b) Prove that if σ is the m-cycle $(a_1\ a_2\ \ldots\ a_m)$, then for all $i = 1, \ldots, m$,

$$\sigma^i(a_k) = a_{\overline{k+i}} \qquad \text{where } \overline{k+i} \text{ is the least residue mod } m.$$

Deduce that $|\sigma| = m$.

(c) Use the last part to prove that the order of an element in S_n equals the least common multiple of the lengths of the cycles in its cycle decomposition (*cycle decomposition* means writing it as the product of disjoint cycles; you may assume such a decomposition exists, and that disjoint cycles commute).
[You may use previous problems in your solution.]

(d) Which values appear as orders of elements of S_5 (for which i is there some element of S_5 that has order i)? For each value, give an example of an element that has that order.

LaTeX Tip: If you need to write several lines of equations, and want the equalities to line up, you can use the align environment (see code to see how this is done):

$$\begin{aligned} f(b_1) &= (-1,1,2) = -b_1 + 2b_2, && \text{and} \\ f(b_2) &= (-1,0,-1) = b_1 + b_2 - 2b_3, && \text{so that} \\ f(b_1) + f(b_2) &= (-1,1,2) + (-1,0,-1) = (-2,1,1) \\ &= (-b_1 + 2b_2) + (b_1 + b_2 - 2b_3) \\ &= -b_2 - 2b_3. \end{aligned}$$

Here, the two backslashes mark breaks the line (\\), the first ampersand in each line (&) is where the first column (right justified) ends and the second column (left justified) begins, and the optional second & in a line moves to the third (right justified) column. Since align is a math environment, it will interpret any letters as math symbols. If I want to write text instead of math symbols (like "and" and "so that"), I surround it by a \text{} command. Again, feel free to copy and past the

above code for your purposes, and replace the math with whatever you need to write. Finally, note the use of my punctuation, even in the system of equations!

Tip: Feel free to delete all these "Tips" in your homework submission. :)