MATH 1530 Problem Set 2

Collaborated with Esmé and Kazuya

February 2023

Problem 1. Prove that the set $\{5, 15, 25, 35\}$ is a group under multiplication mod 40.

Proof. Consider the *Cayley Table* of this set:

	5	15	25	35
5	25	35	5	15
15	35	25	15	5
25	5	15	25	35
35	15	5	35	25

Closure: As can be seen in the table, $a, b \in \{5, 15, 25, 35\}$ implies $ab \bmod 40 \in \{5, 15, 25, 35\}$.

Identity: $(25 \cdot a) \bmod 40 = (a \cdot 25) \bmod 40 = a$ for all $a \in \{5, 15, 25, 35\}$. Therefore, 25 is the identity of this group.

Inverse: Let $a \in \{5, 15, 25, 35\}$. There exists some $b \in \{5, 15, 25, 35\}$ such that $ab \bmod 40 = ba \bmod 40 = 25$.

Associativity: We will first prove the following lemma.

Lemma 1. *Multiplication modulo $n \in \mathbb{Z}$ is associative over the integers.*

Proof. Let $a, b, c, n \in \mathbb{Z}$.

$$\begin{aligned}
(ab \bmod n)c \bmod n &= (ab \bmod n \cdot c \bmod n) \bmod n && \text{(definition of mod)} \\
&= (ab \cdot c) \bmod n && \text{(definition of mod)} \\
&= (a \cdot bc) \bmod n && \text{(associativity)} \\
&= (a \bmod n \cdot bc \bmod n) \bmod n && \text{(definition of mod)} \\
&= a(bc \bmod n) \bmod n && \text{(definition of mod)}
\end{aligned}$$

$\square$

Associativity follows immediately from lemma 1. $\square$

Problem 2. For any integer $n > 2$, prove that there are at least two elements of $U(n)$ that satisfy $x^2 = 1$.

Proof. For all integers $n > 2$, we have that $1, (n-1) \in U(n)$ since the linear combinations $1(1) + n(0)$ and $n(1) + (n-1)(-1)$ both equal 1.

Now, we will prove that both satisfy $x^2 \bmod n = 1$.

$$\begin{aligned}
(n-1)^2 \bmod n &= (n^2 - 2n + 1) \bmod n && \text{(distributive property)}\\
&= (n(n-2) + 1) \bmod n && \text{(polynomial division)}\\
&= 1 && \text{(definition of mod)}
\end{aligned}$$

$$1^2 \bmod n = 1 \qquad \text{(definition of mod)}$$

□

Problem 3. Prove that the set $\{1, 2, \ldots, n-1\}$ is a group under multiplication mod n if and only if n is prime.

Proof. Let $S = \{1, 2, \ldots, n-1\}$.

$\Rightarrow$ Assume S is a group under multiplication modulo n. Suppose n is not prime. Then, there exists some $b, q \in S$ such that $bq = n$. Thus, $bq \bmod n = 0 \notin S$. We have reached a contradiction, since S being a group implies that it is closed. Thus, n must be prime.

$\Leftarrow$ Assume n is prime. We will prove that S is a group under multiplication modulo n.

Closure: Let $a, b \in S$. By definition, $0 \leq ab \bmod n < n$. Additionally, $ab \bmod n \neq 0$ because this would imply that $ab = nq$ where $q \in \mathbb{Z}$. By Euclid's Lemma, this implies that n divides a or b which cannot be true. Therefore, since $0 < ab \bmod n < n$ we have proven that $ab \bmod n \in S$.

Associativity: By lemma 1, we have that multiplication modulo n is associative over the integers.

Identity: $1 \in S$ is the identity since for all $a \in S$, $(1 \cdot a) \bmod n = (a \cdot 1) \bmod n = a$.

Inverses: We will first prove the following lemma.

Lemma 2. *Let $a, x, n \in \mathbb{Z}_{>0}$. $ax \bmod n = 1$ has a solution if and only if a and n are relatively prime.*

Proof. $\Rightarrow$ Assume $ax \bmod n = 1$ has a solution. Then, $ax - nq = 1$ where q is the largest integer such that $nq \leq ax$. Since we have shown that a linear combination of a and n which equals 1 exists, we have proven that they are relatively prime.

$\Leftarrow$ Assume a and n are relatively prime. For some $x, q \in \mathbb{Z}$, we have that the linear combination $ax + n(-q) = 1$. Thus, we have proven that $ax \bmod n = 1$ has a solution. $\square$

Let $a \in S$. a is relatively prime with n because n itself is prime. By lemma 2, there exists some $x \in \mathbb{Z}_{>0}$ such that $ax \bmod n = 1$.

$$
\begin{aligned}
1 &= ax \bmod n && \text{(lemma 2)} \\
&= (a \bmod n \cdot x \bmod n) \bmod n && \text{(definition of mod)} \\
&= (a \cdot x \bmod n) \bmod n && (a < n)
\end{aligned}
$$

Let $b = x \bmod n$. We have that $b \in S$ since $0 < x \bmod n < n$. Therefore, we have proven that for all $a \in S$, there exists some $b \in S$ such that $ab \bmod n = ba \bmod n = 1$. $\square$

Problem 4. Suppose G is a group with identity e such that for all $x \in G$, $x^2 = e$. Prove that G is Abelian.

Proof. Let $a, b \in G$. We will prove that the group operation is commutative by showing that $ab = ba$.

$$\begin{aligned}
a &= a \\
a(bb) &= a && (b^2 = e) \\
(ab)b &= a && \text{(associativity)} \\
(ab)(ba) &= a^2 && \text{(right multiply } a\text{)} \\
(ab)(ba) &= e && (a^2 = e) \\
ab &= ba && \text{(definition of } G\text{)}
\end{aligned}$$

□

Problem 5. Let G be a finite group with identity e. Show that the number of elements x of G such that $x^2 \neq e$ is even.

Proof. Let $S \subseteq G$ be the set of elements in G that are not their own inverse. For all $x \in S$, there must be some unique $x' \in S$ such that $x \neq x'$ and $xx' = x'x = e$ (Gallian, 2.3). Let $K \subseteq S = \{x, x'\}$. For any other $y \in S \setminus K$, we have that there exists another $y' \neq y$ that is in $S \setminus K$; together, these two elements form another set $K_2 \subseteq S = \{y, y'\}$ that is disjoint from K. Thus, this process can be repeated until we can partition S cleanly into sets of exactly two elements. This implies that the elements of S can be divided evenly into pairs, proving that the cardinality of S is even. $\square$