MATH 2100 Assignment 11 Solutions

Problem 1. *If* $n, a \in \mathbb{Z}^+$ *and* $d = (n, a)$*, show that the equation* $ax \equiv 1 \pmod{n}$ *has a solution if and only if* $d = 1$.

Proof. ($\implies$): Let x be a solution to the equation. Then

$$\begin{aligned} ax &\equiv 1 && \pmod{n} \\ ax &= 1 + kn && \text{for some } k \in \mathbb{Z} \\ ax - kn &= 1 \end{aligned}$$

Thus 1 is a linear combination of a and n. But we know (Theorem 0.2) that $d = (a, n)$ is the smallest positive integer we can make that way, so we must have $d = 1$. (Another way to see this is to notice that d divides the left side, so it must divide the right.)

($\impliedby$): If $d = 1$, we can write 1 as a linear combination of a and n. Say

$$as + nt = 1$$

But now

$$\begin{aligned} as &= 1 + nt \\ as &\equiv 1 \pmod{n} \end{aligned}$$

Thus $x = s$ is a solution to the given equation.

$\therefore$ ($\iff$) □

(Note: We *could* do this proof with a chain of if-and-only-ifs, but it would take more care. It's easy for mistakes to creep in when every step has to be reversible. In most cases, proving one direction at a time is wiser.)

Problem 2. *If* $a, x, n \in \mathbb{Z}$*,* $n > 1$*, and* $r \equiv x \pmod{n}$*, then*

$$ax \equiv 1 \pmod{n} \implies ar \equiv 1 \pmod{n}.$$

Proof. Begin by "decoding" the mod statement $r \equiv x \pmod{n}$ to get $r = x + kn$ for some $k \in \mathbb{Z}$. (This is very often a good way to start.) Now

$$\begin{aligned} ar &= a(x + kn) \\ &= ax + akn \\ &\equiv ax && \pmod{n} \\ &\equiv 1 && \pmod{n}, \end{aligned}$$

as required. □

Problem 3. *Show that $U(n) = \{m \in \mathbb{Z}_n : (m,n) = 1\}$ is a group for any $n \in \mathbb{Z}^+$.*

Proof.

- **Associativity:** This property is usually inherited somehow, and $U(n)$ is no exception. It lies inside Z_n, where we know multiplication is associative.
- **Identity:** We know 1 is an identity in Z_n, so we just need to check that it's in $U(n)$. Since $(1,n) = 1$, it is.
- **Inverse:** Let $m \in U(n)$; then $(m,n) = 1$. By problem 1, there is some x such that

$$mx \equiv 1 \pmod{n}.$$

  This x is *not* in general the inverse of m, because it need not be in $U(n)$. We can fix this by using the division algorithm to write $x = qn + r$ for some $q \in \mathbb{Z}$, $0 \leq r < n$. Then $r \equiv x \pmod{n}$, so problem 2 gives

$$mr \equiv 1 \pmod{n}.$$

  Finally, applying problem 1 in reverse, we see that $(r,n) = 1$. Together with $0 \leq r < n$, this gives $r \in U(n)$, and it multiplies with m to make the identity, so $r = m^{-1}$.
- **Closure:** (You were allowed to assume this, but let's prove it anyway.) Let $m, m' \in U(n)$ and suppose $(mm', n) \neq 1$. Then there is at least one prime p that divides both mm' and n. But if $p \mid mm'$, it must divide either m or m' (Euclid's Lemma). If it divides m, we have $p \mid m$ and $p \mid n$, so $p \mid (m,n)$ – impossible since $m \in U(n)$. Similarly, p can't divide m'. This is a contradiction. $\therefore$ $(mm', n) = 1$, and we can convert mm' to an element of $U(n)$ the same way we did with m^{-1}.

□

Problem 4. *Show that U_n is a subgroup of $GL(V)$, where V is a complex finite-dimensional vector space, U_n is the unitary linear operators on V, and $GL(V)$ is the invertible linear operators on V.*

Proof. Clearly $I \in U_n$, so the set is nonempty. We'll use the one-step subgroup test. Let $S, T \in U_n$; then $S^* = S^{-1}$, $T^* = T^{-1}$. We want to check if $ST^{-1} \in U_n$, so we'll see if it has the defining property.

$$\begin{aligned}(ST^{-1})^* &= (T^{-1})^* S^* \\ &= (T^*)^* S^{-1} \\ &= TS^{-1} \\ &= (ST^{-1})^{-1},\end{aligned}$$

so $ST^{-1} \in U_n$. $\therefore$ U_n is a subgroup of $GL(V)$. □

(**Note:** The proof can also be done with inner products, but this method is simpler. Don't forget to ask yourself why U_n is a subset of $GL(V)$.)

Problem 5. *Show that if G meets all group conditions except invertibility, the existence of* **left** *inverses in G is sufficient to show that G is a group.*

Proof. We must show that (two-sided) inverses exist. Let $x \in G$. We know x has a left inverse, i.e. there is some $a \in G$ such that $ax = e$. By the same token, a has a left inverse b such that $ba = e$. Left-multiplying both sides of the first equation by b gives

$$\begin{aligned} b(ax) &= be \\ (ba)x &= b \\ ex &= b \\ x &= b \end{aligned}$$

But now the second equation becomes $xa = e$. Thus a is both a left *and* a right inverse for x, and x was arbitrary, so we have true inverses for every element of G. □

(**Note:** You lost marks here if you used the $^{-1}$ symbol before the end. x^{-1} always means the *two-sided* inverse of x, and you have to show that it exists before you use it.)

Problem 6. *Show that $\mu_n = \{e^{2\pi ik/n} : 0 \leq k < n\}$ is a subgroup of $\mathbb{C}^\times$.*

Proof. Since μ_n is finite, we need only show that it's closed under the group operation. Let $a, b \in \mu_n$; then $a = e^{2\pi ik/n}$, $b = e^{2\pi il/n}$ for some $0 \leq k, l < n$. So

$$\begin{aligned} ab &= e^{2\pi ik/n} e^{2\pi il/n} \\ &= e^{2\pi i(k+l)/n} \end{aligned}$$

If $k + l$ were in the required range, we'd be done, but this is not guaranteed. However, since $e^{2\pi in/n} = e^{2\pi i} = 1$, we can "cast out" any multiple of n from the exponent without changing the answer. This should remind you of modular arithmetic, and we'll use the same tricks here. Let

$$k + l = qn + r$$

where $q \in \mathbb{Z}$, $0 \leq r < n$. Then

$$\begin{aligned} ab &= e^{2\pi i(qn+r)/n} \\ &= e^{2\pi i(qn)/n} e^{2\pi i(r)/n} \\ &= (e^{2\pi in/n})^q e^{2\pi ir/n} \\ &= 1^q e^{2\pi ir/n} \\ &= e^{2\pi ir/n} \in \mu_n. \end{aligned}$$

Thus μ_n is closed under multiplication and is a subgroup of $\mathbb{C}^\times$. □

(**Note:** Some of you noticed that $k + l$ is less than $2n$, so at most one n needs casting out; we don't need the more general approach above. However, it is applicable to other situations, such as looking at *powers* of elements of μ_n.)