Homework #3 Solutions

p 23, #4. $s = -3$ and $t = 2$ work since

$$7s + 11t = -21 + 22 = 1.$$

These choices are not unique since $s = 8$, $t = -5$ also work:

$$7s + 11t = 56 - 55 = 1.$$

p 24, #30. Given any integer n, at least one of the three consecutive numbers $n-1, n, n+1$ must be divisible by 2 and at least one of them must be divisible by 3. Therefore the product $(n-1)n(n+1) = n(n^2-1) = n^3 - n$ must be divisible by $2 \cdot 3 = 6$. It follows that n^3 and n must have the same remainder when divided by 6, i.e. $n^3 \bmod 6 = n \bmod 6$.

p 54, #8 We must verify that the 4 group axioms hold for the set $S = \{5, 15, 25, 35\}$ together with the operation of multiplication modulo 40. Since we know that this operation is associative on all of $\mathbb{Z}_n$, it will be associative on S as well. We need only verify closure, the existence of an identity, and the existence of inverses. We can do this by building a Cayley table for S:

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

The table shows that S is closed under multiplication mod 40, that 25 is the identity of S, and, since 25 appears in each row, every element has an inverse. In fact, each element is its own inverse!

To compare S to $U(8) = \{1, 3, 5, 7\}$, we examine the Cayley table of the latter:

	3	5	1	7
3	1	7	3	5
5	7	1	5	3
1	3	5	1	7
7	5	3	7	1

If we swap symbols in this table according to the following rules

$$1 \leftrightarrow 25,\ 3 \leftrightarrow 5,\ 5 \leftrightarrow 15,\ 7 \leftrightarrow 35$$

then the Cayley table for $U(8)$ is transformed into the Cayley table for S. That is, aside from the way we have labeled our elements, $U(8)$ and S are the *same group*.

p 54, #12. If $n > 2$ then clearly $1, n-1 \in U(n)$ and $n - 1 \neq 1$. We claim that these both satisfy the equation $x^2 = 1$. This is obvious for 1 and easy to show for $n - 1$:

$$(n-1)^2 \bmod n = (n^2 - 2n + 1) \bmod n = (n(n-2) + 1) \bmod n = 1.$$

Handout problem #1. Let $n \in \mathbb{Z}^+$, $a, b \in \mathbb{Z}$, $a \bmod n = b \bmod n$ and suppose $(a, n) = 1$. We can write

$$\begin{aligned} a &= qn + r \\ b &= pn + r \end{aligned}$$

where $p, q \in \mathbb{Z}$ and $r = a \bmod n = b \bmod n$. But then

$$a = qn + r = qn + (b - pn) = b + (q - p)n.$$

Suppose that $d \in \mathbb{Z}^+$ divides both b and n. Then $b = db'$ and $n = dn'$ for some $b', n' \in \mathbb{Z}$. It follows that

$$a = db' + (q-p)dn' = d(b' + (q-p)n')$$

so that d divides a. But d also divides n and $(a, n) = 1$. It follows that $d = 1$. That is, the only divisor common to both b and n is 1, i.e. $(b, n) = 1$.

We now use this to prove that $U(n)$ is closed under multiplication modulo n. Let $a, b \in U(n)$. Then $(a, n) = (b, n) = 1$ so that $(ab, n) = 1$ as well. Let $r = (ab) \bmod n \in \mathbb{Z}_n$. Then $r \bmod n = r = (ab) \bmod n$, so by the preceding paragraph we must have $(r, n) = 1$. That is, $r \in U(n)$, as needed.

Handout problem #2. If $a \bmod n = b \bmod n$ then, as above, we can write

$$\begin{aligned} a &= qn + r \\ b &= pn + r \end{aligned}$$

where $p, q \in \mathbb{Z}$ and $r = a \bmod n = b \bmod n$. If $g^n = e$ it follows that

$$g^a = g^{qn}g^r = (g^n)^q g^r = eg^r = (g^n)^p g^r = g^{pn}g^r = g^b.$$

p 67, #4. We first prove the following: Let G be a group and let $a \in G$. Then for any integer n, $a^n = e$ if and only if $(a^{-1})^n = e$. The proof is simple: if $a^n = e$ then

$$e = e^{-1} = (a^n)^{-1} = (a^{-1})^n$$

and the converse is established by replacing a with a^{-1} throughout.

This result implies that the positive integers that annihilate a are the same as those that annihilate a^{-1}. Hence, the order, which is the smallest positive integer annihilating a given element, must be the same for both a and a^{-1}.

p 67, #10. Let G be an Abelian group and suppose $a, b \in G$, $a \neq b$ and $|a| = |b| = 2$. Let

$$H = \{e, a, b, ab\}.$$

Claim 1: H has order 4. Since $|a| = |b| = 2$, $a \neq e$ and $b \neq e$. Since $a \neq e$ we must show that $ab \neq a$, $ab \neq b$ and $ab \neq e$. If $ab = a$ or $ab = b$, then left or right cancelation imply $b = e$ or $a = e$, either of which is a contradiction. If $ab = e$ then

$$b = eb = a^2b = a(ab) = ae = a$$

which is also a contradiction.

Claim 2: H is a subgroup of G. This is easily seen using the finite subgroup test and a Cayley table:

	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

Here we have made repeated use of the facts: $a^2 = b^2 = e$, $ab = ba$. The table shows that H is closed under the operation of G, so the finite subgroup test implies H is a subgroup of G.

p 67, #12. We are given that $H < \mathbb{Z}$ and $18, 30, 40 \in H$. Since H is a subgroup it is closed under addition and subtraction. Therefore

$$\begin{aligned} 12 &= 30 - 18 \in H \\ 6 &= 18 - 12 \in H \\ 34 &= 40 - 6 \in H \\ 2 &= 6 \cdot 6 - 34 \in H \end{aligned}$$

Again, closure implies that H must contain all the multiples of 2. If H contained any odd integer, say $2n + 1$, then we'd have

$$1 = (2n + 1) - n \cdot 2 \in H$$

which would mean that $H = \mathbb{Z}$, which contradicts our hypothesis. Thus, H must consist of exactly the even integers, i.e.

$$H = \{2n \mid n \in \mathbb{Z}\} = \langle 2 \rangle.$$

p 68, #14. Let G be a group and $H, K \leq G$. We apply the one-step subgroup test to show that $H \cap K \leq G$. First of all, $H \cap K \neq \emptyset$ since $e \in H \cap K$. Now let $a, b \in H \cap K$. Then $a, b \in H$ and, since $H \leq G$, $ab^{-1} \in H$. But also $a, b \in K$ and $K \leq G$ so that $ab^{-1} \in K$. Therefore $ab^{-1} \in H \cap K$. Since a and b were arbitrary, we conclude that for any $a, b \in H \cap K$ we have $ab^{-1} \in H \cap K$. By the one-step subgroup test we conclude that $H \cap K \leq G$.

p 69, #28. We see that

$$\begin{aligned} A^2 &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \\ A^3 &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\ A^4 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I \end{aligned}$$

so that $|A| = 4$. Likewise:

$$\begin{aligned} B^2 &= \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \\ B^3 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I \end{aligned}$$

so that $|B| = 3$. However

$$AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and we showed in class that $|AB| = \infty$. The moral here is that it is possible for group elements with finite order to multiply together to yield an element of infinite order.