Homework 1 (Due Sept 6, 2023)

Jack Hyatt
MATH 546 - Algebraic Structures I - Fall 2023

December 28, 2023

Justify all of your answers completely.

1. Let m, n be positive integers, and let $d = \gcd(m, n)$. Consider the following sets:

$$S_1 = \{km + ln : k, l \in \mathbb{Z}\}, \qquad S_2 = \{dq : q \in \mathbb{Z}\}$$

Prove that $S_1 = S_2$.

Proof. Showing that $S_2 \subseteq S_1$.

$$S_2 = \{dq : q \in \mathbb{Z}\} = \{\gcd(n, m)q : q \in \mathbb{Z}\} = \{(km + ln)q : q \in \mathbb{Z}\} \text{ for some integers } k \text{ and } l.$$
$$= \{(kq)m + (lq)n : q \in \mathbb{Z}\}$$

kq and lq are both integers, so $((kq)m + (lq)n) \in S_1$.
Showing that $S_1 \subseteq S_2$.

$$S_1 = \{km + ln : k, l \in \mathbb{Z}\} = \{(d)\left(\frac{km}{d} + \frac{ln}{d}\right) : k, l \in \mathbb{Z}\}$$

and we know $\frac{km}{d}$ and $\frac{ln}{d}$ are both integers since d is a divisor of m and n. So $\left((d)\left(\frac{km}{d} + \frac{ln}{d}\right)\right) \in S_2$. ∎

2. Recall that we have seen in class (on 8/28) that $f : \mathbb{Z}_5 \to \mathbb{Z}_{10}, f([x]_5) = [x]_{10}$ is not a well-defined function.

   (a) Consider $g : \mathbb{Z}_5 \to \mathbb{Z}_{10}, g([x]_5) = [2x]_{10}$. Is g a well-defined function?

   Proof. Let $x_1 \equiv x_2 \pmod 5$. Then $x_1 - x_2 = 5k$ for some integer k. Multiplying both sides by 2 gives, $2x_1 - 2x_2 = 10k$. So $2x_1 \equiv 2x_2 \pmod{10}$. We find g is a well-defined function. ∎

   (b) Consider $h : \mathbb{Z}_5 \to \mathbb{Z}_{10}, h([x]_5) = [3x]_{10}$. Is h a well-defined function?

   No, since $[6]_5 = [1]_5$, but $h([6]_5) = [18]_{10} = [1]_{10} \neq [3]_{10} = h([1]_5)$.

3.

(a) List all the elements of $\mathbb{Z}_{12}^*$.

$\{[1],[5],[7],[11]\}$

(b) We say that a set S is *closed under addition* if we have $x+y \in S$ for any $x,y \in S$. Is $\mathbb{Z}_{12}^*$ closed under addition?

No, as $[5]+[7] \equiv [0] \notin \mathbb{Z}_{12}^*$.

(c) We say that a set S is *closed under multiplication* if we have $x \cdot y \in S$ for any $x,y \in S$. Is $\mathbb{Z}_{12}^*$ closed under multiplication?

Yes, as $[1]$ times any of the elements is in $\mathbb{Z}_{12}^*$, $[5]\cdot[5] \equiv [1]$, $[5]\cdot[7] \equiv [11]$, $[5]\cdot[11] \equiv [7]$, $[7]\cdot[7] \equiv [1]$, $[7]\cdot[11] \equiv [5]$, $[11]\cdot[11] \equiv [1]$.

4. Let p,q be prime numbers and let n be a positive integer.

(a) Prove that the number of elements of $\mathbb{Z}_{p^n}^*$ is $p^n - p^{n-1}$.

Proof. Let p,q be prime numbers and let n be a positive integer.
Finding the number of integers $0 \le k \le p^n - 1$ coprime to p^n is equivalent to $|\mathbb{Z}_{p^n}^*|$.
Being coprime to a prime power is equivalent to the number not divisible by the prime. In the range 0 to $p^n - 1$, the numbers divisible by p are $0, p, 2p, \ldots, (p^{n-1}-2)p, (p^{n-1}-1)p$. So there are p^{n-1} numbers between 0 and $p^n - 1$ divisible by p.
So there are $p^n - p^{n-1}$ numbers coprime to p^n. The rest follows. ■

(b) Assume $p \neq q$. Prove that the number of elements of $\mathbb{Z}_{pq}^*$ is $(p-1)(q-1)$.

Proof. Let p,q be distinct prime numbers.
Finding the number of integers $0 \le k \le pq - 1$ coprime to pq is equivalent to $|\mathbb{Z}_{pq}^*|$.
Since p and q are prime, the only numbers that divide pq are numbers that are divisible by p or q.
The numbers in 0 to $pq-1$ divisible by p are $0, p, 2p, \ldots, (q-2)p, (q-1)p$. The amount of those numbers is q.
The numbers in 0 to $pq-1$ divisible by q are $0, q, 2q, \ldots, (p-2)q, (p-1)q$. The amount of those numbers is p.
The only number in common between the two sets is 0, so we will have to re-include 0 by inclusion-exclusion principle.
We now have the number of coprime numbers $pq - p - q + 1 = (p-1)(q-1)$. ■