Nathan Bickel
MATH 546: Section 001
Professor: Dr. Vraciu
August 31, 2023

MATH 546 Homework 1

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

$$S_1 = \{km + \ell n \mid k, \ell \in \mathbb{Z}\}, \quad S_2 = \{dq \mid q \in \mathbb{Z}\}.$$

Prove that $S_1 = S_2$.

Solution.

($\subset$) Let $s \in S_1$. Then there exist some $k, \ell \in \mathbb{Z}$ such that we can write

$$s = km + \ell n = kd\left(\frac{m}{d}\right) + \ell d\left(\frac{n}{d}\right) = d\left[k\left(\frac{m}{d}\right) + \ell\left(\frac{n}{d}\right)\right].$$

Since $d \mid n$ and $d \mid m$ by definition, $\frac{m}{d}$ and $\frac{n}{d}$ are both integers and thus s is a multiple of d. Therefore, $s \in S_2$ and so $S_1 \subset S_2$.

($\supset$) Let $s \in S_2$. Then, there exists some $q \in \mathbb{Z}$ such that $s = qd$. By the property we discussed in class, there exist $k, \ell \in \mathbb{Z}$ such that $d = km + \ell n$. So we have $s = q(km + \ell n) = (qk)m + (q\ell)n$, and since $q, k, \ell \in \mathbb{Z}$, we have $qk, q\ell \in \mathbb{Z}$. Therefore, $s \in S_1$ and so $S_2 \subset S_1$. □

Problem 2 Recall that we have seen 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? Prove your answer.

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

Solution.

(a) Yes. Let $[x]_5, [x']_5 \in \mathbb{Z}_5$ such that $[x]_5 = [x']_5$. Since $x \equiv x' \pmod 5$, we have $5 \mid (x - x')$ and so there exists some $k \in \mathbb{Z}$ such that $5k = x - x'$. Thus, we have $10k = 2(x - x') = 2x - 2x'$, and consequently $10 \mid (2x - 2x')$ and $2x \equiv 2x' \pmod{10}$. Therefore,

$$g([x]_5) = [2x]_{10} = [2x']_{10} = g([x']_5),$$

so g is a well-defined function because every element in $\mathbb{Z}_5$ maps to a unique element in $\mathbb{Z}_{10}$.

(b) No. For example, since $0 \equiv 5 \pmod 5$, we have $[0]_5 = [5]_5$, but

$$h([0]_5) = [0]_{10} \neq [5]_{10} = [15]_{10} = h([5]_5).$$

Thus, not every element in $\mathbb{Z}_5$ maps to a unique element in $\mathbb{Z}_{10}$, so h cannot be a function. □

Problem 3

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

(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? Justify your answer.

(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? Justify your answer.

Solution.

(a) By checking the numbers that are co-prime to 12, we can write $\mathbb{Z}_{12}^* = \{[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}\}$.

(b) No. For example, $[1]_{12} + [11]_{12} = [12]_{12} = [0]_{12}$, which is not in $\mathbb{Z}_{12}^*$ even though $[1]_{12}, [11]_{12} \in \mathbb{Z}_{12}^*$. (In fact, $\mathbb{Z}_n^*$ is never closed under addition for $n \geq 3$, since it always contains $[1]_n$ and $[n-1]_n$.)

(c) Yes. Suppose (toward contradiction) that there exist $[x]_{12}, [y]_{12} \in \mathbb{Z}_{12}^*$ such that $[xy]_{12} \notin \mathbb{Z}_{12}^*$. Since $[xy]_{12}$ is not in $\mathbb{Z}_{12}^*$, it does not have a multiplicative inverse, and therefore $\gcd(xy, 12) > 1$. Then, by the fundamental theorem of arithmetic, there must exist some prime p such that $p \mid xy$ and $p \mid 12$. Since p is prime, we must have $p \mid x$ or $p \mid y$: assume WLOG that $p \mid x$. This shows that $\gcd(x, 12) > 1$, so $[x]_{12}$ does not have a multiplicative inverse. Therefore, $[x]_{12} \notin \mathbb{Z}_{12}^*$, a contradiction. □

Problem 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 $p^n - p^{n-1}$.

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

Solution.

(a) We will first find the number of elements in $\mathbb{Z}_{p^n} \backslash \mathbb{Z}_{p^n}^*$. Each such element $[x]_{p^n}$ does not have a multiplicative inverse, so we have $\gcd(x, p^n) \neq 1$. Since p is the only prime factor of p^n, we must have $x = pq$ for some q. To obtain distinct congruence classes, q can take on values in

$$\{0, 1, 2, \ldots, p^{n-1} - 2, p^{n-1} - 1\}$$

before $x \geq p^n$ where the classes start repeating. Thus, p^{n-1} elements in $\mathbb{Z}_{p^n}$ do not have a multiplicative inverse, and since there are p^n total classes, we have $|\mathbb{Z}_{12}^*| = p^n - p^{n-1}$.

(b) We will first find the number of elements in $\mathbb{Z}_{pq} \backslash \mathbb{Z}_{pq}^*$. Each such element $[x]_{pq}$ does not have a multiplicative inverse, so we have $\gcd(x, pq) \neq 1$. Thus, $p \mid x$ or $q \mid x$, since p and q are both prime. There are q possibilities for $p \mid x$ because we could have $x = pk$ for $k \in \{0, 1, \ldots, q-1\}$ before repetition, and similarly there are p possibilities for $q \mid x$ because we could have $x = q\ell$ for $\ell \in \{0, 1, \ldots, p-1\}$. This counts the possibility of $x = 0$ twice, so there are $p + q - 1$ elements in $\mathbb{Z}_{pq}$ without multiplicative inverses. Since there are pq total elements, we have

$$|\mathbb{Z}_{pq}^*| = pq - (p + q - 1) = pq - p - q + 1 = (p-1)(q-1).$$

□