Staff Solutions to Mini-Quiz 10-7

Problem 1 ().
Let $\{1,2,3\}^\omega$ be the set of infinite sequences containing only the numbers 1, 2, and 3. For example, some sequences of this kind are:

$$(1,1,1,1...),$$
$$(2,2,2,2...),$$
$$(3,2,1,3...).$$

Prove that $\{1,2,3\}^\omega$ is uncountable.

Hint: One approach is to define a surjective function from $\{1,2,3\}^\omega$ to the power set $\text{pow}(\mathbb{N})$.

Solution. *Proof.* We can define a surjective function from $f : \{1,2,3\}^\omega \to \text{pow}(\mathbb{N})$ as follows:

$$f(s) ::= \{n \in \mathbb{N} \mid s[n] = 1\}$$

where $s[n]$ is the nth element of sequence s.

Now if there was a surjective function from $g : \mathbb{N} \to \{1,2,3\}^\omega$, then the composition of f and g would be a surjective function from $\mathbb{N}$ to $\text{pow}(\mathbb{N})$ contradicting Cantor's Theorem 7.1.10. ∎

Alternatively, to show that $\{1,2,3\}^\omega$ is uncountable, we can directly use a basic diagonal argument to show that no function, $\sigma : \mathbb{N} \to \{1,2,3\}^\omega$ is a surjection.

Proof. Let σ be a function from $\mathbb{N}$ to the infinite sequences of 1's, 2's, and 3's, that is,

$$\sigma : \mathbb{N} \to \{1,2,3\}^\omega.$$

To show that σ is not a surjection, we will describe a sequence, diag, of 1's, 2's, and 3's that is not in the range of σ.

Let $r : \{1,2,3\} \to \{1,2,3\}$ be defined by

$$r(1) ::= 2,$$
$$r(2) ::= 3,$$
$$r(3) ::= 1.$$

In particular $r(i) \neq i$ for $i = 1,2,3$. Define a sequence $\text{diag} \in \{1,2,3\}^\omega$ as follows:

$$\text{diag}[n] ::= r(\sigma(n)[n]).$$

Now by definition,

$$\text{diag}[n] \neq \sigma(n)[n],$$

for all $n \in \mathbb{N}$, proving that diag is not equal to $\sigma(n)$ for any $n \in \mathbb{N}$. That is, diag is not in the range of σ as claimed. ∎

Problem 2 (). **(a)** Use the Pulverizer to find gcd(84, 108)

Solution. Here is the table produced by the Pulverizer:

x	y	$\text{rem}(x,\ y)$	$=$	$x - q \cdot y$
108	84	24	$=$	$1 \cdot 108 - 1 \cdot 84$
84	24	12	$=$	$-3 \cdot 108 + 4 \cdot 84$
24	12	0		

■

(b) Find integers x, y with $0 \leq y < 84$ such that

$$x \cdot 84 + y \cdot 108 = \text{gcd}(84, 108).$$

Solution. From the table above,

$$4 \cdot 84 - 3 \cdot 108 = \text{gcd}(84, 108).$$

Therefore,

$$(4 - 108 \cdot k) \cdot 84 + (-3 + 84 \cdot k) \cdot 108 = \text{gcd}(84, 108).$$

So, letting $k = 1$, $(x, y) = (4 - 108 \cdot 1, -3 + 84 \cdot 1) = (-104, 81)$ works. ■

(c) Is there a multiplicative inverse of 84 in $\mathbb{Z}_{108}$? If not briefly explain why, otherwise find it.

Solution. There is no inverse of 84 modulo 108. The inverse of a modulo m exists iff $gcd(a, m) = 1$. Clearly $gcd(84, 108) = 12 \neq 1$, so there is no inverse of 84 modulo 108. ■

Problem 3 ().
Prove that if k_1 and k_2 are relatively prime to n, then so is $k_1 \cdot_n k_2 ::= \text{rem}(k_1 \cdot k_2,\ n)$,

(a) ...using the fact that k is relatively prime to n iff k has an inverse modulo n.

Hint: Recall that $k_1 k_2 \equiv k_1 \cdot_n k_2 \pmod{n}$.

Solution. If j_1 is an inverse of k_1 modulo n, that is

$$j_1 k_1 \equiv 1 \pmod{n},$$

and likewise j_2 is an inverse of k_2, then it follows immediately that

$$(j_2 j_1)(k_1 k_2) \equiv 1 \pmod{n}.$$

That is, $k_1 k_2$ also has an inverse. Since we know that $k_1 k_2 \equiv k_1 \cdot_n k_2 \pmod{n}$, any inverse of $k_1 k_2$ will also be an inverse of $k_1 \cdot_n k_2$. ■

(b) ...using the fact that k is relatively prime to n iff k is cancellable modulo n.

Solution. If k_1 and k_2 are cancellable modulo n, then you can cancel $k_1 k_2$ by first cancelling k_1 and then cancelling k_2. Also, it follows from the Congruence Lemma 8.6.4, that if k is cancellable than so is anything congruent to k modulo n, so by the previous Hint, $k_1 \cdot_n k_2$ is cancellable. ■

(c) ...using the Unique Factorization Theorem and the basic GCD properties.

Solution. By Unique Factorization, the primes divisors of $k_1 \cdot k_2$ are the same as the prime divisors of k_1 or of k_2. If k_1 and k_2 are relatively prime to n, they have no prime divisors in common with n, then neither does $k_1 k_2$, so $k_1 k_2$ is relatively prime to n. This is equivalent to $1 = \gcd(k_1 k_2, n)$.

But $k_1 \cdot_n k_2 ::= \text{rem}(k_1 k_2,\ n)$ and $\gcd(n, \text{rem}(k_1 k_2,\ n)) = \gcd(k_1 k_2, n)$ by Lemma 8.2.1, so a$\gcd(n, \text{rem}(k_1 k_2,\ n)) = 1$. ■