Homework 11 (Due Nov 7, 2022)

Jack Hyatt
MATH 574 - Discrete Mathamatics - Fall 2022

November 13, 2022

Justify all of your answers completely.

1. Let $n \in \mathbb{N}$. Prove that if $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then $ab \equiv cd \pmod{n}$.

   Proof. Assume $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$. So $\exists x, y \in \mathbb{Z}$ s.t. $a = c + xn$ and $b = d + yn$. So $ab = (c + xn)(d + yn) = cd + n(cy + dx + xyn) \equiv cd \pmod{n}$. ■

2. Which elements of $\mathbb{Z}_{12}$ are invertible? For each element that is invertible, give its inverse.

   A class will be invertible iff the gcd(a,12)=1, where a is the number we are looking at. By inspection, we see that 1,5,7,11 will fit that criteria. 1 is clearly its own inverse. For the other 3 numbers, we just have to look between them to see which multiply to get 1 $\pmod{12}$.
   $5 \cdot 5 \equiv 1 \pmod{12}$
   $7 \cdot 7 \equiv 1 \pmod{12}$
   $11 \cdot 11 \equiv 1 \pmod{12}$

3. Let $n \in \mathbb{N}$. Define a function $f : \mathbb{Z}_n \to \mathbb{Z}_n$ by $f([a]) = [a^2]$.

   (a) Prove that, if $n = 1$ or $n = 2$, then f is bijective.

   Case n=1:
   In $\mathbb{Z}_1$, there is only 1 congruence class, namely, [0]. *Obviously*, a function that maps a domain of only [0] to a codomain of only [0] is bijective.
   Case n=2:
   In $\mathbb{Z}_2$, there are 2 congruence class, namely, [0] and [1]. 0 and 1 both have the property where they are their own squares. So 0 goes to 0 and 1 goes to 1. So f is bijective.

(b) Prove that for $n \geq 3$, f is not injective. (Hint: try to find two different elements $[a] \neq [b]$ such that $f([a]) = f([b])$.)

Note: $f([1]) = [1]$.
If we can show that there is another class, a, s.t. $f([a]) = [1]$, then we know f isn't injective.
Looking at $[n-1]$, where $n \geq 3$, we see that $f([n-1]) = [(n-1)^2] = [n^2-2n+1] = [n(n-2)+1] \equiv [1]$. Since n≥3, we know that $n - 1 > 1$.■

4. Suppose $m, n \in \mathbb{Z}$ are not both 0. Let $d = \gcd(m, n)$. Prove that $\gcd(\frac{m}{d}, \frac{n}{d}) = 1$.

Let $d = \gcd(m, n)$. Using Jeff Bezos' identity, we know that $\exists a, b \in \mathbb{Z}$ s.t. $d = \gcd(m, n) = am + bn$. Since d isn't 0 and divides both m and n, we can divide by d and get $a\frac{m}{d} + b\frac{n}{d} = 1$. So since the linear combination of two integers is 1, the lowest positive number, and the gcd of two integers is the smallest positive integer to make out of a linear combination, then $\gcd(\frac{m}{d}, \frac{n}{d}) = 1$.

5. Let $a, b \in \mathbb{Z}$ not both zero. Prove or disprove:

(a) If $\gcd(a, b) = 1$, then $\gcd(a^2, b^2) = 1$.

Since a and b are coprime, they have no prime factors in common. Let $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$ and $b = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_m^{\beta_m}$. Since $p_i \neq q_j$ for any pair i,j, doubling all the powers will not change that fact. So a^2 and b^2 will not have any common prime factors, being coprime. ■

(b) If $\gcd(a, b) = 1$, then $\gcd(a, 2b) = 1$.

We see that $a = 2$ and $b = 3$ will disprove this. $\gcd(2, 3) = 1$ and $\gcd(2, 6) = 2$.

6. Let $n \in \mathbb{Z}$. Prove that $\gcd(n, n+2) = 1$ if and only if n is odd.

Proof. Showing if $\gcd(n, n+2) = 1$, then n is odd.
This is clear since if n was even, then the $\gcd(n, n+2)$ will be two.
Showing if n is odd, then $\gcd(n, n+2) = 1$
Assume n is odd, then $\exists k \in \mathbb{Z}$ s.t. $n = 2k+1$. Assume towards contradiction that $\gcd(n, n+2) \geq 2$. Let $d = \gcd(n, n+2)$. So $d|n$ and $d|n+2$. So then $n \equiv 0 \pmod{d}$ and $n+2 \equiv 0 \pmod{d}$. Denote $[a]$ to be $a \pmod{d}$.

$$[n+2] - [n] = [0] \implies [2] = [0] \implies d = 2$$

So then $2|n$, which makes n even. But we assumed n to be odd, a contradiction. ■

7. Let $a, b \in \mathbb{Z}$ not both zero. If $\gcd(a, b) = 1$ and $a \mid n$ and $b \mid n$, prove that $ab \mid n$.

   Assume $\gcd(a, b) = 1$ and $a \mid n$ and $b \mid n$. Since a and b are coprime, then they can be written as a product their prime factors and no prime will be in both a and b. Let $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$ and $b = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_m^{\beta_m}$ where no $p_i = q_j$. Since a and b both divide n, the prime factorization of a and b are in the prime factorization of n. Since a and b share no primes, a and b primes are completely in n's factorization with no overlap. So then $ab \mid n$.

8. Let $a, b \in \mathbb{N}$. Define the least common multiple $\operatorname{lcm}(a, b)$ as the smallest positive integer that is a multiple of both a and b. Prove that $ab = \operatorname{lcm}(a, b)$ if and only if $\gcd(a, b) = 1$.

   Proof. Showing if $\gcd(a, b) = 1$, then $\operatorname{lcm}(a, b) = ab$.
   Assume $\gcd(a, b) = 1$. Let $n = \operatorname{lcm}(a, b)$. So $a \mid n$ and $b \mid n$. So $ab \mid n$ using (7). So $\exists k \in \mathbb{Z}$ s.t. $abk = n$. So $ab = \frac{n}{k}$, and $\frac{n}{k} \in \mathbb{Z}$. But ab is a common multiple of a and b, while n is the least common multiple. So that must make $k = 1$.

   Showing if $\operatorname{lcm}(a, b) = ab$, then $\gcd(a, b) = 1$ by contrapositive.
   Assume $\gcd(a, b) > 1$. Let $d = \gcd(a, b)$. Then $\exists x, y \in \mathbb{Z}$ s.t. $dx = a$ and $dy = b$. Then dxy will divide both a and b. So $\operatorname{lcm}(a, b) \leq dxy < dxdy = ab$.
   So $\gcd(a, b) > 1 \implies \operatorname{lcm}(a, b) < ab$. ∎