21-127 Homework 7

Christian Broms
Section J

Thursday 8th March, 2018

Complete the following problems. Fully justify each response.

1. Let $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$ with $n \geq 1$, and $k, \ell \in \mathbb{N}$ with $k \equiv \ell \pmod{n}$ and $a \equiv b \pmod{n}$.

   (a) Is it true that $a^k \equiv b^k \pmod{n}$? If so, prove it. If not, provide a counterexample.

   Yes.

   Proof. We begin by proving that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ implies $ac \equiv bd \pmod{n}$. We can write $a = kn + b$ and $c = k'n + d$ for some $k, k' \in \mathbb{Z}$. So $ac = k'kn^2 + (bk' + dk)n + bd$. Because this is in mod n, we can eliminate all factors of n so $ac \equiv bd \pmod{n}$.

   Next, we will proceed with induction to show $a^k \equiv b^k \pmod{n}$.

   Base Case: $k = 1$, so $a^1 = b^1 \pmod{n}$ is true by the given information.

   Induction Hypothesis: Assume $a^k \equiv b^k \pmod{n}$. We will show $a^{k+1} \equiv b^{k+1} \pmod{n}$. We know $a \equiv b \pmod{n}$ and $a^k \equiv b^k \pmod{n}$ by IH, so we multiply these together using the proven fact above to get $a^{k+1} \equiv b^{k+1} \pmod{n}$, and the induction holds.

   Thus, we can safely say that $a^k \equiv b^k \pmod{n}$. ■

   (b) Is it true that $a^k \equiv a^\ell \pmod{n}$? If so, prove it. if not, provide a counterexample.

   False. Consider the following counterexample: $a = 3, n = 5, k = 7, \ell = 2$. So $3^7 \not\equiv 3^2 \pmod{5}$

2. Let $a \in \mathbb{Z}$, and let $n \in \mathbb{N}$ with $n \geq 1$. Suppose that $a \perp n$. Show that u, u' are both multiplicative inverses for a if and only if u is a multiplicative inverse for a and $u \equiv u' \pmod{n}$.

   Proof. ($\Rightarrow$) Assume u, u' are multiplicative inverses for a, such that $au \equiv 1 \pmod{n}$ and $au' \equiv 1 \pmod{n}$. Then, since a and n are coprime, we manipulate then divide by a so $a(u-u') \equiv 0 \pmod{n}$ and $u - u' \equiv 0 \pmod{n}$, so $u \equiv u' \pmod{n}$ and we are done.

   ($\Leftarrow$) Assume u is a multiplicative inverse for a and $u \equiv u' \pmod{n}$, so we have $au \equiv 1 \pmod{n}$ and $u \equiv u' \pmod{n}$. We can multiply by a to get $au \equiv au' \pmod{n}$. Since we know $au \equiv 1 \pmod{n}$ and $au \equiv au' \pmod{n}$, we can say $au' \equiv 1 \pmod{n}$. This, taken with the fact $au \equiv 1 \pmod{n}$ implies that u, u' are multiplicative inverses for a.

   Therefore, since we have shown both sides of implication, it follows that u, u' are both multiplicative inverses for a if and only if u is a multiplicative inverse for a and $u \equiv u' \pmod{n}$. ■

3. Let p be a positive prime, and $k \in \mathbb{N}$ with $k \geq 1$. Prove that $\varphi(p^k) = p^k - p^{k-1}$.

   Proof. The totient function is defined as $\varphi(n) =$ the number of integers between 1 and n that are coprime to n. In this case, we are looking for some $m \in \mathbb{Z}$ such that $\gcd\left(m, p^k\right) = 1$, so we need some m that does not divide p^k. We list the number of integers between 1 and p^k that are divisible by p as $1p, 2p, 3p \ldots p^{k-1}p$. So there are p^{k-1} such numbers, and our set $\{1, 2, 3, \ldots p^k\}$ has $p^k - p^{k-1}$ numbers that are not divisible by p^k. Therefore, we conclude $\varphi(p^k) = p^k - p^{k-1}$. ■

4. Read the proof of Theorem 3.3.49 and Example 3.3.51. Then prove that for any $b \in \mathbb{N}$ with $b \geq 2$, and $a \in \mathbb{N}$, a is divisible by $b - 1$ if and only if the sum of the base b digits of a is divisible by $b - 1$.

   Proof. We can write a in its base b expansion as $a = d_r d_{r-1} \ldots d_1 d_0$ base b, such that $a = \sum\limits_{i=0}^{r} d_i b^i$. So the sum of these digits can be written as

$s = \sum_{i=0}^{r} d_i$. Because we defined a as $\sum_{i=0}^{r} d_i b^i$, we can say $s \equiv \sum_{i=0}^{r} d_i b^i \pmod{b-1}$. We can further reduce this $s \equiv \sum_{i=0}^{r} d_i 1^i \pmod{b-1}$ because $b \equiv 1 \pmod{b-1}$. Finally, we can reduce to $s \equiv \sum_{i=0}^{r} d_i \pmod{b-1}$ because 1^i is always 1. So $s \equiv a \pmod{b-1}$. It therefore follows by definition of congruence that a is divisible by $b-1$ if and only if the sum of the base b digits of a is divisible by $b-1$. ■

5. For each of the following functions, determine if it is injective, surjective, both, or neither. Prove that your answers are correct.

   (a) $f : \mathbb{Z} \to \mathbb{N}$, $f(x) = x^2$.
   Injective: No. Consider $f(2) = f(-2)$, but $-2 \neq 2$.
   Surjective: No. Consider $x = 3$, but there is no $z \in \mathbb{Z}$ such that $z^2 = 3$, as $\sqrt{3} \notin \mathbb{Z}$

   (b) $g : \mathbb{N} \to \mathbb{Z}$, $g(x) = x^2$.
   Injective: Yes. Assume $f(x) = f(y)$, so $x^2 = y^2$ and $x = y$.
   Surjective: No. Consider $x = 3$, but there is no $n \in \mathbb{N}$ such that $n^2 = 3$, as $\sqrt{3} \notin \mathbb{N}$

   (c) $h : \mathbb{R} \to \mathbb{Z}$, $h(x) = \lfloor x \rfloor$
   (note: $\lfloor x \rfloor$ is the number you get by rounding x down to the nearest integer. Formally, we define

   $$\lfloor x \rfloor = \max\{y \in \mathbb{Z} \mid y \leq x\}.$$

   You may be reasonably skeptical that such a number exists, since we cannot apply the Well-Ordering Principle here.... so if you are skeptical, prove it.)
   Injective: No. Consider $h(\pi) = h(3)$, but $\pi \neq 3$.
   Surjective: Yes. Let $y \in Z$. Let $x = y + \frac{1}{2}$. then $y < x < y + 1$, so $\max\{n \in \mathbb{Z} \mid n \leq x\} = y$. Thus, $f(x) = \lfloor x \rfloor = y$

   (d) $f : \mathbb{N} \to \mathbb{Z}$, $f(x) = \begin{cases} \frac{x}{2} & x \text{ is even} \\ -\frac{x+1}{2} & x \text{ is odd} \end{cases}$
   Injective: Yes. Suppose $f(x) = f(y)$. So $f(x)$ is either even or odd. In the first case, take $f(x)$ to be odd. Then $f(x) = -\frac{x+1}{2}$

and $f(y) = -\frac{y+1}{2}$, thus $-\frac{x+1}{2} = -\frac{y+1}{2}$, so clearly $x = y$. In the second case, take $f(x)$ to be even. Then $f(x) = \frac{x}{2}$ and $f(y) = \frac{y}{2}$, thus $\frac{x}{2} = \frac{y}{2}$, and therefore $x = y$.

Surjective: Let $y \in \mathbb{Z}$. If y is odd, then $x = -2y - 1$, so $f(-2y - 1) = -\frac{x+1}{2}$ and thus $f(x) = y$. If y is even, then $x = 2y$, so $f(2y) = \frac{y}{2}$, and clearly $f(x) = y$. So the function is surjective.

6. Let $f : X \to Y$ and $g : Y \to Z$ be bijective functions. Prove that $g \circ f$ is also bijective. Is the converse true?

Proof. Since f and g are bijective, then by definiton they are also surjective. So, for some $x \in X$, $y \in Y$, $z \in Z$, we can say $f(x) = y$, $g(y) = z$. So, we know $z = g(y) = g(f(x)) = g \circ f(x) = g \circ f$. Hence, $g \circ f$ is surjective.

Next, since we know f and g are bijective, then by definiton they are also injective. So, for some $x, y \in X$ we say $g \circ f(x) = g \circ f(y)$. Then, $g(f(x)) = g(f(y))$. Since g is injective, this implies $f(x) = f(y)$. Moreover, f is injective, so $x = y$. Hence, $g \circ f$ is injective.

Thus, we can say that if g, f are bijective, then $g \circ f$ is also bijective.

The converse is not true. The converse is let $g \circ f$ be bijective, then g and f are both bijective. We can show this is not true by constructing two functions, g, f that are not bijective, but $g \circ f$ is bijective. If we take $g : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $g(x, y) = (x)$ and $f : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ and $f(x) = (x, 0)$, then $g \circ f$ is bijective, while g is not bijective, because it is not injective, and f also not bijective, because it is not surjective. ■