WN24

EECS 203 Discussion 6

Modular Arithmetic, Functions

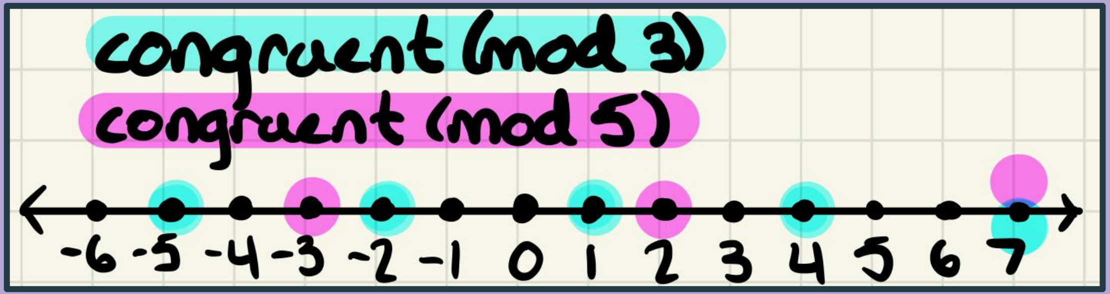
Admin Notes:

- Homework/Groupwork 6 will be due **Mar. 14th**
  - **Don’t forget to match pages!**
  - Please note as soon as you press submit you’ve successfully submitted by the deadline. **You can still match pages** with no rush without adding to your submission time.

Modular Arithmetic

Modular Arithmetic Definitions

- Division Definition
  - **a ≡ b (mod n)** iff **n | (a - b)**
- Remainder Definition
  - **a ≡ b (mod n)** iff **rem(a,n) = rem(b,n)**
- Integer Definition *Useful when working with different mods!
  - **a ≡ b (mod n)** iff there exists integer k such that **a = b + nk**



Modular Addition, Subtraction, and Multiplication

- Addition
  - Given **$a \equiv b \pmod{n}$** and **$c \equiv d \pmod{n}$**, then

    $a + c \equiv b + d \pmod{n}$
- Subtraction
  - Given **$a \equiv b \pmod{n}$** and **$c \equiv d \pmod{n}$**, then

    $a - c \equiv b - d \pmod{n}$
- Multiplication
  - Given **$a \equiv b \pmod{n}$** and **$c \equiv d \pmod{n}$**, then

    $ac \equiv bd \pmod{n}$

Problem:

1. The Mod Operator

Evaluate these quantities:

a) $-17 \bmod 2$

b) $144 \bmod 7$

c) $-101 \bmod 13$

d) $199 \bmod 19$

Problem:

2. Working in Mod

Find the integer a such that

(a) $a \equiv -15 \pmod{27}$ and $-26 \leq a \leq 0$

(b) $a \equiv 24 \pmod{31}$ and $-15 \leq a \leq 15$

(c) $a \equiv 99 \pmod{41}$ and $100 \leq a \leq 140$

Problem:

3. Arithmetic within a Mod

Suppose that a and b are integers, $a \equiv 11 \pmod{19}$, and $b \equiv 3 \pmod{19}$. Find the integer c with $0 \leq c \leq 18$ such that

a) $c \equiv 13a \pmod{19}$.

b) $c \equiv a - b \pmod{19}$.

c) $c \equiv 2a^2 + 3b^2 \pmod{19}$.

d) $c \equiv a^3 + 4b^3 \pmod{19}$.

Problem:

4. Arithmetic in Different Mods $\star$

Suppose that $x \equiv 2 \pmod 8$ and $y \equiv 5 \pmod{12}$. For each of the following, compute the value or explain why it can't be computed.
Hint: Recall that if $a \equiv b \pmod m$ then there exists an integer k such that $a = b + mk$.

(a) $3y \mod 6$

(b) $(x - y) \mod 4$

(c) $xy \mod 24$

Problem:

5. Fast Modular Exponentiation $\star$

Find $a \equiv 5^{20} \pmod{27}$ such that $0 \leq a \leq 26$. In other words, find $5^{20} \mod 27$.

Solution:
$5^{20} \equiv (5^2)^{10} \equiv ((5^2)^2)^5 \equiv (25^5)^2 \equiv ((-2)^5)^2 \equiv (-32)^2 \equiv (-5)^2 \equiv 25 \pmod{27}$

Problem:

6. Extra Practice with Fast Modular Exponentiation

Find each of the following.

a) $9^1 \mod 7$

b) $9^2 \mod 7$

c) $9^9 \mod 7$

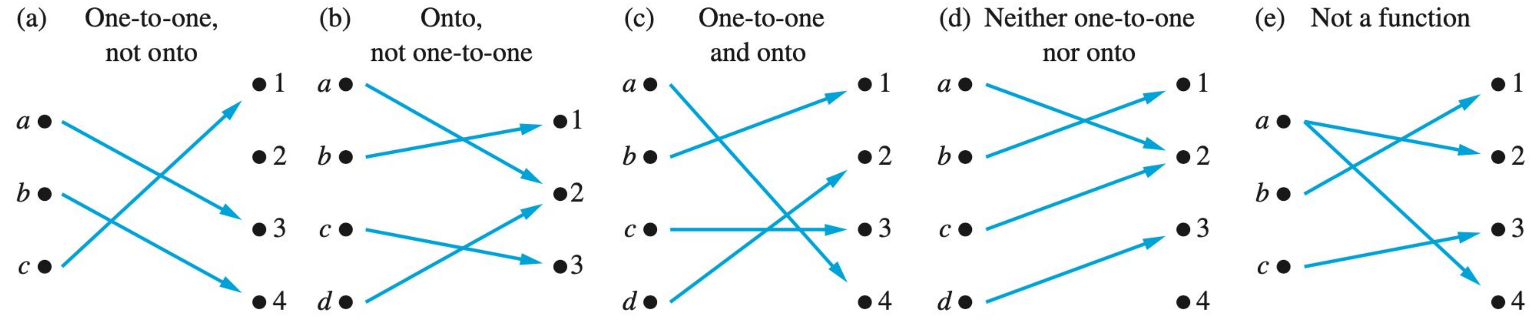
d) $9^{90} \mod 7$

Functions

Onto and One-to-One Functions

*__Bijective:__ onto and one-to-one

- **Function f: A → B:** associates each element of set A to <u>exactly one</u> element in set B
  - **Domain: A**
  - **Codomain: B**
  - **Range of f:** the set of elements in the codomain which are mapped to by an element in the domain, <u>subset of codomain B</u>
- **Onto Function f: A → B:** all elements in B are mapped to by f
- **One-to-One Function f: A → B:** no two elements of A map to the same output in B



Injective (1-1) and Surjective (Onto) Proofs

Suppose that $f : A \to B$.

To show that f is injective Show that if $f(x) = f(y)$ for arbitrary $x, y \in A$, then $x = y$.

To show that f is not injective Find particular elements $x, y \in A$ such that $x \neq y$ and $f(x) = f(y)$.

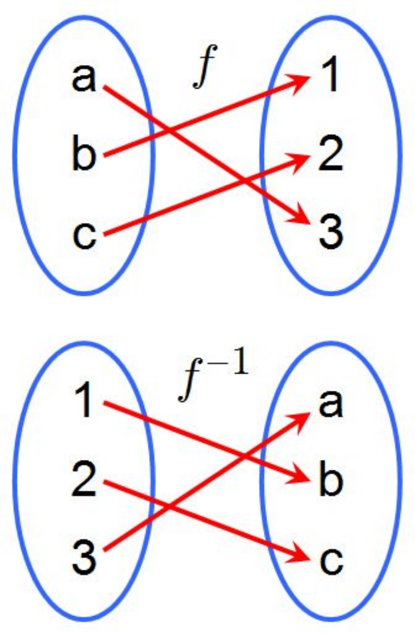
To show that f is surjective Consider an arbitrary element $y \in B$ and find an element $x \in A$ such that $f(x) = y$.

To show that f is not surjective Find a particular $y \in B$ such that $f(x) \neq y$ for all $x \in A$.

More on Functions

- **Function Inverse f^{-1}:** Let f be a **bijection** from set A to set B. The inverse function of f is the function with domain B and codomain A that assigns every element $b \in B$ to the unique element $a \in A$ such that $f(a) = b$. The inverse function of f is denoted by f^{-1}.

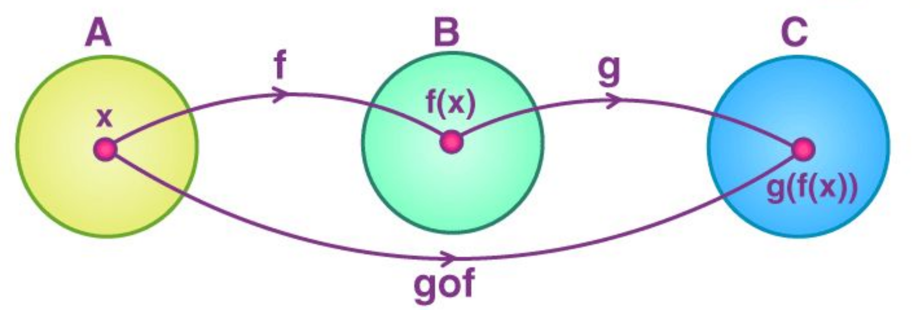
  $f^{-1}(b) = a$ if and only if $f(a) = b$.



- **Function Composition $f \circ g$:** Let g be a function from the set A to the set B and let f be a function from the set B to the set C. The composition of the functions f and g, denoted for all $a \in A$ by $f \circ g$, is defined by

  $$(f \circ g)(a) = f(g(a))$$

- **Adding and Multiplying Functions:**
  - $(f_1 + f_2)(x) = f_1(x) + f_2(x)$
  - $(f_1 f_2)(x) = f_1(x)\, f_2(x)$



Problem:

7. One-to-One and Onto

Give an explicit formula for a function from the set of integers to the set of positive integers $f : \mathbb{Z} \to \mathbb{Z}^+$ that is:

a) one-to-one, but not onto

b) onto, but not one-to-one

c) one-to-one and onto

d) neither one-to-one nor onto

Problem:

8. Bijections

Determine whether each of these functions is a bijection from $\mathbb{R}$ to $\mathbb{R}$. Briefly discuss why or why not. If it is bijective, state the inverse function.

(a) $f(x) = 2x + 1$

(b) $f(x) = x^2 + 1$

(c) $f(x) = x^3$

(d) $f(x) = (x^2 + 1)/(x^2 + 2)$

(e) $f(x) = x^2 + x^3$

Problem:

9. One-to-One and Onto Proofs

Prove or disprove the following.

a) $f : \mathbb{R} \longrightarrow \mathbb{R}, f(x) = \frac{1}{x^2+1}$ is onto

b) $f : \mathbb{R} \longrightarrow \mathbb{R}, f(x) = |3x + 1|$ is one-to-one

c) $f : \mathbb{R} \longrightarrow \mathbb{R}, f(x) = ax + b$ where $a \neq 0$, is a bijection.

Problem:

10. Function Composition

Consider the following two functions:

- $f : \mathbb{Z} \to \mathbb{Q},\ f(x) = \frac{x+1}{3}$
- $g : \mathbb{Z}^+ \to \mathbb{Z}^+,\ g(x) = \frac{x(x+1)}{2}$

For each function, find it if it exists. If it does not, explain why.

a) $f \circ g$

b) $g \circ f$

c) f^{-1}

d) g^{-1}