EECS 203: Discrete Mathematics
Winter 2024
Discussion 6 Notes

1 Definitions

- **Modular Equivalence Definition:**
- **Modular Addition, Subtraction, Multiplication Properties:**
- **Remainder Mod**
- **Function** $f : A \to B$:
- **Domain:**
- **Codomain:**
- **Range:**
- **Onto:**
- **One-to-One:**
- **Bijection:**
- **Function Inverse** f^{-1}:
- **Function Composition** $f \circ g$:
- **Adding and Multiplying Functions:**

1. The Mod Operator

Evaluate these quantities:

a) $-17 \bmod 2$

b) $144 \bmod 7$

c) $-101 \bmod 13$

d) $199 \bmod 19$

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 $100 \leq a \leq 140$

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

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) $xy \mod 24$

5. Fast Modular Exponentiation $\star$

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

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) $9^{90} \mod 7$

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

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

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.

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}