EECS 203: Discrete Mathematics
Winter 2024
FoF Worksheet 6

1 Modular Arithmetic

Modular Equivalence: Let a and b be integers and m be a positive integer. a and b are equivalent (or congruent) modulo m if and only if there is an integer k such that $a = b + km$. This is notated $a \equiv b \pmod{m}$.

Mod expression: The expression "$a \bmod m$" evaluates to the smallest natural number b such that $a \equiv b$. That is, it is the integer b such that $a \equiv b \pmod{m}$ and $0 \leq b < m$

Modular Addition, Subtraction, Multiplication: Given that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then:

- $a + c \equiv b + d \pmod{m}$
- $a - c \equiv b - d \pmod{m}$
- $ac \equiv bd \pmod{m}$

In other words, if we have a modular equivalence, we can add, subtract, or multiply equivalent quantities to each side

1.1 The Mod Operator

Evaluate these quantities:

a) $-17 \bmod 2$

b) $144 \bmod 7$

c) $-101 \bmod 13$

d) $199 \bmod 19$

1.2 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 $100 \leq a \leq 140$

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

1.4 Arithmetic in Different Mods

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) $3y \bmod 6$

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

(c) $xy \bmod 24$

1.5 Fast Modular Exponentiation

Use the fast exponentiation algorithm from lecture to find 5^{20} mod 27. Remember to reduce as you go; your work should not include any numbers greater than 50, or less than -50.

1.6 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) $9^{90} \mod 7$

2 Functions

Function: A mapping from elements of one set (domain) to elements of another set (codomain), where each element in the domain maps to exactly one element of the codomain. This is notated as $f : A \to B$, where A is the domain and B is the codomain

Onto: A function is onto (surjective) iff every element in the codomain is mapped to by at least one element in the domain.

$$f : A \to B \text{ is onto } \longleftrightarrow \forall b \in B, \exists a \in A, f(a) = b$$

One-to-One: A function is one-to-one (injective) iff every element in the codomain is mapped by at most one element in the domain.

$$f : A \to B \text{ is one-to-one } \longleftrightarrow \forall a_1, a_2 \in A, f(a_1) = f(a_2) \to a_1 = a_2$$

Bijection: A function is bijective iff it is both one-to-one and onto. That is, every element in the codomain is mapped to by exactly one element in the domain

2.1 Bijection Identification

Determine whether each of these functions from $\mathbb{R}$ to $\mathbb{R}$ is a bijection. 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) $f(x) = x^2 + x^3$

2.2 One-to-One and Onto Proofs

Prove or disprove the following.

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

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

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

2.3 Function Construction

Give an explicit formula for a function with domain $\mathbb{Z}$ and codomain $\mathbb{N}$ which is:

a) onto, but not one-to-one

b) neither one-to-one nor onto

c) one-to-one and onto

d) one-to-one, but not onto

2.4 Composition

Define $f : \mathbb{N} \to \mathbb{Z}$ with $f(x) = x - 2$ and $g : \mathbb{N} \to \mathbb{Z}^+$ with $g(x) = |x| + 1$. Determine if each of the following functions exist. If it does, give an explicit formula for it. If it does not, explain why not.

(a) $f \circ g$

(b) $g \circ f$

(c) f^{-1}

(d) g^{-1}