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) $199 \bmod 19$

Solution: Express a in (a mod m) as $a = mk + r$ where k is an integer (the quotient when a is divided by m), and r is a positive integer (the remainder when a is divided by m). r is the output of the mod operator.

a) Since $-17 = 2 \cdot (-9) + 1$, the remainder is 1.
Hence $-17 \bmod 2 = 1$
Note that we do not write $-17 = 2 \cdot (-8) - 1$ with $-17 \bmod 2 = -1$ since we want a positive remainder.

b) Since $144 = 7 \cdot 20 + 4$, the remainder is 4.
$144 \bmod 7 = 4$

c) Since $-101 = 13 \cdot (-8) + 3$, the remainder is 3.
$-101 \bmod 13 = 3$

d) Since $199 = 19 \cdot 10 + 9$, the remainder is 9.
$199 \bmod 19 = 9$

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 $100 \leq a \leq 140$

Solution: $(km) \equiv 0 \pmod{m}$. Hence $a + km \equiv a \pmod{m}$. Thus to get the solution in the right range, either add or subtract km, where k is an integer.

1. -15, since it is already within the required range.
2. $24 \equiv 24 - 31 \equiv -7 \pmod{31}$
3. $99 \equiv 99 + 41 \equiv 140 \pmod{41}$

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

Solution:

a) $13 \cdot 11 = 143 \equiv 10 \pmod{19}$

b) $11 - 3 \equiv 8 \pmod{19}$

c) $2 \cdot 11^2 + 3 \cdot 3^2 = 269 \equiv 3 \pmod{19}$

d) $11^3 + 4 \cdot 3^3 = 1439 \equiv 14 \pmod{19}$

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) $xy \bmod 24$

Solution:

(a) Since 12 is a multiple of 6, $y \equiv 5 \pmod{12}$ can be rewritten as, $y = 12k + 5 = 6(2k) + 5$, for some integer k. So $y \equiv 5 \pmod 6$and $3y \equiv 15 \equiv 3 \pmod 6$.
Alternatively, $y = 5{+}12k$ for some integer k, and thus that $3y = 15{+}36k = 15{+}6(6k)$. Therefore $3y \equiv 15 \equiv 3 \pmod 6$.

(b) Since 8 and 12 are both multiples of 4, we know $x \equiv 2 \pmod 4$ and $y \equiv 5 \equiv 1 \pmod 4$. Thus, $x - y \equiv 2 - 1 \equiv 1 \pmod 4$.
Alternatively, $x = 2 + 8n$ for some integer n and $y = 5 + 12m$ for some integer m, and thus that $x - y = -3 + 8n - 12m = -3 + 4(2n - 3m)$. Therefore $x - y \equiv -3 \equiv 1 \pmod 4$.

(c) $xy \pmod{24}$ can't be computed. Note that since $x = 2 + 8n$ for some integer n and $y = 5 + 12m$ for some integer m, $xy = (2 + 8n)(5 + 12m) = 10 + 40n + 24m + 96mn$. Since $40n$ cannot be written as a multiple of 24, we cannot write xy in mod 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.

Solution: $5^{20} \equiv (5^{10})^2$
$5^{10} \equiv (5^5)^2$
$5^5 \equiv ((5^2)^2 * 5) \equiv 25 * 5 \equiv (-2) * 5 \equiv 4 * 5 \equiv 20$
Then since $5^5 \equiv 20$ we can find $5^{10} \equiv (5^5)^2 \equiv 20^2 \equiv (-7)^2 \equiv 49 \equiv 22$
Then $5^{20} \equiv (5^{10})^2 \equiv 22^2 \equiv (-5)^2 \equiv 25 \pmod{27}$

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) $9^{90} \mod 7$

Solution:

a) $9 \equiv 2 \pmod 7$

b) $9^2 \equiv 2^2 \equiv 4 \pmod 7$

c) $9^9 \equiv 2^9 \equiv 2 \cdot 2^8 \equiv 2 \cdot ((2^2)^2)^2 \equiv 2 \cdot (4^2)^2 \equiv 2 \cdot 16^2 \equiv 2 \cdot 2^2 \equiv 2 \cdot 4 \equiv 1 \pmod 7$

d) $9^{90} \equiv (9^9)^{10} \equiv 1^{10} \equiv 1 \pmod 7$

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

Solution:

(a) Yes, f is both one-to-one and onto. $f^{-1}(x) = \dfrac{x-1}{2}$

(b) No (not one-to-one or onto). It is not one to one as take $f(1) = (1)^2+1 = (-1)^2+1 = f(-1)$. It is not onto as we cannot obtain negative numbers or zero.

(c) Yes, $f^{-1}(x) = x^{1/3} = \sqrt[3]{x}$

(d) No (onto but not one-to-one). We can see it is not one-to-one because $f(0) = f(-1) = 0$

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.

Solution:

a) f is not onto. To disprove, we can provide a counterexample. There is no value that will make $\frac{1}{x^2+1} = 2$.

$$\frac{1}{x^2 + 1} = 2$$

$$2x^2 + 2 = 1$$

It is easy to see that $2x^2 + 2$ will never be less than 2, and therefore never equal to 1. There are many other possible counterexamples as well; any value that is not in the range of $(0, 1]$ will not get mapped to.

b) f is not one-to-one. To disprove, we can give a counterexample to show two values from the domain that are not equal map to the same value in the codomain. One

possible counterexample is that $x = 1$ and $x = -\frac{5}{3}$ map to the same value.

$$x = 1$$
$$f(1) = |3(1) + 1|$$
$$f(1) = |4|$$
$$f(1) = 4$$

$$x = -5/3$$
$$f(-5/3) = |3(-5/3) + 1|$$
$$f(-5/3) = |-5 + 1|$$
$$f(-5/3) = |-4|$$
$$f(-5/3) = 4$$

Therefore, $f(x)$ is not one-to-one.

c) f is a bijection. To prove this, we have to prove that it's both one-to-one and onto.

One-to-one:
Suppose that $f(x) = f(y)$. Then,
$ax + b = ay + b$
$ax = ay$
Because we know that $a \neq 0$,
$x = y$
Thus, $f(x) = f(y) \rightarrow x = y$.
This proves that the function is one-to-one.

Onto:
Consider an arbitrary $c \in \mathbb{R}$ (the codomain)
Let $x = \frac{c-b}{a}$.
Note that this value is a real number since $a \neq 0$. Then,

$$\begin{aligned} f(x) &= ax + b \\ &= a\frac{c-b}{a} + b \\ &= c - b + b \\ &= c \end{aligned}$$

Thus, for any $c \in \mathbb{R}$, there is a value in the domain that maps to it through f, and so f must be onto. ($\forall y \in \mathbb{R}\ \exists x \in \mathbb{R}$ ST $f(x) = y$)

Thus, since the function is onto and one-to-one, its 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

Solution: There are many valid answers, but here are some examples. As a reminder, if x is negative, then $-x$ will be a positive number.

a) $a(x) = |x|$

b) $b(x) = x^2$

c) $c(x) = -2x - 1$ when $x < 0$ and $c(x) = 2x$ when $x \geq 0$

d) $d(x) = c(x) + 2$

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}

Solution:

(a) This does exist. $(f \circ g) : \mathbb{N} \to \mathbb{Z}$ with $(f \circ g)(x) = (|x| + 1) - 2 = |x| - 1$

(b) This does not exist. Notice that $f(0) = -2$, but -2 is not in the domain of g (note that we could plug -2 into the formula and get an answer, but it isn't well defined since the domain does not include it)

(c) This does not exist because the function is not onto, since -3 (or anything less) is not mapped to.

(d) This does exist. $g^{-1}(x) = x - 1$. We must prove that for all $x \in \mathbb{N}$ and $y \in \mathbb{Z}^+$, $g(x) = y$ iff $g^{-1}(y) = x$.

Let $x \in \mathbb{N}, y \in \mathbb{Z}^+$ such that $g(x) = y$. Then $g^{-1}(y) = g^{-1}(|x| + 1) = |x| + 1 - 1$. Since $x \in \mathbb{N}$, then $|x| = x$, so $g^{-1}(y) = x$.

Let $x \in \mathbb{N}, y \in \mathbb{Z}^+$ such that $g^{-1}(y) = x$. Then $g(x) = g(y - 1) = |y - 1| + 1$. Since $y \in \mathbb{Z}^+$, then $y - 1 \in \mathbb{N}$, so $|y - 1| = y - 1$, so $g(y - 1) = y - 1 + 1 = y$.