EECS 203: Discrete Mathematics
SEMESTER
Discussion 7 Notes

1 Definitions

- **Divisibility:**
- **Modular Equivalence Definition:**
- **Modular Addition, Subtraction, Multiplication Properties:**
- **Function** $f : A \to B$:
- **Domain:**
- **Codomain:**
- **Range:**
- **Onto:**
- **One-to-One:**
- **Bijection:**
- **Function Inverse** f^{-1}:

Solution:

- **Divisibility:** If a and b are integers with $a \neq 0$, we say that a divides b if there is an integer c such that $b = ac$, or equivalently, if $\frac{b}{a}$ is an integer. The notation $a|b$ denotes that a divides b. This is the same as saying that the remainder is zero when b is divided by a. Examples: $3|6$, $10|100$
- **Modular Equivalence Definitions (All Equivalent)**:
  *Note: "iff" stands for if and only if and denotes that two statements are logically equivalent.
  i. **Definition in terms of equals:**
     $a \equiv b \pmod{n}$ iff there is an integer k such that $a = b + kn$

ii. **Division Definition:**
"a is congruent to b modulo n if and only if n divides $(a-b)$"
$a \equiv b (\text{mod } n) \quad \text{iff} \quad n | (a-b)$
*Note: $|$ means divides, where "$a|b$" says b is a multiple of a.

iii. **Remainder Definition:** "a is congruent to b modulo n if and only if the remainder of a divided by n is equal to the remainder of b divided by n"
$a \equiv b (\text{mod } n)$ iff $\text{rem}(a, n) = \text{rem}(b, n)$
*Note: $\text{rem}(a, n)$ denotes the remainder when a is divided by n

- **Modular Addition, Subtraction, Multiplication Properties**:
Given $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then $a + c \equiv b + d \pmod m$.
Given $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then $a - c \equiv b - d \pmod m$.
Given $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then $ac \equiv bd \pmod m$

- **Function** $f : A \to B$: A function f is a relation between two sets, say A and B, that associates each element of set A to exactly one element from the set B. The set A and set B are respectively called the domain and codomain of f. The range of f is the set of all elements in the codomain which are mapped to by an element in the domain.

- **Domain:** The domain of a function is the set of elements that act as the input of a function.

- **Codomain:** The codomain of a function the set of elements that can act as the output of a function (even if it never actually outputs some of them).

- **Range:** The range of a function is the set of elements in the codomain that get mapped to at least once by the function.

- **Onto:** A function f from A to B is called onto, or a surjection, if and only if for every element $b \in B$, there is an element $a \in A$ with $f(a) = b$. A function f is called surjective if it is onto.

- **One-to-One:** A function f is said to be one-to-one, or an injection, if and only if $f(a) = f(b)$ implies that $a = b$ for all a and b in the domain of f. A function is said to be injective if it is one-to-one.

- **Bijection:** A function f is called a bijection (or one-to-one correspondence) if it is both one-to-one and onto.

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

2 Exercises

1. The Mod Operator $\star$

Evaluate these quantities:

a) $-17 \text{ mod } 2$

b) $144 \text{ mod } 7$

c) $-101 \text{ mod } 13$

d) $199 \text{ mod } 19$

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 $-17 \text{ mod } 2 = 1$
Note that we do not write $-17 = 2 \cdot (-8) - 1$ with $-17 \text{ mod } 2 = -1$ since we're wanting a positive remainder.

b) Since $144 = 7 \cdot 20 + 4$, the remainder is 4.
$144 \text{ mod } 7 = 4$

c) Since $-101 = 13 \cdot (-8) + 3$, the remainder is 3.
$-101 \text{ mod } 13 = 3$

d) Since $199 = 19 \cdot 10 + 9$, the remainder is 9.
$199 \text{ mod } 19 = 9$

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. $99 \equiv 99 + 41 \equiv 140 \pmod{41}$

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 $0 \le c \le 18$ such that

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

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

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

Solution:

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

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

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

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: Consider the integer definition of modular arithmetic.

(a) $3y \mod 6$

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

(c) $xy \mod 24$

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.

5. One-to-One and Onto $\star$

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

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) The function $f(x)$ with $f(x) = 3x + 1$ when $x \geq 0$ and $f(x) = -3x + 2$ when $x < 0$.

b) $f(x) = |x| + 1$

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

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

6. Bijections $\star$

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

Solution:

(a) Yes, $f^{-1}(x) = \dfrac{x-1}{2}$

(b) No (not one-to-one or onto: $f(1) = f(-1)$, $f(x) \neq 0$)

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

(d) No (not one-to-one or onto: $f(1) = f(-1)$, $f(x) \neq 0$)

(e) No (onto but not one-to-one: $f(0) = f(-1) = 0$)

7. 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.

Solution:

a) To disprove this, 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) To disprove this, 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) 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, $f(x) = f(y) \to x = y$.
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.