WN24

EECS 203 Discussion 6

Modular Arithmetic, Functions

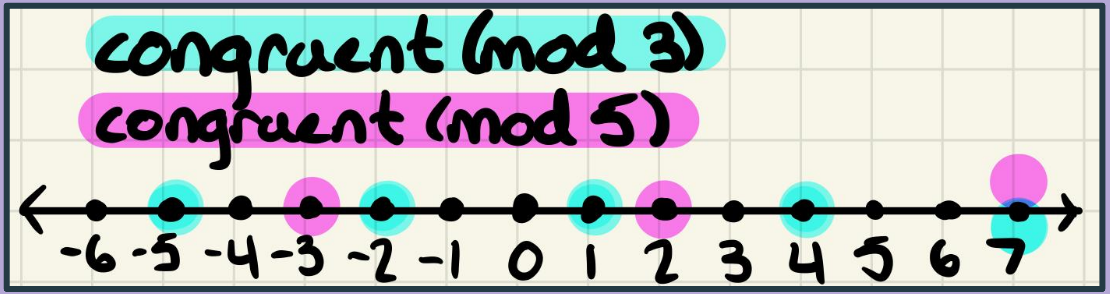
Admin Notes:

- 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
  - **$a \equiv b \pmod{n}$** iff **$n \mid (a - b)$**
- Remainder Definition
  - **$a \equiv b \pmod{n}$** iff **rem(a,n) = rem(b,n)**
- Integer Definition *Useful when working with different mods!
  - **$a \equiv b \pmod{n}$** 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) $199 \bmod 19$

Solution:

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 ($a \bmod m$) 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.
$199 \bmod 19 = 9$

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 $100 \leq a \leq 140$

Solution:

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

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

Solution:

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

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) $xy \mod 24$

Solution:

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) $3y \mod 6$

(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.

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

Solution:

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

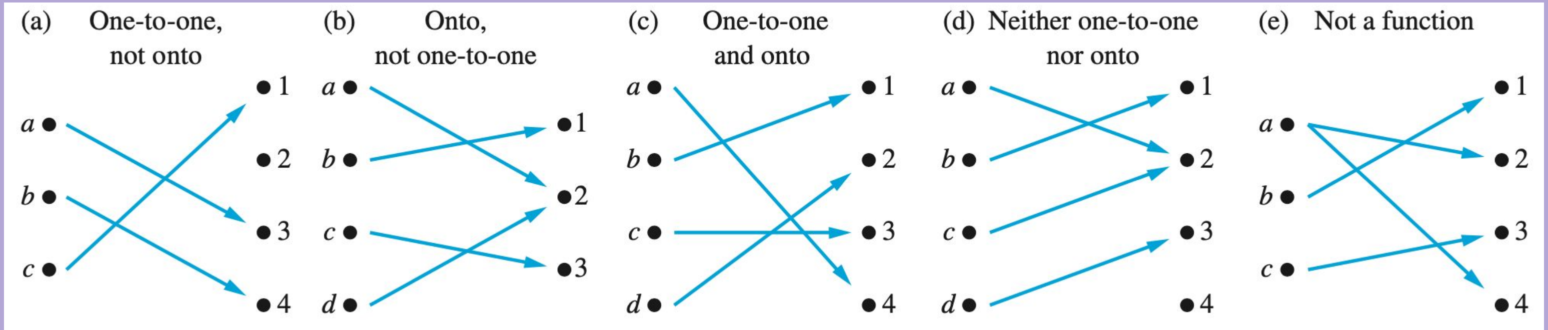
d) $9^{90} \equiv (9^9)^{10} \equiv 1^{10} \equiv 1 \pmod 7$

Functions

Onto and One-to-One Functions

*__Bijective:__ onto and one-to-one

- **Function f: A → B:** associates each element of set A to exactly one 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, subset of codomain B
- **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

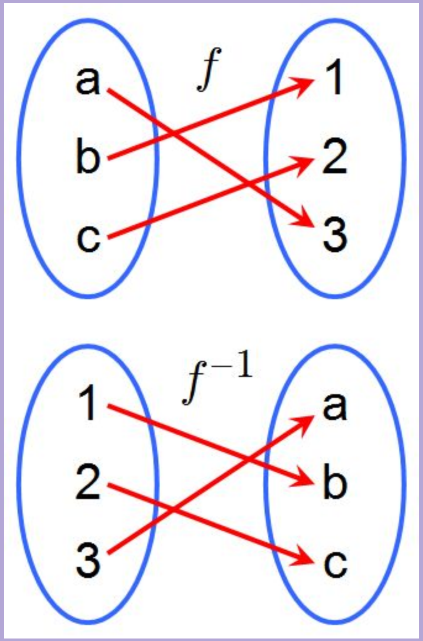
- **Function Inverse f^{-1}:** Let f be a **bijection** from set A to set B. The inverse function of f is the function with domain B and codomain A that assigns every element $b \in B$ to the unique element $a \in A$ such that $f(a) = b$. The inverse function of f is denoted by f^{-1}.

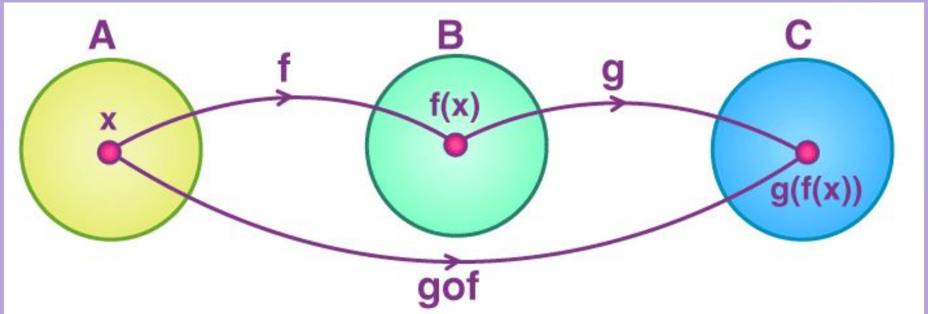
  $$f^{-1}(b) = a \text{ if and only if } f(a) = b.$$

- **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

Solution:

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

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

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

Solution:

Solution:

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

(b) No. 0 in the codomain isn't mapped to, and all numbers greater than 1 are mapped to twice, so it is neither one-to-one nor onto.

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

(d) No. Numbers between $\frac{1}{2}$ and 1 in the codomain are mapped to twice, and any number outside of that range besides $\frac{1}{2}$ isn't mapped to at all, so it is neither one-to-one nor onto.

(e) No. It is onto, but not one-to-one. For example, 0 in the codomain is mapped to twice, by 0 and -1.

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.

Solution:

Solution:

a) f is not onto. To disprove the original statement, 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.

Solution:

b) f is not one-to-one. To disprove the original statement, 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.

Solution:

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.

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}

Solution:

Solution:

a) $f \circ g : \mathbb{Z} \to \mathbb{Q}$
$(f \circ g)(x) = \frac{1}{3}(\frac{x(x+1)}{2} + 1) = \frac{x(x+1)+2}{6} = \frac{x^2+x+2}{6}$

b) $g \circ f$ does not exist, because the codomain of f ($\mathbb{Q}$) is not the same set as the domain of g ($\mathbb{Z}$).

c) f^-1 does not exist, because f is not onto (consider $\frac{1}{2}$ in the codomain, which isn't mapped to).

d) g^{-1} does not exist, because g is not onto (consider 2 in the codomain, which isn't mapped to).