Math 220
Section 108
Lecture 19

15th November 2022

Source: `https://personal.math.ubc.ca/~PLP/auxiliary.html`

Modular Arithmetic

6. Given $n \in \mathbb{N}$, let $[a]_n$ denote the equivalence class of a under the relation "congruence modulo n" on the integers. We define the **multiplicative inverse** of $[a]_n$ to be some $[b]_n$ such that $[a]_n[b]_n = [1]_n$, if it exists.

Multiplicative inverses are nice because they allow us to perform "dividing by $[a]_n$" by multiplying by the multiplicative inverse of $[a]_n$.

(a) Write down the multiplication table for the equivalence classes of the relation "congruence modulo 5". Show that every equivalence class $[k]_5$, where $k \not\equiv 0 \pmod 5$, has a multiplicative inverse.

$$\boxed{[a]_n \cdot [b]_n = [a \cdot b]_n}$$

	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[0]_5$	•	•	•	•	•
$[1]_5$	•	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[2]_5$	•	$[2]_5$	$[4]_5$	$[1]_5$	$[3]_5$
$[3]_5$	•	$[3]_5$	$[1]_5$	$[4]_5$	$[2]_5$
$[4]_5$	•	$[4]_5$	$[3]_5$	$[2]_5$	$[1]_5$

So every equivalence class $[k]_5$ has a multiplicative inverse

(Continued)

(Continued) 6.(a) Write down the multiplication table for “congruence mod 5”. Show that every $[k]_5$, where $k \not\equiv 0 \pmod 5$, has a multiplicative inverse.

(Continued)

(Continued) We see from part (a) that multiplicative inverses of $[1]_5, [2]_5, [3]_5, [4]_5$ are $[1]_5, [3]_5, [2]_5, [4]_5$ respectively.

(b) Prove that if $n \in \mathbb{N}$ is prime, then every nonzero integer modulo n, i.e. $[a]_n$ ~~that~~ does have a multiplicative inverse.

Hint: Bezout's lemma.

$ax + by = \gcd(a,b) = 1$

Now, n is a prime, since $[a]_n \neq [0]_n$ so, $n \nmid a$ & hence

$\gcd(n, a) = 1$

So, $\exists x, y \in \mathbb{Z}$ $nx + ay = \gcd(n,a) = 1$

So, $nx = 1 - ay$

or $n \mid (1 - ay)$

or $[1]_n = [ay]_n$

So, $[1]_n = [an] \cdot [y]_n$

Hence every non zero modulo n, i.e $[a]_n$ does have a multiplicative inverse.

(Continued)

(Continued) 6. (b) Prove that if $n \in \mathbb{N}$ is prime, then every nonzero integer modulo n, i.e. $[a]_n$ that does have a multiplicative inverse.

Functions

Functions

A function from a set A to a set B is something that for each input $a \in A$, it provides exactly one output $b \in B$.

Examples & non-examples:

- $y = x^2$ is a function from $\mathbb{R}$ to $\mathbb{R}$.

- $y = 1/x$ is <u>not</u> a function from $\mathbb{R}$ to $\mathbb{R}$.
  - has no output for 0
  - we can define a fnct from $R - \{0\}$ to R

- The unit circle $\{(x, y) \mid x^2 + y^2 = 1\}$ is <u>not</u> a function from $\mathbb{R}$ to $\mathbb{R}$.
  - $x=0$, $y = +1$ & -1 so, no unique output

Functions - formal definitions

Definition (Definition 10.2.1 of PLP)

For non-empty sets A and B, a **function** f from A to B, written $f : A \to B$, is a subset of $A \times B$ with two further properties

- for every $a \in A$ there is some $b \in B$ so that $(a, b) \in f$,
- if $(a, b) \in f$ and $(a, c) \in f$, then $b = c$.

If $(a, b) \in f$, then we write $f(a) = b$ and we call b the **image** of a.

Definition

We call A the **domain** of f, and B the **co-domain**.
The **range** of f is set the of elements in B that are mapped to by f:

$$\mathrm{range}(f) = \{b \in B \mid \exists a \in A \text{ s.t. } f(a) = b\}.$$

Example: For the functions below, what are their domain, co-domain, & range?

	domain	co-domain	range
$f = \{(x, y) \in \mathbb{R} \times \mathbb{R} : y = x^2\}$ and	$\mathbb{R}$	$\mathbb{R}$	$[0, \infty)$
$g = \{(x, y) \in (\mathbb{R} - \{0\}) \times \mathbb{R} : y = 1/x\}$.	$\mathbb{R} - \{0\}$	$\mathbb{R}$	$\mathbb{R} - \{0\}$

Functions

1. For which values of $a, b \in \mathbb{N}$ does the set $S = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : ax + by = 6\}$ define a function?

(Continued)

(Continued) 1. For which values of $a, b \in \mathbb{N}$ does the set $S = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : ax + by = 6\}$ define a function?

2. Is the set $\theta = \{((x, y), (5y, 4x, x + y)) \in \mathbb{R}^2 \times \mathbb{R}^3 : x, y \in \mathbb{R}\}$ a function? If so, are its co-domain and range equal?

(a) Yes, any (x,y) in $\mathbb{R}^2$ has a unique o/p $(5y, 4x, x+y)$ in $\mathbb{R}^3$

domain $\to \mathbb{R}^2$

co-domain $\to \mathbb{R}^3$

(b) No, the co-domain is $\mathbb{R}^3$

Consider $(5,4,z) \in \mathbb{R}^3$ for $z \in \mathbb{R}$,

If it is in range(θ), it must be of the form $(5y, 4x, x+y)$.

So we must have that $y = 1$ & $x = 1$. So, then z has to be $x + y = 2$.

So, $(5,4,3) \notin$ range (θ)

$\blacksquare$

(Continued)

(Continued) 2. Is the set $\theta = \{((x, y), (5y, 4x, x + y)) \in \mathbb{R}^2 \times \mathbb{R}^3 : x, y \in \mathbb{R}\}$ a function? If so, are its co-domain and range equal?

Old Final question

3. Suppose that $f : A \to B$ is a function and let C be a subset of A.

   a. Prove that $f(A) - f(C) \subseteq f(A - C)$.

   b. Find a counterexample for $f(A - C) \subseteq f(A) - f(C)$.

Hint: Think about for which type of functions part (b) fails.

(Continued)

(Continued) 3. Suppose that $f : A \to B$ is a function and let C be a subset of A.

a. Prove that $f(A) - f(C) \subseteq f(A - C)$.
b. Find a counterexample for $f(A - C) \subseteq f(A) - f(C)$.

Functions

4. Let $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ be a function defined as $f(a, b) = 4a + 6b$. Explicitly describe the set $S =$range(f). Prove your answer.

(Continued)

(Continued) 4. Let $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ be a function defined as $f(a, b) = 4a + 6b$. Explicitly describe the set $S =$range(f). Prove your answer.

Functions (if time)

5. A function $f : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ is defined as $f(n) = (2n+1, n+2)$. Verify whether this function is injective and whether it is surjective.

(Continued)

(Continued) 5. A function $f : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ is defined as $f(n) = (2n+1, n+2)$. Verify whether this function is injective and whether it is surjective.