PROJECTED WRITTEN NOTES FROM THE M325K LECTURE ON TUESDAY, APRIL 9, 2024, ON SECTIONS 7.1 and 7.2: FUNCTIONS IN GENERAL and One-to-One Functions and Onto FUNCTIONS

CLASS #23

Review of the RSA Crypto-System

ENCRYPTION: Two ENCRYPTION KEYS: N, e,

where $N = pq$, a product of two primes numbers

e is a positive integer such that

$$\gcd(e, (p-1)(q-1)) = 1.$$

The ENCRYPTION FORMULA:

$$C = (M^e \bmod pq)$$

M = plaintext

C = Ciphertext

Decryption: Two Decryption Keys: N, d

N = the same as above, $N = pq$

d is a positive inverse of e modulo $(p-1)(q-1)$,

That is, $ed \equiv 1 \pmod{(p-1)(q-1)}$

The Decryption Formula:

$$M = (C^d \bmod pq)$$

Problem: An RSA Crypto-system is being used to Encrypt messages, using $N = 713 = (23)(31)$ and $e = 43$.

Prove that $d = 307$ is a valid decryption key to decrypt ciphertext produced by the above system.

Soln: We need to show that d is an inverse of e modulo $(p-1)(q-1)$,

i.e. that $ed \equiv 1 \pmod{(22)(30)}$

$\uparrow \quad \uparrow$

$(p-1) \quad (q-1)$

$(22)(30) = 660$

We need to show that $d = 307$ is a $\pmod{660}$ inverse of $e = 43$.

We need to show that $(43)(307) \equiv 1 \pmod{660}$

$(43)(307) = (660)(20) + 1$,

So $(43)(307) \equiv 1 \pmod{660}$ by Thm 8.4.1.

So $d = 307$ is a $\pmod{660}$ inverse of $e = 43$.

$\therefore d = 307$ is a valid decryption key, here.

Functions

Let f be a function from set X to set Y.

$f: X \to Y$. X is the Domain of f

Y is the Co-domain of f

Ex: Let $X = \mathbb{R}$ and $Y = \mathbb{R}$.

Define $f: \mathbb{R} \to \mathbb{R}$ by Rule:

for all $x \in \mathbb{R}$, $f(x) = x^2$.

For $x = 3$, $f(x) = f(3) = 9 = 3^2$.

$f(-2) = 4$

The Domain of f is $(-\infty, \infty) = \mathbb{R}$

The Co-Domain of f is $(-\infty, \infty)$

The Range of f $= \{ y \in \mathbb{R} \mid \exists x \in X \text{ with } f(x) = y \}$

The Range of f $= \{ y \in \mathbb{R} \mid y \geq 0 \}$

$= [0, \infty)$

Note: -16 is in the Co-Domain of f

-16 is not in the Range of f

p.294

p.295

• Definition

A **function f from a set X to a set Y**, denoted $f: X \to Y$, is a relation from X, the **domain**, to Y, the **co-domain**, that satisfies two properties: (1) every element in X is related to some element in Y, and (2) no element in X is related to more than one element in Y. Thus, given any element x in X, there is a unique element in Y that is related to x by f. If we call this element y, then we say that "f sends x to y" or "f maps x to y" and write $x \xrightarrow{f} y$ or $f: x \to y$. The unique element to which f sends x is denoted

$f(x)$	and is called	**f of x**, or **the output of f for the input x**, or **the value of f at x**, or **the image of x under f**.

The set of all values of f taken together is called the *range of f* or the *image of X under f*. Symbolically,

$$\textbf{range of } f = \textbf{image of } X \textbf{ under } f = \{y \in Y \mid y = f(x), \text{ for some } x \text{ in } X\}.$$

Given an element y in Y, there may exist elements in X with y as their image. If $f(x) = y$, then x is called **a preimage of y** or **an inverse image of y**. The set of all inverse images of y is called *the inverse image of y*. Symbolically,

$$\textbf{the inverse image of } y = \{x \in X \mid f(x) = y\}.$$

Caution! Use $f(x)$ to refer to the value of the function f at x. Generally avoid using $f(x)$ to refer to the function f itself.

In some mathematical contexts, the notation $f(x)$ is used to refer both to the value of f at x and to the function f itself. Because using the notation this way can lead to confusion, we avoid it whenever possible. In this book, unless explicitly stated otherwise, the symbol $f(x)$ always refers to the value of the function f at x and not to the function f itself.

The concept of function was developed over a period of centuries. A definition similar to that given previously was first formulated for sets of numbers by the German mathematician Lejeune Dirichlet (DEER-ish-lay) in 1837.

Stock Montage

Johann Peter Gustav Lejeune Dirichlet (1805–1859)

Arrow Diagrams

Recall from Section 1.3 that if X and Y are finite sets, you can define a function f from X to Y by drawing an arrow diagram. You make a list of elements in X and a list of elements in Y, and draw an arrow from each element in X to the corresponding element in Y, as shown in Figure 7.1.1.

This arrow diagram does define a function because

1. Every element of X has an arrow coming out of it.
2. No element of X has two arrows coming out of it that point to two different elements of Y.

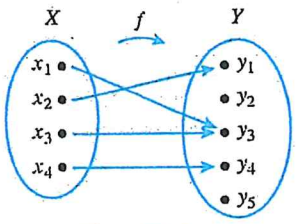
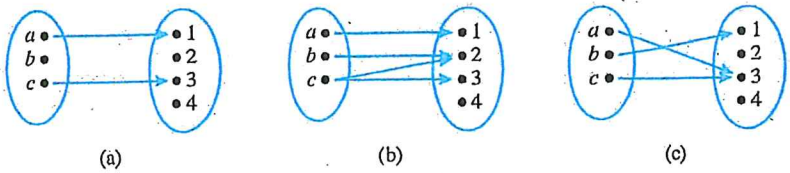


Figure 7.1.1

Example 7.1.1 Functions and Nonfunctions

Which of the arrow diagrams in Figure 7.1.2 define functions from $X = \{a, b, c\}$ to $Y = \{1, 2, 3, 4\}$?



(a) (b) (c)

Figure 7.1.1

4

Requirements for Defining a Function

Requirements for Defining a Function:

To define a function $g : A \to B$, one must:

1) Specify the Domain set A precisely.

2) Specify the Co-domain set B precisely.

3) Specify (by formula or by describing a process) the method for determining $g(z)$, $\forall\ z \in A$ (the Domain set)

Note: Parts 1) and 2) are accomplished by using the phrase "Define function $g : A \to B$" as long as it is clear what particular sets A and B are.

Example 1: The following correctly defines a function named " T ":
" The function $T: \mathbb{Z} \to \mathbb{R}$ is defined as follows:
For each $x \in \mathbb{Z}$, define $T(x) = x^2 + 1$. "

You read the above definition using these words:
"Define the function T from the set of integers to the set of real numbers as follows:
For each x, x an element of $\mathbb{Z}$, define ' T of x ' to be equal to $x^2 + 1$."

This definition specifies that the domain of T is $\mathbb{Z}$ and that the codomain of T is $\mathbb{R}$. It does this by the notation " $T: \mathbb{Z} \to \mathbb{R}$." It then specifies, for each element in the domain of T (here, $\mathbb{Z}$), how to determine which element in the codomain of T (here, $\mathbb{R}$) is to be related by T to that element in the domain of T.

Example 2: Sometimes there are varying procedures for determining the related value f(x) for a given value of x, depending on which subset it is, in a partition of the domain f, that that particular value of x lies.

For example, function $P: \mathbb{Z} \to \mathbb{Z}$ defined below is a function such that all positive even numbers are related to 10, all non-positive even numbers are related to 5, and all odd numbers are related to 0.

"Define the function $P : \mathbb{Z} \to \mathbb{Z}$ as follows: For all $x \in \mathbb{Z}$, define $P(x) = 10$ if x is even and positive; define $P(x) = 5$ if x is even and not positive; and define $P(x) = 0$ if x is odd."

This type of "piecewise defined" function definition is usually presented using the following table format:

4½

A PIECE-WISE DEFINED FUNCTION

$$P(x) = \begin{cases} 10 \text{ , if } x \text{ is even and } x > 0. \\ 5 \text{ , if } x \text{ is even and } x \leq 0. \\ 0 \text{ , if } x \text{ is odd.} \end{cases}$$

$P: \mathbb{Z} \to \mathbb{Z}$

The Domain of P is $\mathbb{Z}$

The Co-Domain of P is $\mathbb{Z}$

The Range of P is $\{0, 5, 10\}$.

Some Common Errors Made When Trying to Define Functions:

1. Failing to specify the domain and codomain. For example,

"Define f to be the function, $f(x) = \frac{x^2 - 1}{x}$."

(In some textbooks, there is a convention which says that, when a function is defined in this truncated way, the domain is considered to be the set of all real numbers such that the formula defining f(x) computes a real number. There is no convention as to what the codomain is beyond that of any set containing the actual range of the function.)

2. Failing to show how to compute f(x) for <u>every</u> element of the domain:

For example, "Define $f: \mathbb{Z} \to \mathbb{Z}$ as follows: For all $x \in \mathbb{Z}$, $f(x) = \begin{cases} x^2 \text{ , if } x > 0. \\ 1 - x \text{ , if } x < 0. \end{cases}$

(Here, $x = 0$ has been left out and so $f(0)$ has not been defined, which is an error.

3. Making the calculation of f(x) ambiguously indeterminate:

For example: Define $f: \mathbb{Z}^+ \to \mathbb{R}$ as follows:
For all $n \in \mathbb{Z}$, define $f(n) = x$ where $x^2 = n$.

You can see the difficulty when you try to figure you what the value of f(n) ought to be when $n = 4$. When $n = 4$, there are two possible values, $x = 2$ and $x = -2$, such that $x^2 = 0$. So, it may be that $f(4) = 2$ or it could be that $f(4) = -2$; we just don't know which.

Finally, the phrase **"Evaluate the function f at x = 2"** is an instruction to determine what particular value y in the range is the image of 2 under f. We evaluate the function f at "a" when we calculate what f(a) is. A common sloppy paraphrase of this is:

"Plug 2 into the function and see what you get."

4 2/3

One-to-One Functions & Onto Functions

Official In-the-book Definitions: Let F be a function from a set X to a set Y.

F is *one-to-one* (or *injective*) $\Leftrightarrow$ For every u and v in X,

If $F(u) = F(v)$, Then $u = v$

Also,

F is *one-to-one* (or *injective*) $\Leftrightarrow$ For every u and v in X,

If $u \neq v$, Then $F(u) \neq F(v)$.

F is *onto* (or *surjective*) $\Leftrightarrow$ For every element $y \in Y$,

there exists some $x \in X$ such that $F(x) = y$.

F is *a one-to-one correspondence* (or a *bijection*) from X to Y

$\Leftrightarrow$ $F: X \rightarrow Y$ is both a one-to-one function and an onto function.

Memorize the above definitions for their use in writing proofs, but a more intuitive definition of these terms is useful and is as follows:

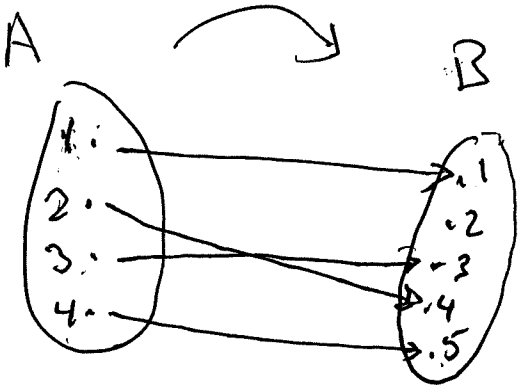
Let $f : X \rightarrow Y$ be a function.

Function f is … { onto / one-to-one / one-to-one and onto } if each element of Y is the image of … { at least one / at most one / exactly one } element of X

If $f : X \rightarrow Y$ is one-to-one and onto, then the *inverse function* $f^{-1} : Y \rightarrow X$ exists and $f^{-1}(y) = x$ if and only if $f(x) = y$, for all x in X and all y in Y.

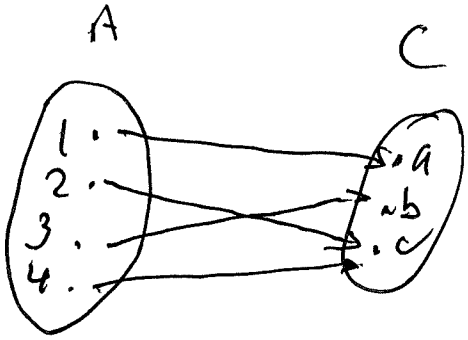
A one-to-one function Example:

Function $f: A \to B$



f is not onto.

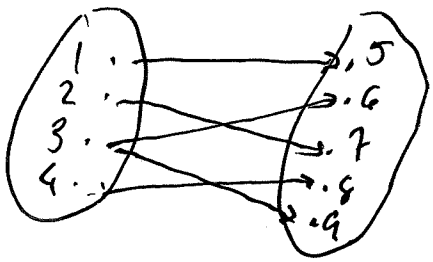
An Onto Function EXAMPLE: function $g: A \to C$



g is onto

f is not one-to-one

A relation that is not a function



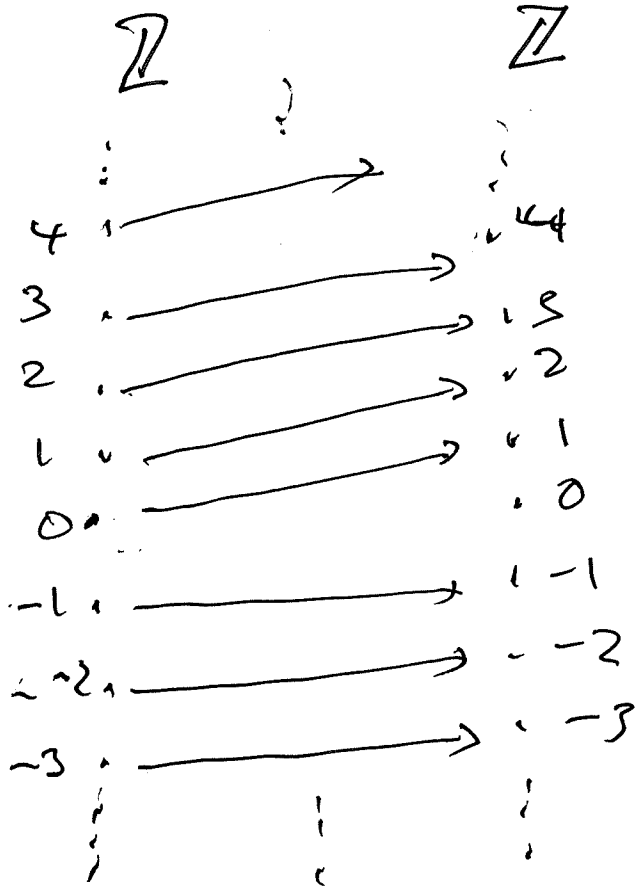
1 R 5
2 R 7
3 R 6
3 R 9
4 R 8

} Does not happen in a function.

Problem: Define function $h: \mathbb{Z} \to \mathbb{Z}$.

such that h is one-to-one but h is not onto

Soln



$h(0) = 1$

h is one-to-one.

h is not onto since $0 \neq f(x)$ for all $x \in \mathbb{Z}$.

Define $h: \mathbb{Z} \to \mathbb{Z}$ by the rule:

For all $n \in \mathbb{Z}$

$$h(n) = \begin{cases} n+1 & \text{if } n \geq 0 \\ n & \text{if } n < 0 \end{cases}$$

Proof Design I for Proving Function F is One-to-One:

Function F: $X \to Y$ is given.

To Prove: Function F is a one-to-one function.

Proof: Suppose that u and v are any two elements of X such that

$F(u) = F(v)$. [We need to show that $u = v$.]

. . .

. . . (Using the formula defining F(x) or some other properties

. . . of the function F we derive simpler and simpler

. . . equations eventually arriving at "u = v".)

$\therefore u = v$.

[$\therefore \forall u, v \in X$, If $F(u) = F(v)$, Then $u = v$.]

$\therefore$ F is one-to-one, by Direct Proof, by Direct Proof. Q E D

Proof Design II for Proving Function F is One-to-One:

Function F: $X \to Y$ is given.

To Prove: Function F is a one-to-one function.

Proof: Suppose that u and v are any two elements of X such that

$u \neq v$. [We need to show that $F(u) \neq F(v)$.]

. . .

. . . (This is often accomplished using a proof-by-contradiction,

. . . but sometimes it can be shown directly that $F(u) \neq F(v)$.)

. . .

$\therefore F(u) \neq F(v)$.

[$\therefore \forall u, v \in X$, If $F(u) = F(v)$, Then $u = v$, by contraposition.]

$\therefore$ F is one-to-one by Direct Proof. Q E D

8

Examples of Proofs That Prove a Function is One-to-one

Example 1: Define $T: \mathbb{Z} \to \mathbb{Z}$ as follows:

For all $n \in \mathbb{Z}$, $T(n) = 7n + 6$.

To Prove: T is a one-to-one function.

Proof: [Recall: $f: X \to Y$ is one-to-one $\Leftrightarrow \forall u, v \in X$, If $f(u) = f(v)$, Then $u = v$.]

Let u and v be integers (in the Domain of T).

Suppose $T(u) = T(v)$.

$\therefore$ By definition of T, $T(u) = 7u + 6$ and $T(v) = 7v + 6$.

$\therefore 7u + 6 = 7v + 6$ by substitution.

$\therefore 7u = 7v$ [subtracting 6]

$\therefore u = v$ [dividing by 7]

$\therefore$ For all $u, v \in \mathbb{Z}$, if $T(u) = T(v)$, THEN $u = v$, by Direct Proof.

$\therefore$ T is one-to-one, by def'n of "one-to-one".

QED

Proof Design for Proving that Function F is Onto:

Function F: X → Y is given.

To Prove: Function F is an onto function.

Proof: Suppose y is any element in Y.

[We need to show that there is some x in X with F(x) = y .]

(Note: In a workspace, and before the writing of the proof has begun, the equation F(x) = y is manipulated in order to solve for x in terms of y deriving a formula: x = "Formula in terms of y" . Use this formula to define the correct pre-image x for the selected y at the start .)

Let x = "Formula in terms of y"

Then, F(x) = (the complicated expression obtained by replacing x by the "Formula in terms of y") = … (simplifications) … = y.

[∴ ∀ y in Y, there exists an element x in X such that F(x) = y .]

∴ F is onto, by Direct Proof. Q E D

Proof Design to Prove that F is a One-to-One Correspondence (or Bijection):

Function F: X → Y is given.

To Prove: F is a One-to-One Correspondence.

Proof:

Part I: [Prove F is one-to-one.] … … ∴ F is one-to-one by Direct Proof .

Part II: [Prove F is onto.] … … ∴ F is onto by Direct Proof.

∴ F is one-to-one and onto .

∴ F is a one-to-one correspondence. Q E D

10

EXAMPLE OF A PROOF THAT PROVES A FUNCTION IS ONTO.

EXAMPLE:

Let $h: \mathbb{R} \to \mathbb{R}^+$ be defined by the rule

$h(x) = e^{(\frac{1}{3}x)}$, for all $x \in \mathbb{R}$.

TO PROVE: FUNCTION h is ONTO.

Proof: [Recall: Function $f: X \to Y$ is ONTO $\Leftrightarrow \forall y_0 \in Y, \exists x_0 \in X$ such that $f(x_0) = y_0$.]

[WORKSPACE:
Given $y_0 \in Y = \mathbb{R}^+$,
we seek $x_0 \in \mathbb{R}$
with
$h(x_0) = y_0$;
That is,
$e^{(\frac{1}{3}x_0)} = y_0$,
That is
$\frac{1}{3}x_0 = \ln(y_0)$
That is
$x_0 = 3\ln(y_0)$
So $h(3\ln(y_0)) = y_0$]

Let $y_0 \in \mathbb{R}^+$ be given.

Let $x_0 = 3\ln(y_0)$, which is defined because $y_0 > 0$.

$h(x_0) = e^{(\frac{1}{3}x_0)}$ by def of h,

$= e^{(\frac{1}{3}(3\ln y_0))}$ by substitution,

$= e^{\ln(y_0)}$

$= y_0$ by properties of e^x and $\ln(x)$.

$\therefore h(x_0) = y_0$.

$\therefore$ For all $y \in \mathbb{R}^+$, there exists an element $x \in \mathbb{R}$ s.t. such that $h(x) = y$, by Direct Proof.

$\therefore h$ is onto, by def'n of "ONTO".

Q.E.D.