15-151 Math Foundations CS – EXCEL

Topic: **Injectivity, Surjectivity, Bijectivity, Inverses**
EXCEL Leader: Sam Yong
Email: myong@andrew.cmu.edu

Session Date: **Thu 18 Oct**
Academic Development
Cyert Hall B5 | 412-268-6878

1. **RSA Review** – a little practice on multiplicative inverse

Let $p = 3, q = 7$. What is n and $\varphi(n)$?

Choose $e = 5$, what is the public key (n, e)? What is the private key (n, d)?

Use the public key to encrypt message $M = 2$. What is the encrypted cipher text K?

Decrypt K with the private key. Can you recover the original message correctly?

Puzzle 001. The four numbers game, again. Now, harder.

4	7	9	13
4	10	12	13

"Do not fear to be eccentric in opinion, for every opinion now accepted was once eccentric."

– **Bertrand Russell**

2. **Euclidean Algorithm Review** – a little practice on arithmetic

Find $\gcd(150, 216)$. Find $x, y \in \mathbb{Z}$ such that $150x + 216y = 12$.

---

3. **Function Diagnosis** – and fix the definitions

Let $f: \mathbb{R} \to \mathbb{R}$ via $f(x) = \sqrt{e^x} \Big/ \sqrt{1 - x}$

Is f well-defined? Why? If not, change only the domain and codomain to fix it.

Let $g: \mathbb{R} \to \mathbb{R}$ via $g(x) = g(x)^2 + \sqrt{g(x) + 1}$

Is g well-defined? Why? If not, change only the domain and codomain to fix it.

4. **Definitions Review** – annoying but important little things

A function $f: X \to Y$ is **injective** if ______________________________ for all $x, x' \in X$.

A function $f: X \to Y$ is **surjective** if ______________________________.

A function is **bijective** if ______________________________.

Let $f: X \to Y$ be a function. A **left inverse** for f is a function $g: Y \to X$ such that ______________________________.

Let $f: X \to Y$ be a function. A **right inverse** for f is a function $g: Y \to X$ such that ______________________________.

Let $f: X \to Y$ be a function. An **inverse** for f is a function ______________________________.

A function $f: X \to Y$ is injective if and only if it has a ______________________________.

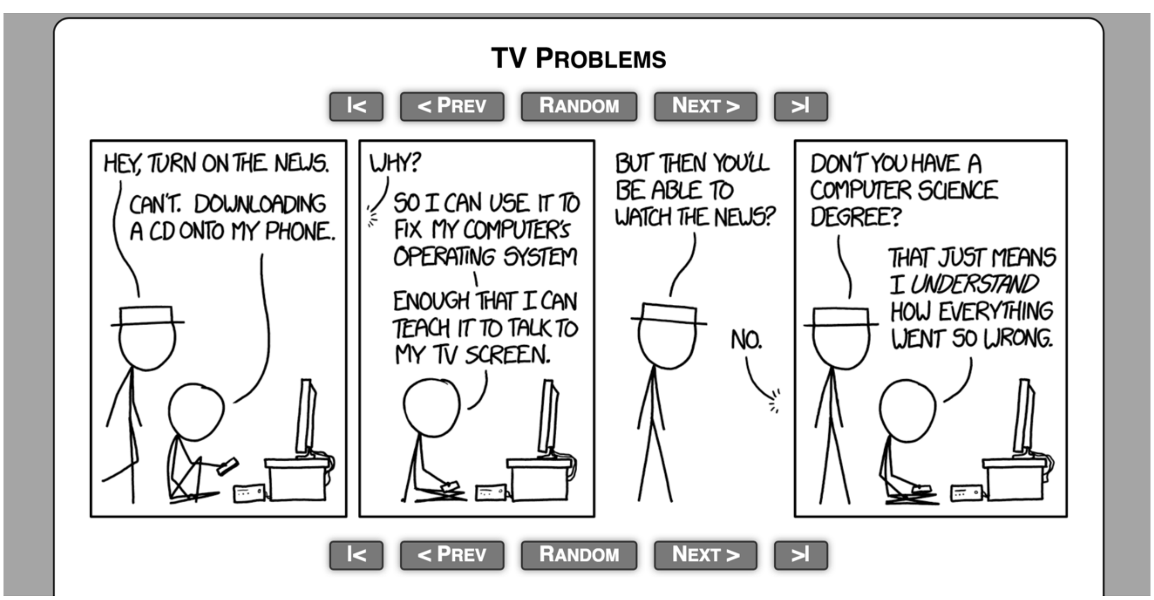
A function $f: X \to Y$ is surjective if and only if it has a ______________________________.

Let $m, n \in \mathbb{N}$.

If there exists an injection $f: [m] \to [n]$, then m____n.

If there exists a surjection $g: [m] \to [n]$, then m____n.

If there exists a bijection $h: [m] \to [n]$, then m____n.



Puzzle 002. Prove $3 < \pi < 4$ **visually**. (Hint: equilateral triangles and a square)

---

5. **Elementary Functions** – the architecture of the universe

For each the following functions, state whether it is injective, surjective, or bijective. Justify your claims.

$$f_1: \mathbb{R} \to \mathbb{R}, f_1(x) = \frac{1}{2}x + 1$$

$$f_2: \mathbb{R} \to \mathbb{R}, f_2(x) = x^2 - 2x$$

$$f_3: \mathbb{R} \setminus \{0\} \to \mathbb{R}, f_3(x) = \frac{1}{x}$$

$$f_4: \mathbb{R} \to \mathbb{R}, f_4(x) = e^x$$

$$g: \mathbb{R} \setminus \{0\} \to \mathbb{R}, g(x) - 3g\left(\frac{1}{2x}\right) = x$$

6. **From Stars to Dots to Stars** – invert back and forth

For each of the following functions, find its left, right, and two-sided inverse(s) if they exist. Remember to prove the function you find is indeed an inverse.

$$f: \mathbb{R} \setminus \{5\} \to \mathbb{R}, f(x) = \frac{4x}{5-x}$$

$$g = \{(-3, 8), (-11, -9), (5, 4), (6, -9)\}$$

$$h: \mathbb{R} \to \mathbb{R}, h(x) = x^3 - 4x$$

---

7. **Piece it together** – some more practice on everything

A group (in mathematics) is a set G with an operation $\oplus$ that combines any two elements a, b to form another element, denoted as $a \oplus b$. $(G, \oplus)$ qualifies as a group if it satisfies all of the following.

Closure: $\forall a, b \in G, a \oplus b \in G$

Associativity: $\forall a, b, c \in G, (a \oplus b) \oplus c = a \oplus (b \oplus c)$

Identity: $\exists e \in G, \forall a \in G, e \oplus a = a \oplus e = a$

Inverse: $\forall a \in G, \exists b \in G, a \oplus b = b \oplus a = e$ where e is the identity element from above

a) Prove $(\mathbb{Z}, +)$ is a group, where $+$ is the regular arithmetic addition.

b) Define $f: \mathbb{R} \to \mathbb{R}, f_{a,b}(x) = ax + b, a \in \mathbb{R}^+, b \in \mathbb{R}$. Show that $\left(\{f_{a,b}: a \in \mathbb{R}^+, b \in \mathbb{R}\}, \circ\right)$ is a group, where $\circ$ is the operation of function composition.

c) [extra] Prove the set of all possible manipulations of a Rubik's Cube with the operation of chaining manipulations form a group. (This is known as the Rubik's Cube group.)

"… I don't believe in the idea that there are a few peculiar people capable of understanding math and the rest of the world is normal. Math is a human discovery, and it's no more complicated than humans can understand. I had a calculus book once that said, 'What one fool can do, another fool can.' What we've been able to work out about nature may look abstract and threatening to someone who hasn't studied it, but it was fools who did it, and in the next generation, all the fools will understand it. There's a tendency to pomposity in all this, to make it all deep and profound…"

– **Richard Feynman**

Happy Mid-Semester Break!

Expert

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