

**SANTA MONICA COLLEGE**  
**Department of Mathematics**  
**Math 10– Midterm Exam**

Instructor: Kevin Arlin

April 8, 2022

---

Submit your work as you would any homework assignment: direct submission of a .pdf is ideal. The exam is open book and open notes. **It is not open Internet.** I take academic honesty during COVID even more seriously than usual, and have been known to be rather vindictive when I see solutions that were garnered online. Nobody wants that. Don't do it. Not even if you're having lots of trouble with the test. It is fine if you only get a 65%; you might even still get an 'A' that way. I am generous with curves as appropriate, and may both award bonus points to the toughest problems here and also curve grades toward the end of the course.

Show your work. Partial credit will be given when earned. Explanations are required unless explicitly not requested.

*Enter your name below to signal your assent to the following honor statement:*

I, **Elias Schablowski** affirm that I have not discussed the contents of this exam with anyone, whether in person or online, except perhaps Kevin Arlin, and that I will not do so before Tuesday, April 12.

**Distribution of Points**

Question	Points	Score	Question	Points	Score
1	4		5	10	
2	10		6	10	
3	10		7	0	
4	10		Total:	54	

This page is intentionally left blank to accommodate work that wouldn't fit elsewhere and/or scratch work.

*Note: this problem serves as your entire quiz 6, but it'll be graded with partial credit.*

## Quiz 6

1. (4 points) Prove that, if  $n > 0$  is any positive integer, then  $\sum_{j=1}^n 4j \cdot 3^j = (6n - 3) \cdot 3^n + 3$ .

**Solution:**

**Definitions:** Let  $f(n) = \sum_{j=1}^n 4j \cdot 3^j$ .

$$f(1) = 12$$

$$f(n) = f(n-1) + 4n \cdot 3^n$$

**Base Step:**  $f(1) = 12 = (6(1) - 3) \cdot 3^{(1)} + 3 = (3) \cdot 3 + 3 = 9 + 3 = 12$

**Inductive Step:** Assume  $f(k) = (6k - 3) \cdot 3^k + 3$  when  $k \geq 1$ . Then  $f(k+1) = f(k) + 4(k+1) \cdot 3^{(k+1)}$ . Substituting  $f(k)$  we get  $f(k+1) = (6k - 3) \cdot 3^k + 3 + 4(k+1) \cdot 3^{(k+1)}$ . Expanding  $f(k+1) = 6k \cdot 3^k + 4k \cdot 3^{(k+1)} + 4 \cdot 3^{(k+1)} - 3 \cdot 3^k + 3$ . Substitute  $3^k = \frac{3^{k+1}}{3}$  we get  $f(k+1) = 2k \cdot 3^{k+1} + 4k \cdot 3^{(k+1)} + 4 \cdot 3^{(k+1)} - 3^{k+1} + 3$ . Simplify  $f(k+1) = 6k \cdot 3^{(k+1)} + 3 \cdot 3^{(k+1)} + 3$ . Simplifying further we get  $f(k+1) = (6k + 3) \cdot 3^{(k+1)} + 3 = (6(k+1) - 3) \cdot 3^{(k+1)} + 3$ .

## Midterm

2. (10 points) The *abc* conjecture states that there is a certain positive real number  $\varepsilon$  such that whenever  $a, b, c$  are natural numbers with  $c = a + b$ , all bigger than a certain  $k \in \mathbb{N}$ , then  $c$  is no bigger than the  $\text{rad}(abc)^{1+\varepsilon}$ . Here  $\text{rad} : \mathbb{N} \rightarrow \mathbb{N}$  is a certain function whose definition you don't have to worry about. A student attempts to formalize this conjecture in predicate logic as follows:

$$\exists \varepsilon \in (0, \infty) \forall (a, b, c) \in \mathbb{N}^3 \exists k \in \mathbb{N} (a > k \wedge b > k \wedge c > k \rightarrow c \leq \text{rad}(abc)^{1+\varepsilon}.)$$

There are exactly two errors in the student's formalization. Explain what they are and how to fix them.

**Solution:** The student's logic equates the sentence "There exists a positive real number  $\varepsilon$  such that for all  $a, b$ , and  $c$  in  $\mathbb{N}$ , there exists a  $k$  in  $\mathbb{N}$  such that  $a, b$ , and  $c$  are larger than  $k$  then  $c \leq \text{rad}(abc)^{1+\varepsilon}$ ."

This has two problems, primarily it does not say anything about  $c = a + b$  (which can be fixed by either adding that  $c = a + b$  to his logic or by substituting  $c$  for  $a + b$  which would also reduce the variables), and furthermore the student switched the relationship between  $k$  and  $a, b$ , and  $c$ , which can be fixed by moving the  $k$  before  $a, b$ , and  $c$ .

$$\exists \varepsilon \in (0, \infty) \exists k \in \mathbb{N} \forall (a, b) \in \{(x, y) | (x, y) \in \mathbb{N}^2 \wedge x > k \wedge y > k\} \exists c \in \{a + b\} (c \leq \text{rad}(abc)^{1+\varepsilon})$$

3. (a) (3 points) How many elements are in  $\mathcal{P}(\{\text{purdy}, \{\text{purdy}\}\}) \cap \{\text{purdy}, \{\text{purdy}\}\}$ , where purdy is my anxious tabby cat? Explain why.

**Solution:**

$$\mathcal{P}(\{\text{purdy}, \{\text{purdy}\}\}) = \{\emptyset, \{\text{purdy}\}, \{\{\text{purdy}\}\}, \{\text{purdy}, \{\text{purdy}\}\}\}$$

The only common element between them is  $\{\text{purdy}\}$  so  $\mathcal{P}(\{\text{purdy}, \{\text{purdy}\}\}) \cap \{\text{purdy}, \{\text{purdy}\}\} = \{\{\text{purdy}\}\}$ , which is one element.

- (b) (7 points) Suppose  $A$  and  $B$  are finite sets with cardinalities  $|A| = a$  and  $|B| = b$ , with  $b \geq a$ . In terms of  $a$  and  $b$ , what are all the possibilities for  $|A \cup B|$ ? Show that all the possibilities you claim are possible, and that no other possibilities are possible.

**Solution:**

**Case  $A \subseteq B$ :** This means that  $\forall x \in A (x \in B)$ . Therefore  $A \cup B = B$  and therefore  $|A \cup B| = |B| = b$ .

**Case  $A \subset B$ :** Let  $C = A \cap B$  and  $c = |C|$ . Then  $|A \cup B| = a + b - c$  where  $c < a \wedge c < b$  since all of  $B$ 's and some of  $A$ 's elements are counted. Therefore  $b < |A \cup B| < a + b$ .

**Case  $A \not\subset B$ :** Then  $|A \cup B| = a + b$  as all elements from both  $A$  and  $B$  are counted.

Thus we have proven:  $b \leq |A \cup B| \leq a + b$ .

4. Say that a function  $f : A \rightarrow B$  has the epi property if the following holds:

$$\forall X \in \text{Set} \forall g, h : B \rightarrow X (g \circ f = h \circ f \rightarrow g = h.)$$

Here Set is the collection of all possible sets, so the first quantifier is over all sets  $X$  and the second, over all functions  $B \rightarrow X$ .

- (a) (2 points) Show that  $f : \{a, b, c\} \rightarrow \{d, e\}$  given by  $f(a) = d, f(b) = d, f(c) = e$  has the epi property.

**Solution:** Let  $z_1, z_2, z_3, z_4 \in X$ . Let  $g(d) = z_1, g(e) = z_2, h(d) = z_3$  and  $h(e) = z_4$ . Then  $g(f(a)) = g(f(b)) = z_1, h(f(a)) = h(f(b)) = z_3$ , and  $g(f(a)) = g(f(b)) = h(f(a)) = h(f(b))$ , therefore  $z_1 = z_3$ . Also  $g(f(c)) = g(f(c)) = z_2, h(f(c)) = z_4$ , and  $g(f(c)) = h(f(c))$ , therefore  $z_2 = z_4$ . Therefore  $g = h$  and  $f$  has the epi property.

- (b) (2 points) Show that  $f : \{1, 2, 3\} \rightarrow \{4, 5\}$  given by  $f(1) = f(2) = f(3) = 4$  does not have the epi property.

**Solution:** Let  $z_1, z_2 \in X$ . Let  $g(e) = z_1, h(e) = z_2$ . Since  $g(e)$  and  $h(e)$  do not exist in  $g \circ f$  and  $h \circ f$ ,  $z_1$  does not have to equal  $z_2$  and therefore  $g$  does not have to equal  $h$ . Thus  $f$  does not have the epi property.

- (c) (6 points) Conjecture and prove a more familiar way of describing a function with the epi property.

**Solution:** If and only if  $\forall b \in B \exists a \in A (f(a) = b)$  ( $f$  is **surjective**), then  $f$  has the epi property.

$g = h \leftrightarrow \forall b \in B (g(b) = h(b))$ , therefore if  $f$  is surjective and  $g \circ f = h \circ f$ , then  $g = h$  as  $\forall b \in B \exists a \in A (g(f(a)) = h(f(a)))$ .

Furthermore if  $f$  isn't surjective,  $\exists b \in B \forall a \in A (f(a) \neq b \rightarrow g(b) \neq h(b))$

5. For any  $n \in \mathbb{Z}_{>0}$  and  $k \in \mathbb{Z}_n$ , let  $\mu_k : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$  be the multiplication-by- $k$  function, so  $\mu_k(m) = k \times_n m$ .

- (a) (2 points) Give an example of an  $n$  and a  $k \neq 0$  for which  $\mu_k$  is not injective. (Explain why not.)

**Solution:** Let  $n = 10$ ,  $k = 5$ .

Since  $\mu_5(5) = 25 \bmod 10 = 5 = \mu_k(1)$

- (b) (2 points) Give an example of an  $n$  and a  $k \neq 1$  for which  $\mu_k$  is injective. (Prove it.)

**Solution:** Let  $n = 3$  and  $k = 2$ .

$$0 \quad \mu_2(0) = 0 \bmod 3 = 0$$

$$1 \quad \mu_2(1) = 2 \bmod 3 = 2$$

$$2 \quad \mu_2(2) = 4 \bmod 3 = 1$$

- (c) (6 points) Do your best to state and prove necessary and sufficient conditions on  $n$  and  $k$  which guarantee  $\mu_k$  is injective.

**Solution:**

$$\forall x \in Z_n \forall y \in Z_n (\mu_k(x) = \mu_k(y) \rightarrow x = y)$$

Therefore  $kx = ky \pmod n \rightarrow x = y$ .

Assume  $k = n - 1 \vee k = 1$  is the sufficient and necessary condition for  $\mu_k$  to be injective.

Let  $f(a) = (na - a) \bmod n$

$$\begin{aligned} f(a) &= ((na \bmod n) - (a \bmod n)) \bmod n \\ &= (((n \bmod n)(a \bmod n)) \bmod n - (a \bmod n)) \bmod n \\ &= (((0)(a \bmod n)) \bmod n - (a \bmod n)) \bmod n \\ &= (((0) \bmod n) - (a \bmod n)) \bmod n \\ &= ((0 - (a \bmod n)) \bmod n \\ &= ((-(a \bmod n)) \\ &= -(a \bmod n) \end{aligned}$$

$k = n - 1$ :

$$\begin{aligned} (n-1)x &= (n-1)y \pmod n \rightarrow x = y \\ nx - x &= ny - y \pmod n \rightarrow x = y \\ (nx - x) \bmod n &= (ny - y) \bmod n \rightarrow x = y \\ f(x) &= f(y) \rightarrow x = y \\ -x &= -y \rightarrow x = y \end{aligned}$$

$k = 1:$ 

$$(1)x = (1)y \rightarrow x = y$$

$$x = y \rightarrow x = y$$

6. Let  $C$  be the set of real numbers defined recursively as follows:

- (Base case)  $\mathbb{Q} \subseteq C$
  - (Recursive step) If  $x, y \in C$  then  $x + y, x - y, xy, x/y$  are in  $C$ , and if  $x \geq 0$  then so is  $\sqrt{x}$ .
- (a) (2 points) Give three examples of elements of  $C$  that are significantly different-looking from each other.

$$(a) \quad 34, \frac{321}{456}, \sqrt{345}, \frac{85\sqrt{432}}{453}$$

(b) (1 point) Give an example of a real number which is not in  $C$ .

$$(b) \quad e, \pi, \tau, \text{etc.}$$

(c) (7 points) Suppose we want to define a function  $d : C \rightarrow \mathbb{N}$  such that  $d(x)$  is the number of nested square roots needed to express  $x$ . What is wrong with this definition, and how could you improve it?

- $d(x) = 0$ , if  $x \in \mathbb{Q}$
- $d(x + y) = d(x - y) = d(xy) = d(x/y) = \max(d(x), d(y))$ , and  $d(\sqrt{x}) = d(x) + 1$ , when  $x > 0$ .

**Solution:** The problem is that it is undefined what happens if  $x < 0$ , one way to mitigate this is to add another case that  $d(xy) = d(y)$  when  $x < 0$ .

7. (Bonus:) Consider an alphabet  $\Sigma$ . In principle,  $\Sigma$  can be any set, but you should think  $\Sigma = \{0, 1\}$  or  $\Sigma = \{a, b, \dots, z\}$ .

The set  $\mathcal{R}_\Sigma$  of *regular languages* over  $\Sigma$  is defined as follows. Every element of  $\mathcal{R}_\Sigma$  is in particular a set of strings over  $\Sigma$ ; that is,  $\mathcal{R}_\Sigma \subseteq \mathcal{P}(\Sigma^*)$ .

- $\emptyset \in \mathcal{R}_\Sigma$
- $\forall s \in \Sigma, \{s\} \in \mathcal{R}_\Sigma$
- $\forall S \in \mathcal{R}_\Sigma, S^* \in \mathcal{R}_\Sigma$ , where  $S^*$  is the smallest set containing  $S$  and closed under concatenation. (So it contains all concatenations of  $n$  strings from  $S$ , for every  $n$ .)
- The union  $S \cup T$  and concatenation  $S \bullet T = \{st \mid s \in S, t \in T\}$  are in  $\mathcal{R}_\Sigma$  whenever  $S$  and  $T$  are.

Prove that, with  $\Sigma = \{0, 1\}$ , the set  $S$  of bit strings that flip bits at most once (so  $S$  contains 000011111 and 11111 but not 010) is a regular language.

**Solution:** Let  $S_k$  be the set of bit strings of  $k$  bits that flip at most once. Let  $T_1 = \{1\}$ . Let  $T_k$  be the set of  $k$  1s. Let  $F_1 = \{0\}$ . Let  $F_k$  be the set of  $k$  0s.

**Base Step:** Since  $\forall s \in \Sigma, \{s\} \in \mathcal{R}_\Sigma$ ,  $T_0 = \{1\}$  is a regular language.

**Inductive Step:** Assume that  $T_k \in \mathcal{R}_\Sigma$ . Since  $S \bullet T = \{st \mid s \in S, t \in T\}$  are in  $\mathcal{R}_\Sigma$ , if we substitute  $T_0$  for  $S$  and  $T_k$  for  $T$ , we get  $T_{k+1} = T_0 \bullet T_k = t_0 t_k \mid t_0 \in T_0, t_k \in T_k$  which is all in  $\mathcal{R}_\Sigma$ .

**Base Step:** Since  $\forall s \in \Sigma, \{s\} \in \mathcal{R}_\Sigma$ ,  $F_0 = \{0\}$  is a regular language.

**Inductive Step:** Assume that  $F_k \in \mathcal{R}_\Sigma$ . Since  $S \bullet F = \{st \mid s \in S, t \in F\}$  are in  $\mathcal{R}_\Sigma$ , if we substitute  $F_0$  for  $S$  and  $F_k$  for  $F$ , we get  $F_{k+1} = F_0 \bullet F_k = f_0 f_k \mid f_0 \in F_0, f_k \in F_k$  which is all in  $\mathcal{R}_\Sigma$ .

**Base Step:** Since  $S \in \mathcal{R}_\Sigma \wedge T \in \mathcal{R}_\Sigma \implies S \cup T \in \mathcal{R}_\Sigma$ , and  $S_0 = T_0 \cup F_0$  and  $T_0, F_0 \in \mathcal{R}_\Sigma$ ,  $S_0 \in \mathcal{R}_\Sigma$ .

**Inductive Step:** Let  $a, b \in \mathbb{N}(a + b = k)$ . Since  $S \bullet F = \{st \mid s \in S, t \in F\}$  and  $S \cup T$  are in  $\mathcal{R}_\Sigma$  if  $S$  and  $T$  are, if we substitute  $T_a \cup F_a$  for  $S$  and  $T_b \cup F_b$  for  $F$ , we get  $S_k = (T_a \cup F_a) \bullet (T_b \cup F_b)$  which is in  $\mathcal{R}_\Sigma$ .

Since  $S = \bigcup_i S_i$ ,  $S \in \mathcal{R}_\Sigma$  as  $S_k \in \mathcal{R}_\Sigma$  and  $S, T \in \mathcal{R}_\Sigma \rightarrow S \cup T$