CSC165 - Problem Set 2

Junaid Arshad, Sadeed Ahmed, & Frederick Meneses

March 4, 2022

1 Number Theory

(a) The following proof will reference the following predicates and facts regarding properties of the greatest common divisor (taken from *Worksheet 6 & 7*):

$$LinComb(a,b,c):\ \exists p,q \in \mathbb{Z}, c = pa + qb, \text{where } a,b,c \in \mathbb{Z} \tag{1}$$
$$\forall n,p \in \mathbb{Z}, Prime(p) \land p \nmid n \Rightarrow gcd(p,n) = 1 \tag{2}$$
$$\forall n,m \in \mathbb{N}, \exists r,s, \in \mathbb{Z}, rn + sm = gcd(n,m) \tag{3}$$

The following is a proof that $\forall\, n \in \mathbb{Z},\ gcd(7n+1, 15n+2) = 1$:

Proof. Let $n \in \mathbb{Z}$. By fact **(1)**, we can re-write $7n+1$ and $15n+2$ as a linear combinations of the form $pa+qb = c$ for some $p,q \in \mathbb{Z}$ where $a,b \in \mathbb{Z}$. $7n+1 = c_1$ and $15n+2 = c_2$ for some $c_1, c_2 \in \mathbb{Z}$. In particular, $c_1 = \gcd(7,1)$ and $c_2 = \gcd(2,15)$. By fact **(2)** and our choices of a and b, we can conclude $\gcd(2,15) = 1$ and $\gcd(7,1) = 1$. By fact **(3)**, it suffices to show that there exists integers r,s such that, $r\gcd(7,1) + s\gcd(2,15) = \gcd(\gcd(7,1), \gcd(2,15)) = \gcd(1,1) = 1$.

□

(b) The following is a proof that there exists only 1 prime in the form of $n^3 - 1$, or that:

$$\exists p \in \mathbb{N}, (Prime(p) \land (\exists n \in \mathbb{Z}, p = n^3 - 1)) \land \big(\forall q \in \mathbb{N}, (Prime(q) \land (\exists m \in \mathbb{Z}, q = m^3 - 1) \Rightarrow p = q\big)$$

Consider the definition of a Prime Number:

$$Prime(n):\ n > 1 \land \big(\forall d \in \mathbb{N}, d | n \Rightarrow d = 1 \lor d = n\big), \text{where } n \in \mathbb{N} \tag{4}$$

Proof.
We will prove the first part of the statement first i.e.,
$\exists p \in \mathbb{N}, (Prime(p) \land (\exists n \in \mathbb{Z}, p = n^3 - 1))$

- Let $p = 7$
- WTS: $(Prime(p) \land (\exists n \in \mathbb{Z}, p = n^3 - 1)$
- $Prime(7)$ is True since $7 > 1$ and the only number that divide 7 are 1 and itself.

- Let $n = 2$

$$n^3 - 1 = (2^3 - 1) = 7 = p$$

We want to show p is a prime number such that $p = n^3 - 1$, where $n \in \mathbb{Z}$.

We know by the definition of a Prime Number that p must be greater than 1, and only be divisible by itself or 1. Since $n^3 - 1$ can be re-written in its factored form as: $(n-1)(n^2+n+1)$, either $(n-1)$ or (n^2+n+1) must be equal to 1. Also, since the resulting value must be greater than 1, it follows that the other must equal p, such that $p > 1$. We will prove this by setting each term to 1 and examining the other term and resulting value to verify if it is a prime number.

Case 1. $(n^2 + n + 1) = 1$ only when $n = 0$ or $n = -1$, but if we substitute either of these values of n into the term $(n-1)$, the resulting value is negative. Since prime numbers cannot be negative, it is clear that $(n^2 + n + 1)$ cannot be 1.

Case 2. $(n - 1) = 1$ if and only if $n = 2$. When $n = 2$, the term $(n^2 + n + 1)$ evaluates to 7, which is a prime number. Additionally, $n^3 - 1$ will evaluate to 7 in this case.

Next, we will prove that this is the only prime number which can take the form of $n^3 - 1$. From the definition of a Prime Number (1) we also know that the only numbers that can divide a Prime Number are 1 and the prime number itself. From **Case 1**, we have seen that the only other values of $n \in \mathbb{Z}$ which evaluate one factor of $n^3 - 1$ do not produce prime numbers. From **Case 2**, we have seen the only value of $n \in \mathbb{Z}$ which produces a prime number. Thus, any other values produces from $n^3 - 1$ must not be prime as they will not be divisible by themselves or 1.

$\square$

2 Floors and Ceilings

The following facts are referenced in this section:

$$\forall x \in \mathbb{R}, 0 \leq x - \lfloor x \rfloor < 1 \tag{1}$$
$$\forall x \in \mathbb{R}, 0 \leq \lceil x \rceil - x < 1 \tag{2}$$

(a) We will use **proof by cases** to show that:

$$\forall x \in \mathbb{Z}, \left\lfloor \frac{x+1}{2} \right\rfloor = \left\lceil \frac{x}{2} \right\rceil \tag{3}$$

Proof. Let x be an arbitrary integer. In order to prove **(3)**, we will examine the cases when x is even and when x is odd.

Case 1 (Even)**.** If x is an even integer, 2 must divide x, or $Even(x) : x = 2k, k \in \mathbb{Z}$. We will evaluate each term in $\lfloor \frac{x+1}{2} \rfloor = \lceil \frac{x}{2} \rceil$ with $2k$ substituted for x below:

$$\begin{aligned} \left\lfloor \frac{x+1}{2} \right\rfloor &= \left\lfloor \frac{(2k)+1}{2} \right\rfloor \\ &= \left\lfloor k + \frac{1}{2} \right\rfloor \\ &= k \end{aligned}$$

$$\begin{aligned} \left\lceil \frac{x}{2} \right\rceil &= \left\lceil \frac{2k}{2} \right\rceil \\ &= \lceil k \rceil \\ &= k \end{aligned}$$

Thus, $\forall\, x \in \mathbb{Z}, Even(x)$, **(3)** holds.

Case 2 (Odd)**.** If x is an odd integer, $Odd(x) : x = 2k - 1, k \in \mathbb{Z}$ must be true. We will evaluate each term in $\lfloor \frac{x+1}{2} \rfloor = \lceil \frac{x}{2} \rceil$ with $2k$ substituted for x below:

$$\begin{aligned} \left\lfloor \frac{x+1}{2} \right\rfloor &= \left\lfloor \frac{(2k-1)+1}{2} \right\rfloor \\ &= \lfloor k \rfloor \\ &= k \end{aligned}$$

$$\begin{aligned} \left\lceil \frac{x}{2} \right\rceil &= \left\lceil \frac{2k-1}{2} \right\rceil \\ &= \left\lceil k - \frac{1}{2} \right\rceil \\ &= k \end{aligned}$$

Thus, $\forall\, x \in \mathbb{Z}, Odd(x)$, **(3)** holds.

From **Case 1** and **Case 2**, we have shown that regardless of whether x is even or odd, **(3)** holds. $\square$

(b) Proof and Disproof:

i The following is a proof that $\forall x, y \in \mathbb{R}, x \leq y \Rightarrow \lceil x \rceil \leq \lceil y \rceil$:

Proof. Let $x, y \in \mathbb{R}$. Assume that $x \leq y$. We will prove that $\lceil x \rceil \leq \lceil y \rceil$.
From **(2)**, we know the following:

$$\begin{aligned} x \leq \lceil x \rceil &< x + 1 \\ &\leq y + 1 && \text{(using our assumption } x \leq y\text{)} \end{aligned}$$

Thus, $\lceil x \rceil < y$.
Similarly, from **(2)** we also know that $y \leq \lceil y \rceil$. Thus, $y + 1 \leq \lceil y \rceil + 1$.

$$\begin{aligned} &\lceil x \rceil < y + 1 \leq \lceil y \rceil + 1 \\ &\lceil x \rceil < \lceil y \rceil + 1 \\ \leftrightarrow\ &\lceil x \rceil \leq \lceil y \rceil \end{aligned}$$

$\square$

ii The following is a disproof that $\forall x, y \in \mathbb{R}, \lceil x \rceil \leq \lceil y \rceil \Rightarrow x \leq y$:

Proof. Statement to disprove:

$$\forall x, y \in \mathbb{R}, \lceil x \rceil \leq \lceil y \rceil \Rightarrow x \leq y \tag{4}$$

We will disprove this statement by proving its negation. The negation of **(4)** is:

$$\exists x, y \in \mathbb{R}, \lceil x \rceil \leq \lceil y \rceil \wedge x > y \tag{5}$$

Let $x = \frac{2}{3}$ and $y = \frac{1}{3}$. Thus, $x > y$ holds.

$$\begin{aligned} &\lceil x \rceil = 1 && \text{(from } \mathbf{(2)}\text{)} \\ &\lceil y \rceil = 1 && \text{(from } \mathbf{(2)}\text{)} \\ &\lceil x \rceil \leq \lceil y \rceil \end{aligned}$$

Thus, $\lceil x \rceil \leq \lceil y \rceil$ holds, proving **(5)** and consequently disproving **(4)**. $\square$

3 Induction

(a) The following is a proof that $3|2^{2n+1}+1$ for all natural numbers n:

Let $P(n) : \exists k \in \mathbb{Z}, 2^{2n+1}+1 = 3k$, where $n \in \mathbb{N}$

Proof. We will prove this by induction. Let $n \in \mathbb{N}$,
Base Case: $(n = 0)$
Let $k = 1$, then

$$\begin{aligned} 2^{2(0)+1}+1 &= 3(1) \\ 2+1 &= 3 \\ 3 &= 3 \end{aligned}$$

Inductive Step:

Let $q \in \mathbb{N}$. Assume $P(q) : \exists k_0 \in \mathbb{Z}, 2^{2q+1}+1 = 3k_0$.

WTS: $P(q+1) : \exists k_1 \in \mathbb{Z}, 2^{2(q+1)+1}+1 = 3k_1$.

Let $k_1 = 2^{2q+1}+k_0$.

We will prove $2^{2(q+1)+1}+1 = 3k_1$

$$\begin{aligned} 2^{2(q+1)+1}+1 &= 2^2 \cdot 2^{2q+1}+1 \\ &= 3 \cdot 2^{2q+1}+2^{2q+1}+1 \\ &= 3 \cdot 2^{2q+1}+3k_0 \qquad \text{(I.H)} \\ &= 3(2^{2q+1}+k_0) \\ &= 3k_1 \end{aligned}$$

□

(b) The following is a proof that $\forall n \in \mathbb{Z}^+$,

$$\frac{1}{2} \times \frac{3}{4} \times ... \times \frac{2n-1}{2n} \leq \frac{1}{\sqrt{3n}}$$

The product above may also be represented as

$$\prod_{i=1}^{n} \frac{2i-1}{2i}$$

We will prove a more stronger statement that the one given above i.e.,

We know that:

$$\sqrt{3n+1} \geq \sqrt{3n}$$

From which we can conclude:

$$\frac{1}{\sqrt{3n+1}} \leq \frac{1}{\sqrt{3n}}$$

We will prove the following statement using induction:

$$\forall n \in \mathbb{Z}^+, \prod_{i=1}^{n} \frac{2i-1}{2i} \leq \frac{1}{\sqrt{3n+1}}$$

Proof. Let $n \in \mathbb{Z}^+$

$$\text{Let } P(n) : \prod_{i=1}^{n} \frac{2i-1}{2i} \leq \frac{1}{\sqrt{3n+1}}$$

Base Case: Let $(n = 1)$

$$\begin{aligned} P(1) : \prod_{i=1}^{1} \frac{2i-1}{2i} &= \frac{1}{2} \\ &\leq \frac{1}{\sqrt{3(1)+1}} = \frac{1}{2} \end{aligned}$$

therefore, the base case holds.
Inductive step: Let $k \in \mathbb{Z}^+$. Assume

$$P(k) : \prod_{i=1}^{k} \frac{2i-1}{2i} \leq \frac{1}{\sqrt{3k+1}}$$

We will prove $P(k) \Rightarrow P(k+1)$ is True.

$$P(k+1) : \prod_{i=1}^{k+1} \frac{2i-1}{2i} \leq \frac{1}{\sqrt{3(k+1)+1}} = \frac{1}{\sqrt{3k+4}}$$

We know $k \geq 1$ implies $k \geq 0$

$$\begin{aligned} k &\geq 0 \\ 20k - 19k &\geq 0 \\ 20k &\geq 19k \end{aligned}$$

Adding $12k^3 + 28k^2 + 4$ to both sides of the inequality preserves the inequality since $k \geq 1$

$$\begin{aligned} 12k^3 + 28k^2 + 20k + 4 &\geq 12k^3 + 28k^2 + 19k + 4 \\ (3k+1)(2k+2)^2 &\geq (3k+4)(2k+1)^2 && \text{(by factoring each side)} \\ \frac{1}{3k+4} &\geq \frac{(2k+1)^2}{(2k+2)^2} \cdot \frac{1}{3k+1} \end{aligned}$$

Taking square root of both sides preserves the inequality since both sides are ≥ 0

$$\begin{aligned}
\frac{1}{\sqrt{3(k+1)+1}} &\geq \frac{(2k+1)^2}{(2k+2)^2} \cdot \frac{1}{\sqrt{3k+1}} \\
&\geq \frac{(2k+1)^2}{(2k+2)^2} \cdot \prod_{i=1}^{k} \frac{2i-1}{2i} && \text{(Using Induction Hypothesis)} \\
&\geq \frac{(2(k+1)-1)^2}{(2(k+1))^2} \cdot \prod_{i=1}^{k} \frac{2i-1}{2i} \\
&\geq \prod_{i=1}^{k+1} \frac{2i-1}{2i} && \text{(combining the terms into a single product)}
\end{aligned}$$

Therefore $P(k+1)$ is True, which makes our inductive step and by extension

$$P(n) : \prod_{i=1}^{n} \frac{2i-1}{2i} \leq \frac{1}{\sqrt{3n+1}}$$

True which implies that

$$\prod_{i=1}^{n} \frac{2i-1}{2i} \leq \frac{1}{\sqrt{3n}}$$

is also True since

$$\frac{1}{\sqrt{3n+1}} \leq \frac{1}{\sqrt{3n}}$$

$\square$

4 Working with Functions

The following definitions will be referenced in this section:

$$\forall a_1, a_2 \in A, f(a_1) = f(a_2) \Rightarrow a_1 = a_2 \quad \text{(one-to-one)}$$
$$\forall b \in B, \exists \in A, f(a) = b \quad \text{(onto)}$$
$$\forall a \in A, (g \circ f)(a) = g(f(a)) \quad \text{(composition)}$$

(a) **Working with functions.**

i The following is the proof that $g_1 : \mathbb{Z} \to \mathbb{Z}; g_1(x) = x - 4$ is both one-to-one and onto:

Proof. First, we will prove that $g_1(x)$ is one-to-one, or that:

$$\forall p, q \in \mathbb{Z}, g_1(p) = g_1(q) \Rightarrow p = q$$

Let $p, q, \in \mathbb{Z}$. Assume $g_1(p) = g_1(q)$. We want to prove that $p = q$.

$$\begin{aligned} g_1(p) &= g_1(q) \\ p - 4 &= q - 4 \\ p &= q && \text{(add 4 to both sides)} \end{aligned}$$

Next, we will prove that g_1 is onto, or that:

$$\forall b \in \mathbb{Z}, \exists a \in \mathbb{Z}, g_1(a) = b$$

Let $b \in \mathbb{Z}$. Let $a = b + 4$.

$$\begin{aligned} b &= g_1(a) \\ &= a - 4 \\ &= (b + 4) - 4 \\ &= b \end{aligned}$$

□

ii The following is the proof that $g_2 : \mathbb{R} \to \mathbb{R}; g_2(x) = |x| + x$ is neither one-to-one not onto:
Proof that $g_2(x) = |x| + x$ is not one-to-one

Proof. WTS: $\exists p, q \in \mathbb{R}, g_2(p) = g_2(q) \wedge p \neq q$

$$\begin{aligned} &\text{let } p = -1 \text{ and } q = -2 \\ &p \neq q \text{ is True} \\ g_2(p) &= g_2(q) \\ |-1| + (-1) &= |-2| + (-2) \\ 0 &= 0 \\ &\text{thus } g_2(p) = g_2(q) \text{ is also True.} \end{aligned}$$

□

Proof that $g_2(x) = |x| + x$ is not onto

Proof. WTS: $\exists b \in \mathbb{R}, \forall a \in \mathbb{R}, g_2(a) \neq b$

- Let $b = -1$
- Let $a \in \mathbb{R}$
- WTS: $g_2(a) \neq b$
- We will split the proof into two cases, namely $a > 0$ and $a \leq 0$

Case 1. $a > 0$

$$\begin{aligned} g_2(a) &= |a| + a \\ &> 0 \neq -1 && \text{(since both } |a| \text{ and } a > 0) \end{aligned}$$

Case 2. $a \leq 0$

$$g_2(a) = |a| + a$$

In this case, since $a \leq 0$, we know $|a| \geq 0$ and that $-a = |a|$ (since $a \leq 0$). Moreover, by using the fact that $|a| = -a$, we can conclude:

$$\begin{aligned} g_2(a) = |a| + a &= -a + a \\ &= 0 \neq -1 \end{aligned}$$

□

(b) The following are definitions and proofs for the two functions:

$$f_1, f_2 : \mathbb{Z} \to \mathbb{Z}^+ \tag{1}$$

such that:

i) f_2 is onto but not one-to-one.
Definition: $f_2(x) = |x|$

Proof. First, we will prove that f_2 is onto i.e., $\forall b \in \mathbb{Z}^+, \exists a \in \mathbb{Z}, f_2(a) = b$.
Let $b \in \mathbb{Z}^+$. Let $a = b$. We want to prove that $f_2(a) = b$.

$$\begin{aligned} f_2(a) &= |a| \\ &= a \\ &= b \end{aligned}$$

□

Next, we will prove that $f_2(x)$ is **not** one-to-one i.e., $\exists p, q, \in \mathbb{Z}, f_2(p) = f_2(q) \wedge p \neq q$.
Let $p = 3$ and $q = -3$.

Proof.

$$
\begin{aligned}
f_2(p) = |3| = 3 = |-3| = f_2(q)& \\
\text{so } f_2(p) = f_2(q) \text{ is True}& \\
3 \neq -3& \\
p \neq q \text{ is also True}&
\end{aligned}
$$

□

ii) f_1 is one-to-one but not onto:
Definition: $f_1(x) = e^x + 2$
We will first prove that $f_1(x)$ is not onto i.e., $\exists b \in \mathbb{Z}^+, \forall a \in \mathbb{Z}, f_1(a) \neq b$

Proof. :

- Let $b = 1$
- Let $a \in \mathbb{Z}$
- <u>WTS</u> : $f_1(a) \neq 1$.
- We will split the proof into two cases, namely $a > 0$ and $a \leq 0$

Case 1. $a > 0$
In this case, $e^a > 1$ and $e^a + 2 > 3 \neq 1$

Case 2.

$$
\begin{aligned}
a &\leq 0 \\
0 < e^a &\leq 1 \Rightarrow 2 < e^a + 2 \leq 3 \\
e^a &+ 2 \neq 1
\end{aligned}
$$

Since in both cases, the least value of $f_1(a)$ is $\neq 1$, we can conclude that $\forall a \in \mathbb{Z}, f_1(a) \neq 1$ □

Next, we will prove that $f_1(a)$ is one-to-one

Proof. WTS: $\forall p, q \in \mathbb{Z}, f_1(p) = f_1(q) \Rightarrow p = q$

- let $p, q \in \mathbb{Z}$
- Assume $f_1(p) = f_1(q)$
- WTS: $p = q$

$$
\begin{aligned}
f_1(p) &= f_2(q) \\
e^p + 2 &= e^q + 2 \\
e^p &= e^q && \text{(subtracting 2 from both sides)} \\
\ln(e^p) &= \ln(e^q) && \text{(Taking ln of both sides)} \\
p \cdot \ln(e) &= q \cdot \ln(e) \\
p &= q && \text{(dividing both sides by } \ln(e))
\end{aligned}
$$

□

(c) Let $f : A \to B$ and $g : B \to C$ be arbitrary functions.

i The following is a proof that if $g \circ f$ is one-to-one, then f is also one-to-one:

Proof. WTS:
$(\forall a_1, a_2 \in A, (g \circ f)(a_1) = (g \circ f)(a_2) \Rightarrow (f(a_1) = f(a_2)) \Rightarrow (\forall p, q \in A, f(p) = f(q) \Rightarrow p = q)$

- Assume $g \circ f$ is one-to-one i.e., $(\forall a_1, a_2 \in A, (g \circ f)(a_1) = (g \circ f)(a_2) \Rightarrow (f(a_1) = f(a_2))$
- let $p, q \in A$
- Assume $f(p) = f(q)$
- WTS: $p = q$

$$\begin{aligned} g(f(p)) &= g(f(q)) \\ (g \circ f)(p) &= (g \circ f)(q) && \text{(By definition of composite functions)} \end{aligned}$$

- Using our assumption that $g \circ f$ is one-to-one, we can conclude that:

$$p = q$$

□

ii The following is a proof that if $g \circ f$ is onto, then f is also onto:

Proof. WTS:
$(\forall c \in C, \exists a \in A, (g \circ f)(a) = c) \Rightarrow (\forall c \in C, \exists b \in B, g(b) = c)$

- Assume that $g \circ f$ is onto i.e., $(\forall c \in C, \exists a \in A, (g \circ f)(a) = c)$
- Let $c \in C$
- Let $b = f(a)$. Since $f(a) \in B$ according to the choice domain and co-domain of function f
- WTS: $g(b) = c_2$

$$\begin{aligned} g(b) &= g(f(a)) \\ &= (g \circ f)(a) && \text{(From the definition of function composition)} \\ &= c && \text{(using assumption that } g \circ f \text{ is onto)} \end{aligned}$$

□

iii The following is a proof that if $g \circ f$ is one-to-one and onto, then f is also both one-to-one and onto:

- We will prove that the given statement is false by proving its negation which states that:

$$\exists f : A \to B \text{ and } g : B \to C,$$
$$(\forall a_1, a_2 \in A, (g \circ f)(a_1) = (g \circ f)(a_2) \Rightarrow a_1 = a_2) \wedge (\forall c_1 \in C, \exists a \in A, (g \circ f)(a) = c_1)$$
$$\wedge$$
$$((\exists p, q \in A, f(p) = f(q) \Rightarrow p = q) \vee (\exists b \in B, \forall a_3 \in A, f(a_3) \neq b)$$
$$\vee$$
$$(\exists p_1, q_1 \in B, g(p_1) = g(q_1) \wedge p_1 \neq q_1) \vee (\exists c_2 \in C, \forall b_1 \in B, g(b_1 0 \neq c_2))$$

Proof.

- Let $A = [1, 2, 3]$
- Let $B = [4, 5, 6, 7]$
- Let $C = [8, 9, 10]$

We define $f : A \to B, g : B \to C$, and $g \circ f : A \to C$ using the following table of values where $a \in A, b \in B$

b	$g(b)$
4	8
5	8
6	9
7	10

a	$f(a)$
1	5
2	6
3	7

a	$g(f(a))$
1	8
2	9
3	10

At this point, we will prove that $\boldsymbol{g \circ f}$ **is both one-to-one** and **onto** and that $\boldsymbol{g}$ **is not one-to-one.**

Proof that $\boldsymbol{g \circ f}$ is one-to-one i.e., $(\forall a_1, a_2 \in A, (g \circ f)(a_1) = (g \circ f)(a_2) \to a_1 = a_2)$:
Let $a_1, a_2 \in A$
Assume $(g \circ f)(a_1) = (g \circ f)(a_2)$.
WTS: $a_1 = a_2$
Since $(g \circ f)(a_1)$ can take on only 3 values, we will split the proof into 3 cases based on these values.

Case 1. Let $(g \circ f)(a_1) = (g \circ f)(a_2) = 8$
From our definition of $(g \circ f)$, this value is only possible when $a_1 = a_2 = 1$

Case 2. Let $(g \circ f)(a_1) = (g \circ f)(a_2) = 9$
From our definition of $(g \circ f)$, this value is only possible when $a_1 = a_2 = 2$

Case 3. Let $(g \circ f)(a_1) = (g \circ f)(a_2) = 10$
From our definition of $(g \circ f)$, this value is only possible when $a_1 = a_2 = 3$

Proof that $\boldsymbol{g \circ f}$ is onto i.e., $(\forall c_1 \in c, \exists a \in A, (g \circ f)(a) = c_1)$: Let $c_1 \in C$
Let $a = c_1 - 7$.
From our definition of $g \circ f$ in the table above, we can see that for any c_1 we pick from the set C, we can choose on a which is 7 less than our chosen c_1
Since c_1 can take on only 3 values, we will split the proof into 3 cases based on these values.

Case 1. Let $c_1 = 8$.

$$\begin{aligned} \text{Let } a &= c_1 - 7 = 1 \\ \text{WTS: } (g \circ f)(a) &= c_1 \\ (g \circ f)(a) &= (g \circ f)(1) \\ &= 8 \\ &= c_1 \end{aligned}$$

Case 2. Let $c_1 = 9$

$$\text{Let } a = c_1 - 7 = 2$$

$$\begin{aligned}
\text{WTS: } (g \circ f)(a) &= c_1 \\
(g \circ f)(a) &= (g \circ f)(2) \\
&= 9 \\
&= c_1
\end{aligned}$$

Case 3. Let $c_1 = 10$.

$$\begin{aligned}
\text{Let } c_1 &= 10 \\
\text{Let } a &= c_1 - 7 = 3 \\
\text{WTS: } (g \circ f)(a) &= c_1 \\
(g \circ f)(a) &= (g \circ f)(3) \\
&= 10 \\
&= c_1
\end{aligned}$$

Proof that g is not one-to-one i.e., $(\exists p_1, q, \in B, g(p_1) = g(q_1) \wedge p_1 \neq q_1)$
Let $p_1 = 4$ and let $q_1 = 5$.

$$\begin{aligned}
&\text{WTS: } g(p_1) = g(q_1) \wedge p_1 \neq q \\
&4 \neq 5 \leftrightarrow p_1 \neq q_1 \\
&g(p_1) = g(4) = 8 = g(5) = g(q_1)
\end{aligned}$$

$\square$