Student Information

Full Name : Mustafa Ozan ALPAY
Id Number : 2309615

Answer 1

Let $f : A \to B$ and $g : B \to C$. Prove the following:

- **a)** If $C_0 \subseteq C$, show that $(g \circ f)^{-1}(C_0) = f^{-1}(g^{-1}(C_0))$.

  1. Let's assume that $(g \circ f)^{-1}(C_0) = f^{-1} \circ (g^{-1}(C_0))$ holds for any C_0 that is inside C.

$$\begin{aligned}
((g \circ f)^{-1} \circ (g \circ f))(C_0) &= ((f^{-1} \circ g^{-1}) \circ (g \circ f))(C_0) \\
&= (((f^{-1} \circ g^{-1}) \circ g) \circ f)(C_0) \\
&= ((f^{-1} \circ (g^{-1} \circ g)) \circ f)(C_0) \\
&= ((f^{-1} \circ I_B) \circ f)(C_0) \\
&= (f^{-1} \circ f)(C_0) \\
&= I_A(C_0) \\
&= C_0
\end{aligned}$$

  2. Similarly,

$$\begin{aligned}
((g \circ f) \circ (g \circ f)^{-1})(C_0) &= ((g \circ f) \circ (f^{-1} \circ g^{-1}))(C_0) \\
&= (((g \circ f) \circ f^{-1}) \circ g^{-1})(C_0) \\
&= (g \circ (f \circ f^{-1})) \circ g^{-1})(C_0) \\
&= ((g^{-1} \circ I_A) \circ g)(C_0) \\
&= (g^{-1} \circ g)(C_0) \\
&= I_B(C_0) \\
&= C_0
\end{aligned}$$

  3. Thus,
     (a) $((g \circ f)^{-1} \circ (g \circ f))(C_0) = C_0$ and
     (b) $((g \circ f) \circ (g \circ f)^{-1})(C_0) = C_0$
     proves that our assumption is correct.

- **b)** If $g \circ f$ is injective, what can be said about the injectivity of f and g?

  1. It is known that $g \circ f$ is injective.
  2. Let us assume, $\exists x_1, x_2 \in A$, which satisfies $f(x_1) = f(x_2)$.
  3. By using our assumption, we can say that $(g \circ f)(x_1) = g(f(x_1)) = g(f(x_2)) = (g \circ f)(x_2)$.

4. Since $g \circ f$ is injective, previous statement implies that $x_1 = x_2$. Therefore f is injective.
5. However we cannot say anything regarding the injectivity of g.

- **c)** If $g \circ f$ is surjective, what can be said about the surjectivity of f and g?

  1. It is known that $g \circ f$ is surjective.
  2. Let $z \in C$.
  3. Since $g \circ f$ is surjective, $\exists x \in A$ such that $(g \circ f)(x) = g(f(x)) = z$
  4. Let $f(x) = y$ and $y \in B$, then $g(y) = z$.
  5. Therefore g is surjective.
  6. However we cannot say anything regarding the surjectivity of f.

Answer 2

- **a)** Show that if f has a left inverse, f is injective; and if f has a right inverse, f is surjective.

  1. (a) Let us assume that f is injective.
     (b) If we choose $x_0 \in A$, the range of f^{-1} would have exactly one element from B.
     (c) Let us select an arbitrary $b \in f(A)$. In that case, $g(b)$ would be the only element of f^{-1}, while if $b \notin f(A)$, the set $g(b) = x_0$.
     (d) Since $\forall x \in A \rightarrow \exists f(x) \in f(A)$, we can summarize this as $\forall x \in A, g(f(x)) = x$
     (e) Therefore, if g is a left inverse for f, f must be injective.
  2. (a) Let us have an arbitrary $b \in B$.
     (b) We would like to find such an $a \in A$ such that $f(a) = b$.
     (c) In order to do so, let us set $a = g(b)$ and that the right inverse condition implies $f(a) = f(g(b)) = b$ as desired.
     (d) Therefore, f is surjective.

- **b)** Can a function have more than one left inverse? What about right inverses?

  1. A function can have more than one left inverse.
     (a) Let us set an arbitrary function as following;
     $f(x) = x^2$
     (b) The inverse of f can take two different values, which are
     $f^{-1}(x) = +\sqrt{x}$ and
     $f^{-1}(x) = -\sqrt{x}$
     (c) Therefore it is possible to have more than one left inverse.
  2. A function can also have more than one right inverse.
     (a) Let us set an arbitrary function that holds the followings;
     $f(1) = f(2) = 1$

(b) The inverse of f can take two different values, which are
$f^{-1}(1) = 2$ and
$f^{-1}(1) = 1$

(c) Therefore it is possible to have more than one right inverse.

- **c)** Show that if f has both a left inverse g and a right inverse h, then f is bijective and $g = h = f^{-1}$.

1. Since g is a left inverse, we can state that
   $(g \circ f)(x) = x$
2. By using the proof that on the part (a) of question 1, we can rewrite the second equation as following,
   $(f \circ g)^{-1}(x) = x$
   $g^{-1} \circ (f^{-1}(x)) = x$
   $g \circ g^{-1} \circ (f^{-1}(x)) = g(x)$
3. Since $g \circ g^{-1} = I_B$,
   $f^{-1}(x) = g(x)$
4. Likewise, since h is a right inverse, we can state that
   $(f \circ h)(x) = x$
5. By using the proof that on the part (a) of question 1, we can rewrite the second equation as following,
   $(f \circ h)^{-1}(x) = x$
   $h^{-1} \circ (f^{-1}(x)) = x$
   $h \circ h^{-1} \circ (f^{-1}(x)) = h(x)$
6. Since $h \circ h^{-1} = I_B$,
   $f^{-1}(x) = h(x)$
7. By combining the results on 3^{rd} and 6^{th} lines, we can say that
   $g(x) = f^{-1}(x) = h(x)$

Answer 3

Answer 4

Answer 5

- The definition of Θ is, a function f is $\Theta(g)$ if and only if there are constants C_1 and C_2 such that $C_1 g(n) \leq f(n) \leq C_2 g(n)$.
- If $n \ln n = \Theta(k)$, we can rewrite this as the following;
  $C_1 k \leq n \ln n \leq C_2 k$

- Since $\ln k \neq 0$, dividing this inequality by $\ln k$ is possible.

  $C_1 \frac{k}{\ln k} \leq n \frac{\ln n}{\ln k} \leq C_2 \frac{k}{\ln k}$

- By applying the limit rules,

  $\lim_{k \to \infty} \frac{\ln n}{\ln k} = 0$

- Therefore we can keep C_1 as the lower bound to show that $n = \Theta(\frac{k}{\ln k})$.

- By using $C_1 k \leq n \ln n \leq C_2 k$ again, we can say that

  $C_1 k \leq n \ln n < n^2$ for any large n.

- By taking the natural logarithm of each side,

  $\ln C_1 + \ln k < 2 \ln n$

- By rearranging the inequality,

  $\frac{\ln k}{\ln n} < 2 - \frac{\ln C_1}{\ln n} < 2$ for any large n

- If we rewrite n and use the equations that we derived above, we can get

  $n = n \frac{\ln k}{\ln n} \frac{\ln n}{\ln k} < 2C_2 \frac{k}{\ln k}$

- Finally, by combining our calculations, we can say that,

  $C_1 \frac{k}{\ln k} \leq n \leq 2C_2 \frac{k}{\ln k}$ for large k values.

- By the definition of Θ, we can conclude that $n = \Theta(\frac{k}{\ln k})$

Answer 6

a) Show that 6 and 28 are perfect.

- The set of positive divisors of 6 are $\{1, 2, 3, 6\}$. The sum of all its positive divisors excluding itself is $1 + 2 + 3 = 6$, thus making it a perfect number.

- The set of positive divisors of 28 are $\{1, 2, 4, 7, 14, 28\}$. The sum of all its positive divisors excluding itself is $1 + 2 + 4 + 7 + 14 = 28$, thus making it a perfect number.

b) Show that $2^{p-1}(2^p - 1)$ is a perfect number when $2^p - 1$ is prime.

- Since $2^p - 1$ is prime, the prime divisors of $2^{p-1}(2^p - 1)$ would be only 2 and $2^p - 1$. By using this information, we can denote the set of all positive divisors of $2^{p-1}(2^p - 1)$ as $\{1, 2, ..., 2^{p-1}, 1 * (2^p - 1), 2 * (2^p - 1), ..., 2^{p-1} * (2^p - 1)\}$

- To sum all the positive divisors, we can write the following;

$$\sum_{n=0}^{p-1} 2^n + (2^p - 1)\sum_{n=0}^{p-1} 2^n$$

- Since the summation operator has associativity, we can rearrange the equation as;

$$= (2^p) * \sum_{n=0}^{p-1} 2^n$$

- By using the formula

$$= \sum_{n=0}^{x} 2^n = 2^{x+1} - 1$$

- We can rearrange the equation;

$$= (2^p) * \sum_{n=0}^{p-1} 2^n = (2^p) * (2^p - 1)$$

- Since this summation includes all positive divisors, we need to subtract the actual number from it.

  $(2^p) * (2^p - 1) - (2^{p-1}) * (2^p - 1) = (2^{p-1}) * (2^p - 1)$

- Therefore, from this formula, we can see that the sum of all positive divisors excluding the number itself is equal to the number if and only if $2^p - 1$ is prime and the number is $2^{p-1}(2^p - 1)$.

Answer 7

a) Given $x \equiv c_1 (\bmod\ m)$ and $x \equiv c_2 (\bmod\ n)$ where c_1, c_2, m, n are integers with $m > 0, n > 0$ show that the solution x exists if and only if $\gcd(m, n)|c_1 - c_2$.

- Let us say that the system has a solution x.
- We can say that $t = gcd(m, n)$ exists.
- By using the properties of the modulo, we can say that $x - c_1 = m.\alpha$, which is also a multiple of t.
- Similarly, for the second statement, we can say that $x - c_2 = n.\beta$, which is again a multiple of t.
- Therefore, $c_1 - c_2 = (x - c_2) - (x - c_1)$ is also a multiple of t.
- Thus, $t|(c_1 - c_2)$, which is $\gcd(m, n)|c_1 - c_2$.