Student Information

Full Name : Zeynep Özalp
Id Number : 2237691

Answer 1

a)

If f^{-1}, g^{-1} and $(gof)^{-1}$ do not exist, there is nothing to prove. So assuming that they exist, let $g \circ f = z$. Then, $z^{-1} = (gof)^{-1}$. Let a, b, c such that

$$(a \in A_0) \wedge (b \in B_0 \wedge f(a) = b) \wedge (c \in C_0 \wedge g(b) = c)$$

$$(A_0 \subseteq A) \wedge (B_0 \subseteq B) \wedge (C_0 \subseteq C)$$

Therefore,

$$z(a) = c$$
$$z^{-1}(c) = a$$

Note that, $g^{-1}(c) = b$ and $f^{-1}(b) = a$. Thus,

$$f^{-1}(g^{-1}(c)) = a$$

which is equal to equation $z^{-1}(c) = a$.

$$z^{-1}(c) = f^{-1}(g^{-1}(c))$$

$$(g \circ f)^{-1}(c) = f^{-1}(g^{-1}(c))$$

Since the last equation is true for some arbitrary element of C_0, one can conclude that the equation is valid for all elements of C_0. Hence,

$$(g \circ f)^{-1}(C_0) = f^{-1}(g^{-1}(C_0))$$

b)

Injectivity of f

Assume that f is not injective.

$$(f(a_1) = f(a_2)) \wedge (a_1 \neq a_2)$$

Therefore,

$$((g \circ f)(a_1) = (g \circ f)(a_2)) \wedge (a_1 \neq a_2)$$

$$\perp$$

Contradiction since $g \circ f$ is injective. Therefore, our assumption is false and f is injective.

Injectivity of g

When the domain of g is the range of f, g must be injective. However, g may have other other elements in its domain such that those elements are not in the range of f and g may not be injective for those elements. Therefore, g is not necessarily injective. It can be injective or not.

c)

Surjectivity of g

Assume that there exists some z such that

$$(z \in C) \wedge (z \notin g(B_0)) \; where \; B_0 \subset B$$

Therefore,

$$(z \in C) \wedge (z \notin (g \circ f)(A_0)) \; where \; A_0 \subset A \; and \; f(A_0) = B_0$$

$$\bot$$

Contradiction since $(g \circ f)$ is surjective. Therefore, our assumption is false and f is injective.

Surjectivity of f

i) Assume that f is not surjective so that its range is B_0.

$$f(A) = B_0 \subset B$$

$$(g \circ f)(A) = g(B_0) = C$$

This equation is valid and makes no contradiction since we know that $g \circ f$ is surjective.
ii) Assume that f is surjective so that its range is B.

$$f(A) = B$$

$$(g \circ f)(A) = g(B) = C$$

This equation is valid and makes no contradiction since we know that $g \circ f$ is surjective.
Therefore, f is not necessarily surjective. It can be surjective or not.

Answer 2

a)

Injectivity of f

Assume that

$$f(x) = f(y)$$

$$(g \circ f)(x) = (g \circ f)(y)$$

$$x = y \; since \; (g \circ f)(x) = x \; and \; (g \circ f)(y) = y$$

Therefore, f is injective.

Surjectivity of f

For some $b \in B$ the following is true.

$$(f \circ h)(b) = b$$

Thus, every element in of B has a pre-image in A and f is surjective.

b)

Yes, a function can have more than one left and right inverses. Consider these examples:
$f : \{1, 2\} \to \{1\}$ defined by $f(1) = f(2) = 1$

$g_1 : \{1\} \to \{1, 2\}$ defined by $g_1(1) = 1$ so that $(g_1 \circ f)(1) = 1$
$g_2 : \{1\} \to \{1, 2\}$ defined by $g_2(1) = 2$ so that $(g_2 \circ f)(2) = 2$

$h_1 : \{1\} \to \{1, 2\}$ defined by $h_1(1) = 1$ so that $(f \circ h_1)(1) = 1$
$h_2 : \{1\} \to \{1, 2\}$ defined by $h_2(1) = 2$ so that $(f \circ h_2)(1) = 1$

Clearly, g_1 and g_2 are left inverses of f and h_1 and h_2 are right inverses of f.

c)

If f has a left inverse g then it is injective and if f has a right inverse h then it is subjective. Since f has both right and left inverses, it is both injective and subjective, i.e., f is bijective.
Now, choose an arbitrary $x \in B$.

$$f(h(x)) = x$$

Apply g to both sides.

$$g(f(h(x))) = g(x)$$

However, for all $x_0 \in A$, $g(f(x_0)) = x_0$. Thus,

$$g(f(h(x))) = h(x) = g(x)$$

Therefore, $g = h = f^{-1}$.

Answer 3

Bijectivity of f

Choose arbitrary x_1, x_2 in the domain of f and y_1, y_2 in A such that $f(x_1, y_1) = f(x_2, y_2)$. Therefore,

$$(x_1 + y_1 - 1, y_1) = (x_2 + y_2 - 1, y_2)$$

Thus, $x_1 + y_1 - 1 = x_2 + y_2 - 1$ and $y_1 = y_2$. Since $x_1 + y_1 = x_2 + y_2$ and $y_1 = y_2$, clearly $x_1 = x_2$. Thus, f is injective.

$$f(x_1, y_1) = (x_1 + y_1 - 1, y_1)$$

For all positive integers x_1 and y_1, $y_1 \leq x_1 + y_1 - 1$. Since for all of the pairs $(x_1 + y_1 - 1, y_1)$ is in A, f is surjective.
Function f is bijective.

Bijectivity of g

Let $h, i : Z^+ \to Z^+$, $h(x) = \frac{1}{2}(x^2 - x)$ and $i(y) = y$.

$$i(y_1) = i(y_2) \wedge (y_1 \neq y_2))$$
$$y_1 = y_2$$
$$\perp$$
$$h(x_1) = h(x_2) \wedge (x_1 \neq x_2)$$
$$\frac{1}{2}({x_1}^2 - x_1) = \frac{1}{2}({x_2}^2 - x_2)$$
$${x_1}^2 - x_1 = {x_2}^2 - x_2$$
$${x_1}^2 - {x_2}^2 = x_1 - x_2$$

Since $x_1 \neq x_2$, $x_1 - x_2 \neq 0$, we can divide the equation by $x_1 - x_2$.

$$x_1 + x_2 = 1$$
$$\perp$$

Contradiction since x_1 and x_2 are defined as positive integers. So, h and i is injective.

Note that the sum of injective functions may not injective since for some function $k(x) = x$, $l(x) = -x$ and then $(k + l)(x) = 0$ is not injective. However, the domain of $g(x, y)$ is A such that $x, y \in Z^+$; therefore, the sum of injective functions is injective on that domain. Thus, $g(x, y) = h(x) + i(y)$ is injective.

By Theorem.2 on p.239, $\forall a, d \in Z$, $d > 0$, there exists unique q, r such that $a = qd + r$ where $0 \leq r < d$.

$$q = 1/2(x - 1)$$
$$d = x$$
$$r = y$$
$$g(x, y) = qd + r$$

The function g is surjective. Thus, it is bijective.

Answer 4

a)

WE know that the set of positive rational numbers are countable from ex.4/p.172 in our textbook. Since the mapping $Q^+ \to Q^-$ is bijective, Q^- is also countable. The union of countable sets Q^+, Q^-, $\{0\}$ is also countable. So, the set of rational numbers is countable.

Let

$$P_n = \{x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 \mid a_i \in Q,\ i = 0, ..., n-1\}$$

and

$$Q^n = \{(a_{n-1}, ..., a_0) \mid a_i \in Q,\ i = 0, ..., n-1\}$$

. Clearly, the mapping $P_n \to Q^n$ is a bijective from P_n to Q^n and therefore, P_n has the same cardinality with Q^n.

Q^n is the set of n-tuples where all $a_i \in Q,\ i = 0, ..., n-1$. The elements of $a_0, ..., a_{n-1}$ need not to be distinct, so Q^n is also countable. So is P_n. Since the set of all polynomials with rational coefficients is the union of all P_i's where $i = 0, ..., n$, it is countable. Since each polynomial has finite number of roots, the set of all polynomials with countable roots are also countable. Thus, the set of algebraic real numbers is countable.

b)

Let A be the set of algebraic real numbers and T is the set of trancendental real numbers. Note that $A \subset R$, $T \subset R$, $A = R - T$ and A is countable, so is $R - T$. Assume that T is countable.

$$T \cup (R - T) = R$$

From our assumption, the union of two countable sets should be countable. Hovewer, the set of real numbers are not countable and our assumption is false. Thus, the set of trancendental real numbers are not countable.

Answer 5

For positive a_1, a_2 where $a_1 < a_2$ and sufficiently large n

$$a_1 n.ln(n) < k < a_2 n.ln(n)$$

$$ln(a_1 n.ln(n)) < ln(k) < ln(a_2 n.ln(n))$$

Divide the first equation by the second one.

$$\frac{a_1 n.ln(n)}{ln(a_1 n.ln(n))} < \frac{k}{ln(k)} < \frac{a_1 n.ln(n)}{ln(a_2 n.ln(n))}$$

$$a_1 n.ln(n - a_1 n.ln(n)) < \frac{k}{ln(k)} < a_2 n.ln(n - a_2 n.ln(n))$$

$$n - a_1 n.ln(n) > 0$$

by the definiton of ln. Thus,

$$n > a_1 n.ln(n)$$

Since $n \neq 0$, divide by n.

$$a_1 ln(n) < 1$$

Assume that $ln(n - a_1 n.ln(n)) > n$. We can write

$$ln(n - a_1 n.ln(n)) > a_1 n.ln(n)$$

since $n > a_1 n.ln(n)$. Divide by $ln(n) \neq 0$.

$$ln(a_1 n.ln(n)) > a_1 n$$

Let $b_1 = a_1 ln(n)$ and thus $b_1 < 1$. Put b_1.

$$ln(b_1 a_1) > a_1 n$$

$$\perp$$

Contradiction since $b_1 < 1$, $a_1 > 0$ and n is sufficiently large. So, our assumption is false and $ln(n - a_1 n.ln(n)) < n$. The same steps is valid for a_2 and $b_2 = a_2 ln(n)$. Therefore,

$$\Theta(\frac{k}{ln(k)}) = n$$

Answer 6

a)

$$6 = 1 + 2 + 3$$

$$28 = 1 + 2 + 4 + 7 + 14$$

b)

Suppose $k = 2^p - 1$ is prime and let $n = 2^{p-1}(2^p - 1)$.
Let $f(n)$ be the sum of the positive divisors of n. Note that:
1. When n is perfect, $f(n) = 2n$.
2. When n is prime, $f(n) = n + 1$.
3. $f(2^a) = 1 + 2^1 + 2^2 + ... + 2^{a-1} = 2^a - 1$
4. $f(n) = f(p_1^{a_1})f(p_2^{a_2})...f(p_n^{a_n})$ where p_i's are prime divisors of n and a_i's are the powers of them. So, $f(mn) = f(m)f(n)$ where m and n are relatively prime.

Since $2^p - 1$ is prime, $2^p - 1$ and 2^{p-1} are relatively prime. Therefore,

$$f(n) = f(2^{p-1})f(2^p - 1) = (2^p - 1)2^p = 2n$$

Thus, $n = 2^{p-1}(2^p - 1)$ is perfect when $2^p - 1$ is prime.

Answer 7

a)

By the definition,

$$x = nd_2 + c_2 = md_1 + c_1$$

$$nd_2 - md_1 = c_1 - c_2$$

Let $gcd(m, n) = g$. Take $(mod\ g)$ of both sides.

$$0 \equiv c_2 - c_1 (mod\ g)$$

Therefore, $gcd(m, n) \mid c_2 - c_1$.

b)

Let $d = gcd(m, n)$. By Bezout's Theorem on p.269 in our textbook, there exist $s, t \in Z$ such that $d = sm + tn$. Let (q_1, r) and (q_2, r) be the quotient and remainder of c_1 and c_2 upon division by d. Then $x = q_1 sm + q_2 tn + r$ is a unique modulo $lcm(m, n)$.

Assume that there is two distinct $x_1 > 0,\ x_2 > 0$ and $m,\ n$ are relatively prime. Therefore, $lcm(m, n) = mn$.

$$x_1 - x_2 = 0$$

$$x_1 - x_2 \equiv 0(mod\ m) \equiv 0(mod\ n)$$

$$x_1 - x_2 \equiv 0(mod\ mn)$$

Since $x_1 - x_2$ has no remainder, $x_1 - x_2 \geq lcm(mn)$. Thus, there is no distict $x_1 > 0,\ x_2 > 0$ in the interval $[0,\ lcm(m, n))$.
Now, suppose that $m,\ n$ are not relatively prime. Let $m = ay$ and $n = by$ then $lcm(m, n) = aby$. Since m, n are not relatively prime, $c_1 = c_2$.

$$x_1 \equiv c_1 (mod\ ay) \equiv c_1 (mod\ by)$$

$$x_2 \equiv c_1 (mod\ ay) \equiv c_1 (mod\ by)$$

Therefore,

$$x_1 - x_2 = ay(d_1 - d_3)$$

$$or$$

$$x_1 - x_2 = by(d_2 - d_4)$$

Clearly, x_1 and x_2 are divisable by both ay and by. Thus,

$$x_1 - x_2 \equiv 0(mod\ aby)$$

Since $x_1 - x_2$ has no remainder, $x_1 - x_2 \geq lcm(mn)$. Thus, there is no distict $x_1 > 0,\ x_2 > 0$ in the interval $[0,\ lcm(m, n))$.