Student Information

Full Name : Ceydanur Köylü
Id Number : 2633386

Answer 1

a) The statement is true for a fixed $m > 3$, and I picked $m = 4$ for the proof. Assume

$$\forall x_1, x_2 \in C, t_0, t_1, t_2, t_3 \in [0, 1]$$

Where C is a convex set with the given definition, such that $C \subseteq R^n$. So we can derive from the convex set definition:

$$tx_1 + (t-1)x_2 = x_3 \in C$$

$$t_1x_3 + (1-t_1)x_2 = t_1(tx_1 + (t-1)x_2) + (1-t_1)x_2 = (t_1t)x_1 + (-t_1t + 1)x_2 = x_4 \in C$$

Then we can use this method of substituting to further discover elements of C as linear combinations of others:

$$t_2x_4 + (1-t_2)x_3 = (t_2t_1t)x_1 + (-t_2t_1t + t_2)x_2 + (-t_2 + 1)x_3 = x_5 \in C$$

$$t_3x_5 + (1-t_3)x_4 = (t_3t_2t_1t)x_1 + (-t_3t_2t_1t + t_3t_2)x_2 + (-t_3t_2 + t_3)x_3 + (-t_3 + 1)x_4 = x_6 \in C$$

We can set $\lambda_1 = (t_3t_2t_1t)$, $\lambda_2 = (-t_3t_2t_1t + t_3t_2)$, $\lambda_3 = (-t_3t_2 + t_3)$, $\lambda_4 = (-t_3 + 1)$ where $i \in \{1, ..., m\}$, $\lambda_i \geq 0$ and $\lambda_i \in \mathbb{R}$ since $t, t_1, t_2, t_3 \in [0, 1]$. Thus we can observe that for arbitrary t, t_1, t_2, t_3:

$$\sum_{i=1}^{m} \lambda_i = 1 \text{ and } \sum_{i=1}^{m} \lambda_i x_i \in C \text{ where } x_i \in C$$

Also observe that this procedure can be replicated for all $m > 3$. Take the above part as the base case and assume that this statement is true for $m = k$ as the inductive hypothesis. Then we can simply write $t_{k-1}x_{k+1} + (1-t_{k-1})x_k$ as a linear combination of x_i's such that $i \in \{1, 2, 3, ..., k\}$ which is the same procedure as exampled above. So by this inductive step, we can say that this statement is true for all $m > 3$.

b) This statement is false and we can prove this by contradiction:

Let $g(x) = x^2$ such that $\forall x_1, x_2 \in \mathbb{R}^n, \quad t \in [0, 1] \quad f(tx_1 + (1-t)x_2) \leq tf(x_1) + (1-t)f(x_2)$

To prove this claim:

$$f(tx_1+(1-t)x_2) = t^2x_1^2+(1-2t+t^2)x_2^2+2(t-t^2)x_1x_2 \leq tf(x_1)+(1-t)f(x_2) = tx_1^2+(1-t)x_2^2$$

Subtract from both sides, $t^2x_1^2$ and $(1-2t+t^2)x_2^2$:

$$2(t-t^2)x_1x_2 \leq (t-t^2)x_1^2 + (t-t^2)x_2^2$$

Since $t \in [0,1], \quad t \geq t^2$ and $t - t^2 \geq 0$ we can divide by $(t-t^2)$ and then subtract $2(x_1x_2)$ from both sides:

$0 \leq x_1^2 - 2x_1x_2 + x_2^2 = (x_1 - x_2)^2$ which is true $\forall x_1, x_2 \in \mathbb{R}^n$ and hence $f(x)$ is a convex function.

Also let $g(x) = x^2 - 1$ such that $\forall x_1, x_2 \in \mathbb{R}^n, \quad t \in [0,1] \quad g(tx_1 + (1-t)x_2) \leq tg(x_1) + (1-t)g(x_2)$

To prove this claim:

$$g(tx_1 + (1-t)x_2) = t^2x_1^2 + (1-2t+t^2)x_2^2 + 2(t-t^2)x_1x_2 - 1$$

$$tg(x_1) + (1-t)g(x_2) = t(x_1^2 - 1) + (1-t)(x_2^2 - 1) = tx_1^2 + (1-t)x_2^2 - 1$$

If we subtract -1 from both sides, we get the exact same statement that we have proved for $f(x)$. So $g(x)$ is a convex function.

Then, let $f \circ g = h$ such that $h(x) = f(g(x)) = x^4 - 2x^2 + 1$. According to the given statement if f and g are convex functions, $f \circ g$ is a convex function as well, so for the statement to be true:

$$\forall x_1, x_2 \in \mathbb{R}^n, \quad t \in [0,1], \quad h(tx_1 + (1-t)x_2) \leq th(x_1) + (1-t)h(x_2)$$

However consider the case where $x_1 = -1, x_2 = 1, t = 0.5$. Then we have:

$$h(tx_1 + (1-t)x_2) = h(0) = 1 \quad th(x_1) + (1-t)h(x_2) = 0$$

Which means $\exists x_1, x_2 \quad h(tx_1 + (1-t)x_2) > th(x_1) + (1-t)h(x_2)$ which is a contradiction with the given statement, hence it is proven to be false.

c) Since the claim is an "if and only if" statement we need to go step by step and prove both forward and backward implications.

Forward Implication:

Assume that a function $f(\cdot) : S \subseteq \mathbb{R}^n \rightarrow \mathbb{R}$ is a convex function. We want to show that S is a convex set, and for any $x \in S$ and $v \in \mathbb{R}^n$, the function $g(t) = f(x + tv)$ is convex for all $t \in \mathbb{R}$ such that $x + tv \in S$.

For S to be convex, we need to show that for any $x_1, x_2 \in S$ and $t \in [0,1]$, the point $tx_1 + (1-t)x_2$ is also in S.

Take $x_1, x_2 \in S$ and $t \in [0,1]$ such that $f(x_1), f(x_2)$ exists since f is defined on S. Since $f(\cdot)$ is convex, according to the convexity definition:

$$f(tx_1 + (1-t)x_2) \leq tf(x_1) + (1-t)f(x_2)$$

This implies that $f(tx_1+(1-t)x_2)$ exists, and since $f(\cdot)$ is defined on S, $tx_1+(1-t)x_2 \in S$. Therefore, S is convex.

Now, let's consider the function $g(t) = f(x+tv)$. We want to show that $g(t)$ is convex for all $t \in \mathbb{R}$ such that $x + tv \in S$. Then let's take $t_1, t_2 \in \mathbb{R}$ and $k \in [0,1]$:

$$g(t_1) = f(x + t_1 v), \quad g(t_2) = f(x + t_2 v)$$

Where $(x+tv) \in S$ because of the definition of the relation between f and g. Then using the definition of g(t):

$$g(kt_1 + (1-k)t_2) = f(x + t_1 kv + (1-k)t_2 v) = f(k(x + t_1 v) + (1-k)(x + t_2 v))$$

And also,

$$kg(t_1) + (1-k)g(t_2) = kf(x + t_1 v) + (1-k)f(x + t_2 v)$$

Notice that since by definition, f is a convex function, so:

$$f(k(x + t_1 v) + (1-k)(x + t_2 v)) \leq kf(x + t_1 v) + (1-k)f(x + t_2 v)$$

Now we can replace the above statement by using the equalities that we obtained:

$$g(kt_1 + (1-k)t_2) \leq kg(t_1) + (1-k)g(t_2)$$

And thus we have proved that g(t) is a convex function, implied by our first assumption.

Backward Implication:

Assume that S is a convex set, and for any $x \in S$ and $v \in \mathbb{R}^n$, the function $g(t) = f(x+tv)$ is convex for all $t \in \mathbb{R}$ such that $x + tv \in S$. We want to show that $f(\cdot) : S \subseteq \mathbb{R}^n \to \mathbb{R}$ is a convex function. Let's take $t_1, t_2 \in \mathbb{R}$ and $k \in [0,1]$ such that $(x + t_1 v), (x + t_2 v), k(x + t_1 v) + (1-k)(x + t_2 v) \in S$ since S is defined as a convex set. Now, since the function f's domain is S, the following can be written:

$$g(t_1) = f(x + t_1 v), \quad g(t_2) = f(x + t_2 v)$$

Then we can also write:

$$g(kt_1 + (1-k)t_2) = f(x + t_1 kv + (1-k)t_2 v) = f(k(x + t_1 v) + (1-k)(x + t_2 v))$$

$$kg(t_1) + (1-k)g(t_2) = kf(x + t_1 v) + (1-k)f(x + t_2 v)$$

Since g(t) is defined as a convex function:

$$g(kt_1 + (1-k)t_2) \leq kg(t_1) + (1-k)g(t_2)$$

Then we can rewrite the above statement using the equalities we obtained:

$$f(k(x + t_1 v) + (1-k)(x + t_2 v)) \leq kf(x + t_1 v) + (1-k)f(x + t_2 v)$$

And hence, $f(\cdot)$ is a convex function, implied by our assumption.

Answer 2

Answer 3

a) The statement is true and we can show this by proving the two way implications.

Forward Implication:

Assume that the congruence $ax \equiv b \pmod{p}$ has a solution, which means there exists an integer x such that $ax \equiv b \pmod{p}$. This implies that there exists an integer k such that $ax - b = kp$.

Now, let's apply Bezout's identity. By Bezout's identity, there exist integers s and t such that $as + pt = \gcd(a, p)$. Multiplying both sides by k, we get:

$$kas + kpt = k\gcd(a, p)$$

Then we can substitute kp by the above statement:

$$ksa + (ax - b)t = k\gcd(a, p)$$

By a rearrangement of the terms:

$$ksa + ax - k\gcd(a, p) = bt$$

Notice that the LHS is divisible by $\gcd(a, p)$ since $\gcd(a, p) \mid a$ by its definition. Then since s, t, x, k are all integers, the RHS must also be divisible by $\gcd(a, p)$ such that:

$$(ksa + ax - k\gcd(a, p))/(\gcd(a, p)) = y \in \mathbb{Z}$$

$$y = bt/(gcd(a, p)$$

Note that this statement must hold for all possible s, t pairs so we have to choose b such that $gcd(a, p) \mid b$. Which means our assumption implies $gcd(a, p) \mid b$.

Backward Implication:

Assume that $\gcd(a, p) \mid b$. This means that there exists an integer k such that $b = k\gcd(a, p)$. Note that we can express $k\gcd(a, p)$ as $ksa + ktp$ using Bezout's identity since the identity says $\exists s, t \in \mathbb{Z}$ such that $as + pt = \gcd(a, p)$. Then:

$$ksa + ktp = k\gcd(a, p) = b$$

Replace $ks = x$, $kt = -y$ where $x, y \in \mathbb{Z}$ since $k, s \in \mathbb{Z}$. Then we have:

$$ax - py = b \text{ which implies } ax - b = py$$

And since $x, y \in \mathbb{Z}$:

$$ax \equiv b \pmod{p}$$

b) The statement is true such that pair of congruences $a_1x \equiv b_1 \pmod{p_1}$ and $a_2x \equiv b_2 \pmod{p_2}$ has a solution for x if $\gcd(p_1, p_2) = 1$, $\gcd(a_1, p_1) \mid b_1$, and $\gcd(a_2, p_2) \mid b_2$. Note that in part (a) we have proven that there exists a solution for $x \in \mathbb{Z}$ in $ax \equiv b \pmod{p}$ if $\gcd(a, p) \mid b$. So we can say that there exists solutions $x_1, x_2 \in \mathbb{Z}$ for the below equations:

$$a_1x_1 \equiv b_1 \pmod{p_1} \text{ since } \gcd(a_1, p_1) \mid b_1$$

$$a_2x_2 \equiv b_2 \pmod{p_2} \text{ since } \gcd(a_2, p_2) \mid b_2$$

Now assume that $x_1 = x_2 = x \in \mathbb{Z}$. Multiply the congruences by a_2 and a_1 correspondingly:

$$a_1a_2x \equiv a_2b_1 \pmod{p_1} \text{ which means } a_1a_2x = a_2b_1 + sp_1, \quad s \in \mathbb{Z}$$

$$a_1a_2x \equiv a_1b_2 \pmod{p_2} \text{ which means } a_1a_2x = a_1b_2 + tp_2, \quad t \in \mathbb{Z}$$

Then we can replace a_1a_2x in the second congruence by the first equation obtained:

$$a_2b_1 + sp_1 \equiv a_1b_2 \pmod{p_2}$$

Subtract a_2b_1 from both sides:

$$sp_1 \equiv a_1b_2 - a_2b_1 \pmod{p_2}$$

Note that since $\gcd(p_1, p_2) = 1$ we know that $p_1 \pmod{p_2}$ is invertible. So let p_1' be an inverse for this mod, such that $p_1p_1' \equiv 1 \pmod{p_2}$. So multiply the above equation by p_1':

$$s \equiv p_1'(a_1b_2 - a_2b_1) \pmod{p_2} \text{ which means } s = p_1'(a_1b_2 - a_2b_1) + p_2t, \quad t \in \mathbb{Z}$$

Then we can write a_1a_2x in the form of:

$$a_1a_2x = a_2b_1 + sp_1 = a_2b_1 + p_1(p_1'(a_1b_2 - a_2b_1) + p_2t)$$

$$a_1a_2x = a_2b_1 + p_1p_1'(a_1b_2 - a_2b_1) + p_1p_2t$$

So if x is a solution for both congruences, the above form should satisfy both equations:

$$a_2b_1 + p_1p_1'(a_1b_2 - a_2b_1) + p_1p_2t \equiv a_2b_1 \pmod{p_1}$$

$$a_2b_1 + p_1p_1'(a_1b_2 - a_2b_1) + p_1p_2t \equiv a_2b_1 + 1(a_1b_2 - a_2b_1) + 0 \equiv a_1b_2 \pmod{p_2}$$

Thus we can conclude that $a_1a_2x_1 = a_1a_2x_2 = a_1a_2x$ which means there exists a solution $x \in \mathbb{Z}$ such that $x_1 = x_2 = x$ where x satisfies both congruences.

c) The case of one modulus is trivial, the solutions can be found easily with using the given congruence.

In part (b) I have proven the case where all of the conditions are the same, and there are two congruences. To prove by induction, I will use this as the base case.

Assume that there is a solution if there exists k congruences. Then in the case of $(k+1)$ congruences, the problem can be reduced to k congruences, by converting two of the given congruences into one, as shown in part (b), and thus a solution can be found by using the k congruences. So with this inductive step, I have shown that there exists a solution for x for any number of congruences with the given conditions.

Answer 4

a) The Cartesian product of a countable set with itself is still countable, so the statement is true. Note that for any $i \in \mathbb{Z}^+$, the Cartesian product X^i represents the set of all i-tuples where each of these tuples' elements are picked from X.

Let us consider $X^1, X^2, \ldots$:

- X^1 is the set of all single letters from X, such that $X^1 = \{a, b, c, \ldots\}$ which is X itself. Since X is finite, X^1 is also finite.
- X^2 is the set of all ordered pairs of letters from X, such that $X^2 = \{(a, a), (a, b), (b, a), \ldots\}$. Since $|X| = 29$, $|X^2| = |X| \times |X| = 29 \times 29$ is finite.

  Similarly, $X^3, X^4, \ldots X^i, \ldots$ represent sets of ordered i elemented tuples. Each of these sets is also finite since we can calculate the cardinality of any such given Cartesian product.

Thus we can conclude that the Cartesian product X^i for any positive integer i is a finite set, and the union of all these sets is also finite. Therefore, since the product of all X sets, which is the union of $X^1, X^2, X^3, \ldots$, is finite; it is a countable set.

b) Assume that for every element in $\{Y_i\}_{i\in\mathbb{Z}^+}$ there exists some surjective function $f_i : \mathbb{Z} \to Y_i$ such that it connects all the elements in that Y_i to an element in $\mathbb{Z}$. Which is true since $\{Y_i\}_{i\in\mathbb{Z}^+}$ consists of only countably infinite elements.

Then we can define a new function $g : \mathbb{Z} \times \mathbb{Z} \to \bigcup_{i\in\mathbb{Z}^+ Y_i}$ such that $g(i, x) = f_i(x)$ where the first element maps to the i^{th} element of the union, and the second element maps to the elements of the set Y_i. Since we know that each Y_i is countably infinite, we can map to the elements of each set using $\mathbb{Z}$.

Thus we can say that the newly created function g is surjective, since for every element in $\bigcup_{i\in\mathbb{Z}^+ Y_i}$ there exists a pair (i, x) such that $g(i, x) = b \in \bigcup_{i\in\mathbb{Z}^+ Y_i}$. And since it is given with the question, we know that $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{Z}|$ and since $\mathbb{Z}$ is countable, $\mathbb{Z} \times \mathbb{Z}$ is also countable.

In conclusion there exists a surjective function $g : \mathbb{Z} \times \mathbb{Z} \to \bigcup_{i\in\mathbb{Z}^+ Y_i}$ which means there exists a surjective mapping from a countably infinite set to the given union of sets. Which means the given union of sets must be countably infinite too.