CS201 Discrete Mathematics Midterm-24Spring

Total: **110 pts**

Problem 1. 12 pts

Description

S is a set of connectives. If any truth function can be expressed by a propositional formula containing only the connectives in S, then S is called a universal functional set. In this question, the domains of all propositions are the same.

(a) It is known that $\neg$, $\vee$ and $\wedge$ can form a universal functional set. Prove that $\neg$ and $\vee$ can also form a universal functional set.

(b) Prove that $((\neg p \vee q) \wedge (p \vee r)) \to (q \vee r)$ is a tautology.

(c) Given that $\forall x(P(x) \to (Q(x) \wedge R(x)))$, $\forall x(P(x) \wedge S(x))$, use rules of inference to prove it, do not use logical equivalences.

Answer

(a) By **De Morgan's laws**, we have $p \wedge q \equiv \neg(\neg p \vee \neg q)$, thus every $\wedge$ can be replaced by $\neg$ and $\vee$.

(b)

$$((\neg p \vee q) \wedge (p \vee r)) \to (q \vee r)$$

$$\equiv \neg((\neg p \vee q) \wedge (p \vee r)) \vee (q \vee r)$$

$$\equiv (\neg(\neg p \vee q) \vee \neg(p \vee r)) \vee q \vee r$$

$$\equiv (p \wedge \neg q) \vee (\neg p \wedge \neg r) \vee q \vee r$$

$$\equiv ((p \wedge \neg q) \vee q) \vee ((\neg p \wedge \neg r) \vee r)$$

$$\equiv ((p \vee q) \wedge (\neg q \vee q)) \vee ((\neg p \vee r) \wedge (\neg r \vee r))$$

$$\equiv ((p \vee q) \wedge T) \vee ((\neg p \vee r) \wedge T)$$

$$\equiv (p \vee q) \vee (\neg p \vee r)$$

$$\equiv (p \vee \neg p) \vee q \vee r$$

$$\equiv T \vee q \vee r$$

$$\equiv T$$

thus it is a tautology.

(c)

$$\forall a(P(a) \wedge S(a)) \ (1)$$

$$\forall a \ P(a) \ (2)$$

$$\forall a \ S(a) \ (3)$$

$$\forall a(P(a) \rightarrow (Q(a) \wedge R(a))) \ (4)$$

By (2) and (4), we have:

$$\forall a \ Q(a) \ (5)$$

$$\forall a \ R(a) \ (6)$$

By (3) and (6), we have:

$$\forall a(R(a) \wedge S(a)) \ (7)$$

So $\forall x(R(x) \wedge S(x))$.

Problem 2. 10 pts

Description

(a) Prove or disprove that for $x, y \in \mathbb{N}_+$, $x^4 + y^4 = 625$ exists a solution.

(b) Prove or disprove $n^2 - 79n + 1601$ is a prime for $\forall n \in \mathbb{N}_+$.

Answer

(a) Disprove: Notice that $5^4 = 625$, thus $x, y \leq 5$.

If $x = 1$, then $y^4 = 624$, invalid;
if $x = 2$, then $y^4 = 609$, invalid;
if $x = 3$, then $y^4 = 544$, invalid;
if $x = 4$, then $y^4 = 369$, invalid;
If $x = 5$, then $y = 0$, $y \notin \mathbb{N}_+$.

Thus there does not exist a solution.

(b) Disprove: $n^2 - 79n + 1601 = (n-40)^2 + (n+1)$. If $k(n-40) = n+1$ $(k \in \mathbb{N}_+)$, then $n^2 - 79n + 1601$ is not a prime. Let $k = 2$, which means when $n = 81$, $n^2 - 79n + 1601 = 1763 = 41 * 43$ is not a prime.

Problem 3. 10 pts

Description

Prove or disprove that there exists $x \in \mathbb{Q}$ and $y \in \mathbb{R} \setminus \mathbb{Q}$, such that $x^y \in \mathbb{R} \setminus \mathbb{Q}$. In this problem, you can directly use $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$.

Answer

Prove: Consider $2^{\sqrt{2}}$.

If $2^{\sqrt{2}} \in \mathbb{R} \setminus \mathbb{Q}$, then we are done.

If $2^{\sqrt{2}} \in \mathbb{Q}$, for $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$, then $\frac{\sqrt{2}}{4} \in \mathbb{R} \setminus \mathbb{Q}$. Consider $(2^{\sqrt{2}})^{\frac{\sqrt{2}}{4}}$, and it is equal to $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$, we still find an example.

Thus this kind of x^y always exists.

Problem 4. 10 pts

Description

A function $f: A \to B$, S is a subset of B, then $f^{-1}(S)$ is defined as $f^{-1}(S) = \{a \in A \mid f(a) \in S\}$. Prove or disprove that $\forall S,\ f^{-1}(\overline{S}) = \overline{f^{-1}(s)}$.

Answer

Prove: $\forall a \in f^{-1}(\overline{S}) = \{a \in A \mid f(a) \in \overline{S}\}$, then $f(a) \in \overline{S}$, which means $f(a) \in B \setminus S$, $f(a) \notin S$, thus $a \notin f^{-1}(S)$, $a \in \overline{f^{-1}(S)}$. So $f^{-1}(\overline{S}) \subseteq \overline{f^{-1}(S)}$.

$\forall a \in \overline{f^{-1}(S)}$, $a \notin f^{-1}(S)$, $f(a) \notin S$. For $f(a) \in B$, then $f(a) \in B \setminus S$, thus $a \in f^{-1}(\overline{S})$. So $\overline{f^{-1}(S)} \subseteq f^{-1}(\overline{S})$.

Thus, $f^{-1}(\overline{S}) = \overline{f^{-1}(S)}$.

Problem 5. 8 pts

Description

Given the function $f(x) = \frac{x^2+1}{x^2+2}$, domain and range are both $\mathbb{R}$.

(a) Prove or disprove that $f(x)$ is injective.
(b) Prove or disprove that $f(x)$ is surjective.

Answer

(a) Disprove: Notice that $f(x) = f(-x)$, but $x \neq -x$, thus $f(x)$ is not injective.

(b) Disprove: $f(x) = 1 - \frac{1}{x^2+2}$. For $x^2 + 2 > 0$, $f(x) < 1$, which can not cover the range $\mathbb{R}$, thus $f(x)$ is not surjective.

Problem 6. 10 pts

Description

Prove that if n is odd, then $n^2 \equiv 1 \ (mod\ 8)$.

Answer

For n is odd, suppose that $n = 2k+1\ (k \in \mathbb{Z})$, then $n^2 = (2k+1)^2 = 4k(k+1)+1$. k and $k+1$ must be an even and an odd, then $k(k+1)$ must be even. Thus $2 \mid k(k+1)$, $8 \mid 4k(k+1)$, so $n^2 = 4k(k+1)+1 \equiv 1\ (mod\ 8)$.

Problem 7. 10 pts

Description

Prove that there does not exist an one-to-one correspondence from $\mathbb{Z}^+$ to $\mathcal{P}(\mathbb{Z}^+)$. In this problem, $\mathcal{P}(\mathbb{Z}^+)$ is countable or not is unknown, expect proving it.

Answer

Same as:

Theorem: The set $\mathcal{P}(\mathbf{N})$ is uncountable.

Proof by contradiction:

Assume that $\mathcal{P}(\mathbb{N})$ is countable. This implies that the elements of this set can be listed as $S_0, S_1, S_2, \ldots$, where $S_i \subseteq \mathbb{N}$, and each S_i can be represented uniquely by the bit string $b_{i0}b_{i1}b_{i2}\ldots$, where $b_{ij} = 1$ if $j \in S_i$ and $b_{ij} = 0$ if $j \notin S_i$

- $S_0 = b_{00}b_{01}b_{02}b_{03}\cdots$
- $S_1 = b_{10}b_{11}b_{12}b_{13}\cdots$
- $S_2 = b_{20}b_{21}b_{22}b_{23}\cdots$

$\vdots$

all $b_{ij} \in \{0, 1\}$.

Form a new set called $R = b_0b_1b_2b_3\ldots$, where $b_i = 0$ if $b_{ii} = 1$, and $b_i = 1$ if $b_{ii} = 0$. R is different from each set in the list. Each bit string is unique, and R and S_i differ in the i-th bit for all i.

Problem 8. 8 pts ANSWER ONLY!

Description

(a) Write the simplest Big-O functions for the following three polynomials (simplicity means there are no terms in the form of coefficients and exponents multiplied together). For example, the simplest Big-O function for $5n! + 10n^3$ is $n!$.

1. $n \log(n^2 + 1) + (n^2 + n) \log n$
2. $n^{2^n} + n^{n^2}$
3. $10(n!)^3 + 2^n$

(b) Compare the two Big-Os of (1) and (2) when n is very large.

Answer

(a)

1. $O(n^2 \log n)$
2. $O(n^{2^n})$
3. $O((n!)^3)$

(b) $O(n^2 \log n) < O(n^{2^n})$ $(n \to \infty)$

Problem 9. 10 pts

Description

Use the Chinese Remainder Theorem to solve linear congruence equations:

$$\begin{cases} x \equiv 1 \mod 2 \\ x \equiv 2 \mod 3 \\ x \equiv 3 \mod 5 \\ x \equiv 4 \mod 11 \end{cases}$$

Answer

$$m = 2 * 3 * 5 * 11 = 330$$

$$\begin{cases} M_1 = \frac{m}{m_1} = 165 \\ M_2 = \frac{m}{m_2} = 110 \\ M_3 = \frac{m}{m_3} = 66 \\ M_4 = \frac{m}{m_4} = 30 \end{cases}$$

We can take the modular inverse as:

$$\begin{cases} y_1 = 1 \\ y_2 = -1 \\ y_3 = 1 \\ y_4 = -4 \end{cases}$$

Thus:

$$x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 + a_4M_4y_4 = -337 \equiv 323 \mod 330$$

which means $x = 330k + 323 \ (k \in \mathbb{Z})$.

Problem 10. 12 pts

Description

In a certain RSA encryption, $p = 53$, $q = 61$, $e = 17$, and the codes for the letters A to Z are $00, 01, \dots, 25$.

(a) Request the decryption key d for RSA encryption.

(b) Briefly explain the maximum length of information that this RSA encryption algorithm can encrypt, and provide the reasons.

(c) Calculate what the ciphertext is after the information AB is encrypted by the encryption key.

Answer

(a)

$$ed \equiv 1 \mod (p-1)(q-1)$$

$$17d \equiv 1 \mod 3120$$

Thus we can take $d = -367$.

(b) $n = pq = 3233$. Because $2525 < 3233 < 252525$, so we have 4 digits at most, which means the maximum length of information is 2 letters.

(c) Translate AB into digits: $M = 0001$.

$$C = M^e \equiv 1^{17} \equiv 1 \mod n$$

So the encrypted message is still 0001.

Problem 11. 10 pts bonus-Hilbert Hotel

Description

(a) If another new Hilbert Hotel is built beside the original one, prove that the guests in the original Hilbert Hotel can still fill both the original and the new Hilbert Hotels.

(b) If there are infinite but countable buses coming beside the Hilbert Hotel, each bus carrying infinite but countable guests, prove that the new guests can still successfully check into the Hilbert Hotel.

Answer

(a) Suppose the number of old hotel's room is $\{2k-1 \mid k \in \mathbb{N}_+\}$, and the new hotel's room is $\{2k \mid k \in \mathbb{N}_+\}$, let the n-th guest live in the room n. Then the numbers of both hotel are countable, and guests are set $\mathbb{N}_+$ which is also countable.

(b) Let the n-th guest on the m-th bus live in room number $2^n \cdot 3^m$. For $n, m \in \mathbb{R}_+$, $2^n \cdot 3^m \in \mathbb{R}_+$ and clearly it is injective.