



PONTIFICIA UNIVERSIDAD CATOLICA DE CHILE
 ESCUELA DE INGENIERIA
 DEPARTAMENTO DE CIENCIA DE LA COMPUTACION

Matemáticas Discretas - IIC1253
Interrogación 2

1. [1.5 puntos] ¿Es la siguiente afirmación cierta?

$$\{\forall x\forall y R(x, y) \rightarrow R(y, x), \forall x\forall y\forall z (R(x, y) \wedge R(y, z)) \rightarrow R(x, z), \\ \forall x\forall y\forall z (R(x, y) \wedge R(x, z)) \rightarrow y = z\} \models \forall x\forall y R(x, y) \rightarrow x = y$$

Demuestre o de un contraejemplo.

2. [1.5 puntos] Dado un vocabulario $\mathcal{L}$, una $\mathcal{L}$ -estructura $\mathfrak{A}$ con dominio A y un conjunto $S \subseteq A$, decimos que S es definible en $\mathfrak{A}$ si existe una $\mathcal{L}$ -fórmula $\varphi(x)$ tal que:

$$S = \{a \in A \mid \mathfrak{A} \models \varphi(a)\}$$

Suponga que $\mathcal{L} = \{+, \cdot\}$, donde $+$, $\cdot$ son símbolos de funciones binarias, y suponga que $\mathfrak{A} = \langle \mathbb{N}, +^{\mathfrak{A}}, \cdot^{\mathfrak{A}} \rangle$, donde $+$, $\cdot$ son las funciones de suma y multiplicación sobre los números naturales. En esta pregunta, usted debe demostrar que el conjunto

$$S = \{a \in \mathbb{N} \mid \text{existe un número primo } p \text{ y un número } b \in \mathbb{N} \text{ tal que } p^b = a\}$$

es definible en $\mathfrak{A}$.

Importante: Cada fórmula auxiliar usada en esta pregunta debe estar definida en la pregunta.

3. [1.5 puntos] Sea p un número primo de la forma $4 \cdot k + 3$ y $a \in \{1, \dots, p-1\}$. Demuestre que si

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

entonces $-a$ tiene raíz cuadrada en módulo p (vale decir, existe b tal que $b^2 \equiv -a \pmod{p}$).

4. [1.5 puntos] Sean p, q números primos distintos, $n = p \cdot q$ y a, b números naturales. En esta pregunta usted debe demostrar que si la ecuación:

$$a^x \equiv b \pmod{n} \tag{1}$$

tiene solución, entonces esta ecuación tiene solución en el intervalo $\{0, \dots, n-1\}$. Vale decir, usted debe demostrar que si la ecuación (1) tiene solución, entonces existe $c \in \{0, \dots, n-1\}$ tal que:

$$a^c \equiv b \pmod{n}.$$