Questionario

Domanda n. 1: La funzione $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ definita da: $f(n) = (n, n+1)$, è invertibile.
Risp: (A) Falso (B) Vero

Domanda n. 2: Il numero 8 è invertibile modulo 16.
Risp: (A) Falso (B) Vero

Domanda n. 3: Se due numeri sono congruenti modulo 6 allora sono congruenti modulo 2.
Risp: (A) Falso (B) Vero

Domanda n. 4: $25^{11} \equiv_{13} 1$.
Risp: (A) Vero (B) Falso

Domanda n. 5: L'insieme $A = \{5, 6, 7, 8, 9\}$ è un insieme di rappresentanti per le classi d'equivalenza della congruenza modulo 5 sugli interi.
Risp: (A) Falso (B) Vero

Domanda n. 6: Nella congruenza modulo 5, tutti i numeri della forma $5k - 3$ appartengono alla classe d'equivalenza del numero 2.
Risp: (A) Falso (B) Vero

Domanda n. 7: Se $f : A \to B$, $b \in B$ e $a \in f^{-1}(b)$ allora vale sempre che:

1. $f(a) = b$; (A) Falso (B) Vero
2. $f(a) \in b$; (A) Falso (B) Vero
3. $f(b) = a$; (A) Falso (B) Vero
4. $f(a) = f(b)$ (A) Falso (B) Vero

Domanda n. 8: La funzione $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \times \mathbb{Z}$ definita da: $f(n, m) = (n, -m)$, è suriettiva.
Risp: (A) Falso (B) Vero

Domanda n. 9: Quale fra le seguenti formule è equivalente alla traduzione formale della frase
tutti i gatti odiano almeno un cane
dove $g(x)$ sta per *"x è un gatto"*, $c(x)$ sta per "x è un cane" e $o(x, y)$ sta per *"x odia y"*?

1. $\forall x\, \forall y\, (g(x) \wedge c(y) \wedge o(x, y))$; (A) Falso (B) Vero
2. $\forall x\, \exists y\, (g(x) \wedge c(y) \wedge o(x, y))$; (A) Falso (B) Vero
3. $\forall x\, (g(x) \to \exists y\, (c(y) \wedge o(x, y)))$; (A) Falso (B) Vero
4. $\forall x\, (g(x) \wedge \exists y\, (c(y) \to o(x, y)))$. (A) Falso (B) Vero

Domanda n. 10: La formula proposizionale $\neg P \to Q$ è equivalente alla formula $P \vee Q$.
Risp: (A) Falso (B) Vero

ESERCIZI

1. INDUZIONE

   (a) Dimostrare per induzione che per ogni $n \geq 1$ si ha

$$\frac{1}{1(1+1)} + \frac{1}{2(2+1)} + \frac{1}{3(3+1)} + \dots \frac{1}{n(n+1)} = \frac{n}{(n+1)}$$

   (b) Dimostrare per induzione che per ogni $n \geq 1$ il numero $5^n - 1$ è divisibile per 4.

2. FUNZIONI

   (a) Sia $f : \mathbb{Z} \to \mathbb{N}$ la funzione definita da $f(x) = x^2 + 1$.
      i. Determinare $f(5)$, $f^{-1}(5)$ e $f^{-1}(\{1, 5, 3\})$.
      ii. Determinare se f è iniettiva o suriettiva.

   (b) Sia $\mathbb{N}^*$ l'insieme dei numeri naturali non nulli e $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ la funzione definita da $f(n) = (0, n)$. Determinare se la funzione f è iniettiva, suriettiva o biunivoca.

3. RELAZIONI

   (a) Considerare la relazione d'equivalenza R sui numeri naturali non nulli $\mathbb{N}^*$ definita da

$$aRb \Leftrightarrow \text{ massima potenza di 5 che divide } a = \text{ massima potenza di 5 che divide } b$$

   (ad esempio 50 R 75 (perché $50 = 2 \cdot 5^2$ e $75 = 3 \cdot 5^2$ quindi la massima potenza di 5 che divide 50 è 2 e lo stesso vale per 75) mentre 30 $\not R$ 7 (perché $30 = 2 \cdot 3 \cdot 5$ quindi la massima potenza di 5 che divide 30 è 1 mentre è 0 per 7)
      i. Determinare se 15 appartiene alla classe d'equivalenza di 30. VERO
      ii. Descrivere la classe di equivalenza del numero 5. tutti i numeri che hanno come MCD(a, 5)=5
      iii. Determinare se R ha un numero finito o un numero infinito di classi d'equivalenza. INF
      iv. Determinare quale fra i seguenti insiemi è un insieme di rappresentanti per le classi d'equivalenza di R su $\mathbb{N}$:
         A. $\{1, 2, 3, 4, 5\}$;
         B. $\{10^n : n \in \mathbb{N}\}$;
         C. $\{5^n : n \in \mathbb{N}\}$;
         D. $\mathbb{N}$.

4. ARITMETICA

   =2 13 -3 MCD(14,60)!=1 NO!

   (a) Trova due interi h, k tali che $MCD(14, 60) = h14 + k60$. Il numero 14 è invertibile modulo 60?
   (b) Se $a, m \in \mathbb{N}$ sono tali che $MCD(a, m) = 1$, dimostrare che l'inverso di a modulo m è una potenza di a. (suggerimento: il teorema di Eulero ci dice che $a^{\phi(m)} \equiv_m 1$).
   (c) Trovare l'inverso di 7 modulo 60 in due modi: usando l'algoritmo di Euclide, o usando il punto precedente.
   (SOLUZIONE risultato usando il punto precedente: $\phi(60) = \phi(2^2 \cdot 3 \cdot 5) = \phi(2^2) \cdot \phi(3) \cdot \phi(5) = 16$. Per il Teorema di Eulero, $7^{16-1} = 7^{15} = 7^{12} 7^3 = (7^4)^3 7^3 = (2401)^3 \cdot 343 \equiv_{60} 1 \cdot 43 = 43$. SOLUZIONE usando Euclide: $1 = 2 \cdot 60 - 17 \cdot 7$, $-17 \equiv_{60} 43$).

MCD(a,m) = 1   a*x%m=1   x=?a^k con k Naturale?
a^phi(m)%m=1
a*a*...................*a%m=1
- phi(m) volte - %m = 1
a* a^(phi(m)-1)%m=1
phi(m) appartiene ai numeri naturali, perchè indica una lunghezza di un insieme
perciò anche phi(m)-1 perche phi(m) è definita per ogni numero intero positivo