SCRITTO MATEMATICA DI BASE E LOGICA 11/07/2016

NOME COGNOME MATRICOLA ____________________

QUIZ: ogni risposta corretta vale 1 punto, sbagliata −1, non data 0.

1. La funzione $f : \mathbb{N} \to \mathbb{N}$ definita da $f(n) = 2n + 7$ è iniettiva. **V** | **F**
2. Se A è un insieme con 4 elementi e B un insieme con 3 elementi, il numero delle funzioni che hanno dominio A e codominio B è maggiore del numero delle funzioni che hanno dominio B e codominio A. **V** | **F**
3. Se A è un insieme con 10 elementi, esistono più di 80 sottoinsiemi di A di cardinalità 3. **V** | **F**
4. Il numero -2 è equivalente a 5 modulo 7. **V** | **F**
5. La formula proposizionale $\neg P \to Q$ è equivalente alla formula $P \wedge \neg Q$. **V** | **F**
6. La funzione $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ definita da $f(n) = (n, 2n)$ è iniettiva. **V** | **F**
7. La funzione $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ definita da $f(n) = (n, 2n)$ è suriettiva. **V** | **F**
8. Se A è un insieme con 5 elementi, ci sono 5! funzioni con dominio e codominio uguali ad A **V** | **F**

9. Quale fra le seguenti formule è logicamente equivalente alla formula $\neg P \wedge \neg Q$?
   (a) $\neg(P \vee \neg Q)$;
   (b) $\neg P \to Q$;
   (c) $\neg(\neg P \to Q)$;
   (d) $P \wedge Q$.

10. Se $P(x)$ sta per "x è un professore", $St(x, y)$ sta per "x è uno studente del corso tenuto da y", $Sp(x)$ sta per "x è simpatico" $C(x, y)$ sta per "x compra il manuale di y", quale formula fra le seguenti significa

    "se un professore è simpatico, gli studenti del suo corso comprano il suo manuale"?

    (a) $\forall x \forall y (P(x) \wedge Sp(x) \wedge St(y, x) \wedge C(y, x))$
    (b) $\forall x (P(x) \wedge Sp(x) \to \forall y (St(y, x) \to C(y, x)))$
    (c) $\forall x \exists y (St(x, y) \wedge P(y) \wedge Sp(y) \wedge C(x, y))$
    (d) $\forall x (P(x) \wedge Sp(x) \to \exists y (St(y, x) \wedge C(y, x)))$

ESERCIZI

NOTA BENE: TUTTE LE RISPOSTE VANNO GIUSTIFICATE

1. **INDUZIONE** Dimostrare per induzione che per ogni $n \geq 2$ vale
$$(1-\frac{1}{4})\cdot(1-\frac{1}{9})\cdot\ldots\cdot(1-\frac{1}{n^2}) = \frac{(1+n)}{2n} \tag{1}$$

2. **INDUZIONE** Utilizzando il principio d'induzione, dimostrare che per ogni $n \geq 2$ vale
$$3^n > 2^{n+1}. \tag{2}$$

3. **CARDINALITÀ DI INSIEMI FINITI** Sia X un insieme finito, non vuoto, di cardinalità 5 e $P(X)$ l'insieme delle parti di X. Determinare la cardinalità dei seguenti insiemi:
   (a) $A = X \times P(X)$;
   (b) $B = P(X \times X)$;
   (c) $C = \{(x, \{x\}) : x \in X\}$;
   (d) $D = \{(x, Y) \in A : x \in Y\}$.

4. **CALCOLO COMBINATORIO** Dobbiamo confezionare delle bandierine a 3 strisce verticali avendo a disposizione i colori rosso, bianco, verde e blu. In quante maniere diverse possiamo:
   (a) confezionare bandierine con 3 strisce di differenti colori;
   (b) confezionare bandierine con 3 strisce di differenti colori ma senza il colore rosso;
   (c) confezionare bandierine con 3 strisce di differenti colori di cui uno è il colore rosso.

5. **CONGRUENZE** Considera la relazione di congruenza modulo 9 sugli interi.
   (a) È vero che $-5 \equiv_9 5$?
   (b) Il numero 5 è invertibile modulo 9? Se si, trovane l'inverso nell'insieme $\{0, 1, 2, \ldots, 8\}$.
   (c) Calcolare il resto di 29^{15} nella divisione per 9.

6. **RELAZIONI D'EQUIVALENZA** Considerare la relazione d'equivalenza R su $\mathbb{N}$ definita da
$$aRb \quad \Leftrightarrow \quad \text{nella scrittura decimale, } a \text{ e } b \text{ hanno la stessa cifra delle unità}$$
   (ad esempio 5 R 15 (5 unità) mentre non vale 213 R 10)
   (a) Determinare se 123 appartiene alla classe d'equivalenza di 32.
   (b) Descrivere la classe di equivalenza del numero 0.
   (c) Determinare il numero di classi d'equivalenza della relazione R.
   (d) Determinare quale fra i seguenti insiemi è un insieme di rappresentanti per le classi d'equivalenza di R su $\mathbb{N}$:
      i. $\{10^n : n \in \mathbb{N}\}$;
      ii. $\{0, 1, 2, 3, 4, \ldots, 9\}$;
      iii. $\{0, 11, 22, 33, 44, \ldots 99\}$;
      iv. l'insieme dei numeri primi.

7. **RSA** La coppia $(m, s) = (11, 7)$ può essere scelta come chiave pubblica per un codice RSA? In caso affermativo, qual è la corrispondente chiave privata e quale numero si utilizza per criptare 2?

Answer Key for Exam $\boxed{\text{A}}$

QUIZ: ogni risposta corretta vale 1 punto, sbagliata −1, non data 0.

1. La funzione $f : \mathbb{N} \to \mathbb{N}$ definita da $f(n) = 2n + 7$ è iniettiva. **V** **F** V
2. Se A è un insieme con 4 elementi e B un insieme con 3 elementi, il numero delle funzioni che hanno dominio A e codominio B è maggiore del numero delle funzioni che hanno dominio B e codominio A. **V** **F** V
3. Se A è un insieme con 10 elementi, esistono più di 80 sottoinsiemi di A di cardinalità 3. **V** **F** V
4. Il numero -2 è equivalente a 5 modulo 7. **V** **F** V
5. La formula proposizionale $\neg P \to Q$ è equivalente alla formula $P \wedge \neg Q$. **V** **F** F
6. La funzione $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ definita da $f(n) = (n, 2n)$ è iniettiva. **V** **F** V
7. La funzione $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ definita da $f(n) = (n, 2n)$ è suriettiva. **V** **F** F
8. Se A è un insieme con 5 elementi, ci sono 5! funzioni con dominio e codominio uguali ad A **V** **F** F

9. Quale fra le seguenti formule è logicamente equivalente alla formula $\neg P \wedge \neg Q$?

   (a) $\neg(P \vee \neg Q)$;

   (b) $\neg P \to Q$;

   $\boxed{\text{(c)}}$ $\neg(\neg P \to Q)$;

   (d) $P \wedge Q$.

10. Se $P(x)$ sta per "x è un professore", $St(x, y)$ sta per "x è uno studente del corso tenuto da y", $Sp(x)$ sta per "x è simpatico" $C(x, y)$ sta per "x compra il manuale di y", quale formula fra le seguenti significa

    "se un professore è simpatico, gli studenti del suo corso comprano il suo manuale"?

    (a) $\forall x \forall y(P(x) \wedge Sp(x) \wedge St(y, x) \wedge C(y, x))$

    $\boxed{\text{(b)}}$ $\forall x(P(x) \wedge Sp(x) \to \forall y(St(y, x) \to C(y, x)))$

    (c) $\forall x \exists y(St(x, y) \wedge P(y) \wedge Sp(y) \wedge C(x, y))$

    (d) $\forall x(P(x) \wedge Sp(x) \to \exists y(St(y, x) \wedge C(y, x)))$

ESERCIZI

NOTA BENE: TUTTE LE RISPOSTE VANNO GIUSTIFICATE

1. **INDUZIONE** Dimostrare per induzione che per ogni $n \geq 2$ vale

$$(1-\frac{1}{4})\cdot(1-\frac{1}{9})\cdot\ldots\cdot(1-\frac{1}{n^2}) = \frac{(1+n)}{2n} \tag{1}$$

SOL

La base dell'induzione è:

$$(1-\frac{1}{4}) = \frac{(1+2)}{4};$$

poiché entrambi i membri dell'uguaglianza sono uguali a $\frac{3}{4}$, la base è verificata.

Per il passo induttivo, dobbiamo dimostrare che vale

$$(1-\frac{1}{4})\cdot(1-\frac{1}{9})\cdot\ldots\cdot(1-\frac{1}{n^2})\cdot(1-\frac{1}{(n+1)^2}) = \frac{(n+2)}{2(n+1)}$$

usando l'uguaglianza in (1) si ha

$$(1-\frac{1}{4})\cdot(1-\frac{1}{9})\cdot\ldots\cdot(1-\frac{1}{n^2})\cdot(1-\frac{1}{(n+1)^2}) = \frac{(1+n)}{2n}\cdot(1-\frac{1}{(n+1)^2}) = \frac{(1+n)}{2n}\cdot\frac{n^2+2n}{(n+1)^2} = \frac{n^2+2n}{2n(n+1)} = \frac{n+2}{2(n+1)}$$

2. **INDUZIONE** Utilizzando il principio d'induzione, dimostrare che per ogni $n \geq 2$ vale

$$3^n > 2^{n+1}. \tag{2}$$

SOL

La base dell'induzione è $3^2 > 2^3$, ed è banalmente verificata.

Per il passo induttivo, dobbiamo dimostrare che vale

$$3^{n+1} > 2^{n+2},$$

sapendo che vale (2).

Si ha

$$3^{n+1} = 3^n \cdot 3 > 2^{n+1}\cdot 3 > 2^{n+1}\cdot 2 = 2^{n+2}$$

3. **CARDINALITÀ DI INSIEMI FINITI** Sia X un insieme finito, non vuoto, di cardinalità 5 e $P(X)$ l'insieme delle parti di X. Determinare la cardinalità dei seguenti insiemi:

   (a) $A = X \times P(X)$;
   (b) $B = P(X \times X)$;
   (c) $C = \{(x, \{x\}) : x \in X\}$;
   (d) $D = \{(x, Y) \in A : x \in Y\}$.

   SOL

   (a) $|A| = 5 \cdot 2^5$;
   (b) $|B| = 2^{5^2}$;
   (c) $|C| = 5$;
   (d) $|D| = 5 \cdot 2^4$.

4. **CALCOLO COMBINATORIO** Dobbiamo confezionare delle bandierine a 3 strisce verticali avendo a disposizione i colori rosso, bianco, verde e blu. In quante maniere diverse possiamo:

(a) confezionare bandierine con 3 strisce di differenti colori;

(b) confezionare bandierine con 3 strisce di differenti colori ma senza il colore rosso;

(c) confezionare bandierine con 3 strisce di differenti colori di cui uno è il colore rosso.

SOL

(a) $4 \cdot 3 \cdot 2 = 24$;
(b) $3 \cdot 2 = 6$;
(c) per la regola del complementare, $24 - 6 = 18$.

5. **CONGRUENZE** Considera la relazione di congruenza modulo 9 sugli interi.

(a) È vero che $-5 \equiv_9 5$?
(b) Il numero 5 è invertibile modulo 9? Se si, trovane l'inverso nell'insieme $\{0, 1, 2, \ldots, 8\}$.
(c) Calcolare il resto di 29^{15} nella divisione per 9.

SOL

(a) NO: infatti $-5 - 5 = -10$ non è divisibile per 9.
(b) Il numero 5 è invertibile modulo 9 perché $MCD(5, 9) = 1$. Poiché $5 \times 2 = 10 \equiv_9 1$ l'inverso di 5 modulo 10 è 2.
(c) Siccome $29 \equiv_9 2$ si ha $29^{15} \equiv_9 2^{15} = 2^{3 \cdot 5} = (2^3)^5 \equiv_9 (-1)^5 = -1 \equiv_9 8$ ed il resto cercato è uguale ad 8.

6. **RELAZIONI D'EQUIVALENZA** Considerare la relazione d'equivalenza R su $\mathbb{N}$ definita da

$$aRb \quad \Leftrightarrow \quad \text{nella scrittura decimale, } a \text{ e } b \text{ hanno la stessa cifra delle unità}$$

(ad esempio 5 R 15 (5 unità) mentre non vale 213 R 10)

(a) Determinare se 123 appartiene alla classe d'equivalenza di 32.
(b) Descrivere la classe di equivalenza del numero 0.
(c) Determinare il numero di classi d'equivalenza della relazione R.
(d) Determinare quale fra i seguenti insiemi è un insieme di rappresentanti per le classi d'equivalenza di R su $\mathbb{N}$:
   i. $\{10^n : n \in \mathbb{N}\}$;
   ii. $\{0, 1, 2, 3, 4, \ldots, 9\}$;
   iii. $\{0, 11, 22, 33, 44, \ldots 99\}$;
   iv. l'insieme dei numeri primi.

SOL

(a) 123 non appartiene alla classe d'equivalenza di 32 perché non vale 123 R 32.
(b)
$$[0] = \{n \in \mathbb{N} : 0 \; R \; n\} = \{n \in \mathbb{N} : n \text{ ha zero unità}\} = \{n \in \mathbb{N} : 10 \text{ divide } n\}$$
(c) R ha 10 classi d'equivalenza e sono $[0], [1], \ldots, [9]$. Infatti ogni numero naturale appartiene ad una di queste classi che sono tutte distinte.
(d) Determinare quale fra i seguenti insiemi è un insieme di rappresentanti per le classi d'equivalenza di R su $\mathbb{N}$:

i. NO: se $n = 0$ allora $10^n = 1$, mentre se $n \neq 0$, 10^n è divisibile per 10 e appartiene alla classe di 0. Quindi solo le classi di 0 e di 1 sono rappresentate.

ii. SI: sono rappresentate tutte le possibili classi e due elementi distinti appartengono a classi distinte.

iii. SI: sono rappresentate tutte le possibili classi e due elementi distinti appartengono a classi distinte.

iv. NO: ad esempio 11 e 31 sono entrambi primi ma appartengono alla stessa classe d'equivalenza di R, quindi l'insieme dei primi non è un insieme di rappresentanti.

7. **RSA** La coppia $(m, s) = (11, 7)$ può essere scelta come chiave pubblica per un codice RSA? In caso affermativo, qual è la corrispondente chiave privata e quale numero si utilizza per criptare 2?
SOL La coppia $(m, s) = (11, 7)$ può essere scelta come chiave pubblica per un codice RSA perché $\phi(11) = 10$ e 7 è invertibile modulo 10, con inverso uguale a 3: infatti $7 \cdot 3 = 21 \equiv_{10} 1$. Per criptare il numero 2 utilizziamo la chiave pubblica s: il numero 2 criptato si ottiene calcolando il resto modulo 11 di $2^7 = 2^4 \cdot 2^3 = 16 \cdot 8 \equiv_{11} 5 \cdot (-3) = -15 \equiv_{11} -4 \equiv_{11} 7$.