SCRITTO MATEMATICA DI BASE E LOGICA del ——

NOME COGNOME ______________________________

MATRICOLA ______________________________

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

1. Una relazione d'equivalenza su un insieme infinito ha sempre un numero infinito di classi d'equivalenza. **V** | **F**
2. La formula proposizionale $((\neg P \vee Q) \wedge P) \to Q$ è una tautologia. **V** | **F**
3. Il numero 5 ha un inverso moltiplicativo modulo 16. **V** | **F**
4. Se A è un insieme con 10 elementi, ci sono più di 1000 funzioni $f : A \to \{0, 1\}$. $< 2^{10}$ **V** | **F**
5. La funzione $f : \mathbb{N} \to \mathbb{Z} \times \mathbb{Z}$ definita da $f(n) = (n, 0)$ è iniettiva. **V** | **F**
6. Se ϕ è la funzione di Eulero, allora
$$\phi(44) = \phi(2 \cdot 22) = \phi(2) \cdot \phi(22).$$
V | **F**
7. La relazione R sui numeri naturali definita da
$$n \; R \; m \Leftrightarrow \; n + m \text{ è divisibile per } 3$$
è: **V** | **F** riflessiva; **V** | **F** simmetrica; **V** | **F** transitiva.
8. Due numeri congruenti modulo 10 sono anche congruenti modulo 5. **V** | **F**
9. Se $f : A \to B$, $b \in B$ e $a \in f^{-1}(b)$ allora vale sempre che:
   - (a) $f(a) = b$;
   - (b) $f(a) \in b$;
   - (c) $f(b) = a$;
   - (d) $f(a) = f(b)$.
10. Se $P(x)$ sta per "x è un poliziotto", $L(x)$ sta per "x è un ladro", $A(x, y)$ sta per "x arresta y", quale formula fra le seguenti significa "c'è un poliziotto che non arresta alcun ladro"?
    - (a) $\exists x \; (P(x) \wedge \exists y \; (L(y) \wedge \neg A(y, x)))$
    - (b) $\exists x \; (P(x) \wedge \forall y \; (L(y) \wedge \neg A(x, y)))$
    - (c) $\exists x \; (P(x) \wedge \forall y \; (L(y) \to \neg A(x, y)))$
    - (d) $\exists x \forall y \; (P(x) \wedge L(y) \to \neg A(x, y))$

ESERCIZI

NOTA BENE: TUTTE LE RISPOSTE VANNO GIUSTIFICATE

(n+k-1)!/k!(n-1)! = (8+4-1)!/4!*3! =
11*10*9*8*7*6*5 / 3*2 = 277200

1. (a) In quanti modi 8 professori possono essere assegnati a 4 distinte scuole (con la possibilità che ad una o più scuole non venga assegnato alcun professore)?

   (b) E se ad ogni scuola vengono assegnati esattamente 2 professori? n! / k! (n-k)! = 8! / 2! + 6! = 8*7/2 / 28

   (c) E se ad ogni scuola viene assegnato almeno un professore?

2. Considerare la relazione d'equivalenza E sull'insieme $A = \mathbb{N}^* \times \mathbb{N}^*$ delle coppie di numeri naturali non nulli definita da:

   m%n   == k%h

   $(m, n)\ E\ (k, h) \Leftrightarrow$ (resto della divisione intera di m per n) $=$ (resto della divisione intera di k per h).

   (ad esempio, $(8, 3)\ E\ (9, 7)$ perché la divisione di 8 per 3 ha resto 2, come la divisione di 9 per 7; la coppia $(6, 4)$ non è in relazione E con la coppia $(9, 2)$ perché il resto della prima divisione è 2 mentre il resto della seconda divisione è 1).

   NO

   (a) Determinare se la coppia $(5, 2)$ appartiene alla classe d'equivalenza della coppia $(12, 10)$ e se la coppia $(4, 2)$ appartiene alla classe d'equivalenza della coppia $(1, 1)$. SI

   (b) Determinare la classe d'equivalenza della coppia $(1, 1)$. 1%1 = 0, quindi qualsiasi m tale che m=k*n con k appartenente a N

   (c) Quale dei seguenti insiemi è un insieme di rappresentanti per le classi d'equivalenza di E su A? (giustificare le risposte!)

   n%n = 0

   $\{(n, n) : n \in \mathbb{N}^*\}$; $\{(n, m) : n, m \in \mathbb{N}^*, n < m\}$; $\{(1, 1)\} \cup \{(n, n + 1) : n \in \mathbb{N}^*\}$.

   NO

3. (a) Esiste un codice RSA che ha chiave pubblica uguale a $(15, 5)$ e chiave privata uguale a $(15, 3)$?

   (b) Dimostrare la coppia $(m, s) = (11, 7)$ può essere scelta come chiave pubblica per un codice RSA e trovare la chiave privata corrispondente.

   MCD(11,7)=1 chiave privata = inverso moltiplicativo di s % phi (m)   phi(m) = phi(11) = 10
   7*x%10==1   x=3

   (c) Criptare il numero 2 nel codice RSA del punto precedente.

   2^s%m = 2^7%11= -4 = 7   7^t%m = 7^3%11=

4. (a) Dimostrare per induzione che per ogni $n \geq 0$ il numero $n^3 + 5n$ è divisibile per 6.

   (b) Dimostrare il punto precedente senza usare il principio d'induzione, ma ragionando modulo 6.

5. Dimostrare per induzione che per ogni $n \geq 1$ si ha

$$1^3 + 2^3 + \ldots + n^3 \;=\; (1 + 2 + \ldots + n)^2.$$

6. (a) Trovare l'opposto additivo di 7 modulo 11 e l'inverso moltiplicativo di 4 modulo 11.

   (b) Determinare, se possibile, due interi h, k tali che $h \cdot 11 + k \cdot 13 = 3$.

   (c) Se p, q sono primi distinti, determinare $L(p, q)$ (l'insieme delle combinazioni lineari di p e q).

7. (a) Se $f : A \to B$ è una funzione con dominio A e codominio B, scrivere le formule che esprimono l'iniettività e la suriettività della funzione f.

   iniettiva per qualsiasi a != b entrambi appartenenti al Dominio f(a) != f(b)

   (b) Sia $f : \mathbb{N} \to \mathbb{Z} \times \mathbb{N}$ la funzione definita da $f(n) = (-n, n + 2)$.

   i. Determinare $f(5)$ e gli insiemi $f^{-1}((0, 0))$ e $f^{-1}(\{(0, 0), (-5, 7)\})$.

   ii. Determinare se f è iniettiva o suriettiva.

   Suriettiva qualsiasi b appartenente a Codominio f^-1(b) appartiene ad Dominio