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

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. $\boxed{\textbf{V}}\boxed{\textbf{F}}$ F

2. La funzione $f : \mathbb{N} \to \mathbb{Z} \times \mathbb{Z}$ definita da $f(n) = (n, 0)$ è iniettiva. $\boxed{\textbf{V}}\boxed{\textbf{F}}$ V

3. Due numeri congruenti modulo 10 sono anche congruenti modulo 5. $\boxed{\textbf{V}}\boxed{\textbf{F}}$ V

4. Se A è un insieme con 10 elementi, ci sono più di 1000 funzioni $f : A \to \{0, 1\}$. $\boxed{\textbf{V}}\boxed{\textbf{F}}$ V

5. La formula proposizionale $((\neg P \vee Q) \wedge P) \to Q$ è una tautologia. $\boxed{\textbf{V}}\boxed{\textbf{F}}$ V

6. Il numero 5 ha un inverso moltiplicativo modulo 16. $\boxed{\textbf{V}}\boxed{\textbf{F}}$ V

7. La relazione R sui numeri naturali definita da

$$n\ R\ m \Leftrightarrow\ n + m \text{ è divisibile per } 3$$

è: F $\boxed{\textbf{V}}\boxed{\textbf{F}}$ riflessiva; V $\boxed{\textbf{V}}\boxed{\textbf{F}}$ simmetrica; F $\boxed{\textbf{V}}\boxed{\textbf{F}}$ transitiva.

8. Se ϕ è la funzione di Eulero, allora

$$\phi(44) = \phi(2 \cdot 22) = \phi(2) \cdot \phi(22).$$

$\boxed{\textbf{V}}\boxed{\textbf{F}}$ F

9. Se $f : A \to B$, $b \in B$ e $a \in f^{-1}(b)$ allora vale sempre che:
   - $\boxed{\text{(a)}}$ $f(a) = b$;
   - (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) $\exists x\ (P(x) \wedge \forall y\ (L(y) \wedge \neg A(x, y)))$
    - $\boxed{\text{(c)}}$ $\exists x\ (P(x) \wedge \forall y\ (L(y) \to \neg A(x, y)))$
    - (d) $\exists x \forall y\ (P(x) \wedge L(y) \to \neg A(x, y))$

ESERCIZI

NOTA BENE: TUTTE LE RISPOSTE VANNO GIUSTIFICATE

1. (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.
   (c) Criptare il numero 2 nel codice RSA del punto precedente.

   SOL

   (a) $\phi(15) = \phi(3 \cdot 5) = \phi(3) \cdot \phi(5) = 2 \cdot 4 = 8$. Inoltre $MCM(8, 5) = 1$, quindi la chiave pubblica è corretta, ma non corrisponde alla chiave provata perché $3 \cdot 5 = 15 \not\equiv_8 1$.
   (b) 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 $7 \cdot 3 = 21 \equiv_{10} 1$.
   (c) Per criptare il numero 2 utilizziamo la chiave pubblica $(11, 7)$ bisogna calcolare il resto modulo 11 di 2^7. Si ha:
   $$2^7 = 2^4 \cdot 2^3 = 16 \cdot 8 \equiv_{11} 5 \cdot (-3) = -15 \equiv_{11} -4 \equiv_{11} 7.$$
   Quindi il numero 2 criptato con chiave $(11, 7)$ è uguale a 7.

2. (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.
   (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.

3. (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).

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. Per dimostrare che $n^3 + 5n$ è divisibile per 6 basta dimostrare che $n^3 + 5n \equiv_6 0$. Considerando i diversi possibili resti di n modulo 6 osserviamo che:
   - Se $n \equiv_6 0$ allora $n^3 + 5n \equiv_6 0^3 + 5 \cdot 0 = 0$;
   - Se $n \equiv_6 1$ allora $n^3 + 5n \equiv_6 1^3 + 5 \cdot 1 = 6 \equiv_6 0$;
   - Se $n \equiv_6 2$ allora $n^3 + 5n \equiv_6 2^3 + 5 \cdot 2 = 18 \equiv_6 0$;
   - Se $n \equiv_6 3$ allora $n^3 + 5n \equiv_6 3^3 + 5 \cdot 3 = 42 \equiv_6 0$;
   - Se $n \equiv_6 4$ allora $n^3 + 5n \equiv_6 4^3 + 5 \cdot 4 \equiv_6 (-2)^3 - 1 \cdot 4 \equiv_6 -12 \equiv_6 0$;
   - Se $n \equiv_6 5$ allora $n^3 + 5n \equiv_6 5^3 + 5 \cdot 5 \equiv_6 (-1)^3 + (-1) \cdot (-1) \equiv_6 -1 + 1 \equiv_6 0$.

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

   $(m, n)\ E\ (k, h) \Leftrightarrow$ (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).

(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 $(1, 1)$. **SOL** Il resto della divisione di 5 per 2 è 1, mentre il resto della divisione di 12 per 10 è 2; quindi $(5, 2)$ non è in relazione con (12.10) e $(5, 2) \notin [(12, 10)]$. La coppia $(4, 2)$ invece appartiene a $[(1, 1)]$ perché in entrambi i casi il resto della divisione è uguale a zero.

(b) Determinare la classe d'equivalenza della coppia $(1, 1)$. **SOL**

$$[(1, 1)] = \{(a, b) \in \mathbb{N}^* \times \mathbb{N}^* : \text{ il resto della divisione di } a \text{ per } b \text{ è } 0\} =$$

$$= \{(a, b) \in \mathbb{N}^* \times \mathbb{N}^* : a = k \cdot b + 0, k \in N^*\} = \{(k \cdot b, b) \in \mathbb{N}^* \times \mathbb{N}^* : k \in \mathbb{N}^*\}$$

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

$\{(n, n) : n \in \mathbb{N}^*\}$; $\{(n, m) : n, m \in \mathbb{N}^*, n < m\}$; $\{(1, 1)\} \cup \{(n, n + 1) : n \in \mathbb{N}^*\}$.
SOL $\{(n, n) : n \in \mathbb{N}^*\}$ NO: tutte queste coppie appartengono ad un'unica classe, quella di $(1, 1)$.
$\{(n, m) : n, m \in \mathbb{N}^*, n < m\}$ NO: ad esempio, $(1, 2)$ e $(1, 3)$ appartengono all'insieme dato, ma stanno nella stessa classe d'equivalenza.
$\{(1, 1)\} \cup \{(n, n+1) : n \in \mathbb{N}^*\}$ SI: la coppia $(n, n+1)$ rappresenta tutte le coppie che hanno resto n, mentre $(1, 1)$ rappresenta le coppie che hanno resto 0.

7. (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)? **SOL** Per ogni professore, abbiamo 4 possibili scelte. Quindi ci sono in tutto 4^8 scelte possibili.

(b) E se ad ogni scuola vengono assegnati esattamente 2 professori? **SOL** Ordiniamo le scuole da 1 a 4. Possiamo scegliere i due professori della prima scuola in $\binom{8}{2}$ modi, quelli per la seconda scuola in $\binom{6}{2}$ modi (dobbiamo escludere i due professori della seconda scelta) e cosi' via. In tutto avremo

$$\binom{8}{2} \cdot \binom{6}{2} \cdot \binom{5}{2} \cdot \binom{4}{2}$$

possibili scelte.

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

SOL Questo esercizio è molto più complesso dei precedenti (non verrà proposto ad un vero esame!)

Per la regola del complementare, le possibili scelte saranno $4^8 - k$, dove 4^8 rappresenta tutte le possibili assegnazioni di 8 professori a 4 scuole, senza limitazioni, e k è il numero delle scelte per cui non è vero che ad ogni scuola venga assegnato almeno un professore. Per calcolare k, possiamo ragionare nel modo seguente. Dividiamo l'insieme delle scelte per cui non è vero che ad ogni scuola venga assegnato almeno un professore in tre sottoinsiemi disgiunti. Il primo sottoinsieme contiene tutte le assegnazioni per cui esiste esattamente una scuola che a cui non viene assegnato alcun professore, il secondo sottoinsieme contiene tutte le assegnazioni per cui esistono esattamente due scuole che a cui non viene assegnato alcun professore, il terzo sottoinsieme contiene tutte le assegnazioni per cui esistono esattamente tre scuole che a cui non viene assegnato alcun professore.

Iniziamo a calcolare la cardinalità del terzo sottoinsieme. In questo caso ci sarà un'unica scuola a cui verranno assegnati tutti gli 8 professori e possiamo scegliere questa scuola in 4 modi diversi. Quindi il terzo sottoinsieme ha cardinalità 4.

La cardinalità del secondo sottoinsieme si ottiene scegliendo in $\binom{4}{2}$ modi le 2 scuole che riceveranno almeno un professore e moltiplicandolo per il numero k_2 delle possibili assegnazioni di 8 professori a 2 scuole, in modo che ad ogni scuola venga assegnato almeno un professore. Il secondo sottoinsieme ha quindi cardinalità $\binom{4}{2} \cdot k_2$. Per calcolare k_2 usiamo ancora la regola del complementare: abbiamo 2^8 assegnazioni possibili senza vincoli, a cui dobbiamo sottrarre le due possibili assegnazioni in cui tutti i professori vanno in una singola scuola. Quindi $k_2 = 2^8 - 2$. In totale, il secondo sottoinsieme ha cardinalità $\binom{4}{2} \cdot k_2 = 6 \cdot (2^8 - 2)$.

La cardinalità del primo sottoinsieme si ottiene scegliendo in 4 modi diversi la scuola che non riceverà alcun professore. Fissata questa scuola, le tre restanti scuole devono ricevere almeno un professore. Se k_3 è il numero delle possibili assegnazioni di 8 professori a 3 scuole in modo che ogni scuola riceva almeno un professore, la cardinaltà del terzo sottoinsieme è quindi $4k_3$. Per calcolare k_3, adoperiamo ancora la regola del complementare. Esistono 3^8 assegnazioni di 8 professori a 3 scuole senza vincoli a cui dobbiamo sottrarre il numero k_4 di assegnazioni di 8 professori a 3 scuole in cui esattamente una scuola rimane senza professore e il numero k_5 di assegnazioni di 8 professori a 3 scuole in cui esattamente due scuole rimangono senza professore.

Ragionando come sopra abbiamo che $k_4 = 3 \cdot k_2 = 3 \cdot (2^8 - 2)$ mentre $k_5 = 3$. Mettendo insieme i calcoli fatti otteniamo che la cardinalità del primo sottoinsieme è $4k_3 = 4(3^8 - 3(2^8 - 2) - 3) = 4(3^8 - 3 \cdot 2^8 + 3)$.

Poiché k equivale alla somma della cardinalità dei tre sottoinsiemi, abbiamo

$$k = 4 + 6(2^8 - 2) + 4(3^8 - 3 \cdot 2^8 + 3) = 4 + 4 \cdot 3^8 - 6 \cdot 2^8.$$

Finalmente, la risposta alla domanda originale è

$$4^8 - k = 4^8 - 4 - 4 \cdot 3^8 + 6 \cdot 2^8$$