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

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

1. Se $f : \mathbb{N} \to \mathbb{N}$ e f è iniettiva, allora per ogni $n \in \mathbb{N}$ esiste $m \in \mathbb{N}$ con $f(m) = n$. $\boxed{\textbf{V}}\boxed{\textbf{F}}$
   FALSO: la proprietà "per ogni $n \in \mathbb{N}$ esiste $m \in \mathbb{N}$ con $f(m) = n$" è la definizione di suriettività ed esistono funzioni iniettive che non sono suriettive, ad esempio $f : \{0\} \to \{0, 1\}$ con $f(0) = 0$.

2. Il numero 4 è invertibile modulo 16. $\boxed{\textbf{V}}\boxed{\textbf{F}}$
   FALSO: $MCD(4, 16) = 4 \neq 1$

3. Se $f : A \to B$ è una funzione e $f^{-1}(b) = \emptyset$ per qualche $b \in B$,
   allora f non può essere suriettiva. $\boxed{\textbf{V}}\boxed{\textbf{F}}$
   VERO: se $f^{-1}(b) = \emptyset$ allora non esiste alcun $a \in A$ tale che $f(a) = b$

4. La funzione $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ definita da $f(n, m) = m$ è iniettiva. $\boxed{\textbf{V}}\boxed{\textbf{F}}$
   FALSO: $f(0, 1) = f(1, 1)$

5. Se una funzione $f : A \to B$ è suriettiva, allora ha un'inversa. $\boxed{\textbf{V}}\boxed{\textbf{F}}$
   FALSO: per avere un'inversa, una funzione deve essere iniettiva e suriettiva. Ad esempio, la funzione $f : \{0, 1\} \to \{0\}$ definita da $f(0) = f(1) = 0$ è suriettiva ma non invertibile

6. Se due numeri sono congruenti modulo 10 allora sono congruenti modulo 5. $\boxed{\textbf{V}}\boxed{\textbf{F}}$
   VERO: se $a - b$ è divisibile per 10, allora è anche divisibile per 5

7. Nella congruenza modulo 4, tutti i numeri della forma 5^n appartengono alla classe d'equivalenza del numero 9. $\boxed{\textbf{V}}\boxed{\textbf{F}}$
   VERO $5^n \equiv_4 1^n = 1 \equiv_4 9$

8. La formula proposizionale $P \wedge (P \to Q)$ è equivalente alla formula $P \wedge Q$. $\boxed{\textbf{V}}\boxed{\textbf{F}}$
   VERO: le due formule hanno la stessa tavola di verità

9. La formula $\forall x \exists y R(x, y)$ è equivalente a
   (a) $\forall x \neg \exists y \neg R(x, y)$;
   (b) $\exists y \forall x R(x, y)$;
   (c) $\exists y \neg \forall x R(x, y)$;
   $\boxed{\text{(d)}}$ $\forall x \neg \forall y \neg R(x, y)$.

10. Se A è un insieme con 3 elementi e B è un insieme con 6 elementi, il numero dei sottoinsiemi di $A \times B$ è
    (a) 6×3
    $\boxed{\text{(b)}}$ 2^{18}
    (c) $18!$
    (d) 18^2

ESERCIZI

NOTA BENE: TUTTE LE RISPOSTE VANNO GIUSTIFICATE

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

$$1 \cdot 2 + 2 \cdot 3 + \ldots + n \cdot (n+1) \;=\; \frac{n(n+1)(n+2)}{3}$$

SOL. Per $n = 1$ l'uguaglianza
$$1 \cdot 2 = \frac{1 \cdot 2 \cdot 3}{3}$$
è verificata. Nel passo induttivo occorre mostrare che

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

Usando l'ipotesi induttiva si ha:

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

quindi è sufficiente verificare che valga la seguente uguaglianza:
$$\frac{n(n+1)(n+2)}{3} + (n+1) \cdot (n+2) = \frac{(n+1)(n+2)(n+3)}{3}.$$
Raccogliendo il fattore $(n+1) \cdot (n+2)$ a sinistra dell'uguaglianza abbiamo

$$\frac{n(n+1)(n+2)}{3} + (n+1) \cdot (n+2) = (n+1) \cdot (n+2)(\frac{n}{3} + 1) = \frac{(n+1)(n+2)(n+3)}{3},$$
come volevasi dimostrare.

2. **INDUZIONE**
Dimostrare per induzione che, per ogni $n \geq 0$, il numero $n^2 + n + 2$ è divisibile per 2.
SOL. Per $n = 0$ si ha $n^2 + n + 2 = 2$, che è divisibile per 2. Nel passo induttivo occorre mostrare che

$$(n+1)^2 + (n+1) + 2$$

è divisibile per 2, supponendo che $n^2 + n + 2$ lo sia. Si ha:

$$(n+1)^2 + (n+1) + 2 = n^2 + 2n + 1 + n + 1 + 2 = (n^2 + n + 2) + 2(n+1);$$

poiché l'addendo (n^2+n+2) è divisibile per 2 per ipotesi induttiva e $2(n+1)$ è divisibile per 2, anche la loro somma è divisibile per 2.

3. **FUNZIONI E RELAZIONI**

   (a) Considerare la funzione $f : \mathbb{N} \to \mathbb{Z}$ definita da $f(a) = a^2 - 2a$. Determinare gli insiemi $f(\{0, 1, 2\})$, $f^{-1}(\{0\})$, $f^{-1}(\{-2, -1, 5\})$.

   (b) Considerare la funzione $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ definita da $f(a, b) = a - b$. Determinare se f è iniettiva o suriettiva.

   (c) Dimostrare che la funzione $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ definita da $f(n, m) = (m + 1, n - 1)$ è invertibile e determinarne l'inversa.

SOL.

(a)

$$f(\{0,1,2\}) = \{f(0), f(1), f(2)\} = \{0, -1\}$$
$$f^{-1}(\{0\}) = \{n \in \mathbb{N} : f(n) = 0\} = \{n \in \mathbb{N} : n^2 - 2n = 0\} = \{n \in \mathbb{N} : n(n-2) = 0\} = \{0, 2\}$$
$$f^{-1}(\{-2, -1, 5\}) = \{n \in \mathbb{N} : f(n) = -2 \ \vee \ f(n) = -1 \ \vee \ f(n) = 5\} =$$
$$= \{n \in \mathbb{N} : n^2 - 2n = -2 \ \vee \ n^2 - 2n = -1 \ \vee \ n^2 - 2n = 5\} =$$
$$= \{n \in \mathbb{N} : n^2 - 2n + 2 = 0 \ \vee \ n^2 - 2n + 1 = 0 \ \vee \ n^2 - 2n - 5 = 0\}$$

Cerchiamo quindi le soluzioni delle equazioni coinvolte, considerando però solo le soluzioni che sono numeri natuali.
L'equazione $x^2 - 2x + 2 = 0$ non ha soluzioni reali (il discriminante è negativo) quindi non ne ha neanche di naturali.
L'equazione $x^2 - 2x + 1 = 0$ è equivalente a $(x-1)^2 = 0$ e quindi ha un'unica soluzione $x = 1$ che è un numero naturale.
L'equazione $x^2 - 2x - 5 = 0$ ha soluzioni reali $x_1 = 1 + \sqrt{1+5} = 1 + \sqrt{6}$ e $x_2 = 1 - \sqrt{6}$, ma nessuna di queste soluzioni è un numero naturale. In definitiva abbiamo

$$f^{-1}(\{-2, -1, 5\}) = \{1\}.$$

(b) La funzione $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ definita da $f(a, b) = a - b$ non è iniettiva perché, ad esempio, $f(1, 1) = f(2, 2)$. La funzione f è suriettiva: se z è un elemento del codominio, allora z appartiene all'immagine di f perché, ad esempio, $f(z, 0) = z$.

(c) Data la funzione $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ definita da $f(n, m) = (m+1, n-1)$ consideriamo un generico elemento del codominio, (x, y), e calcoliamo le sue controimmagini:

$$(a, b) \in f^{-1}(x, y) \ \Leftrightarrow \ f(a, b) = (x, y) \ \Leftrightarrow \ (b+1, a-1) = (x, y) \ \Leftrightarrow \ b + 1 = x \ \wedge \ a - 1 = y \ \Leftrightarrow$$
$$\Leftrightarrow \ b = x - 1 \ \wedge \ a = y + 1.$$

Quindi, ogni elemento del codominio ha un'unica controimmagine; ne segue che la funzione f è biunivoca e quindi invertibile. L'inversa f^{-1} è la funzione che porta l'elemento (x, y) del codominio di f nell'elemento (a, b) che abbiamo trovato sopra, ovvero $f^{-1} : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ e $f^{-1}(x, y) = (y + 1, x - 1)$.

4. **CALCOLO COMBINATORIO** (ANCORA DA SVOLGERE IN CLASSE)

5. **ARITMETICA E CONGRUENZE** Considera la relazione $\equiv_9$ di congruenza modulo 9.

(a) È vero che $-5 \equiv_9 5$?

(b) Quale classe d'equivalenza fra $[0], [1], [2]. \ldots, [8]$ contiene il numero -13?

(c) Il numero 5 è invertibile modulo 9? Se si, trovane l'inverso nell'insieme $\{0, 1, 2, \ldots, 8\}$.

(d) Calcola il resto nella divisione per 9 del numero $90^{134} - 12^3 + 8^5$.

SOL.

(a) Non vale $-5 \equiv_9 5$ perché $-5 - 5 = -10$ non è divisibile per 9.

(b) Poiché $-13 \equiv_9 5$ (infatti $-13 = (-2) \cdot 9 + 5$), si ha $-13 \in [5]$.

(c) Il numero 5 è invertibile modulo 9 ed il suo inverso è 2: infatti, $5 \cdot 2 = 10 \equiv_9 1$.

(d) Si ha

$$90^{134} - 12^3 + 8^5 \equiv_9 0^{134} - 3^3 + (-1)^5 = -27 - 1 = -28 \equiv_9 8.$$

Quindi il resto è 8.

6. **RELAZIONI D'EQUIVALENZA** Considerare la relazione d'equivalenza R sulle coppie di numeri naturali $\mathbb{N} \times \mathbb{N}$ definita da

$$(a, b)R(c, d) \qquad \Leftrightarrow \qquad \text{a-b=c-d}$$

(a) Determinare se $(5,2)R(2,5)$ e se $(5,2)R(7,4)$.

(b) Descrivere la classe di equivalenza di $(0,0)$.

(c) Determinare quali fra i seguenti insiemi sono insiemi di rappresentanti per le classi d'equivalenza di R su $\mathbb{N}$:

i. $\{(a,b) \in \mathbb{N} \times \mathbb{N} : a = b\}$;

ii. $\{(a,b) \in \mathbb{N} \times \mathbb{N} : b = 0\}$;

iii. $\{(a,0) : a \in \mathbb{N}\} \cup \{(0,b) : b \in \mathbb{N}, b \neq 0\}$.

SOL.

(a) $(5,2)R(2,5)$ non vale perché $5-2 \neq 2-5$ mentre $(5,2)R(7,4)$ perché $5-2 = 7-4$.

(b)
$$[(0,0] = \{(a,b) \in \mathbb{N} \times \mathbb{N} : (0,0)R(a,b)\} = \{(a,b) \in \mathbb{N} \times \mathbb{N} : a = b\}.$$

(c) Determinare se uno dei seguenti insiemi è un insieme di rappresentanti per le classi d'equivalenza di R su $\mathbb{N}$:

i. $\{(a,b) \in \mathbb{N} \times \mathbb{N} : a = b\}$; non è un insieme di rappresentanti perché tutti gli elementi dell'insieme appartengono alla stessa classe di $(0,0)$ e quindi non rappresentano tutte le possibili classi;

ii. $\{(a,b) \in \mathbb{N} \times \mathbb{N} : b = 0\}$; non è un insieme di rappresentanti perché, ad esempio, non vi è nell'insieme nessun rappresentante per la coppia $(0,1)$: infatti
$$(a,0)R(0,1) \;\Leftrightarrow\; a = -1,$$
ma a deve essere un numero naturale, quindi è impossibile.

iii. $\{(a,0) : a \in \mathbb{N}\} \cup \{(0,b) : b \in \mathbb{N}, b \neq 0\}$ è un insieme di rappresentanti: ogni coppia (a,b) per cui $a-b \geq 0$ sta nella stessa classe di $(a-b,0)$, mentre ogni coppia (a,b) per cui $a-b < 0$ sta nella stessa classe di $(0,b-a)$. Inoltre, elementi diversi dell'insieme
$$\{(a,0) : a \in \mathbb{N}\} \cup \{(0,b) : b \in \mathbb{N}, b \neq 0\}$$
non sono mai in relazione fra loro: se $(a,0)R(a',0)$ allora $a-0 = a'-0$ ovvero $a = a'$; se $(0,b)R(0,b')$ allora $0-b = 0-b'$ ovvero $b = b'$; inoltre, non è possibile che un elemento della forma $(a,0)$ sia in relazione con un elemento della forma $(0,b)$ con $b \neq 0$, perché se $(a,0)R(0,b)$ allora $a-0 = 0-b$ ovvero $a = -b$ e $a+b = 0$, impossibile perché $a,b \in \mathbb{N}$ e $b \neq 0$.

7. **RSA**

(a) Sotto quali condizioni la coppia di interi positivi (m,s) può essere scelta come chiave pubblica in un codice RSA? E se queste condizioni sono soddisfatte, quale sarà la chiave privata corrispondente?

(b) Trova un numero s per cui $(33,s)$ può essere scelta come chiave pubblica in un codice RSA e fornisci la chiave privata corrispondente.

(c) Verificare che $(22,3)$ e $(22,7)$ possono essere scelti, rispettivamente, come chiave pubblica e chiave privata di un codice RSA; cifrare il numero 5 e decifrare il numero 3 usando questo codice.

SOL.

(a) La coppia di interi positivi (m,s) può essere scelta come chiave pubblica in un codice RSA se e solo se $MCD(s,\phi(m)) = 1$, dove ϕ è la funzione di Eulero. Se questa condizione vale, allora s è invertibile modulo $\phi(m)$, quindi esiste un (unico) numero t con $0 < t < \phi(m)$ tale che $s \cdot t \equiv_{\phi(m)} 1$. La coppia (m,t) è allora la corrispondente chiave privata.

(b) Se $m = 33$ allora $\phi(m) = \phi(3 \cdot 11) = 2 \cdot 10 = 20$. Basta quindi scegliere s in modo che $MCD(s,20) = 1$, ad esempio $s = 7$. La chiave privata sarà allora 3 perché $3 \cdot 7 = 21 \equiv_{20} 1$.

(c) $(22, 3)$ e $(22, 7)$ possono essere scelti, rispettivamente, come chiave pubblica e chiave privata di un codice RSA, perché

$$\phi(22) = \phi(2 \cdot 11) = \phi(2) \cdot \phi(11) = 1 \cdot 10 = 10, \quad MCD(3, 10) = 1, \quad 3 \cdot 7 = 21 \equiv_{20} 1.$$

Per cifrare il numero 5 basta calcolare 5^3 modulo 22:

$$5^3 = 5^2 \cdot 5 = 25 \cdot 5 \equiv_{22} 3 \cdot 5 = 15.$$

Per decifrare il numero 3 dobbiamo calcolare 3^7 modulo 22:

$$3^7 = (3^3)^2 \cdot 3 = (27)^2 \cdot 3 \equiv_{22} 5^2 \cdot 3 = 25 \cdot 3 \equiv_{22} 3 \cdot 3 = 9.$$