

COGNOME NOME ANNO

Inserire le risposte negli spazi predisposti, accompagnandole con *spiegazioni chiare ed essenziali*.
 NON SI ACCETTANO RISPOSTE SCRITTE SU ALTRI FOGLI. Ogni esercizio vale 6 punti.

1. Determinare la tavola di verità della forma proposizionale $(\neg p) \rightarrow (q \wedge r)$.

p	q	r	$\neg p$	$q \wedge r$	$(\neg p) \rightarrow (q \wedge r)$
0	0	0	1	0	0
0	0	1	1	0	0
0	1	0	1	0	0
0	1	1	1	1	1
1	0	0	0	0	1
1	1	0	0	0	1
1	0	1	0	0	1
1	1	1	0	1	1

2. Dimostrare per induzione che $\sum_{k=1}^n (2k-1)^2$ è uguale a $\frac{n(2n-1)(2n+1)}{3}$.

Abbiamo che

$$\sum_{k=1}^{n+1} (2k-1)^2 = \sum_{k=1}^n (2k-1)^2 + (2n+1)^2.$$

Per induzione questo è uguale a

$$\begin{aligned} \frac{n(2n-1)(2n+1)}{3} + (2n+1)^2 &= \frac{2n+1}{3} (n(2n-1) + 3(2n+1)), \\ &= \frac{(2n+1)(2n+3)(n+1)}{3}. \end{aligned}$$

Concludiamo che la formula vale per $n+1$ quando vale per n . Siccome vale anche per $n=1$, la dimostrazione è completa.

3. Sia $n = 55$. Sia $D = 17$ e sia $x = 9$. Determinare un esponente E tale che $(x^D)^E \equiv x \pmod{n}$.

Sia $p = 5$ e $q = 11$. Siccome p e q sono primi, abbiamo che $x^{(p-1)(q-1)} \equiv 1 \pmod{n}$. Quindi, se E soddisfa $DE \equiv 1 \pmod{(p-1)(q-1)}$, allora $((x^D)^E = x^{DE} \equiv 1 \pmod{n})$. Sostituendo $D = 17$ e $(p-1)(q-1) = 4 \cdot 10 = 40$ basta quindi risolvere l'equazione $17E \equiv 1 \pmod{40}$. Abbiamo che

$$\begin{aligned} 1 \cdot 40 + 0 \cdot 17 &= 40, \\ 0 \cdot 40 + 1 \cdot 17 &= 17, \\ 1 \cdot 40 + (-2) \cdot 17 &= 6, & (1^{\text{a}} \text{ eq.} - 2 \cdot 2^{\text{a}} \text{ eq.}) \\ (-2) \cdot 40 + 5 \cdot 17 &= 5, & (2^{\text{a}} \text{ eq.} - 2 \cdot 3^{\text{a}} \text{ eq.}) \\ 3 \cdot 40 + (-7) \cdot 17 &= 1. & (3^{\text{a}} \text{ eq.} - 4^{\text{a}} \text{ eq.}) \end{aligned}$$

e quindi $E = -7 \equiv 23 \pmod{40}$ è una soluzione.

4. Trovare tutte le soluzioni $x \in \mathbf{Z}$ del sistema di congruenze $\begin{cases} x \equiv 6 \pmod{9}; \\ x \equiv 4 \pmod{8}. \end{cases}$

Siano $n, m, r, s \in \mathbf{Z}$. Se $a, b \in \mathbf{Z}$ soddisfano $an + bm = 1$, allora le soluzioni $x \in \mathbf{Z}$ del sistema di congruenze $\begin{cases} x \equiv r \pmod{n}, \\ x \equiv s \pmod{m}, \end{cases}$ sono $x \equiv san + brm \pmod{nm}$.

Sia $n = 9$, $m = 8$, $r = 6$ e $s = 4$. Siccome $1 \cdot 9 + (-1) \cdot 8 = 1$ possiamo prendere $a = 1$ e $b = -1$. Le soluzioni sono quindi $x = 4 \cdot 1 \cdot 9 + (-1) \cdot 6 \cdot 8 = -12 \equiv 60 \pmod{72}$.

Alternativamente: dalla prima equazione segue che $x = 6 + 9h$ per un $h \in \mathbf{Z}$. Sostituendo nella seconda, abbiamo che $6 + 9h \equiv 4 \pmod{8}$. Da cui $9h \equiv -2 \pmod{8}$, cioè $h \equiv -2 \pmod{8}$. In altre parole $h = -2 + 8s$ per un $s \in \mathbf{Z}$ e quindi $x = 6 + 9(-2 + 8s) = -12 + 72s$ per un $s \in \mathbf{Z}$.

5. Costruire una biezione da $\mathbf{Z}$ all'insieme dei numeri interi congrui a 3 $\pmod{7}$.

Sia $S = \{m \in \mathbf{Z} : m \equiv 3 \pmod{7}\}$. Allora la mappa $f : \mathbf{Z} \rightarrow S$ data da $f(n) = 3 + 7n$ è una biezione. In effetti, se $f(n) = f(n')$, allora $3 + 7n = 3 + 7n'$ e quindi $n = n'$ e si vede che f è iniettiva. D'altraparte f è suriettiva, perché ogni $m \in S$ ha la forma $3 + 7n$ e quindi $m = f(n)$ per un $n \in \mathbf{Z}$.