**Geometria e Combinatoria**

Esercitazione

1. Usando l'algoritmo euclideo, calcolare il massimo comun divisore $d$ fra gli interi $a$ e $b$; trovare poi due interi $s$ e $t$ tali che si abbia $d = as + bt$.
   (a) $a$=72, $b$=58.
   (b) $a$=418, $b$=321.

2. Trovare, se è possibile, soluzioni intere per le seguenti equazioni:
   (a) $13x + 4y = 1$.
   (b) $13x + 4y = 7$.
   (c) $4x + 18y = 6$.
   (d) $215x + 175y = 60$.

3. Per quali valori del parametro $k$ la seguente equazione ammette soluzioni intere?

$$30x + ky = 35$$

| | | | | | |
|---|---|---|---|---|---|
| $k = 25$ | ☐ | $k = 26$ | ☐ | $k = 27$ | ☐ |
| $k = 30$ | ☐ | $k = 33$ | ☐ | $k = 35$ | ☐ |
| $k = 45$ | ☐ | $k = 46$ | ☐ | $k = 47$ | ☐ |

4. Dimostrare che se $n$ è un intero non primo $\geq 2$, allora esiste un numero primo $p$ tale che $p|n$ e $p^2 \leq n$.

5. Mostrare che $a|bc$ e $(a, c) = 1$ implica $a|b$.

6. Sia $n$ un intero maggiore di 1.
   (a) Calcolare $2n \pmod{n}$, $(5n+7) \pmod{n}$, $(3n-2) \pmod{n}$.
   (b) Calcolare $(n + 2) \pmod{n + 1}$, $(2n + 2) \pmod{n + 1}$, $n^2 \pmod{n + 1}$, $(n^2 + 1) \pmod{n + 1}$, $(n^2 - 1) \pmod{n + 1}$.
   (c) Calcolare $(n+1)^2 \pmod{n}$, $(n^3+2n^2+4) \pmod{n}$, $n! \pmod{n}$.

7. Senza eseguire le moltiplicazioni per esteso, mostrare che si ha
   (a) $1234567 \times 90123 \equiv 1 \pmod{10}$;
   (b) $2468 \times 13579 \equiv -3 \pmod{25}$.

8. Dimostrare che la somma di tre interi consecutivi è zero modulo 3.

9. Quando è possibile, trovare tutte le soluzioni delle seguenti congruenze.

   (a) $7x \equiv 3 \pmod{10}$;
   (b) $5x \equiv 3 \pmod{10}$;
   (c) $3x \equiv 19 \pmod{29}$;
   (d) $6x \equiv 21 \pmod{15}$;
   (e) $-4x \equiv 6 \pmod{10}$;
   (f) $x \equiv 4^{2546} \pmod{5}$.

10. Descrivere l'insieme degli interi $b$ tali che $34x \equiv b \pmod{51}$ sia risolubile.

11. Dimostrare che, se $y$ è soluzione della congruenza $ax \equiv b \pmod{n}$, allora $z = y + k\frac{n}{(a,n)}$ è soluzione della congruenza per ogni $k \in \mathbb{Z}$.

12. Verificare quali delle seguenti relazioni $R$ (in cui $A$ è l'insieme su cui sono definite, e $x$ e $y$ sono elementi di $A$) sono riflessive, quali simmetriche, quali transitive, quali di equivalenza o di ordine. Per le relazioni di equivalenza, capire come è fatto l'insieme $A/R$ delle classi di equivalenza.

    (a) $A = \mathbb{Z}$, $xRy$ se e solo se $\mathrm{MCD}(x, y) = 1$;
    (b) $A = \mathbb{Z}$, $xRy$ se e solo se $x + y$ è un multiplo di 4;
    (c) $A = \mathbb{Z}$, $xRy$ se e solo se $x - y$ è un multiplo di 4;
    (d) $A$ è l'insieme delle stringhe binarie di lunghezza $n$; $xRy$ se $x$ contiene lo stesso numero di 1 di $y$;
    (e) $A$ è l'insieme delle rette nel piano, $xRy$ se e solo se $x$ e $y$ sono perpendicolari.

13. Sia $f : A \to B$ un'applicazione. Sia $Re_f$ la relazione definita su $A$ tale che $x\, Re_f\, y$ se e solo se $f(x) = f(y)$. Dimostrare che $Re_f$ è una relazione di equivalenza. Studiare l'insieme quoziente modulo $Re_f$ per le seguenti applicazioni:

    (a) $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = x^2$.
    (b) $f : \mathbb{Z} \to \mathbb{Z}$, $f(x)$ è il resto nella divisione di $x$ per 4.