

TRENTO, A.A. 2011/12
CORSO DI ALGEBRA
FOGLIO DI ESERCIZI # 1

Esercizio 1.1. Si trovi quanto grande devo prendere l'intero x perché 2^x sia (in centimetri)

- maggiore del raggio della galassia in cui viviamo,
- maggiore del raggio dell'Universo conosciuto.

Esercizio 1.2. Si mostri che l'unico numero intero divisibile per ogni numero intero positivo è 0.

Nell'esercizio seguente, si assuma come noto il teorema della divisione con resto, nella forma seguente.

Teorema. *Dati due numeri interi a, b , con $a \geq 0$, e $b > 0$, esistono unici due numeri $q, r \in \mathbf{Z}$ che soddisfano le proprietà:*

$$\begin{cases} a = b \cdot q + r, \\ 0 \leq r < b. \end{cases}$$

Esercizio 1.3 (Facoltativo). Si dimostri il seguente

Teorema (Un resto diverso). *Dati due numeri interi a, b , con $b > 0$, esistono unici due numeri $q, r \in \mathbf{Z}$ che soddisfano le proprietà:*

$$\begin{cases} a = b \cdot q + r, \\ -\frac{b}{2} \leq r < \frac{b}{2} \quad (\text{ovvero } -b \leq 2r < b). \end{cases}$$

Esercizio 1.4. Sia $D(a)$ l'insieme dei divisori di $a \in \mathbf{Z}$, e $D(a, b) = D(a) \cap D(b)$ l'insieme dei divisori comuni di $a, b \in \mathbf{Z}$. Si mostri che

$$D(a) = D(-a),$$

e

$$D(a, b) = D(-a, b) = D(a, -b) = D(-a, -b).$$

(In altre parole, $D(a, b) = D(|a|, |b|)$.)

Se ne deduca che nel calcolare il MCD di $a, b \in \mathbf{Z}$, ci si può sempre ridurre al caso in cui siano entrambi non negativi.

Esercizio 1.5. Siano $a, b \in \mathbf{Z}$, non entrambi nulli. Sia $d = (a, b)$ il loro massimo comun divisore.

Si supponga di aver trovato (per esempio mediante l'algoritmo di Euclide esteso) una coppia x_0, y_0 tale che $ax_0 + by_0 = d$.

Si enunci e si dimostri la formula per *tutte* le coppie x, y tali che $ax + by = d$.

(SUGGERIMENTO: Si rifaccia la dimostrazione fatta a lezione, ma scambiando i ruoli di a e b , e si discuta in particolare come si aggira il problema che uno dei due potrebbe essere zero.)

Esercizio 1.6. Per ognuna delle seguenti coppie (a, b) , usando l'algoritmo di Euclide (esteso),

- si trovi il massimo comun divisore d di a e b ;
- si trovi il minimo comune multiplo di a e b ;
- si trovi *una coppia* di numeri (x, y) tali che $ax + by = d$;
- si trovino *tutte le coppie* di numeri (x, y) tali che $ax + by = d$.

a	b
55	34
89	55
957	115
10946	6766
9762	501
736	337

Esercizio 1.7. Si mostri che per $a, b \in \mathbf{Z}$ sono equivalenti le seguenti asserzioni:

- $(a, b) = 1$, e
- esistono $x, y \in \mathbf{Z}$ tali che

$$ax + by = 1.$$

Esercizio 1.8. Siano $a, b, c \in \mathbf{Z}$. Supponiamo che esistano $x, y \in \mathbf{Z}$ tali che

$$ax + by = c.$$

- (1) Posso dire che $(a, b) = c$? (SUGGERIMENTO: No: occorrerà un esempio.)
- (2) Cosa posso dire dei legami fra c e (a, b) ?

Esercizio 1.9. Siano $a, b \in \mathbf{Z}$. Si mostri che se m_1 e m_2 sono due minimi comuni multipli di a e b , allora $m_2 = \pm m_1$.

Esercizio 1.10. Sappiamo che se a e b sono due interi non entrambi nulli (e dunque $(a, b) \neq 0$), allora si ha

$$\left(\frac{a}{(a, b)}, \frac{b}{(a, b)} \right) = 1.$$

Si consideri la seguente affermazione:

Siano $a, b \in \mathbf{Z}$, non entrambi nulli. Allora si ha

$$\left(\frac{a}{(a, b)}, b \right) = 1 \quad \text{oppure} \quad \left(a, \frac{b}{(a, b)} \right) = 1$$

Si mostri o che l'affermazione è vera, o che non lo è, esibendo in questo caso un controesempio.

Esercizio 1.11. Si mostri che sono equivalenti le affermazioni

- $a \equiv b \pmod{n}$, e
- $a \equiv b \pmod{-n}$.

Esercizio 1.12. Dimostrare *usando direttamente la definizione* che la relazione di congruenza è di equivalenza.

Esercizio 1.13. Sia A un insieme non vuoto, e R una relazione di equivalenza su di esso. Si mostri che per $a, b \in A$ sono equivalenti:

- aRb ,
- $a \in [b]$,
- $[a] \subseteq [b]$,
- $[a] = [b]$.

Si mostri che per ogni $a \in A$ si ha $a \in [a]$.

Esercizio 1.14. Si consideri la relazione di congruenza modulo n sugli interi, per $n \geq 0$.

Per ogni $a \in \mathbf{Z}$, sia $[a] = \{x \in \mathbf{Z} : x \equiv a \pmod{n}\}$ la sua classe di congruenza. Si mostri che $[a] = \{a + n \cdot t : t \in \mathbf{Z}\}$.

Esercizio 1.15 (Del tutto facoltativo). Si consideri l'insieme $\mathbf{R}^{\mathbf{N}}$ delle successioni $(a_0, a_1, a_2, a_3, \dots)$ a coefficienti reali. $\mathbf{R}^{\mathbf{N}}$ è uno spazio vettoriale su \mathbf{R} , con le operazioni naturali per componenti.

Si consideri

$$\mathcal{F} = \{(a_0, a_1, a_2, a_3, \dots) : a_{i+2} = a_{i+1} + a_i, \text{ per } i \in \mathbf{N}\} \subseteq \mathbf{R}^{\mathbf{N}}.$$

- Si mostri che \mathcal{F} è un sottospazio di $\mathbf{R}^{\mathbf{N}}$, e che ha dimensione 2. Se ne trovi una base formata da successioni della forma $a_i = q^i$, per opportuni $q \in \mathbf{R}$.
- La successione di Fibonacci f_i , ove $f_0 = 0, f_1 = 1$, e $f_{i+2} = f_{i+1} + f_i$, appartiene a \mathcal{F} . La si scriva come combinazione lineare della base precedente.
- Vogliamo mostrare che il massimo comun divisore $(f_n, f_{n-1}) = 1$ per ogni n . Questo si può per esempio vedere dimostrando prima che per ogni $n > k$ si ha

$$(-1)^{k+1} f_n f_k + (-1)^k f_{n-1} f_{k+1} = f_{n-k-1}.$$

In particolare per ogni $n \geq 2$ si ha

$$(-1)^{n-1} f_n f_{n-2} + (-1)^n f_{n-1}^2 = 1,$$

e per ogni $n \geq 3$ si ha

$$(-1)^n f_n f_{n-3} + (-1)^{n-1} f_{n-1} f_{n-2} = 1.$$