TRENTO, A.A. 2019/20
CORSO DI ALGEBRA A
FOGLIO DI ESERCIZI # 2

Esercizio 2.1. Trovate x tale che 2^x rappresenti approssimativamente in centimetri

- la distanza della Terra dalla Luna;
- la distanza della Terra dal Sole;
- il diametro della nostra Galassia;
- il raggio dell'Universo osservabile.

Esercizio 2.2. Si mostri che per $a, b \in \mathbf{Z}$ sono equivalenti le seguenti asserzioni:

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

$$ax + by = 1.$$

Esercizio 2.3. Siano $a, b, c \in \mathbf{Z}$. Supponiamo che esistano $x, y \in \mathbf{Z}$ tali che

$$ax + by = c.$$

(1) Posso dire che $\gcd(a, b) = c$? (SUGGERIMENTO: La risposta è no. Occorrerebbe un esempio.)
(2) Cosa posso dire comunque dei legami fra c e $\gcd(a, b)$?

Esercizio 2.4. Si enuncino e si dimostrino i Lemmi Aritmetici.

Esercizio 2.5. Si dia la definizione di minimo comune multiplo di due interi.

Esercizio 2.6. Siano $a, b, m \in \mathbf{Z}$. Si dimostri che sono equivalenti

- m è un minimo comune multiplo di a e b;
- $\mathfrak{M}(a) \cap \mathfrak{M}(b) = \mathfrak{M}(m)$.

Qui $\mathfrak{M}(c) = \{ x \in \mathbf{Z} : c \mid x \}$ è l'insieme dei *multipli* di $c \in \mathbf{Z}$.

Esercizio 2.7. Si mostri che

(1) se m è un minimo comune multiplo di a e b, allora anche $-m$ lo è, e che
(2) se m_1 e m_2 sono due minimi comuni multipli di a e b, allora $m_2 = \pm m_1$.

Si faccia l'esercizio in due modi, una volta usando direttamente la definizione di mcm, e un'altra usando l'Esercizio 2.6.

Esercizio 2.8 (Facoltativo). Sappiamo che se a e b sono due interi non entrambi nulli (e dunque $\gcd(a, b) \neq 0$), allora si ha

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

Si consideri la seguente affermazione:

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

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

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

Esercizio 2.9. Siano a, b interi *positivi*. Si dimostri la formula

$$\gcd(a,b) \cdot \operatorname{lcm}(a,b) = a \cdot b.$$

Esercizio 2.10 (Lo trovate svolto negli appunti, sottosezione 1.3.1). Si mostri che se a, b, c sono interi positivi, si ha

$$\gcd(a, \operatorname{lcm}(b,c)) = \operatorname{lcm}(\gcd(a,b), \gcd(a,c)),$$
$$\operatorname{lcm}(a, \gcd(b,c)) = \gcd(\operatorname{lcm}(a,b), \operatorname{lcm}(a,c)).$$

Esercizio 2.11. Siano $a, b \in \mathbf{Z}$, non entrambi nulli. Sia $d = \gcd(a,b)$ 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 2.12 (Facoltativo, ma vale la pena conoscere gli enunciati, e sapere che sono equivalenti).

Tradizionalmente l'induzione viene usata nel modo seguente.

Induzione 1.1. Sia P una proprietà definita sui numeri naturali. Supponiamo che valgano le seguenti ipotesi:

(1) è vera $P(0)$,
(2) per ogni $a \in \mathbf{N}$, se è vera $P(a)$, allora è vera $P(a+1)$.

Allora $P(a)$ è vera per ogni $a \in \mathbf{N}$.

Una forma alternativa, che è spesso più utile in Algebra, è

Induzione 2.1. Sia Q una proprietà definita sui numeri naturali. Supponiamo che valgano le seguenti ipotesi:

(1) esiste un numero naturale N tale che siano vere $Q(0), Q(1), \ldots, Q(N)$,
(2) per ogni $a \geq N$, se sono vere $Q(0), Q(1), \ldots, Q(a)$, allora è vera $Q(a+1)$.

Allora $Q(a)$ è vera per ogni $a \in \mathbf{N}$.

Fate vedere che le due forme somo *equivalenti*. Si tratta dunque di assumere una delle due, e usarla per dimostrare l'altra, e poi viceversa.

Entrambe si possono riformulare in termini di insiemi.

Induzione 1.2. Sia $A \subseteq \mathbf{N}$. Supponiamo che

(1) $0 \in A$, e
(2) per ogni $a \in \mathbf{N}$, se $a \in A$, allora $a+1 \in A$.

Allora $A = \mathbf{N}$.

Induzione 2.2. Sia $A \subseteq \mathbf{N}$. Supponiamo che

(1) esista un numero naturale N tale che $0, 1, \dots N \in A$,
(2) per ogni $a \in \mathbf{N}$, con $a \geq N$, se $0, 1, \dots, a \in A$, allora $a + 1 \in A$.
Allora $A = \mathbf{N}$.

Conviene considerare anche il

Principio del minimo intero. Sia $A \subseteq \mathbf{N}$. Allora

- *o A è vuoto,*
- *oppure A ha un minimo.*

Qui per minimo si intende un elemento $m \in A$ tale che $m \leq a$ per ogni $a \in A$.

Si può per esempio dimostrare che dalla seconda forma dell'induzione segue il principio del minimo intero, dal principo del minimo intero segue la prima forma, e da quest'ultima segue la seconda forma.

Esercizio 2.13. Si dimostri, per induzione o con il principio del minimo intero, il

Teorema. Siano $a, b \in \mathbf{Z}$ con $a \geq 0$ e $b > 0$. Allora esistono $q, r \in \mathbf{N}$ tali che

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

Esercizio 2.14.

(1) Si definisca la relazione di congruenza modulo n.
(2) Si dimostri, *usando direttamente la definizione* che la relazione di congruenza è una relazione di equivalenza.
(3) Si mostri che per $n > 0$ sono equivalenti
   (a) $a \equiv b \pmod{n}$, e
   (b) a e b divisi per n danno lo stesso resto.
(4) Si deduca dal punto (3) che la congruenza modulo n è una relazione di equivalenza.

Esercizio 2.15. Si mostri che sono equivalenti le affermazioni

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

Esercizio 2.16. Sostituito con l'Esercizio 11.3.

Esercizio 2.17. Sia A un insieme non vuoto, e R una relazione di equivalenza su di esso.

- Si mostri che per ogni $a \in A$ si ha $a \in [a]$.
- Si mostri che per $a, b \in A$ sono equivalenti:
  (1) aRb,
  (2) $a \in [b]$,
  (3) $[a] \subseteq [b]$,
  (4) $[a] = [b]$.

Esercizio 2.18. Sia $A \neq \emptyset$ un insieme, e $\mathcal{P}$ un insieme di sottoinsiemi non vuoti di A. Si mostri che sono equivalenti

(1) ogni $a \in A$ sta in uno e un solo elemento di $\mathcal{P}$, e

(2) A è unione disgiunta degli elementi di $\mathcal{P}$, ovvero $A = \bigcup \mathcal{P}$, e se $P \neq Q \in \mathcal{P}$, allora $P \cap Q = \emptyset$.

(Vi ricordo che $\bigcup \mathcal{P} = \{\, x \in A : \text{esiste } P \in \mathcal{P} \text{ tale che } a \in P \,\}$.)

Esercizio 2.19. Si mostri che se A è un insieme non vuoto, R è una relazione di equivalenza su A, e per $a \in A$ definiamo la sua classe

$$[a] = \{\, x \in A : xRa \,\},$$

allora

$$\{\, [a] : a \in A \,\}$$

è una partizione di A.