TRENTO, A.A. 2015/16
CORSO DI ALGEBRA
FOGLIO DI ESERCIZI # 2

Esercizio 2.1. Completate l'Esercizio 1.16 in tutte le sue parti.

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. Si enuncino e si dimostrino i Lemmi Aritmetici.

Esercizio 2.4. 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 dei legami fra c e $\gcd(a, b)$?

Esercizio 2.5 (Facoltativo). Siano $a, b, m \in \mathbf{Z}$. Si dimostri che sono equivalenti

- m è un minimo comun multiplo di a e b;
- $M(a, b) = M(a) \cap M(b) = M(m)$.

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

Esercizio 2.6. Siano $a, b \in \mathbf{Z}$. Si mostri che se m_1 e m_2 sono due minimi comun multipli di a e b, allora $m_2 = \pm m_1$.

Esercizio 2.7 (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 2.8. 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 2.9 (Da cui segue che il nostro MCD è lo stesso della scuola). Si consideri l'affermazione:

$$\text{Se } a, b \in \mathbf{Z}, \text{ e } b \mid a, \text{ allora } b \leq a,$$

Si mostri che l'affermazione, cosí come è scritta, è falsa. (Basta *un* esempio.) Si veda come aggiustarla.
(SUGGERIMENTO: E' grosso modo una questione di segni...)

Esercizio 2.10. Dimostrare *usando direttamente la definizione* che la relazione di congruenza è una relazione di equivalenza.

Esercizio 2.11.

- Si definisca la relazione di congruenza modulo n.
- Si mostri che per $n \neq 0$ sono equivalenti
  (1) $a \equiv b \pmod{n}$, e
  (2) a e b divisi per n danno lo stesso resto.
- Se ne deduca che la congruenza modulo n è una relazione di equivalenza.

Esercizio 2.12. Si mostri che sono equivalenti le affermazioni

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

Esercizio 2.13. 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 2.14. 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 2.15. 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.

Esercizio 2.16. Si enuncino e dimostrino i criteri di divisibilità per n, ove

$$n \in \{ 2, 4, 8, 5, 25, 125, 500, 3, 7, 9, 11, 13 \}.$$

Con questo intendo un modo di calcolare la classe $[a]$ di congruenza modulo n di un intero a, a partire dalle sue cifre decimali.

Esercizio 2.17.

(1) Si mostri che per calcolare il resto della divisione di x per $n = 2^a 5^b$ è sufficiente guardare le ultime c cifre decimali di x, ove $c = \max\{a, b\}$.
(2) (Facoltativo) Supponiamo che per calcolare il resto della divisione per n di ogni numero x sia sufficiente guardare le ultime c cifre decimali di x. Si mostri che n è della forma $2^a 5^b$ (con $c \geq a, b$).

Esercizio 2.18. Mostrate che le operazioni

$$[a] + [b] = [a + b], \quad [a] \cdot [b] = [ab].$$

fra classi resto modulo n sono ben definite.

Esercizio 2.19. Si mostri che se $n > 0$ ci sono esattamente n classi resto distinte modulo n, e che esse sono $[0], [1], \ldots, [n-1]$.

Esercizio 2.20. Fissiamo un intero $n > 0$. Sia $a \in \mathbf{Z}$. Si mostri che sono equivalenti le seguenti affermazioni:

- n divide a,
- $a \equiv 0 \pmod{n}$,
- $[a] = [0]$,

dove queste ultime classi sono le classi modulo n.

Esercizio 2.21 (Assolutamente facoltativo).

Si consideri la seguente procedura. Parto da un numero scritto in forma decimale $a_n \ldots a_1 a_0$. Moltiplico fra loro le cifre, calcolo dunque $a_n \cdot \cdots \cdot a_1 \cdot a_0$. Ripeto la procedura. Per esempio parto da 382, ottengo $3 \cdot 8 \cdot 2 = 48$, ricalcolo $4 \cdot 8 = 32$, e infine $3 \cdot 2 = 6$, e qui mi fermo.

- Dimostrare che a un certo punto arrivo a un numero di una cifra, e qui dunque mi fermo.
- Trovare tutti i numeri tali che applicando la procedura arrivo alla cifra 1. Naturalmente fra questi ci sono i numeri $111\ldots111$. Si tratta di mostrare che sono gli unici.

Esercizio 2.22. Sia $n \geq 2$, e consideriamo le classi resto modulo n.

Si mostri che esse sono

$$[0], [1], \ldots, [n/2] = [-n/2], [-(n/2-1)], [-(n/2-2)], \ldots, [-2], [-1]$$

se n è pari, e

$$[0], [1], \ldots, [(n-1)/2], [-(n-1)/2], \\ [-((n-1)/2)-1)], [-((n-1)/2)-2)], \ldots, [-2], [-1]$$

se n è dispari.

Per esempio, se $n = 6$ le classi sono

$$[0], [1], [2], [3] = [-3], [-2], [-1];$$

se $n = 7$, le classi sono

$$[0], [1], [2], [3], [-3], [-2], [-1].$$

Attenzione! Non c'è alcuna contraddizione con il fatto che le classi sono

$$[0], [1], [2], \ldots, [n-1].$$

Sappiamo infatti che una stessa classe si può scrivere in molti modi diversi.

Esercizio 2.23. Siano $a, r, n \in \mathbf{Z}$, con $n \geq 2$, e $0 \leq r < n$. Si consideri la relazione di congruenza modulo n, e la classe resto $[a] = \{\, x \in \mathbf{Z} : x \equiv a \pmod{n} \,\}$.

- Si mostri che
$$[a] = \{\, a + nk : k \in \mathbf{Z} \,\}$$
- Si mostri che sono equivalenti:
  (1) r è il resto della divisione di a per n, e
  (2) $[a] = [r]$.

Esercizio 2.24. Si consideri il numero scritto in forma decimale

$$a = 126191x,$$

ove l'incognita x è la cifra decimale delle unità, dunque $0 \leq x < 10$.

- Per ogni $n \in \{\, 2, 3, 4, 7, 9, 11 \,\}$ si trovi x, se esiste, in modo che a sia divisibile per n.
- Se invece per un particolare n si ha che x non esiste, si spieghi perché.

Attenzione! x dipende da n, non è detto (né richiesto) che lo stesso x vada bene per tutti gli n.

Esercizio 2.25.

(1) Si dia la definizione di operazione (binaria) su un insieme non vuoto S. (SUGGERIMENTO: Per la verità non l'ho detto a lezione, o l'ho detto solo fuggevolmente, ma una funzione binaria "$*$" su $S \neq \emptyset$ è semplicemente una funzione $S \times S \to S$, in cui l'immagine dell'elemento (a, b) viene denotata $a * b$.)
(2) Si dica quando un'operazione è associativa.
(3) Si dia la definizione di semigruppo.
(4) Si dia la definizione di elemento neutro in un semigruppo.
(5) Si mostri che l'elemento neutro, se esiste, è unico.
(6) Si dia la definizione di monoide.
(7) Si dia la definizione di elemento simmetrizzabile e simmetrico in un monoide.
(8) Si mostri che se un elemento di un monoide ha un simmetrico, questo è unico.
(9) Si dia la definizione di gruppo.
(10) Sia $(M, \cdot, 1)$ un monoide, a $a, b \in M$ elementi invertibili.
  (a) Si mostri che 1 è invertibile, e $1^{-1} = 1$,
  (b) si mostri che a^{-1} è invertibile, e $(a^{-1})^{-1} = a$,
  (c) si mostri che ab è invertibile, e $(ab)^{-1} = b^{-1}a^{-1}$.

(11) Si mostri che se $(M, \cdot, 1)$ è un monoide, e G è l'insieme degli elementi invertibili di M, allora $(G, \cdot, 1)$ è un gruppo.

Esercizio 2.26. Si considerino le matrici a coefficienti razionali

$$a = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \qquad b = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

(1) Si mostri che $ab \neq ba$.
(2) Si mostri che entrambe le matrici sono invertibili, e si calcolino a^{-1}, b^{-1}.
(3) Si mostri che $(ab)^{-1} = b^{-1}a^{-1}$, ovvero che
$$(ab)(b^{-1}a^{-1}) = 1,$$
ove "1" denota la matrice identica 2×2..
(4) Si mostri che
$$(ab)(a^{-1}b^{-1}) \neq 1.$$
(5) Si mostri che $ba^{-1} \neq a^{-1}b$, il che spiega l'apparente contrasto fra gli ultimi due punti precedenti. (SUGGERIMENTO: Quest'ultimo punto andrebbe fatto senza calcoli espliciti di matrici, perché segue da alcuni dei punti precedenti.)