TRENTO, A.A. 2019/20
CORSO DI ALGEBRA A
FOGLIO DI ESERCIZI # 3

Esercizio 3.1. Sia $n \geq 2$. Si mostri che la classe di congruenza modulo n di $a \in \mathbf{Z}$ è

$$[a] = \{\, a + nt : t \in \mathbf{Z} \,\}.$$

Esercizio 3.2. Siano $x, n \in \mathbf{Z}$, con $n \neq 0$. Sia $[x]$ la classe di congruenza di x modulo n,

Si mostri che sono equivalenti

(1) n divide x,
(2) $x \equiv 0 \pmod{n}$,
(3) $[x] = [0]$.

Esercizio 3.3. Siano $a, r, n \in \mathbf{Z}$, con $n > 0$, e $0 \leq r < n$. Si mostri che sono equivalenti

(1) $a \in [r]$, e
(2) r è il resto della divisione di a per n.

Esercizio 3.4. Sia $n \geq 2$. Si mostri che le classi di congruenza modulo n sono n (distinte), e sono

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

Esercizio 3.5. Si diano le definizioni di gruppo e di anello.

Esercizio 3.6 (Facoltativo). Sia A un insieme non vuoto, su cui è definita una operazione $\cdot$. Supponiamo che $\cdot$ sia associativa, che cioè per $a, b, c \in A$ valga

$$a(bc) = (ab)c.$$

(Qui indichiamo l'operazione semplicemente con la giustapposizione, $ab = a \cdot b$.)

Siano $a_1, \ldots, a_n \in A$. Si mostri che tutti i possibili prodotti di $a_1, \ldots, a_n$ in quest'ordine coincidono.

Occorre per prima cosa precisare questa ultima espressione. Definiamo dunque, per ricorrenza su n, un *prodotto ammissibile* di $a_1, \ldots, a_n$.

Se $n = 1$, l'unico prodotto ammissibile è a_1. Se $n = 2$, l'unico prodotto ammissibile è $a_1 a_2$. Se $n \geq 3$, i prodotti ammissibili si ottengono scrivendo $n = s + t$, con $s, t \geq 1$, e prendendo il prodotto di un prodotto ammissibile di $a_1, \ldots, a_s$ con un prodotto ammissibile di $a_{s+1}, \ldots, a_n$.

Adesso provate a dimostrare per induzione su n che tutti i prodotti ammissibili di $a_1, \ldots, a_n$ coincidono col *prodotto normato a sinistra*

$$((\ldots(a_1 a_2)a_3)\ldots)a_n),$$

cioè col prodotto in cui prima calcolo $a_1 a_2$, poi moltiplico il risultato a destra per a_3, poi moltiplico il risultato a destra per a_4, ecc.

(SUGGERIMENTO: (Lascio però da parte qualche dettaglio.) Sia P un prodotto ammissibile di $a_1, \ldots, a_n$. Per definizione sarà della forma $P = ST$, ove S è un

prodotto ammissibile di $a_1, \dots, a_s$, e T è un prodotto ammissibile di $a_{s+1}, \dots, a_n$, con $s + t = n$.

Procedo a una doppia induzione, prima su n, e in subordine su t.

Se $t = 1$, per induzione su n si ha che S è un prodotto normato a sinistra, e dunque lo è anche P.

Se $t > 1$, allora posso scrivere $T = UV$, ove U, V sono due prodotti ammissibili. Per l'associatività (su tre termini) ho $P = ST = S(UV) = (SU)V$. Ora V è un prodotto di un numero di a_i minore di t, dunque per l'induzione su t, il prodotto $(SU)V$ si scrive come un prodotto normato a sinistra.)

Esercizio 3.7 (Facoltativo, magari lo espando). Il numero di modi per mettere le parentesi in un prodotto di $a_1, \dots, a_n$ è dato dal *numero di Catalan* C_{n-1}. Per questo al momento vi rimando alla Wikipedia

Esercizio 3.8. Sia $a_k a_{k-1} \cdots a_1 a_0$ un numero scritto in forma decimale. Si mostri che se $n = 9$ o $n = 3$, si ha per le classi di congruenza

$$[a_k a_{k-1} \cdots a_1 a_0] = [a_k + a_{k-1} + \cdots + a_1 + a_0].$$

Come caso particolare, si dica quando il numero fatto di tutti uni $11 \cdots 1$ è divisibile per 3.

Esercizio 3.9. Si enuncino e dimostrino i criteri di divisibilità per n, ove

$$n \in \{\, 2, 5, 3, 7, 9, 11 \,\}.$$

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

(Suggerimento: Quello per 3 non l'abbiamo fatto, ma è simile a quello per 9.)

Esercizio 3.10. 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 $n \in \{\, 2, 3, 7, 9, 11 \,\}$ 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 3.11 (Facoltativo). Si consideri la seguente procedura. Parto da un numero scritto in forma decimale

$$a_n \dots a_1 a_0 = a_0 + a_1 \cdot 10 + \cdots + a_n \cdot 10^n.$$

Ad esempio

$$2018 = 8 + 1 \cdot 10 + 0 \cdot 10^2 + 2 \cdot 10^3.$$

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.

  (SUGGERIMENTO: Per questo è sufficiente mostrare che se $n > 1$, e $a_n \neq 0$, allora $a_n \dots a_1 a_0 > a_n \cdot (a_{n-1} \dots a_1 a_0)$. Ad esempio $382 > 3 \cdot 82$. Per questo, notate che $a_{n-1} \dots a_1 a_0 < 10^n$.)
- Trovare tutti i numeri tali che applicando la procedura arrivo alla cifra 1. Naturalmente fra questi ci sono i numeri $111 \dots 111$. Si tratta di mostrare che sono gli unici.

Esercizio 3.12. Sia $n \geq 2$. Sia $a \in \mathbf{Z}$. Si mostri che per la classe $[a] \in \mathbf{Z}/n\mathbf{Z}$ si ha

$$[a] \text{ è } \begin{cases} \text{invertibile} & \text{se e e solo se } \gcd(a, n) = 1, \\ \text{uno 0-divisore} & \text{se e solo se } \gcd(a, n) > 1. \end{cases}$$

Esercizio 3.13. Si consideri $n = 12827$, e le classi $[a] = [4064], [4085] \in \mathbf{Z}/n\mathbf{Z}$. Per ognuna di esse, si dica se è invertibile (esibendo in tal caso come "prova" l'inverso) o se è un divisore dello zero (esibendo in tal caso come "prova" un elemento $[b] \neq [0]$ tale che $[a][b] = [0]$).

Attenzione! Per trovare le "prove", è obbligatorio usare l'algoritmo di Euclide.

Esercizio 3.14. Si trovino gli inversi di tutti gli elementi diversi da zero di $\mathbf{Z}/19\mathbf{Z}$.

Qui non è richiesto di usare l'algoritmo di Euclide, ma bisogna giustificare le risposte. Risposte valide sono ad esempio le seguenti.

- Dato che $2 \cdot 10 = 20$, si ha $[2] \cdot [10] = [1]$, dunque l'inverso di $[2]$ è $[10]$.
- Dato che $[10] \cdot [2] = [1]$, l'inverso di $[10]$ è $[2]$.
- Dato che $[-2] \cdot [-10] = [1]$, l'inverso di $[-2] = [17]$ è $[-10] = [9]$.
- Dato che $[1] = [2] \cdot [10] = [2] \cdot [2] \cdot [5]$, l'inverso di $[4]$ è $\dots$, e l'inverso di $[5]$ è $\dots$

Esercizio 3.15. Si dica quali elementi di $\mathbf{Z}/35\mathbf{Z}$ sono invertibili e quali sono divisori dello zero, indicando per ognuno una "prova", nel senso dell'Esercizio 3.13.

Qui basta dare le risposte.

Esercizio 3.16. Sia $A \neq \{ 0 \}$ un anello *commutativo*. Si mostri che sono equivalenti

- in A vale la legge di annullamento del prodotto, e
- l'unico 0-divisore in A è 0.

Un anello commutativo con unità in cui valga uno o l'altra di queste proprietà si dice un *dominio*.

Esercizio 3.17. Sia A un anello con unità. Si mostri che sono equivalenti

- $A = \{ 0 \}$, e
- $0 = 1$.

Esercizio 3.18. Sia $n \geq 2$. Si mostri che

- se n è primo, allora $\mathbf{Z}/n\mathbf{Z}$ è un campo,
- se n non è primo, allora $\mathbf{Z}/n\mathbf{Z}$ non è un dominio.

(SUGGERIMENTO: Questo non l'ho fatto (tutto) a lezione, ma l'idea è che se n non è primo, allora si può scrivere $n = ab$, con $1 < a < n$, e $1 < a < n$. In particolare, $[a] \neq [0] \neq [b]$. D'altra parte $[0] = [n] = [ab] = [a][\cdot[b].)$

Esercizio 3.19. Questo esercizio a volte crea qualche confusione, per cui tanto vale premettere due casi particolari. Se $n = 5$, si ha

$$\mathbf{Z}/5\mathbf{Z} = \{\, [0], [1], [2], [3], [4] \,\},$$

ma anche

$$\mathbf{Z}/5\mathbf{Z} = \{\, [-2], [-1], [0], [1], [2] \,\},$$

dato che $[4] = [-1]$ e $[3] = [-2]$. Invece se $n = 6$, si ha

$$\mathbf{Z}/6\mathbf{Z} = \{\, [0], [1], [2], [3], [4], [5] \,\},$$

ma anche

$$\mathbf{Z}/6\mathbf{Z} = \{\, [-2], [-1], [0], [1], [2], [3] = [-3] \,\},$$

dato che ecc. ecc. L'esercizio che segue non fa altro che generalizzare queste osservazioni.

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

Si mostri che esse sono

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

se n è pari, e

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

se n è dispari.

Importante! 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.