ESERCIZI STRUTTURE ALGEBRICHE

1. Sia $m \in N$. Definiamo l'insieme $E_m = \left\{ n \in N \mid 1 \le n < m, \quad MCD(n,m) = 1 \right\}$ formato dai numeri naturali minori di *m* primi con *m*. Dimostrare che l'insieme $Z_{12}^* = \left\{ [n] \in Z_{12} \mid n \in E_m \right\}$ è un gruppo rispetto all'operazione di moltiplicazione tra classi di resto in Z_{12}.
2. Risolvere la seguente equazione: $[18x] = [16] \bmod 40$.
3. Si stabilisca se $3^{155} + 2$ è divisibile per 7.
4. Si spieghi perché l'insieme Z_n munito dell'operazione di moltiplicazione tra classi di resto, non può essere un gruppo se *n* è un numero naturale composto. Quale struttura algebrica origina? Cosa possiamo dire, in tal senso, di $Z_n - [0]$?
5. Il numero di elementi dell'insieme $E_m = \left\{ n \in N \mid 1 \le n < m, \quad MCD(n,m) = 1 \right\}$, al variare di $m \in N$ dà origine alla funzione nota come "$\varphi(m)$ di Eulero". Si dimostri che dal *Teorema di Eulero*: "se $a < m$ e $MCD(a,m) = 1$, allora $a^{\varphi(m)} \equiv 1 \bmod m$" è possibile dedurre come corollario il celebre *Teorema di Fermat:* "se $a < p$, *p* primo e $MCD(a,p) = 1$, allora $a^{p-1} \equiv 1 \bmod p$.
6. Un numero è divisibile per tre se la somma delle cifre è un multiplo di tre. Giustificare quest'affermazione.
7. (Problema 25 libro di testo). Un marziano, dopo aver visto scritta l'equazione $x^2 - 16x + 41 = 0$, invitato a scrivere la differenza delle radici, scrive 10. Sapendo che i numeri tra 0 e 6 coincidono con quelli in base 10, si dica quante dita ha il marziano.
8. Si attribuisca un significato alla frazione $\frac{1}{4} \bmod(7)$.
9. Si attribuisca un significato alla frazione $\frac{1}{4} \bmod(6)$.
10. Dimostrare che per ogni $n > 0$ il numero $5^n + 2 \cdot 3^{(n-1)} + 1$ è divisibile per 8.
11. Dire a quale classe di resto modulo 5 appartiene il numero $1 + 2 + 2^2 + ... + 2^{19}$.
12. (Problema 34 libro di testo) E' dato un cesto di uova; si sa che se si tolgono a due a due resta un uovo, se si tolgono a tre a tre ne restano due, mentre se si tolgono a quattro a quattro ne restano tre. Dire qual è il numero minimo di uova nel cesto.
13. Dimostrare che in Z_p con *p* primo vale l'uguaglianza $(x+y)^p = x^p + y^p$.
14. (Problema 74 libro di testo). Due cercatori d'oro hanno due grandi sacchi di pezzi d'oro. Il primo ha solo pezzi da 15 grammi, il secondo solo pezzi da 21 grammi. Può il primo pagare al secondo un debito di 27 grammi d'oro? Potrebbe il secondo pagare al primo un debito di 29 grammi d'oro?

Soluzioni

1. Dalla definizione risulta $E_{12} = \{1,5,7,11\}$. Se associamo agli elementi di E_{12} le rispettive classi di resto in Z_{12}, otteniamo l'insieme che, munito dell'operazione di prodotto in Z_n, vogliamo verificare essere un gruppo: $Z_{12}^* = \{[1],[5],[7],[11]\}$. Per questo scopo è sufficiente costruire la tavola della moltiplicazione:

Z_{12}^*	1	5	7	11
1	1	5	7	11
5	5	1	11	7

7	7	11	1	5
11	11	7	5	1

- Osserviamo che l'insieme è chiuso rispetto all'operazione di moltiplicazione, che questa è associativa, che esiste l'elemento neutro ($[1]$), e che ogni elemento è inverso di se stesso.

2. $40 \mid (18x-16) \Rightarrow 18x-16 = 40y \Rightarrow 9x-20y = 8$. Le soluzioni dell'equazione omogenea sono $\begin{cases} x_0 = 20n \\ y_0 = 9n \end{cases}$, una soluzione particolare è data da $\begin{cases} x' = 9 \cdot 8 = 72 \\ y' = 4 \cdot 8 = 32 \end{cases}$ per cui $x = 20n + 72 = 20n + 32$.

3. Risulta $MCD(3,7) = 1$, 7 è un numero primo, quindi si può applicare il teorema di Fermat: $3^6 \equiv 1 \bmod 7$. Ora, $155 = 25 \cdot 6 + 5 \Rightarrow [3^{155}] = [3^{25 \cdot 6} \cdot 3^5] = [3^5] = [5]$. Allora $[3^{155} + 2] = [5] + [2] = [0]$. Il numero $3^{155} + 2$ è quindi divisibile per 7.

4. Nell'insieme Z_n munito dell'operazione di moltiplicazione tra classi di resto, ad esempio in Z_6 esiste un elemento, $[2]$, che non ha inverso rispetto alla suddetta operazione. Ciò è sufficiente per affermare che Z_6 è un *monoide associativo*, ma non un gruppo. In generale questo accade in Z_n se *n* è composto e si considera la classe di resto di un divisore primo di *n*. Per quanto riguarda $Z_n - [0]$, in base a quanto appena affermato possiamo concludere che *non* risulta chiuso rispetto alla moltiplicazione, quindi non è neppure una struttura algebrica.

5. La chiave per la soluzione del problema è rappresentata dal fatto che, se *m* è un numero primo *p*, allora *tutti* gli interi minori di *p* sono primi con *p*. Poiché tali interi sono, ovviamente, in numero di $\varphi(p) = p - 1$, allora $a^{\varphi(m)} \equiv 1 \bmod m$ è proprio la tesi del teorema.

6. Si osserva che $10 \equiv 1 \bmod 3 \Rightarrow [10] = [1] \Rightarrow [10^n] = [10]^n = [1]^n = [1]$, di conseguenza un qualsiasi numero intero $z = a_n a_{n-1} ... a_0 = a_n 10^n + a_{n-1} 10^{n-1} + ... + a_0$, è tale che $[z] = [a_n + a_{n-1} + ... a_0]$, come volevasi dimostrare.

7. Indicato con *n* il numero di dita del marziano (si suppone che abbia due mani, ognuna con lo stesso numero di dita), ragionando come faremmo in base dieci scriviamo: $16 = 1 \cdot n^1 + 6 \cdot n^0$; $41 = 4 \cdot n^1 + 1 \cdot n^0$; $10 = 1 \cdot n + 0 \cdot n^0$. In questo modo i coefficienti dell'equazione di secondo grado sono $a = 1 = 1 \cdot n^0$; $b = -16 = -(n+6)$; $c = 41 = (4n+1)$, e la differenza delle radici, espressa dalla condizione $x_2 - x_1 = \frac{\sqrt{\Delta}}{a} \Rightarrow 10 = n = \frac{\sqrt{(n+6)^2 - 4(4n+1)}}{1} \Rightarrow n = 8$.

8. Si tratta di trovare il "reciproco di 4 modulo 7", ovvero la classe di resto che, moltiplicata per la classe di 4, dà come risultato la classe di 1: si tratta della classe di resto modulo 2: $\frac{1}{4} \bmod(7) = [2]_7$. Infatti $[2]_7 \cdot [4]_7 = [8]_7 = [1]_7$.

9. Stavolta non è possibile attribuire un significato alla frazione. Infatti, se moltiplichiamo 4 per ognuno dei numeri da 1 a 5, non otteniamo mai un numero che, diviso per 6, dà come resto uno.
10. Dall'osservazione delle successive potenze di 5 possiamo concludere che $5^n \in [5]_8$ se n è dispari, oppure che $5^n \in [1]_8$ se n è pari. Ora, sempre per n pari, $3^{(n-1)} \in [3]_8$ e per n dispari $3^{(n-1)} \in [1]_8$. Ricapitolando, $5^n + 2 \cdot 3^{(n-1)} + 1 \in [1] + 2[3] + [1] = [0]$ se n è pari, e $5^n + 2 \cdot 3^{(n-1)} + 1 \in [5] + 2[1] + [1] = [0]$ se n è dispari. In ogni caso giungiamo al risultato cercato.
11. Osserviamo che le classi di resto a cui appartengono le potenze di 2 che costituiscono i singoli addendi si ripetono con questa periodicità:

    $1 \in [1] \quad 2 \in [2] \quad 4 \in [4] \quad 8 \in [3] \quad 16 \in [1] \quad 32 \in [2] \quad 64 \in [4] \quad 128 \in [3]$. La periodicità è giustificata dalle proprietà aggiuntive. Quindi la somma fino all'addendo 2^{19} avviene contando $[1] + [2] + [4] + [3] = [1 + 2 + 4 + 3] = [10] = [0]$ esattamente 5 volte. La somma è quindi divisibile per 5, quindi appartiene alla classe di resto 0.

12. Il numero minimo di uova N appartiene alla classe di resto 1 modulo due, a quella 2 modulo tre, e a quella 3 modulo quattro:

    $N \in [1]_2 \Rightarrow N = 2m + 1; \quad N \in [2]_3 \Rightarrow N = 3n + 2; \quad N \in [3]_4 \Rightarrow N = 4k + 3$. I numeri di uova possibili si ottengono risolvendo le equazioni diofantee (a soluzioni intere!) che si ottengono uguagliando le espressioni sopra: $\begin{cases} 2m - 3n = 1 \\ 2m - 4k = 2 \Rightarrow m - 2k = 1 \end{cases}$. Dalla prima equazione segue, ad esempio, $m = 5$ e $n = 3$. Sostituendo nella seconda equazione otteniamo $k = 2$. Per questi valori risulta $N = 11$.
13. Per il teorema di Fermat risulta $x^p \equiv x \bmod(p)$ e $y^p \equiv y \bmod(p)$. Di conseguenza $\left(x^p + y^p\right) \equiv (x + y) \bmod(p)$ e, poiché, sempre per il teorema di Fermat, $(x + y)^p \equiv (x + y) \bmod(p)$, la tesi segue per la proprietà transitiva.

14. Nella transazione (con resto) indicati con x e con y il numero di pezzi rispettivamente da 15 e da 21 grammi, per rispondere alla domanda occorre risolvere l'equazione diofantea $15x - 21y = 27 \Rightarrow 5x - 7y = 9$. Le soluzioni sono $x = 3$ e $y = 2$. Nel secondo caso, poiché $MCD(15,21) = 3$ non divide 29, l'equazione risolvente $21y - 15x = 29$ non ha soluzioni intere; il pagamento non può quindi avvenire.