A.A. 2015-2016. CORSO DI ALGEBRA 1.
PROFF. P. PIAZZA, E. SPINELLI.
ESERCITAZIONI. FOGLIO 4.

Esercizio 4.1. Data una coppia $a, b \in \mathbb{N}^*$, consideriamo la loro fattorizzazione in primi. Esprimere in termini di $\mathrm{MCD}(a,b)$ e $a \cdot b$ il prodotto dei fattori non comuni nelle fattorizzazioni di a e b. Determinare eventuali coppie $(a,b) \in \mathbb{N}^* \times \mathbb{N}^*$ tali che:

$$\mathrm{MCD}(a,b) = 77\,,\ a \cdot b = 847\,; \quad \mathrm{MCD}(a,b) = 21\,,\ a \cdot b = 9261$$
$$\mathrm{MCD}(a,b) = 70\,,\ a \cdot b = 9800\,; \quad \mathrm{MCD}(a,b) = 75\,,\ a \cdot b = 2025$$

Esercizio 4. 2. Siano dati due numeri primi distinti p e q. Utilizzando l'esercizio precedente determinare al variare di $(i,j) \in \mathbb{N}^* \times \mathbb{N}^*$ il numero di coppie $(a,b) \in \mathbb{N}^* \times \mathbb{N}^*$ tali che: $\mathrm{MCD}(a,b) = p \cdot q$ e $a \cdot b = p^i \cdot q^j$.

Esercizio 4.3. Denotiamo con $\mathbb{Z}_n$ il gruppo $\mathbb{Z}/n\mathbb{Z}$ e con $\mathcal{U}(\mathbb{Z}_n)$ l'insieme degli elementi invertibili.
(A) Determinare $\mathcal{U}(\mathbb{Z}_{24})$.
(B) Dire se esistono elementi che sono inversi di se stessi. In caso affermativo determinare l'insieme di tali elementi.
(C) Verificare che il sottoinsieme degli elementi di $\mathcal{U}(\mathbb{Z}_n)$ il cui quadrato è congruo ad 1 modulo n è chiuso rispetto al prodotto.
(D) Siano ora $R_{yz} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ e $R_{xy} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Verificare che hanno entrambe ordine[1] 2 ma che il loro prodotto non ha tale ordine. Quale argomento utilizzato nel punto precedente non può essere applicato in questa nuova situazione?

Esercizio 4.4. Siano dati $a, n \in \mathbb{Z}$. Mostrare che vale una delle due condizioni:

- $\exists b \neq 0$ tale che $a \cdot b \equiv 1 \ (mod\, n)$
- $\exists b \neq 0$ tale che $a \cdot b \equiv 0 \ (mod\, n)$

Verificare con un esempio che se $a \cdot b \equiv a \cdot c \ (mod\, n)$ (con a, b, c non nulli) non necessariamente risulta $b \equiv c \ (mod\, n)$. [*Suggerimento. (A) Trovare una condizione necessaria e sufficiente affinché l'applicazione data da $\mathbb{Z}_n \to \mathbb{Z}_n$, $b \to a \cdot b$ sia biettiva. (B) Ricordare che un'applicazione tra due insiemi finiti della stessa cardinalità è biettiva sse iniettiva sse suriettiva*]

Ricordiamo che un elemento $a \neq 0_A$ di un anello (associativo) unitario $(A, +, \cdot)$ è detto *nilpotente* se $a^n = 0_A$ per un'opportuna potenza $n \in \mathbb{N} \setminus \{0\}$.

Esercizio 4.5. Sia $n = p_1^{h_1} \cdots p_m^{h_m}$ con $p_i \neq p_j$ per $i \neq j$ la fattorizzazione in primi di n.
(A) Sia $a \in \mathbb{Z}$ tale che $0 \leq a < n$; $\overline{a} \in \mathbb{Z}_n$ è nilpotente se e soltanto se $a = m \cdot p_1^{k_1} \cdots p_m^{k_m}$ e $1 \leq k_i \leq h_i$ (dove $m \in \mathbb{N}$). [*Suggerimento. Utilizzare il Lemma di Euclide.*]
(B) Determinare i nilpotenti di $\mathbb{Z}_{150}$.
(C) Dimostrare che $\mathbb{Z}_n$ contiene nilpotenti se e solo se $h_i > 1$ per almeno un indice i.

[1] Dato un gruppo G e un elemento $a \in G \setminus \{1_G\}$ l'ordine dell'elemento a è definito come il più piccolo intero positivo k tale che $a^k = 1_G$.

ESERCIZI PER CASA

Digressione. Un'equazione congruenziale lineare è un'equazione del tipo $a\,X \equiv b\ (mod\, n)$. Una soluzione è un intero x tale che $ax = b + k\,n$, per un qualche $k \in \mathbb{Z}$. Utilizzando quanto visto negli esercizi precedenti è possibile osservare che non tutte le equazioni congruenziali ammettono soluzione: utilizzando gli esercizi 4.3 e 4.4 è facile accorgersi che l'equazione congruenziale lineare $2\,X \equiv 1\ (mod\, 24)$ non ammette soluzione (infatti una soluzione di tale equazione determinerebbe un inverso moltiplicativo -naturalmente $(mod\, 24)$- dell'elemento 2 in $\mathbb{Z}_{24}$). Come vedrete (o avete visto) durante il corso, condizione necessaria e sufficiente affinché tale equazione ammetta soluzione è che $\mathrm{MCD}(a, n) \mid b$. Non è difficile osservare (Cap. 2, Sezione 5, Proposizione 3 di *Appunti di Algebra 1*, G. Campanella) che x è una soluzione dell'equazione congruenziale lineare $a\,X \equiv b\ (mod\, n)$, se e solo se $x + j\,\frac{n}{\mathrm{MCD}(a,n)}$ è soluzione per ogni $j \in \mathbb{Z}$.

Esercizio 4. 6. Siano $a, b, n \in \mathbb{N}$. Sia $d = \mathrm{MCD}(a, n)$. Dimostrare che l'insieme delle soluzioni di $a\,X \equiv b\,(mod\, n)$ coincide con l'insieme delle soluzioni di $\frac{a}{d}\,X \equiv \frac{b}{d}\,(mod\,\frac{n}{d})$.

Esercizio 4.7. Determinare l'insieme delle soluzioni delle seguenti equazioni congruenziali lineari.

$$\bullet\ 10X \equiv 2\,(mod\, 12); \quad \bullet 121X \equiv 3\,(mod\, 13)\,; \quad \bullet\ 15 \equiv 5\,(mod\, 81)$$
$$\bullet\ 96X \equiv 14\,(mod\, 16)\,; \quad \bullet\ 117\,X \equiv 72\,(mod\, 13)$$

Piccolo Teorema di Fermat (Seconda formulazione)**.** *Siano $a, p \in \mathbb{Z}$ tali che* $\mathrm{MCD}(a, p) = 1$*; se p è primo allora*

$$a^{p-1} \equiv 1\,(mod\, p)$$

Esercizio 4.8. Dato che $2 \cdot 3^{n-1} \equiv 2\,(mod\, n)$ dimostrare che n è primo o alternativamente fornire un controesempio.