A.A. 2015-2016. CORSO DI ALGEBRA 1.
PROFF. P. PIAZZA, E. SPINELLI.
SOLUZIONE ESERCIZI 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:

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

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

Soluzione. Sia $M = \mathrm{MCD}(a,b)$ allora $a = \alpha \cdot M$ e $b = \beta \cdot M$. Vogliamo scrivere il prodotto $\alpha \cdot \beta$ in termini di $a \cdot b$ e $\mathrm{MCD}(a,b)$:

$$\alpha \cdot \beta = \frac{a \cdot b}{M^2} = \frac{a \cdot b}{\mathrm{MCD}(a,b)^2}$$

Individuata la relazione che sussiste tra il prodotto dei fattori non comuni e le quantità $a \cdot b$ e $\mathrm{MCD}(a,b)$, osserviamo che essa ci fornisce un rapido test per verificare se una coppia di naturali $(k_1, k_2) \in \mathbb{N}^* \times \mathbb{N}^*$ può essere l'MCD e il prodotto di una coppia di numeri $(a,b) \in \mathbb{N}^* \times \mathbb{N}^*$: $k_2/(k_1)^2$ deve infatti essere un numero naturale.

$\mathrm{MCD}(a,b) = 77$, $a \cdot b = 847$; cominciamo sfruttando quanto appreso nella prima parte: è facile vedere che $847/77^2$ non è un numero naturale, pertanto non può esistere alcuna coppia $(a,b) \in \mathbb{N}^* \times \mathbb{N}^*$ tale che $\mathrm{MCD}(a,b) = 77$ e $a \cdot b = 847$. Si può anche procedere in modo meno brutale utilizzando la scomposizione in fattori primi dei due numeri: $77 = 7 \cdot 11$ mentre $847 = 7 \cdot 11^2$; la fattorizzazione in primi del prodotto di a e b deve contenere il quadrato della fattorizzazione in primi del MCD, ne deduciamo che una tale coppia di numeri naturali (a,b) non può esistere.

$\mathrm{MCD}(a,b) = 21$, $a \cdot b = 9261$; sfruttiamo il test di compatibilità dimostrato nella prima parte: $9261/21^2 = 21$, è quindi possibile trovare coppie che realizzino le due condizioni sul MCD e sul prodotto. Fattorizziamo in primi: abbiamo che $\mathrm{MCD}(a,b) = 7 \cdot 21$, $a \cdot b = 3^3 \cdot 7^3$ e, utilizzando la notazione precedentemente introdotta, $\alpha \cdot \beta = 3 \cdot 7$. Per trovare le coppie $(a,b) \in \mathbb{N}^* \times \mathbb{N}^*$ che risolvono il problema ci basta "redistribuire" il prodotto dei fattori non comuni in modo tale da mantenere fissato il Massimo Comun Divisore: abbiamo dunque 4 possibilità: $(7^2 \cdot 3, 7 \cdot 3^2)$, $(7 \cdot 3^2, 7^2 \cdot 3)$, $(7 \cdot 3, 7^2 \cdot 3^2)$ e $(7^2 \cdot 3^2, 7 \cdot 3)$.

$\mathrm{MCD}(a,b) = 70$, $a \cdot b = 9800$; calcoliamo $\frac{a \cdot b}{\mathrm{MCD}(a,b)^2}$: $\frac{9800}{70^2} = 2$, possiamo quindi trovare delle coppie $(a,b) \in \mathbb{N}^*$ che realizzano i valori scelti per il Massimo Comun Divisore e per il prodotto. Ragionando in analogia con il caso precedente ci accorgiamo che vi sono due coppie possibili: $(70, 140)$ e $(140, 70)$.

$\mathrm{MCD}(a,b) = 75$, $a \cdot b = 2025$. Utilizziamo il test di compatibilità per le due condizioni: $\frac{a \cdot b}{\mathrm{MCD}(a,b)^2} = \frac{2025}{75^2} = \frac{9}{25}$. Il numero così trovato non è un naturale, quindi non possono esistere coppie $(a,b) \in \mathbb{N}^* \times \mathbb{N}^*$ compatibili. □

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 $a \cdot b = p^i \cdot q^j$.

Soluzione. In questo esercizio si chiede di formalizzare in astratto quanto fatto nell'esercizio precedente. Si chiede di determinare al variare delle coppie $(i,j) \in \mathbb{N}^* \times \mathbb{N}^*$ il numero di coppie (ordinate)

$(a,b) \in \mathbb{N}^* \times \mathbb{N}^*$ che realizzano $\mathrm{MCD}(a,b) = p \cdot q$ e $a \cdot b = p^i \cdot q^j$, dove p e q sono due numeri primi distinti.

La prima osservazione è che, per via della condizione di compatibilità dimostrata nell'esercizio 4.1, il rapporto $\frac{a \cdot b}{\mathrm{MCD}(a,b)^2} = \frac{p^i \cdot q^j}{p^2 \cdot q^2}$ deve essere un numero intero. Questo implica che il numero di coppie che realizzano $\mathrm{MCD}(a,b) = p \cdot q$ e $a \cdot b = p^i \cdot q^j$ è zero per le coppie $(i,j) \in \{(1,1),(1,2),(2,1)\}$. Supponiamo quindi che si abbia $i, j \geq 2$. Cominciamo con tre casi semplici.

$i = j = 2$. Sappiamo che $a = \alpha \cdot \mathrm{MCD}(a,b)$ e che $b = \beta \cdot \mathrm{MCD}(a,b)$. Dobbiamo quindi avere $p^2 \cdot q^2 = a \cdot b = \alpha \cdot \beta \cdot (p \cdot q)^2$. Questo implica $\alpha = \beta = 1$ e dunque per $i = j = 2$ vi è un'unica coppia $(a,b) \in \mathbb{N}^* \times \mathbb{N}^*$ che realizza le condizioni imposte, ovvero $a = p \cdot q$ e $b = p \cdot q$.

$i = 2$, $j = 3$. In tal caso si verifica facilmente che il prodotto dei fattori non comuni $\alpha \cdot \beta$ è proprio uguale a q. Abbiamo quindi $p^2\, q^3 = a \cdot b = q \cdot (p\, q)^2$. Le soluzioni $(a,b) \in \mathbb{N}^* \times \mathbb{N}^*$ sono quindi $(p\, q^2, p\, q)$ e $(p\, q, p\, q^2)$.

$i = 3$, $j = 2$. In analogia con il caso precedente si fa vedere che le soluzioni sono $(p\, q, p^2\, q)$ e $(p^2\, q, p\, q)$.

$i = 3$, $j = 3$. In questo caso il prodotto dei fattori non comuni $\alpha \cdot \beta = \frac{a \cdot b}{\mathrm{MCD}(a,b)^2} = \frac{p^3\, q^3}{p^2\, q^2} = p\, q$. Tale prodotto può essere redistribuito senza restrizioni; le soluzioni sono quindi $(p\, q, p^2\, q^2)$, $(p^2\, q^2, p\, q)$, $(p^2\, q, p\, q^2)$, $(p\, q^2, p^2\, q)$.

Affrontiamo ora il caso generale. Poiché il prodotto di a e b si fattorizza come potenze di p e q e poiché sia in a che in b devono apparire sia p che q almeno con potenza 1, il problema si riduce a trovare tutte le coppie di prodotti $p^{i_1} q^{j_1}, p^{i_2} q^{j_2}$ con $i_1 + i_2 = i$, $j_1 + j_2 = j$ e $\min\{i_1, i_2\} = \min\{j_1, j_2\} = 1$. Ne segue che, non appena $i \geq 3$ e $j \geq 3$, il numero di coppie compatibili con le condizioni $a \cdot b = p^i q^j$, $\mathrm{MCD}(a,b) = p \cdot q$ è sempre uguale a 4 e le coppie sono $(p^{i-1}\, q^{j-1}, p\, q)$, $(p\, q, p^{i-1}\, q^{j-1})$, $(p^{i-1} q, p q^{j-1})$, $(p\, q^{j-1}, p^{i-1}\, q)$. □

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?

Soluzione. Ricordiamo che per trovare gli invertibili di $\mathcal{U}(\mathbb{Z}_n)$ è sufficiente trovare tutti i numeri $1 \leq x \leq n-1$ che sono coprimi con n e poi considerare le loro classi modulo n.

Tenendo a mente il fatto precedente cominciamo fattorizzando 24 come prodotto di primi: $24 = 2^3 \cdot 3$. Dobbiamo quindi trovare tutti i numeri tra 1 e 23 che non hanno fattori in comune con 24 (quindi numeri la cui fattorizzazione in primi non contenga né 2 né 3). La lista completa degli elementi di $\mathcal{U}(\mathbb{Z}_{24})$ è quindi la seguente: $\mathcal{U}(\mathbb{Z}_{24}) = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}\}$. Questo risolve il punto (A) dell'esercizio.

[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 $a^k = 1_G$.

Nel punto (B) veniva chiesto di individuare eventuali elementi di $\mathcal{U}(\mathbb{Z}_{24})$ che fossero inversi di sé stessi, ovvero elementi di $\mathcal{U}(\mathbb{Z}_{24})$ il cui quadrato fosse uguale ad $\overline{1}$, l'unità del gruppo moltiplicativo degli invertibili di $\mathbb{Z}_{24}$. A tale scopo è sufficiente prendere dei rappresentanti delle classi modulo 24 (ad esempio scegliamo i rappresentanti $1, 5, 7, 11, 13, 17, 19, 23$) farne i quadrati e vedere se qualcuno di essi è congruo ad 1 modulo 24. Ovviamente 1 è congruo ad 1 modulo 24; $5^2 = 25 = 1 + 24$ dunque è congruo ad 1 modulo 24; $7^2 = 49 = 1 + 48 = 1 + 2 \cdot 24$ e dunque anche $\overline{7}^2 = \overline{1}$ in $\mathcal{U}(\mathbb{Z}_{24})$. Stessa cosa si verifica per tutti gli altri rappresentanti scelti. Ne segue che $\mathcal{U}(\mathbb{Z}_{24})$ è composto esclusivamente da elementi il cui quadrato è uguale a $\overline{1}$.

Nel punto (C) si torna a considerare il caso generale $\mathbb{Z}_n$. Viene chiesto di dimostrare che il sottoinsieme degli elementi di $\mathcal{U}(\mathbb{Z}_n)$ il cui quadrato è uguale ad $\overline{1}$ è un sottoinsieme chiuso rispetto al prodotto. Per dimostrare questo fatto il modo più semplice è osservare che il gruppo $\mathcal{U}(\mathbb{Z}_n)$ è commutativo. Siano quindi $\overline{a}, \overline{b}$ due elementi di $\mathcal{U}(\mathbb{Z}_n)$ tali che $\overline{a}^2 = \overline{b}^2 = \overline{1}$. Per commutatività del gruppo abbiamo che $(\overline{a}\,\overline{b})^2 = \overline{a}^2\,\overline{b}^2 = \overline{1}$, questo prova che il prodotto di due elementi di quadrato uguale ad $\overline{1}$ è ancora un elemento il cui quadrato è uguale a $\overline{1}$.

Il punto (D) dell'esercizio aveva invece lo scopo di farvi osservare che, dato un generico gruppo (ad esempio il gruppo $GL(3, \mathbb{R})$, delle matrici 3×3 invertibili) e presi due elementi di quadrato uguale all'identità del gruppo, il loro prodotto può non essere di quadrato uguale all'identità. A tale scopo è sufficiente osservare che $R_{yz}R_{xy} \neq R_{xy}R_{yz}$ e che la matrice

$$R_{yz} \cdot R_{xy} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

non è di quadrato uguale ad Id nonostante $R_{yz}^2 = \mathrm{Id}$ e $R_{xy}^2 = \mathrm{Id}$. □

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 biiettiva. (B) Ricordare che un'applicazione tra due insiemi finiti della stessa cardinalità è biiettiva sse iniettiva sse suriettiva*]

Soluzione. Per quanto riguarda la prima parte vi sono due modi di procedere. Il primo è sfruttando il Massimo Comun Divisore: sappiamo dalla teoria che un numero a è invertibile modulo n se e solo se $\mathrm{MCD}(a, n) = 1$. Supponiamo ora che a sia un numero non congruo a 0 modulo n e tuttavia non coprimo con n; sia dunque $1 < M = \mathrm{MCD}(a, n)$. In particolare $n = \alpha \cdot M$. Osserviamo che $0 < \alpha < n$, poiché $M > 1$, e dunque esso è un elemento che non è congruo a 0 modulo n. Ma allora abbiamo che $\alpha \cdot a \equiv 0 \ (mod\ n)$ con $\overline{\alpha}$ non banale in $\mathbb{Z}_n$. Il caso in cui a è congruo a 0 modulo n è banale. Abbiamo quindi dimostrato che, assegnato n, per ogni numero a vale una delle due alternative enunciate nel testo dell'esercizio.

La via alternativa per risolvere questo esercizio è la seguente: possiamo definire la seguente mappa:

$$\ell_{\overline{a}} : \mathbb{Z}_n \to \mathbb{Z}_n \ , \qquad \ell_{\overline{a}} : \overline{b} \mapsto \overline{a} \cdot \overline{b}$$

Osserviamo che tale applicazione è biiettiva se e solo se $\overline{a}$ è invertibile: supponiamo che $\overline{a}$ sia invertibile allora è possibile esplicitare un'inversa alla mappa $\ell_{\overline{a}}$ semplicemente prendendo $\ell_{\overline{a}^{-1}}$; viceversa supponiamo che $\ell_{\overline{a}}$ sia biiettiva. In particolare la mappa è suriettiva e dunque esiste $\overline{b} \in \mathbb{Z}_n$ tale che $\overline{a} \cdot \overline{b} = \overline{1}$, ne segue che $\overline{b}$ è l'inverso di $\overline{a}$ e che $\overline{a}$ è dunque invertibile.

Supponiamo quindi che la mappa non sia biiettiva. Poiché si parla di un'applicazione tra insiemi della stessa cardinalità ne segue che la mappa non è iniettiva. Siano quindi $\overline{b}_1$ e $\overline{b}_2$ due elementi distinti con

la stessa immagine tramite $\ell_{\overline{a}}$. Ne segue che l'elemento $\overline{b}_1 - \overline{b}_2 \neq \overline{0}$ viene inviato in $\overline{0}$ da $\ell_{\overline{a}}$. Ne segue che $\overline{a}$ deve essere un divisore dello zero. Questo conclude la seconda dimostrazione della prima parte dell'esercizio.

Nella seconda parte veniva chiesto di verificare con un esempio che $a \cdot b \equiv a \cdot c \ (mod\ n)$ non necessariamente implica $b \equiv c \ (mod\ n)$. Si osservi quindi che $6 \equiv 4 \ (mod\ 2)$ mentre $3 \not\equiv 2 \ (mod\ 2)$. □

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 $a = b \cdot p_1^{k_1} \cdots p_m^{k_m}$ e $1 \leq k_i \leq h_i$ (dove $b \in \mathbb{N}^*$).
(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.

Soluzione. 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 $n \in \mathbb{N} \setminus \{0\}$.

Partiamo dal punto (A). Sia $\overline{a} \in \mathbb{Z}_n$ un elemento nilpotente. Sia a un rappresentante tra 0 ed n di $\overline{a}$. $\overline{a}$ è nilpotente se e soltanto se esiste una potenza $k \in \mathbb{N}$ tale che $\overline{a}^k = \overline{0}$ se e soltanto se esiste una potenza $k \in \mathbb{N}$ tale che $a^k \equiv 0 \ (mod\, n)$ se e soltanto se esiste una potenza $k \in \mathbb{N}$ tale che $n \mid a^k$. Sia ora $q_1^{j_1} \cdots q_\ell^{j_\ell}$ la scomposizione in fattori primi di a. Per unicità della fattorizzazione in primi abbiamo che $\overline{a}$ è nilpotente se e solo se $q_1^{k\, j_1} \cdots q_\ell^{k\, j_\ell} = b \cdot p_1^{h_1} \cdots p_m^{h_m}$. Questo è possibile se e soltanto se nella scomposizione in fattori primi di a compare ogni p_i della scomposizione in fattori primi di n con potenza almeno 1. Questo conclude la dimostrazione del punto (A).

Nel punto (B) ci viene chiesto di determinare i nilpotenti di $\mathbb{Z}_{150}$. Lo faremo sfruttando quanto visto nel punto (A). Fattorizziamo: $150 = 2 \cdot 3 \cdot 5^2$. I nilpotenti di $\mathbb{Z}_{150}$ sono quindi gli elementi che ammettono i seguenti rappresentanti: $m \cdot 2 \cdot 3 \cdot 5$ dove $0 < m < 5$, sono quindi $\overline{30}$, $\overline{60}$, $\overline{90}$, $\overline{120}$.

Per risolvere il punto (C) osserviamo che se $h_i > 1$ per almeno un indice i allora il numero $p_1 \cdots p_n$ non è congruo a zero modulo n, ed esso è quindi un rappresentante per un elemento nilpotente in $\mathbb{Z}_n$. Viceversa supponiamo che $h_i = 1$ per ogni indice i. Se $\overline{a} \in \mathbb{Z}_n$ fosse un elemento nilpotente di $\mathbb{Z}_n$ e se $0 < a < n$ fosse un suo rappresentante dovremmo avere, per il punto (A), $a = m \cdot p_1 \cdots p_n$ con $m > 0$. Ma questo è incompatibile con l'ipotesi $a < n$. □

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 $d = \mathrm{MCD}(a, n)$. Assumiamo che $d \mid b$. Dimostrare che l'insieme delle soluzioni di $a\, X \equiv b \ (mod\, n)$ coincide con l'insieme delle soluzioni di $\frac{a}{d}\, X \equiv \frac{b}{d} \ (mod\, n)$.

Soluzione. Sia x_0 una soluzione della prima equazione. Questo significa che $a\, x_0 = b + k_0\, n$. Ora osserviamo che $a = \alpha \cdot d$, $b = m \cdot d$ e $n = \nu \cdot d$. Possiamo quindi dividere l'equazione precedente per d e ricavare la seguente: $\frac{a}{d}\, x_0 = \alpha\, x_0 = m + k_0 \cdot \nu = \frac{b}{d} + k_0 \cdot \frac{n}{d}$. Dunque x_0 è anche soluzione dell'equazione $\frac{a}{d}\, X \equiv \frac{b}{d} \ (mod\ \frac{n}{d})$. Viceversa sia x_0 tale che $\frac{a}{d}\, x_0 = \frac{b}{d} + k_0 \frac{n}{d}$ moltiplicando tutto per d osserviamo che x_0 risolve anche l'equazione $a\, X \equiv b \ (mod\ n)$. Ne segue che i rispettivi insiemi delle soluzioni

coincidono. □

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

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

Soluzione. Cominciamo dalla prima equazione. L'equazione è compatibile infatti $\mathrm{MCD}(12, 10) = 2 \mid 2$.

$$10\,X \equiv 2\ (mod\ 12)\ \Leftrightarrow 5\ X \equiv 1(mod\ 6)$$

Osserviamo che $25 \equiv 1\ (mod\ 6)$ e quindi

$$X \equiv 5\ (mod\ 6)$$

La generica soluzione è quindi $x_k = 5 + k\,6$.
Consideriamo ora l'equazione $121\,X \equiv 3\ (mod\ 13)$. Riduciamo 121 modulo 13: $121 - 13 \cdot 9 = 4$, quindi l'equazione precedente è equivalente a $4\,X \equiv 3\ (mod\ 13)$. Osserviamo che l'equazione è compatibile, infatti $\mathrm{MCD}(4, 13) = 1 \mid 3$. Notiamo che 10 è un inverso aritmetico modulo 13 di 4, quindi abbiamo:

$$4\,X \equiv 3\ (mod\ 13)\ \Leftrightarrow\ X \equiv 30\ (mod\ 13)\ \Leftrightarrow\ X \equiv 4\ (mod\ 13)$$

La soluzione generica della seconda equazione è pertanto $x_k = 4 + k \cdot 13$.
Verifichiamo la compatibilità della terza equazione: $\mathrm{MCD}(15, 81) = 3$ e $\mathrm{MCD}(15, 81) = 3 \not| 5$. Dunque l'equazione non è compatibile, ovvero non vi sono soluzioni all'equazione congruenziale in esame.
Verifichiamo la compatibilità della quarta equazione: $\mathrm{MCD}(96, 16) = 16$. $16 \not| 15$. Quindi l'equazione non è compatibile, ovvero non ammette soluzione.
Verifichiamo la compatibilità della quinta equazione: $\mathrm{MCD}(117, 13) = 13$. Anche in questo caso l'equazione congruenziale non ammette soluzioni infatti $13 \not| 72$. □

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

Soluzione. Innanzitutto ricordiamo l'enunciato del Piccolo Teorema di Fermat (seconda formulazione):

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

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

È possibile esibire un controesempio: si consideri $n = 4$; tale numero evidentemente non è primo e tuttavia verifica l'equazione precedente. □