A.A. 2015-2016. CORSO DI ALGEBRA 1.
PROFF. P. PIAZZA, E. SPINELLI.
SOLUZIONE ESERCIZI FOGLIO 5.

Esercizio 5.1. Determinare le ultime tre cifre di $n = 13^{1625}$. (*Suggerimento. Sfruttare il Teorema di Eulero-Fermat*)

Soluzione. Per trovare le ultime 3 cifre di n dobbiamo risolvere la seguente equazione congruenziale:

$$13^{1625} \equiv X \ (mod\ 1000)$$

Sfruttiamo il suggerimento; calcoliamo $\varphi(1000) = (5^3 - 5^2) \cdot (2^3 - 2^2) = 400$. Essendo $\mathrm{MCD}(13, 1000) = 1$, per il Teorema di Eulero-Fermat, risulta che $13^{400} \equiv 1 \ (mod\, 1000)$. Abbiamo quindi:

$$13^{1625} \equiv X \ (mod\ 1000) \ \Leftrightarrow \ 13^{400 \cdot 4 + 25} \equiv X \ (mod\ 1000) \ \Leftrightarrow \ 13^{25} \equiv X \ (mod\ 1000)$$

Dobbiamo calcolare 13^{25}. Scriviamo 25 come somma di potenze di 2, in modo da poter calcolare più facilmente 13^{25} modulo 1000. $25 = 2^4 + 2^3 + 1$; sappiamo che $13^2 = 169$, calcoliamoci quindi $(169)^8$ e $(169)^4$ modulo 1000: $169^2 \equiv 561 \ (mod\ 1000)$ e dunque $(169)^4 \equiv (561)^2 \equiv 721 \ (mod\ 1000)$ e quindi $169^8 \equiv (721)^2 \equiv 841 \ (mod\ 1000)$; abbiamo quindi:

$$13^{1625} \equiv 13^{400 \cdot 4 + 25} \equiv 13^{25} \equiv 13^{2^4} \cdot 13^{2^3} \cdot 13 \equiv 841 \cdot 721 \cdot 13 \equiv 693 \ (mod\ 1000)$$

Questo conclude la soluzione del primo esercizio. □

Esercizio 5.2. Risolvere il seguente sistema di equazioni congruenziali lineari:

$$\begin{cases} 13\,X \equiv 2 \pmod{21} \\ 9\,X \equiv 3 \pmod{10} \\ 23\,X \equiv 12 \pmod{43} \end{cases}$$

Risolvere lo stesso sistema sostituendo alla prima equazione la seguente:

$$7\,X \equiv 2 \pmod{21}$$

Soluzione. Verifichiamo la compatibilità di ogni equazione del sistema: $\mathrm{MCD}(13, 21) = 1 \mid 2$, $\mathrm{MCD}(9, 10) = 1 \mid 3$, $\mathrm{MCD}(23, 43) = 1 \mid 12$. Moltiplichiamo ciascuna delle equazioni congruenziali del sistema per l'inverso aritmetico del coefficiente della X. Per quanto riguarda le prime due equazioni: verificate che $13^2 \equiv 169 \equiv 1 (mod\ 21)$ e $9^2 \equiv 1 \ (mod\ 10)$. Più complesso è determinare l'inverso aritmetico di 23 modulo 43. Per far questo calcoliamo una identità di Bézout tra 43 e 23. Applichiamo l'algoritmo delle divisioni successive:

$$43 = 23 + 20$$
$$23 = 20 + 3$$
$$20 = 3 \cdot 9 + 2$$
$$3 = 2 + 1$$

Risolvendo per sostituzione a ritroso dalla prima all'ultima troviamo:

$$1 = 15 \cdot 23 - 8 \cdot 43$$

Dunque 15 è un inverso aritmetico modulo 43 di 23. Osserviamo ora che $15 \cdot 12 = 180 \equiv 8 \ (mod\ 43)$; il nostro sistema è quindi equivalente al sistema cinese:

$$\begin{cases} X \equiv 5 \pmod{21} \\ X \equiv 7 \pmod{10} \\ X \equiv 8 \pmod{43} \end{cases}$$

Sappiamo per il Teorema Cinese del resto che il sistema è compatibile ed ammette un'unica soluzione modulo 9030. Cerchiamo quindi tale soluzione. Lo faremo per sostituzione. Sappiamo che una

soluzione generica della prima equazione è $x_Y = 5 + 21\,Y$. Sostituiamo la soluzione generica nella seconda equazione e troviamo un'equazione congruenziale nella variabile Y:

$$5 + 21Y \equiv 7\ (mod\ 10) \ \Leftrightarrow\ Y \equiv 2\ (mod\ 10)$$

La soluzione generica di tale equazione è dunque $y_Z = 2 + 10\,Z$. Abbiamo quindi che $x_Z = 47 + 210\ Z$ risolve simultaneamente le prime due equazioni. Andiamo quindi a sostituire nella terza equazione del sistema:

$$47 + 210\,Z \equiv 8\ (mod\ 43) \ \Leftrightarrow\ 210\ Z \equiv 4\ (mod\ 43) \ \Leftrightarrow\ 38\,Z \equiv 4\ (mod\ 43)$$

Dobbiamo quindi determinare un'inverso aritmetico modulo 43 per 38. Procedendo come fatto in precedenza si può dimostrare che 17 è un inverso aritmetico modulo 43 di 38. La nostra equazione è quindi equivalente a $Z \equiv 4 \cdot 17 \equiv 25\ (mod\,43)$. La soluzione generica di tale equazione è dunque $z = 25 + k\,43$. Andando a sostituire abbiamo quindi che $x = 5297 + k\,9030$ è la soluzione del sistema di equazioni congruenziali lineari.

Consideriamo ora il nuovo sistema:

$$\begin{cases} 7\,X \equiv 2 \quad (mod\ 21) \\ 9\,X \equiv 3 \quad (mod\ 10) \\ 23\,X \equiv 12 \quad (mod\ 43) \end{cases}$$

È semplice accorgersi che tale sistema non è compatibile. Infatti la prima equazione è tale che $\mathrm{MCD}(7, 21) = 7 \not| 2$, quindi non è compatibile, inficiando così l'esistenza di una soluzione. □

Esercizio 5. 3. Stabilire per quali valori del parametro a il sistema è compatibile; per tali valori determinare la generica soluzione:

$$\begin{cases} 11\,X \equiv 4a \quad (mod\ 9) \\ 4\,X \equiv a \quad (mod\ 5) \\ 106\,X \equiv a + 1 \quad (mod\ 26) \end{cases}$$

Soluzione. Osserviamo che per quanto riguarda le prime due equazioni $\mathrm{MCD}(9, 11) = \mathrm{MCD}(5, 4) = 1$ e dunque sono entrambe compatibili. Poiché i moduli sono tutti coprimi (verificate!) per il Teorema Cinese del Resto (Seconda Formulazione), il sistema è equivalente ad un sistema cinese (e dunque ammette un'unica soluzione modulo il prodotto dei moduli del sistema cinese) se e soltanto se tutte le equazioni sono compatibili. Poiché abbiamo visto all'inizio che la compatibilità delle prime due equazioni non dipende dal parametro a è sufficiente determinare per quali valori di a la terza equazione è compatibile. Affinché ciò avvenga deve risultare $\mathrm{MCD}(106, 26) = 2 \mid a + 1$, pertanto la condizione da imporre sul parametro a affinché il sistema sia compatibile è $a = 2k + 1$ con $k \in \mathbb{Z}$.

Supponiamo quindi che $a = 2k+1$ con $k \in \mathbb{Z}$. La terza equazione del sistema è equivalente all'equazione $53\,X \equiv \frac{a+1}{2}\ (mod\ 13)$ che può essere espressa in funzione di k: $53\,X \equiv k + 1\ (mod\ 13)$. Quindi, esprimendo in funzione di k anche le prime due equazioni del sistema abbiamo:

$$\begin{cases} 11\,X \equiv 8k + 4 \quad (mod\ 9) \\ 4\,X \equiv 2k + 1 \quad (mod\ 5) \\ 53\,X \equiv k + 1 \quad (mod\ 13) \end{cases}$$

Osserviamo che $11 \equiv 2\ (mod\ 9)$ e $53 \equiv 1\ (mod\ 13)$. Calcoliamo gli inversi aritmetici di 4 modulo 5 e di 2 modulo 9. Il primo è 4 ($4^2 = 16 = 3 \cdot 5 + 1$) e il secondo è 5 ($10 = 1 \cdot 9 + 1$). Il nostro sistema è dunque equivalente al sistema cinese:

$$\begin{cases} X \equiv 4k + 2 \quad (mod\ 9) \\ X \equiv 3k + 4 \quad (mod\ 5) \\ X \equiv k + 1 \quad (mod\ 13) \end{cases}$$

A questo punto scriviamo la generica soluzione al variare di k. Scriviamo la soluzione generica della prima equazione: $x_Y = (4k + 2) + 9\,Y$ dove $Y \in \mathbb{Z}$. Sostituiamo la soluzione generica della prima equazione nella seconda: $(4k + 2) + 9\,Y \equiv 3k + 4\ (mod\ 5)$; tale equazione è equivalente alla seguente $4Y \equiv 4k + 2\,(mod\ 5)$ che è a sua volta equivalente a $Y \equiv k + 3\ (mod\ 5)$. La soluzione generica di tale equazione è $y_Z = (k + 3) + 5\,Z$. Dunque sostituendo ad Y in x_Y la soluzione generica troviamo $x_Z = [(4k+2)+9k+27]+45\,Z = (13k+29)+45\,Z$. Sostituiamo x_Z nell'ultima equazione: $(13k+29)+$

$45\,Z \equiv k+1\,(mod\ 13)$ questa è equivalente a $6\,Z \equiv k+11\ (mod\ 13)$ che a sua volta è equivalente a $Z \equiv 11k+4\ (mod\ 13)$. La soluzione generica dell'equazione è dunque $z_j = (11k+4)+13\,j$. Sostituiamo in x_Z e troviamo così la soluzione generica del sistema:

$$x_j = (508\,k + 209) + 585\,j$$

Questo conclude l'esercizio. □

Esercizio 5.4. Determinare le soluzioni $(mod\ 315)$ del seguente sistema:

$$\begin{cases} 14\,X \equiv 21 \pmod{63} \\ 3\,X \equiv 4 \pmod{5} \end{cases}$$

Soluzione. Verifichiamo la compatibilità del sistema: $\mathrm{MCD}(63,14) = 7 \mid 21$ e $\mathrm{MCD}(3,5) = 1 \mid 4$, inoltre $\mathrm{MCD}(63,5) = 1$ e dunque, per il Teorema Cinese del Resto nella sua seconda formulazione il sistema è compatibile; riduciamo quindi il sistema ad un sistema cinese; innanzitutto osserviamo che la prima equazione può essere ridotta a $2\,X \equiv 3\ (mod\ 9)$. Il sistema è dunque equivalente a

$$\begin{cases} 2\,X \equiv 3 \pmod{9} \\ 3\,X \equiv 4 \pmod{5} \end{cases}$$

Osserviamo che 5 è un inverso aritmetico di 2 modulo 9 e 2 è un inverso aritmetico di 3 modulo 5. Il precedente sistema è quindi equivalente al seguente:

$$\begin{cases} X \equiv 6 \pmod{9} \\ X \equiv 3 \pmod{5} \end{cases}$$

Risolviamo per sostituzione; osserviamo che $x_Y = 6 + 9\,Y$ risolve la prima equazione. Sostituiamo la generica soluzione della prima equazione nella seconda equazione e risolviamo quanto ottenuto in Y:

$$6 + 9\,Y \equiv 3\ (mod\ 5) \ \Leftrightarrow\ 4\,Y \equiv 2\ (mod\ 5) \ \Leftrightarrow Y \equiv 3\ (mod\ 5)$$

La soluzione generica di tale equazione è $Y = 3 + 5\,k$. Sostituendo in x_Y troviamo la generica soluzione del sistema $x_k = 33 + 45\,k$. Questa è l'unica soluzione del sistema modulo 45. L'esercizio chiede tuttavia di calcolare le soluzioni modulo 315. Bisogna quindi considerare le soluzioni comprese tra 0 e 314. Sono quelle tali che $k = 0, ..., 6$: 33, 78, 123, 168, 213, 258, 303. □

Esercizio 5.5. Sia $\{a_1, ..., a_n\}$ una collezione di numeri interi:
(A) Mostrare che $(a_1 + \cdots + a_n)^3 \equiv a_1^3 + \cdots + a_n^3 \pmod 3$;
(B) Trovare un'espressione modulo 4 per $(a_1 + \cdots + a_n)^4$ come funzione dei soli quadrati degli a_i.

Soluzione. Cominciamo con il dimostrare (A). Procediamo per induzione su n. Per $n = 1$ non c'è nulla da dimostrare. Supponiamo quindi che sia l'affermazione sia vera per n, dimostriamo che allora essa è vera per $n + 1$:

$$(a_1 + \cdots + a_n + a_{n+1})^3 = (a_1 + \cdots + a_n)^3 + 3 \cdot (a_1 + \cdots + a_n)^2 a_{n+1} + 3 \cdot (a_1 + \cdots + a_n)\, a_{n+1}^2 + a_{n+1}^3$$

riducendo modulo 3 la precedente espressione troviamo:

$$(a_1 + \cdots + a_n + a_{n+1})^3 \equiv (a_1 + \cdots a_n)^3 + a_{n+1}^3\ (mod\ 3)$$

Applichiamo quindi l'ipotesi induttiva $(a_1 + \cdots + a_n)^3 \equiv a_1^3 + \cdots + a_n^3$ e concludiamo:

$$(a_1 + \cdots + a_{n+1})^3 \equiv a_1^3 + \cdots + a_{n+1}^3\ (mod\ 3)$$

Dimostriamo ora il punto (B). In analogia con il caso precedente si può dimostrare che:

$$(a_1 + \cdots + a_n)^4 \equiv (a_1^2 + \cdots + a_n^2)^2\ (mod\ 4)$$

Anche in questo caso si può procedere per induzione. Per $n = 1$ abbiamo che $a_1^4 = (a_1^2)^2$ e dunque non vi è nulla da dimostrare. Supponiamo ora che la precedente relazione sia vera per $n \in \mathbb{N}$ dimostriamo che allora è vera anche per $n + 1$:

$$(a_1+\cdots+a_n+a_{n+1})^4 = (a_1+\cdots+a_n)^4+4\,(a_1+\cdots+a_n)^3\,a_{n+1}+6\,(a_1+\cdots+a_n)^2\,a_{n+1}^2+4\,(a_1+\cdots+a_n)\,a_{n+1}^3+a_{n+1}^4$$

Riducendo la precedente espressione modulo 4 troviamo quindi:

$$(a_1 + \cdots + a_n + a_{n+1})^4 \equiv (a_1 + \cdots + a_n)^4 + 2\,(a_1 + \cdots + a_n)^2 a_{n+1}^2 + a_{n+1}^4\ (mod\ 4)$$

sfruttando l'ipotesi induttiva l'espressione a destra è uguale a

$$(a_1^2 + \cdots + a_n^2)^2 + 2\sum_{i=1}^{n} a_i^2 a_{n+1}^2 + a_{n+1}^2$$

Sviluppando il quadrato della somma dei quadrati degli a_i con $i = 1, .., n$ otteniamo allora:

$$a_1^4 + \cdots a_n^4 + a_{n+1}^4 + 2 \sum_{1 \le i < j \le n+1} 2\, a_i^2 a_j^2$$

che è precisamente $(a_1^2 + \cdots a_{n+1}^2)^2$. Questo conclude l'esercizio. □

Esercizio 5.6. [1] Sia φ la funzione di Eulero. Per ogni intero positivo n, sia $\omega(n)$ il numero dei fattori primi distinti di n. Dimostrare che:

$$\frac{\varphi(n)}{n} \ge \frac{1}{\omega(n)+1}$$

(*Suggerimento. Procedere per induzione su* $\omega(n)$. *Può essere utile ricordare che dati* m *interi distinti* $n_1, .., n_m$ *strettamente maggiori di* 1 *allora* $n_m \ge m+1$)

Soluzione. Procediamo per induzione su $\omega(n)$. Per $\omega(n) = 0$ abbiamo che $n = 1$ e dunque $\varphi(1) = 1 \ge 1 = \frac{1}{+\omega(1)}$. Supponiamo ora che l'affermazione sia vera per i numeri n tali che $\omega(n) = m$, mostriamo che è vero per quei numeri n tali che $\omega(n) = m+1$.
Sia $\omega(n) = m+1$, allora esistono $m+1$ primi distinti $p_1 < p_2 < \cdots < p_m < p_{m+1}$ e delle potenze $h_i \ge 1$ tali che $n = p_1^{h_1} \cdots p_{m+1}^{h_{m+1}}$. Per le proprietà della funzione φ di Eulero sappiamo che

$$\varphi(n) = \varphi(p_1^{h_1} \cdots p_m^{h_m}) \cdot (p_{m+1}^{h_{m+1}} - p_{m+1}^{h_{m+1}-1})$$

Abbiamo quindi:

$$\frac{\varphi(n)}{n} = \frac{\varphi(p_1^{h_1} \cdots p_m^{h_m})}{p_1^{h_1} \cdots p_m^{h_m}} \cdot \frac{(p_{m+1}^{h_{m+1}} - p_{m+1}^{h_{m+1}-1})}{p_{m+1}^{h_{m+1}}} \ge \frac{1}{\omega(p^{h_1} \cdots p^{h_m}) + 1} \cdot \left(1 - \frac{1}{p_{m+1}}\right)$$

Si osservi quindi che $p_{m+1} \ge m+2$, da cui segue che $(1 - 1/p_{m+1}) \ge \frac{m+1}{m+2}$. Pertanto:

$$\frac{\varphi(n)}{n} \ge \frac{1}{m+1} \cdot \frac{m+1}{m+2} = \frac{1}{m+2} = \frac{1}{\omega(n)+1}\,. \quad \square$$

Esercizio 5. 7. [2] Determinare le soluzioni di $X^{27} \equiv X^{15} \pmod{77}$. (*Suggerimento. Tradurre la precedente equazione in un sistema — sfruttare la scomposizione in primi di* 77 *— e risolverlo*)

Soluzione. Cominciamo l'esercizio osservando che risolvere l'equazione in questione è equivalente a risolvere l'eqauzione $X^{15} \cdot (X^{12} - 1) \equiv 0 \pmod{77}$. Tale equazione a sua volta è equivalente al seguente sistema:

$$\begin{cases} X^{15}(X^{12} - 1) \equiv 0 \pmod 7 \\ X^{15}(X^{12} - 1) \equiv 0 \pmod{11} \end{cases}$$

Essendo 7 ed 11 coprimi, le soluzioni del precedente sistema sono in realtà l'unione delle soluzioni dei due sistemi seguenti:

$$\begin{cases} X^{15} \equiv 0 \pmod 7 \\ X^{12} - 1 \equiv 0 \pmod{11} \end{cases} \qquad \begin{cases} X^{12} - 1 \equiv 0 \pmod 7 \\ X^{15} \equiv 0 \pmod{11} \end{cases}$$

Risolviamo il primo sistema. Cominciamo assumendo che $X \equiv 0 \pmod 7$. Dunque $X = 7Y$, dove $Y \in \mathbb{Z}$. Sostituiamo questa espressione nella seconda equazione. $(7Y)^{12} - 1 \equiv 0 \pmod{11}$. Osserviamo che $Y \equiv 0 \pmod{11}$ non è una soluzione dell'equazione. Possiamo quindi assumere che $Y \neq 11j$. Essendo 11 primo ne deduciamo che $\mathrm{MCD}(7Y, 11) = 1$, e possiamo quindi applicare il Teorema di Eulero-Fermat: ricordiamo che $\varphi(11) = 10$. Possiamo quindi semplificare la nostra equazione: $(7Y)^2 - 1 \equiv 0 \pmod{11}$ abbiamo quindi $5Y^2 \equiv 1 \pmod{11}$ da cui otteniamo $Y^2 \equiv 9 \pmod{11}$. Tale equazione ammette le due soluzioni $3 + 11k$ e $8 + 11k$ (ovvero $-3 + 11k$). Quindi per $X \equiv 0 \pmod 7$

[1] Esercizio tratto da un compito del Prof. R. Dvornicich — Università di Pisa — A.A. 2005-2006.
[2] Esercizio tratto da un compito del Prof. R. Dvornicich — Università di Pisa — A.A. 2005-2006.

le soluzioni sono $\{21 + 77k \mid k \in \mathbb{Z}\} \cup \{56 + 77k \mid k \in \mathbb{Z}\}$
Andiamo ora a considerare il caso in cui X non è congruo a 0 modulo 7. In questo caso, essendo 7 un numero primo, abbiamo che X è necessariamente coprimo con 7; pertanto $\overline{X} \in \mathcal{U}(\mathbb{Z}_7)$ e lo stesso vale per tutte le sue potenze (ricordiamo infatti che $\mathcal{U}(\mathbb{Z}_n)$ è un gruppo rispetto alla moltiplicazione). In particolare $X^k \not\equiv 0 \ (mod\ 7)$, qualsiasi sia k. Dunque le soluzioni del primo sistema sono tutte e sole quelle precedentemente elencate:

$$\{21 + 77k \mid k \in \mathbb{Z}\} \cup \{56 + 77k \mid k \in \mathbb{Z}\}$$

Per trovare tutte le soluzioni dell'equazione iniziale non ci resta che risolvere il secondo sistema che abbiamo derivato dall'equazione iniziale e prendere l'unione delle soluzioni di tale sistema con quelle precedentemente trovate per il primo sistema.

Risolviamo quindi il secondo sistema. Come nel primo sistema osserviamo che, essendo 11 un numero primo, l'equazione $X^k \equiv 0 \ (mod\ 11)$ ammette soluzione se e soltanto se $X \equiv 0 \ (mod\ 11)$. Se così non fosse infatti avremmo che $\overline{X} \in \mathcal{U}(\mathbb{Z}_{11})$ e dunque tutte le sue potenze devono essere in $\mathcal{U}(\mathbb{Z}_{11})$ e dunque $\overline{X}^k \neq \overline{0}$ in $\mathbb{Z}_{11}$.
Assumiamo pertanto che $X \equiv 0 \ (mod\ 11)$, $X = 11\,Y$ al variare di $Y \in \mathbb{Z}$ ed andiamo a sostituire tale espressione nell'equazione $X^{12} - 1 \equiv 0 \ (mod\ 7)$. Otteniamo così l'equazione:

$$(11\,Y)^{12} - 1 \equiv 0 \ (mod\ 7) \ \Leftrightarrow (5Y)^{12} \equiv 1 \ (mod\ 7)$$

Osserviamo ora che $Y \equiv 0 \ (mod\ 11)$ non è una soluzione dell'equazione; essendo 7 un numero primo abbiamo che $Y \not\equiv 0 \ (mod\ 7) \ \Rightarrow \ 5Y \in \mathcal{U}(\mathbb{Z}_7)$ ovvero $\mathrm{MCD}(5Y, 7) = 1$. Possiamo quindi applicare il Teorema di Eulero-Fermat; a tal scopo calcoliamo $\varphi(7) = (7 - 1) = 6$. Abbiamo quindi che se $Y \not\equiv 0 \ (mod\ 7)$ l'equazione precedente diventa $1 \equiv 1 \ (mod\ 7)$ ed è dunque sempre verificata. Le soluzioni del secondo sistema sono quindi:

$$\{11{+}77k \mid k \in \mathbb{Z}\} \cup \{22{+}77k \mid k \in \mathbb{Z}\} \cup \{33{+}77k \mid k \in \mathbb{Z}\} \cup \{44{+}77k \mid k \in \mathbb{Z}\} \cup \{55{+}77k \mid k \in \mathbb{Z}\} \cup \{66{+}77k \mid k \in \mathbb{Z}\}$$

Possiamo dunque scrivere tutte le soluzioni dell'equazione iniziale:

$$\{21 + 77k \mid k \in \mathbb{Z}\} \cup \{56 + 77k \mid k \in \mathbb{Z}\} \cup \{11j + 77k \mid j = 1, ..6;\ k \in \mathbb{Z}\}. \quad \square$$

Esercizio 5.8. [3] Siano $a, b, c \in \mathbb{N}^*$ e supponiamo che valgano le seguenti:

$$\begin{cases} a \equiv b & (mod\ c) \\ b \equiv c & (mod\ a) \\ c \equiv a & (mod\ b) \end{cases}$$

(A) Cosa possiamo dedurre sugli MCD delle tre coppie?
(B) Quale relazione sussiste tra a, b e c?

Soluzione. Il sistema precedente è compatibile se e solo se valgono le seguenti:

$$\mathrm{MCD}(a, c) \mid b \ ; \ \mathrm{MCD}(a, b) \mid c \ ; \ \mathrm{MCD}(b, c) \mid a$$

Osserviamo che, in tal caso, poiché $\mathrm{MCD}(a, c)$ divide sia a che b esso deve dividere $\mathrm{MCD}(a, b)$; viceversa dalla relazione $\mathrm{MCD}(a, b) \mid c$ ne segue che $\mathrm{MCD}(a, b) \mid \mathrm{MCD}(a, c)$; ne concludiamo che $\mathrm{MCD}(a, b) = \mathrm{MCD}(a, c)$. Con un ragionamento analogo si mostra che $\mathrm{MCD}(a, b) = \mathrm{MCD}(b, c)$. La risposta alla domanda (A) è dunque: $\mathrm{MCD}(a, b) = \mathrm{MCD}(a, c) = \mathrm{MCD}(b, c)$.

Supponiamo adesso che non valga $a = b = c$. In particolare vi sarà un elemento maggiore o uguale agli altri due, e strettamente maggiore di uno dei due. Ricordiamo che a, b, c sono interi positivi. Supponiamo che tale elemento sia c, allora $a \equiv b \ (mod\ c)$ assieme alla condizione $0 < a, b \leq c$ implica che $a = b$. In tale situazione le due equazioni $a \equiv c \ (mod\ b)$ e $c \equiv b \ (mod\ a)$ sono in realtà equivalenti, e possono essere verificate se e solo se $c = ka = kb$. Dunque deve risultare una delle seguenti:

$$a = b,\ c = ka = kb \ \text{ oppure } b = c,\ a = kb = kc \ \text{ oppure } a = c,\ b = ka = kc$$

[3] Esercizio tratto da *A concrete introduction to Higher Algebra* di L. N. Childs