1 Proprietà elementari delle congruenze

Un altro metodo di approccio alla teoria della divisibilità in $\mathbb{Z}$ consiste nello studiare le proprietà aritmetiche del resto della divisione euclidea, o, come si dice abitualmente, la teoria delle congruenze. Tale teoria è stata iniziata da Gauss nel suo celebre *Disquisitiones Arithmeticae* [G], apparso nel 1801 (quando Gauss aveva soltanto ventiquattro anni).

Definizione 1.1. Sia n un intero fissato. Si dice che $a, b \in \mathbb{Z}$ sono *congruenti* $\pmod n$ e si scrive:

$$a \equiv b \pmod n$$

se risulta che $a - b \in n\mathbb{Z}$ (cioè, se n *divide* $a - b$, in altri termini, se esiste un intero $k \in \mathbb{Z}$ tale che $kn = a - b$; in simboli, scriveremo $n|(a - b)$).

Osservazione 1.2. Siano $a, b, n \in \mathbb{Z}$. Dalla definizione precedente segue subito che:
(a) se $n = 1$, allora $a \equiv b \pmod 1$, presi comunque $a, b \in \mathbb{Z}$;
(b) se $n = 0$, allora $a \equiv b \pmod 0 \iff a = b$;
(c) $a \equiv b \pmod n \iff a \equiv b \pmod{-n} \iff a \equiv b \pmod{|n|}$.

Per evitare casi banali, è quindi evidente che ci si può limitare a considerare congruenze modulo $n \geq 2$. In particolare, due interi sono congruenti (modulo 2) se, e soltanto se, hanno la stessa parità.
È evidente che "la congruenza $\pmod n$" stabilisce una relazione (binaria) tra gli elementi di $\mathbb{Z}$. Le prime proprietà di tale relazione sono raccolte nella seguente:

Proposizione 1.3. *Siano n, m due interi positivi fissati e siano a, b, c, $d \in \mathbb{Z}$. Allora:*
(1) *Proprietà riflessiva della "congruenza $\pmod n$":*
$a \equiv a \pmod n$, per ogni $a \in \mathbb{Z}$;
(2) *Proprietà simmetrica della "congruenza $\pmod n$":*
$a \equiv b \pmod n \iff b \equiv a \pmod n$;
(3) *Proprietà transitiva della "congruenza $\pmod n$":*
$a \equiv b \pmod n, b \equiv c \pmod n \Rightarrow a \equiv c \pmod n$;
(4) *Proprietà di compatibilità con la somma della "congruenza $\pmod n$":*
$a \equiv b \pmod n, c \equiv d \pmod n \Rightarrow a + c \equiv b + d \pmod n$;
(5) *Proprietà di compatibilità con il prodotto della "congruenza $\pmod n$":*
$a \equiv b \pmod n$, $c \equiv d \pmod n$, $\Rightarrow ac \equiv bd \pmod n$;
(6) $a \equiv b \pmod n \iff a + c \equiv b + c \pmod n$ *per ogni* $c \in \mathbb{Z}$;
(7) $a \equiv b \pmod n \iff ac \equiv bc \pmod n$ *per ogni* $c \in \mathbb{Z}$;
(8) $a \equiv b \pmod n \iff a^k \equiv b^k \pmod n$ *per ogni intero* $k \geq 0$;
(9) $a \equiv b \pmod n$, $m \mid n \Rightarrow a \equiv b \pmod m$;
(10) $a \equiv b \pmod n$, $m \neq 0 \Rightarrow am \equiv bm \pmod{nm}$;

(11) *Se* $a \equiv b \pmod{n}$, $d \neq 0$, $d \mid a$, $d \mid b$, $d \mid n$ *allora*

$$\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{n}{d}}.$$

Dimostrazione. Le semplici verifiche sono lasciate come esercizio. □

Corollario 1.4. *Siano* n *ed* m *due interi positivi fissati.*

(1) *Siano* $a_1, ..., a_m, b_1, ..., b_m, c_1, ..., c_m \in \mathbb{Z}$ *tali che* $a_i \equiv b_i \pmod{n}$ $(1 \leqslant i \leqslant m)$. *Allora:*

$$\sum_{i=1}^{m} a_i c_i \equiv \sum_{i=1}^{m} b_i c_i \pmod{n}$$

(2) *Siano* $a, b \in \mathbb{Z}$ *ed* $f(X) \in \mathbb{Z}[X]$. *Se* $a \equiv b \pmod{n}$, *allora:*

$$f(a) \equiv f(b) \pmod{n}$$

Dimostrazione. Basta utilizzare alcune proprietà della proposizione precedente. □

Osservazione 1.5. Le proprietà (4) e (5) della Proposizione 1.3 permettono di (ben) definire, in modo naturale, sull'insieme quoziente $\mathbb{Z}/n\mathbb{Z}$ delle operazioni di somma e prodotto che determinano su $\mathbb{Z}/n\mathbb{Z}$ una struttura canonica di anello.
La relazione di congruenza (modulo n) corrisponde alla relazione di uguaglianza nell'anello quoziente $\mathbb{Z}/n\mathbb{Z}$. Se infatti, $a, b \in \mathbb{Z}$ e se

$$\bar{a} := a + n\mathbb{Z}, \quad \bar{b} := b + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z},$$

allora:

$$\begin{aligned} &a \equiv b \pmod{n} \iff \bar{a} = \bar{b}\,, \\ &\bar{a} + \bar{b} := a + b + n\mathbb{Z}\,, \\ &\bar{a} \cdot \bar{b} := ab + n\mathbb{Z}\,. \end{aligned}$$

Proposizione 1.6. *Siano* $a, b \in \mathbb{Z}, n > 0$. *Allora,* $a \equiv b \pmod{n}$ *se, e soltanto se,* a, b *hanno lo stesso resto nella divisione per* n.

Dimostrazione. Se $a \equiv b \pmod{n}$, allora esiste $k \in \mathbb{Z}$ in modo tale che $a = kn + b$. Dividendo b per n, si ottiene $b = qn + r$, con $0 \leqslant r < n$ e, sostituendo, $a = (k + q)n + r$. Viceversa, se $a = q'n + r$, $b = qn + r$ con $0 \leqslant r < n$, allora $a - b = (q' - q)n$ e, dunque, $a \equiv b \pmod{n}$. □

Corollario 1.7. *Ogni intero è congruente (modulo* n*) ad uno ed uno soltanto tra gli interi* $0, 1, ..., n - 1$. □

Tale fatto giustifica la seguente definizione:

Definizione 1.8. Si chiama *sistema completo di residui (modulo n)* ogni insieme $S \subset \mathbb{Z}$ (formato da n interi) tale che ogni $a \in \mathbb{Z}$ è congruente (modulo n) ad uno ed un solo elemento di S.

Ad esempio $S := \{0, 1, ..., n-1\}$ è un sistema completo di residui (modulo n), detto *sistema completo minimo* (mod n).
Se n è dispari, allora $S := \{-\frac{n-1}{2}, -\frac{n-3}{2}, ..., -1, 0, 1, ..., \frac{n-3}{2}, \frac{n-1}{2}\}$ è anch'esso un *sistema completo di residui*, detto *minimo in valore assoluto*, (mod n).
Se n è pari, ci sono due sistemi completi di residui che hanno una proprietà di minimalità rispetto al valore assoluto e sono:
$S_1 := \{-\frac{n-2}{2}, ..., -1, 0, 1, ..., \frac{n-2}{2}, \frac{n}{2}\}$, $S_2 := \{-\frac{n}{2}, -\frac{n-2}{2}, ..., -1, 0, 1, ..., \frac{n-2}{2}\}$.
Ad esempio, se $n = 6$, allora:

$$S_1 = \{-2, -1, 0, 1, 2, 3\} \quad \text{e} \quad S_2 = \{-3, -2, -1, 0, 1, 2\}.$$

È subito visto che n interi formano un sistema completo di residui (modulo n), se, e soltanto se, sono a due a due incongruenti modulo n. Torneremo in seguito sui sistemi completi di residui (cfr. Esercizi 1.4 e 1.5); vogliamo tuttavia dimostrare subito alcune regole di cancellazione.

Proposizione 1.9. *Siano $a, b, c, n \in \mathbb{Z}, n > 0$. Se $d := \mathrm{MCD}(c, n)$, allora:*

$$ac \equiv bc \pmod{n} \Rightarrow a \equiv b \pmod{\frac{n}{d}}.$$

Dimostrazione. Per ipotesi, esiste $k \in \mathbb{Z}$ tale che $c(a-b) = kn$. Inoltre, esistono $x, y \in \mathbb{Z}$ tali che $c = dx$, $n = dy$ e $\mathrm{MCD}(x, y) = 1$. Da ciò segue che $x(a-b) = ky$ e dunque $y \mid x\,(a-b)$. In base al Lemma di Euclide, $y \mid (a-b)$ e cioè $a \equiv b \pmod{y}$. $\square$

Osservazione 1.10. Si noti che vale anche il viceversa nella precedente Proposizione. Precisamente, se $a - b = h(\frac{n}{d})$ per qualche $h \in \mathbb{Z}$ allora $ac \equiv bc \pmod{n}$. Infatti, se come sopra $c = dx, n = dy$, allora $(a-b)d = hn$, quindi $(a-b)dx = hnx$ cioè $(a-b)c = hnx$. Pertanto, $ac - bc \equiv 0 \pmod{n}$.

Corollario 1.11. *Siano $a, b, c, n, p \in \mathbb{Z}$, con $n > 0$ e p numero primo. Si ha:*

(a) *se $ac \equiv bc \pmod{n}$ e $\mathrm{MCD}(n, c) = 1 \Rightarrow a \equiv b \pmod{n}$;*

(b) *se $ac \equiv bc \pmod{p}$ e $p \nmid c \Rightarrow a \equiv b \pmod{p}$.* $\square$

Osservazione 1.12. **(a)** Per la validità delle proprietà di cancellazione, le ipotesi nel corollario relative al massimo comun divisore sono essenziali. Ad esempio:
$4 * 2 \equiv 1 * 2 \pmod{6}$ mentre $4 \not\equiv 1 \pmod{6}$ (in tal caso $\mathrm{MCD}(2, 6) = 2$).
(b) L'impossibilità di cancellare (in generale) un fattore di una congruenza

è strettamente connessa col fatto che (in generale) $\mathbb{Z}/n\mathbb{Z}$ non è un anello integro. A questo proposito, è opportuno ricordare il seguente fatto ben noto:
Sia $n \in \mathbb{Z}$, $n > 0$. Le seguenti condizioni sono equivalenti:

(i) *$\mathbb{Z}/n\mathbb{Z}$ è un anello integro;*

(ii) *$\mathbb{Z}/n\mathbb{Z}$ è un campo;*

(iii) *n è un numero primo.*

Definizione 1.13. Siano $a, n \in \mathbb{Z}, n > 0$. Si chiama *inverso aritmetico di a (modulo n)* un elemento $a^* \in \mathbb{Z}$ tale che:

$$aa^* \equiv 1 \pmod{n}.$$

Si noti che un siffatto elemento non sempre esiste (ad esempio, 2 non ammette inverso aritmetico (modulo 4)), e, se esiste, non è necessariamente unico (ad esempio, 3, 7, 11, ... sono inversi aritmetici di 3 (modulo 4)). Il seguente risultato precisa tali questioni:

Proposizione 1.14. *Siano $a, n \in \mathbb{Z}, n > 0$. Risulta:*

(a) *a ammette inverso aritmetico (modulo n) se e soltanto se* $\mathrm{MCD}(a, n) = 1$;

(b) *se a_1^*, a_2^* sono due inversi aritmetici di $a \pmod{n}$, allora $a_1^* \equiv a_2^* \pmod{n}$.*

Dimostrazione. (a) ($\Leftarrow$) L'identità di Bézout ci assicura che esistono $x, y \in \mathbb{Z}$ tali che $ax + ny = 1$. Dunque $ax \equiv 1 \pmod{n}$ e pertanto $x = a^*$. ($\Rightarrow$) Esiste $k \in \mathbb{Z}$ tale che $aa^* - 1 = kn$. Se quindi $d := \mathrm{MCD}(a, n)$, allora $d \mid (aa^* - kn)$ e dunque $d = 1$.
(b) Si ha: $a_1^* \equiv a_1^*(aa_2^*) = (a_1^* a)a_2^* \equiv a_2^* \pmod{n}$. $\square$

Osservazione 1.15. La dimostrazione della Proposizione 1.14 (a) suggerisce un metodo pratico per il calcolo di un inverso aritmetico (modulo n) di un elemento assegnato $a \in \mathbb{Z}$ con $\mathrm{MCD}(a, n) = 1$: l'algoritmo euclideo delle divisioni successive. Questo algoritmo, infatti, come è ben noto, permette di calcolare esplicitamente "i coefficienti" nell'identità di Bézout relativa ad $1 = \mathrm{MCD}(a, n)$.
Un metodo, a volte, di più facile applicazione, usando l'esponenziazione modulare, si ricaverà nel seguito, come conseguenza del "Piccolo Teorema di Fermat" (cfr. Paragrafo 3).

Osservazione 1.16. Esprimendo le congruenze modulo n tramite uguaglianze in $\mathbb{Z}/n\mathbb{Z}$ (cfr. Osservazione 1.5), è chiaro che la ricerca di un inverso aritmetico di $a \in \mathbb{Z}$ (modulo n) equivale alla ricerca dell'inverso moltiplicativo di $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$.

Nel paragrafo successivo torneremo sul problema della ricerca degli inversi aritmetici allo scopo di risolvere le congruenze lineari in una indeterminata; per il momento vogliamo applicare i risultati precedenti per "ritrovare" alcuni criteri di divisibilità elementarmente noti.

Teorema 1.17. *Sia N un intero tale che $|N|$ ammette la seguente espressione in base 10, ovvero decimale:*

$$|N| = a_m 10^m + a_{m-1} 10^{m-1} + ... + a_2 10^2 + a_1 10 + a_0,$$

con $0 \leqslant a_i \leqslant 9$, $0 \leqslant i \leqslant m$ e $a_m \neq 0$. Posto

$$S(N) := \sum_{i=0}^{m} a_i \quad e \quad A(N) := \sum_{i=0}^{m} (-1)^i a_i,$$

si ha:

(a) $2 \mid N \iff 2 \mid a_0$;

(b) $3 \mid N \iff 3 \mid S(N)$;

(c) $4 \mid N \iff 4 \mid a_1 10 + a_0$;

(d) $5 \mid N \iff 5 \mid a_0$;

(e) $9 \mid N \iff 9 \mid S(N)$;

(f) $11 \mid N \iff 11 \mid A(N)$;

(g) *Sia i tale che $1 \leqslant i \leqslant m$. Allora:*

$$2^i \mid N \iff 2^i \mid (a_{i-1} 10^{i-1} + ... + a_1 10 + a_0)$$

Dimostrazione. (a; d) Sia $a = 2$ (oppure $a = 5$). Risulta:

$$a \mid N \iff N = \sum_{k=0}^{m} a_k 10^k \equiv 0 \pmod{a}.$$

Ma $10 \equiv 0 \pmod{a}$ e quindi:

$$a \mid N \iff a_0 \equiv 0 \pmod{a} \iff a \mid a_0.$$

(b; e) Sia $b = 3$ (oppure $b = 9$). Poichè $10 \equiv 1 \pmod{b}$, si ha:

$$b \mid N \iff \sum_{k=0}^{m} a_k \equiv 0 \pmod{b} \iff b \mid S(N).$$

(f) Poichè $10 \equiv -1 \pmod{11}$, $10^k \equiv (-1)^k \pmod{11}$ e dunque:

$$11 \mid N \quad \Longleftrightarrow \quad 0 \equiv \sum_{k=0}^{m} a_k 10^k \equiv \sum_{k=0}^{m} (-1)^k a_k = A(N) \pmod{11}$$

$$\Longleftrightarrow \quad 11 \mid A(N).$$

(g; c) Poichè $10^j \equiv 0 \pmod{2^i}$ se $j \geqslant i$, si ha:

$$2 \mid N \quad \Longleftrightarrow \quad 0 \equiv \sum_{k=0}^{m} a_k 10^k \equiv \sum_{k=0}^{i-1} a_k 10^k \pmod{2^i}$$

$$\Longleftrightarrow \quad 2^i \mid (a_{i-1} 10^{i-1} + \cdots + a_0). \qquad \square$$

I precedenti criteri di divisibilità in base 10 sono casi particolari di criteri di divisibilità che possono essere formulati in una base b qualunque.

Siano N, b due interi positivi e sia:

$$N = (a_m \ldots a_1 a_0)_b := a_m b^m + a_{m-1} b^{m-1} + \cdots + a_1 b + a_0$$

l'espressione esplicita di N in base b, con $0 \leqslant a_i \leqslant b-1$, $0 \leqslant i \leqslant m$, $a_m \neq 0$.

Proposizione 1.18. *Se d è un intero positivo tale che $d \mid b$ e se $k < m$ allora*

$$d^k \mid (a_m \ldots a_1 a_0)_b \quad \Longleftrightarrow \quad d^k \mid (a_{k-1} \ldots a_1 a_0)_b$$

In particolare, se $k = 1$, allora:

$$d \mid N \quad \Longleftrightarrow \quad d \mid a_0.$$

Dimostrazione. Basta osservare che:

$$d \mid b \Rightarrow d^k \mid b^k, \text{ per ogni } \quad k \geqslant 1,$$

e dunque:

$$N = a_m b^m + \cdots + a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0 \equiv$$

$$\equiv a_{k-1} b^{k-1} + \cdots + a_1 b + a_0 \pmod{d^k}. \qquad \square$$

Proposizione 1.19. *Se d è un intero positivo tale che $d \mid (b-1)$ allora:*

$$d \mid N \quad \Longleftrightarrow \quad d \mid \sum_{k=0}^{m} a_k.$$

Dimostrazione. Basta osservare che:

$$d \mid (b-1) \quad \Longleftrightarrow \quad b \equiv 1 \pmod{d},$$

e dunque:

$$N = a_m b^m + \cdots + a_1 b + a_0 \equiv a_m + \cdots + a_1 + a_0 \pmod{d}. \qquad \square$$

Proposizione 1.20. *Se d è un intero positivo tale che $d \mid (b+1)$ allora:*

$$d \mid N \quad \Longleftrightarrow \quad d \mid \sum_{k=0}^{m} (-1)^k a_k .$$

Dimostrazione. Basta osservare che

$$d \mid (b+1) \quad \Longleftrightarrow \quad b \equiv -1 \pmod{d},$$

e dunque:

$$N = a_m b^m + \cdots + a_1 b + a_0 \equiv (-1)^m a_m + \cdots + a_2 - a_1 + a_0 \pmod{d}. \qquad \square$$

Osservazione 1.21. Si noti che gli enunciati (a), (c), (d) e (g) del Teorema 1.17 sono casi particolari della Proposizione 1.18; gli enunciati (b) ed (e) del Teorema 1.17 sono casi particolari della Proposizione 1.19; l'enunciato (f) è un caso particolare della Proposizione 1.20.

Osservazione 1.22. Particolarmente interessante è il seguente criterio di divisibilità dimostrato da B. Pascal attorno al 1654.
Conserviamo le notazioni del Teorema 1.17.
Sia a un intero non nullo e siano $r_1, r_2, \ldots$ i resti della divisione di $10, 10r_1, 10r_2, \ldots$ per a. Allora:

$$a \mid N \quad \Longleftrightarrow \quad a \mid (a_0 + a_1 r_1 + \cdots + a_m r_m) .$$

Basta osservare che $10 \equiv r_1 \pmod{a}, 10^2 \equiv 10r_1 \equiv r_2 \pmod{a}$ ed, in generale, $10^k \equiv 10^{k-1} r_1 \equiv \cdots \equiv r_k \pmod{a}$ per ogni $1 \leqslant k \leqslant m$.
Ad esempio 1261 è divisibile per 13. Infatti, in questo caso $r_1 = 10$, $r_2 = 9, r_3 = 12$, dunque $1 + 6 \cdot 10 + 2 \cdot 9 + 1 \cdot 12 = 91$ e $13 \mid 91 = 13 \cdot 7$.

Vogliamo concludere il paragrafo con alcune osservazioni generali sulla teoria delle congruenze. L'importanza e l'interesse di tale teoria risiede essenzialmente nel fatto che essa gioca un ruolo fondamentale nella risoluzione delle cosidette "equazioni diofantee", cioè equazioni polinomiali a coefficienti interi di cui si ricercano le soluzioni intere.
Si consideri infatti la seguente equazione diofantea:

$$f(X_1, \ldots, X_r) = 0, \tag{1}$$

dove f è un polinomio a coefficienti interi in r indeterminate, cioè:
$f = f(X_1, \ldots, X_r) \in \mathbb{Z}[X_1, \ldots, X_r]$, con $r \geqslant 1$.
All'equazione diofantea (1) è associata una congruenza polinomiale $\pmod{n}$ per ogni n:

$$f(X_1, \ldots, X_r) \equiv 0 \pmod{n} \tag{2}$$

Definizione 1.23. Si chiama *soluzione della congruenza*:

$$f(X_1, \ldots, X_r) \equiv 0 \pmod{n}, \text{ dove } f(X_1, \ldots, X_r) \in \mathbb{Z}[X_1, \ldots, X_r],$$

ogni r-upla $(a_1, \ldots, a_r)$ di interi tale che $f(a_1, \ldots, a_r) \equiv 0 \pmod{n}$.
Due soluzioni $(a_1, \ldots, a_r)$, $(b_1, \ldots, b_r)$ sono dette *distinte* o *incongruenti (modulo n)* se esiste un indice i $(1 \leqslant i \leqslant r)$ per cui risulti che $a_i \not\equiv b_i \pmod{n}$.

L'ultima parte della definizione è giustificata dal seguente risultato (semplice conseguenza delle proprietà elementari delle congruenze; cfr. Proposizione 1.3).

Proposizione 1.24. *Siano $a_1, \ldots, a_r, b_1, \ldots, b_r$ interi tali che si abbia: $a_i \equiv b_i \pmod{n}$ per ogni i, $(1 \leqslant i \leqslant r)$. Se $(a_1, \ldots, a_r)$ è soluzione della congruenza:*

$$f(X_1, \ldots, X_r) \equiv 0 \pmod{n},$$

anche $(b_1, \ldots, b_r)$ è soluzione della stessa congruenza. □

È ovvio che se $(b_1, \ldots, b_r) \in \mathbb{Z}^r$ è soluzione dell'equazione diofantea (1), allora $(b_1, \ldots, b_r)$ è anche soluzione della congruenza (2), per ogni $n > 0$. Pertanto, se per qualche $n > 0$, (2) non è risolubile, non sarà risolubile l'equazione diofantea (1).

Nel seguito considereremo principalmente congruenze in una sola indeterminata X.

Osservazione 1.25. (a) L'omomorfismo suriettivo canonico

$$\varphi_n : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$

(con $n \geqslant 2$) di anelli si estende in modo ovvio ad un omomorfismo suriettivo tra anelli di polinomi:

$$\bar{\varphi}_n : \mathbb{Z}[X_1, \ldots, X_r] \longrightarrow (\mathbb{Z}/n\mathbb{Z})[X_1, \ldots, X_r].$$

All'equazione (1) resta quindi associata una famiglia di equazioni polinomiali:

$$\bar{f}_n(X_1, \ldots, X_r) = 0 \tag{3}$$

(con $\bar{f}_n = \bar{\varphi}_n(f) \in (\mathbb{Z}/n\mathbb{Z})[X_1, \ldots, X_r]$, $n \geqslant 2$).
È chiaro che un eventuale soluzione di (1) (cioè una r-upla di interi) determina una soluzione di ogni equazione (3) e quindi, dall'impossibilità di risolvere almeno una delle (3) segue l'irrisolubilità di (1). Più generalmente, qualunque condizione necessaria possa essere provata su almeno una delle (3) si riflette in una condizione necessaria per (1). Ad esempio il fatto che

l'equazione diofantea $X^2+1-3Y^k=0$ è irrisolubile, per ogni $k \geqslant 1$, discende dal fatto che la congruenza: $X^2+1-3Y^k \equiv 0 \pmod 3$ non ha soluzioni.
D'altra parte, con le notazioni dell'Osservazione 1.16, è subito visto che, se $a_1, \ldots, a_r \in \mathbb{Z}$, si ha:

$$\bar{f}_n(\bar{a}_1, \ldots, \bar{a}_r) = \bar{0} \quad \Longleftrightarrow \quad f(a_1, \ldots, a_r) \equiv 0 \pmod n.$$

(b) In generale, una congruenza $f(X) \equiv 0 \pmod n$ può ammettere soluzioni per alcuni valori di n, mentre può esserne priva per altri valori di n. Ad esempio $X^2+1 \equiv 0 \pmod 8$ oppure $2X+3 \equiv 0 \pmod 4$, non ammettono soluzioni, mentre $X^2+1 \equiv 0 \pmod 2$ e $2X+3 \equiv 0 \pmod 5$ ammettono soluzioni (come si può verificare sperimentalmente).
(c) Semplici esempi mettono in evidenza il fatto che la risolubilità della congruenza $f(X) \equiv 0 \pmod n$, anche per infiniti valori di n, non implica la risolubilità dell'equazione diofantea $f(X) = 0$.
Ad esempio $2X+1=0$ è un'equazione diofantea non risolubile, mentre $2X+1 \equiv 0 \pmod n$ è risolubile per ogni intero n dispari, perché $n = 2k+1$ per un qualche intero $k \geqslant 1$.
(d) Si noti che l'equazione diofantea in due indeterminate:

$$(2X-1)(3Y-1) = 0$$

non ha soluzioni, mentre la congruenza:

$$(2X-1)(3Y-1) \equiv 0 \pmod n$$

è risolubile, per ogni $n \geqslant 2$. Infatti, n si può sempre scrivere nella forma $n = 2^e(2k-1)$ con $e \geqslant 0$ e $k \geqslant 1$.
Inoltre, $2^{2e+1}+1 = (2+1)(2^{2e}-2^{2e-1}+\cdots-2+1)$ dunque $(3h-1) = 2^{2e+1}$, con $h := (2^{2e}-2^{2e-1}+\cdots-2+1)$. Pertanto $2^{e+1}n = (2k-1)(3h-1)$.
Si può dimostrare, in generale, che se $a, b, c, d \in \mathbb{Z}$, se $\mathrm{MCD}(a,c) = 1$ e se $n \geqslant 2$ allora:

$$(aX+b)(cY+d) \equiv 0 \pmod n$$

è risolubile per ogni n.

1. Esercizi e Complementi

1.1. Provare che:

$$a \equiv b \pmod{n} \Rightarrow \mathrm{MCD}(a,n) = \mathrm{MCD}(b,n).$$

[Suggerimento. Basta provare che l'insieme dei divisori comuni di a ed n coincide con l'insieme dei divisori comuni di b ed n. Si noti che non vale il viceversa: basta prendere $a = 3, b = 5, n = 4$.]

1.2. Provare che:

$$a \equiv b \pmod{n},\ a \equiv b \pmod{m},\ \mathrm{MCD}(n,m) = 1 \Rightarrow a \equiv b \pmod{nm}.$$

[Suggerimento. Applicare il Lemma di Euclide, esistendo $k, h \in \mathbb{Z}$ in modo tale che $kn = a - b = hm$.]

1.3. Verificare che:
(a) il quadrato di ogni intero è congruente a 0 oppure 1 (mod 4);
(b) il quadrato di ogni intero è congruente a 0, oppure 1, oppure 4 (mod 8);
(c) nessun intero congruente a 3 (mod 4) può essere somma di due quadrati (di numeri interi);
(d) nessun intero congruente a 7 (mod 8) può essere somma di tre quadrati (di numeri interi).

1.4. Sia $S := \{r_1, \ldots, r_n\}$ un sistema completo di residui (modulo n). Provare che: scelti $a, b \in \mathbb{Z}$ con $\mathrm{MCD}(a,n) = 1$, l'insieme $S' := \{ar_1 + b, \ldots, ar_n + b\}$ è ancora un sistema completo di residui (modulo n).
[Suggerimento. Provare che: $ar_i + b \equiv ar_j + b \pmod{n} \iff i = j$.]

1.5. Siano n, m interi positivi relativamente primi.
Sia $\{x_1, \ldots, x_n\}$ (rispettivamente $\{y_1, \ldots, y_m\}$) un sistema completo di residui (modulo n) (rispettivamente (modulo m)). Provare che gli elementi $mx_i + ny_j$ (con $1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m$) descrivono un sistema completo di residui (modulo nm).
[Suggerimento. Provare che $mx_i + ny_j \equiv mx_h + ny_k \pmod{nm} \iff i = h$ e $j = k$.]

1.6. Siano $a, b, k, p \in \mathbb{Z}$ con k e p positivi e p primo. Mostrare che:
(a) $a^2 \equiv b^2 \pmod{p} \iff a \equiv b \pmod{p}$ oppure $a \equiv -b \pmod{p}$
(b) $a^k \equiv b^k \pmod{p}$, $a^{k+1} \equiv b^{k+1} \pmod{p}$, $p \nmid a \Rightarrow a \equiv b \pmod{p}$.
[Suggerimento. **(a)** $a^2 - b^2 = (a-b)(a+b)$; **(b)** se $p \nmid a$ allora $p \nmid a^k$ quindi $p \nmid b^k$, pertanto a^k e b^k possiedono un inverso aritmetico (mod p).]

1.7. Sia $n \geqslant 2$. Mostrare che:
(a) se n è dispari, allora:

$$1 + 2 + 3 + \cdots + (n-1) \equiv 0 \pmod{n};$$

(b) se n è dispari oppure se n è un multiplo di 4, allora:

$$1^3 + 2^3 + 3^3 + \cdots + (n-1)^3 \equiv 0 \pmod{n};$$

(c) se $n \equiv 1, 5 \pmod 6$, allora:

$$1^2 + 2^2 + 3^2 + \cdots + (n-1)^2 \equiv 0 \pmod n.$$

Dare un controesempio esplicito per **(a)**, quando n è pari, e per **(c)**, quando $n \not\equiv 1, 5 \pmod 6$.
[Suggerimento. Per induzione su n abbiamo dimostrato (Capitolo 0) che:

$$1 + 2 + \cdots + (n-1) = \frac{n(n-1)}{2};$$

$$1^2 + 2^2 + \cdots + (n-1)^2 = \frac{n(n-1)(2n-1)}{6};$$

$$1^3 + 2^3 + \cdots + (n-1)^3 = \left[\frac{n(n-1)}{2}\right]^2 .]$$

1.8. Mostrare che per ogni intero a:

$$a(a+1)(2a+1) \equiv 0 \pmod 6 .$$

[Suggerimento. Per verifica diretta, facendo variare a nel sistema ridotto di residui minimale in valore assoluto $S = \{-2, -1, 0, 1, 2, 3\}$, oppure osservando che:
$6 \mid a(a+1)(2a+1)$ se e soltanto se $2 \mid a(a+1)(2a+1)$ e $3 \mid a(a+1)(2a+1)$.]

1.9. Mostrare che il seguente polinomio non ha radici intere:

$$f(X) := X^3 - X + 1 .$$

[Suggerimento. Basta osservare che la congruenza $f(X) \equiv 0 \pmod 2$ non ha soluzioni.]

2 Congruenze lineari ed equazioni diofantee lineari

Lo studio della congruenza $f(X) \equiv 0 \pmod{n}$ è particolarmente semplice nel caso in cui $f(X)$ sia un polinomio di grado 1, cioè nel caso di una *congruenza lineare*.

Definizione 2.1. Si chiama *congruenza lineare in una indeterminata X (modulo n)* una congruenza del tipo:

$$aX \equiv b \pmod{n} \tag{1}$$

con $a, b, n \in \mathbb{Z}, n > 0$.

In base alla Definizione 1.23, *una soluzione di* (1) è un intero $\mathring{x}$ tale che $a\mathring{x} \equiv b \pmod{n}$ e due *soluzioni* di (1) sono *distinte* o *incongruenti* se non sono congrue modulo n. Vale il seguente fondamentale risultato:

Teorema 2.2. *Siano $a, b, n \in \mathbb{Z}, n > 0$ e sia $d := \mathrm{MCD}(a, n)$. Allora:*
(1) *la congruenza* (1) *è risolubile se, e soltanto se, $d \mid b$;*
(2) *se $d \mid b$,* (1) *ha esattamente d soluzioni distinte* $\pmod{n}$*, che sono date da:*

$$x_k = \alpha^* \cdot b/d + k \cdot n/d, \text{ al variare di } k \text{ con } 0 \leqslant k \leqslant d-1;$$

dove α^* è un inverso aritmetico di $a/d \pmod{n/d}$ (cfr. Proposizione 1.14(a)).

Dimostrazione. **(1)** Se (1) è risolubile, allora esiste $\mathring{x} \in \mathbb{Z}$ in modo tale che $n \mid (a\mathring{x} - b)$, cioè esiste $k \in \mathbb{Z}$ tale che $a\mathring{x} - b = nk$. Quindi $d \mid (a\mathring{x} - nk) = b$. Viceversa, se $b = d\delta$ e $d = ar + ns$ (identità di Bézout), con $\delta, r, s \in \mathbb{Z}$, allora $ar\delta + ns\delta = b$ e quindi $r\delta$ è soluzione di (1).

Alla dimostrazione di **(2)** premettiamo il seguente lemma:

Lemma 2.3. *Siano $a, b, n \in \mathbb{Z}, n > 0$. Se $\mathrm{MCD}(a, n) = 1$, la congruenza* (1) *ha un'unica soluzione $\mathring{x} \pmod{n}$, e risulta:*

$$\mathring{x} \equiv a^* b \pmod{n},$$

dove a^* è un'inverso aritmetico di a (modulo n).

Dimostrazione (Lemma 2.3)**.** È immediata conseguenza della Proposizione 1.3 (5), della Definizione 1.13 e della Proposizione 1.14.
Infatti, $a\mathring{x} \equiv aa^*b \equiv b \pmod{n}$. Viceversa, se x è tale che $ax \equiv b \pmod{n}$, allora moltiplicando ambo i membri della congruenza per a^*, otteniamo che $x \equiv a^*b \pmod{n}$. $\square$

Dimostrazione (Teorema 2.2 (2)). Poichè $d \mid b$ e $\mathrm{MCD}(a,n) = d$, esistono $\alpha, \beta, \nu \in \mathbb{Z}$ tali che $b = d\beta, a = d\alpha, n = d\nu$ e $\mathrm{MCD}(\alpha, \nu) = 1$. Per (1), esiste $x \in \mathbb{Z}$ tale che $ax \equiv b \pmod{n}$ e dunque $\alpha dx \equiv \beta d \pmod{n}$.
Dalla Proposizione 1.3 (11), si ha $\alpha x \equiv \beta \pmod{\nu}$ e quindi, dal Lemma 2.3, $x \equiv \alpha^* \beta \pmod{\nu}$. Dunque, esiste $t \in \mathbb{Z}$ tale che $x = \alpha^* b/d + tn/d$. Se t non è compreso tra 0 e $d-1$ allora, dividendo t per d, otteniamo $t = dq + k$, con $0 \leqslant k < d-1$, e quindi $x = \alpha^* b/d + tn/d \equiv \alpha^* b/d + kn/d = x_k \pmod{n}$.
D'altra parte, tenendo presente che $d \mid a$ è facile verificare che x_k è una soluzione di (1) e per ogni k, con $0 \leqslant k \leqslant d-1$.
Se h, k sono interi tali che $0 \leqslant h \leqslant d-1, \quad 0 \leqslant k \leqslant d-1$ e se

$$\alpha^* b/d + hn/d \equiv \alpha^* b/d + kn/d \pmod{n},$$

allora $hn/d \equiv kn/d \pmod{n}$. Dal momento che $\mathrm{MCD}(n, n/d) = n/d$ e $n/(n/d) = d$, cancellando (cfr. Proposizione 1.9), otteniamo $h \equiv k \pmod{d}$, cioè $h = k$, essendo $0 \leqslant h, k \leqslant d-1$. Se invece $h \equiv k \pmod{d}$, allora si ha subito $\alpha^* b/d + hn/d \equiv \alpha^* b/d + kn/d \pmod{n}$. Dunque la (2) è completamente dimostrata. $\square$

Il Teorema 2.2 riduce in pratica la ricerca delle soluzioni di (1) alla determinazione di α^*, cioè alla ricerca delle soluzioni della congruenza:

$$\alpha X \equiv 1 \pmod{\nu}, \tag{1'}$$

(con $\alpha := a/d$, $\nu := n/d$). Su questo problema ritorneremo tra breve.

Osservazione 2.4. Sfruttando meglio l'argomentazione della dimostrazione del Teorema precedente, si ottiene un metodo effettivo per il calcolo di tutte (e sole) le d soluzioni di (1) che sono date da:

$$x_k = \mathring{x} + k\frac{n}{d}, \text{ al variare di } k \text{ con } 0 \leqslant k \leqslant d-1,$$

dove $\mathring{x}$ è una soluzione della congruenza (1') (univocamente determinata $(\mathrm{mod}\ \nu)$).

Il problema della ricerca delle soluzioni di una congruenza lineare in una indeterminata è equivalente a quello della ricerca delle soluzioni di una equazione diofantea in due indeterminate.
Infatti, $\mathring{x}$ è una soluzione di $aX \equiv b \pmod{n}$ se, e soltanto se, esiste $\mathring{y} \in \mathbb{Z}$ tale che $n\mathring{y} = a\mathring{x} - b$, ovvero se, e soltanto se, $(\mathring{x}, \mathring{y})$ è soluzione dell'equazione diofantea $aX - nY = b$.
È comunque opportuno esaminare direttamente la risoluzione di queste equazioni diofantee, in quanto ciò offrirà un diverso punto di vista per la risoluzione delle congruenze lineari.

Teorema 2.5. *L'equazione diofantea lineare:*

$$aX + cY = b \tag{2}$$

è risolubile se, e soltanto se, $d \mid b$, *dove* $d := \mathrm{MCD}(a, c)$. *Se* $(\mathring{x}, \mathring{y})$ *è una particolare soluzione di* (2), *tutte e sole le soluzioni di* (2) *sono date da* (x_t, y_t), *con:*

$$x_t := \mathring{x} + \frac{c}{d}t, \quad y_t := \mathring{y} - \frac{a}{d}t,$$

al variare di $t \in \mathbb{Z}$.

Dimostrazione. Siano $\alpha, \gamma \in \mathbb{Z}$ tali che $d\alpha = a, d\gamma = c$ e $\mathrm{MCD}(\alpha, \gamma) = 1$. Se $(\mathring{x}, \mathring{y})$ è soluzione di (2), si ha $b = a\mathring{x} + c\mathring{y} = d(\alpha\mathring{x} + \gamma\mathring{y})$ e dunque $d \mid b$. Viceversa, siano $\beta, r, s \in \mathbb{Z}$ tali che $b = d\beta$ e $d = ar + cs$ (identità di Bézout). Si verifica subito che $\mathring{x} := \beta r$, $\mathring{y} := \beta s$ è una soluzione di (2).
Proviamo ora la seconda parte dell'enunciato. Sia $(\mathring{x}, \mathring{y})$ una fissata soluzione di (2). È immediato verificare che ogni coppia (x_t, y_t) (al variare di $t \in \mathbb{Z}$) è ancora una soluzione di (2).
Viceversa, sia (x', y') soluzione di (2). Si ha allora $a\mathring{x} + c\mathring{y} = b = ax' + cy'$, ovvero $a(\mathring{x} - x') = c(y' - \mathring{y})$, da cui $\alpha(x' - \mathring{x}) = \gamma(\mathring{y} - y')$. In base al Lemma di Euclide, $\gamma \mid (\mathring{x} - x')$, quindi esiste $t \in \mathbb{Z}$ tale che $x' - \mathring{x} = \gamma t$ e, dunque, $-\alpha\gamma t = \gamma(y' - \mathring{y})$. Pertanto, si ha $x' = \mathring{x} + (c/d)t$ e $y' = \mathring{y} - (a/d)t$, da cui la tesi. □

Torniamo a considerare la congruenza lineare (1):

$$aX \equiv b \pmod{n}.$$

Da quanto precede, è chiaro che il problema della ricerca di *tutte* le soluzioni di (1) si riduce alla ricerca di *una* soluzione dell'equazione diofantea nelle indeterminate X ed Y:

$$aX - nY = b,$$

oppure, come già osservato, alla ricerca di *un* inverso aritmetico di a/d (modulo n/d). Nel primo caso, *una* soluzione può essere esplicitamente trovata (come indicato nella dimostrazione del Teorema 2.5 riducendo il problema alla risoluzione dell'equazione diofantea nelle indeterminate X' ed Y':

$$aX' + nY' = d$$

(ovvero, calcolando i coefficienti della relazione di Bézout che esprime $d := \mathrm{MCD}(a, n) = \mathrm{MCD}(a, -n)$ in funzione di a e $-n$) e ciò può essere fatto applicando l'algoritmo euclideo delle divisioni successive.
Nel secondo caso, ci si è ricondotti allo studio di una congruenza del tipo:

$$aX \equiv 1 \pmod{n} \quad \text{con} \quad \mathrm{MCD}(a, n) = 1,$$

la cui unica soluzione (cfr. Lemma 2.3) fornisce appunto l'inverso aritmetico a^* di $a \pmod n$. Perverremo ad un metodo effettivo per la determinazione esplicita di a^* nel paragrafo successivo, come conseguenza del Teorema di Euler-Fermat. Per il momento concludiamo il paragrafo con alcune definizioni e risultati utili per il seguito e, comunque, propedeutici a tale teorema.

Proposizione 2.6. *Sia n un intero $n \geqslant 2$ ed $S := \{0, 1, \ldots, n-1\}$ il sistema completo di residui (modulo n) minimo. Sia, inoltre, S^* il sottoinsieme di S così definito:*

$$S^* := \{k \in S \quad : \quad \mathrm{MCD}(k, n) = 1\}.$$

Un intero a ammette inverso aritmetico (modulo n) se, e soltanto se, esiste $k \in S^*$ in modo tale che $a \equiv k \pmod n$.

Dimostrazione. Tenuto conto della Proposizione 1.14 (a) e dell'Esercizio 1.1 otteniamo che a ammette inverso aritmetico (modulo n) se, e soltanto se, $\mathrm{MCD}(a, n) = 1$, ovvero se, e soltanto se, esiste $k \in S$ tale che $a \equiv k \pmod n$ e $\mathrm{MCD}(k, n) = 1$. La conclusione è ormai evidente. □

Definizione 2.7. Si chiama *sistema ridotto di residui (modulo n)* ogni insieme $S^* := \{k_1, \ldots, k_t\}$, con $k_i \in \mathbb{Z}$ per $1 \leqslant i \leqslant t$, tale che, per ogni $a \in \mathbb{Z}$ verificante la condizione $\mathrm{MCD}(a, n) = 1$, esiste un unico $k_i \in S^*$ tale che $a \equiv k_i \pmod n$.

È subito visto che $\mathrm{MCD}(n, k_i) = 1$, per ogni $k_i \in S^*$.

Osservazione 2.8. Lo studio dei sistemi ridotti di residui può essere efficacemente effettuato studiando il gruppo delle unità degli anelli del tipo $\mathbb{Z}/n\mathbb{Z}$. Lasciamo al lettore il piacere di esprimere in termini gruppali la teoria che svilupperemo nel seguente scorcio di paragrafo e nel paragrafo successivo.

Definizione 2.9. Si chiama *indicatore* (o *funzione φ*) *di Eulero* l'applicazione $\varphi : \mathbb{N}^+ \to \mathbb{N}$ che associa ad ogni intero $n > 0$ il numero $\varphi(n)$ degli interi compresi tra 1 e $n - 1$ che sono relativamente primi con n.

Si verifica facilmente che ogni sistema ridotto di residui (modulo n) può essere posto in corrispondenza biunivoca con quello definito nella Proposizione 2.6, che chiameremo *sistema ridotto di residui (modulo n) minimo positivo* il quale, ovviamente, ha cardinalità $\varphi(n)$. Dunque:

Proposizione 2.10. *Ogni sistema ridotto di residui (modulo n) ha cardinalità $\varphi(n)$.* □

2. Esercizi e Complementi

2.1. Trovare tutte le eventuali soluzioni delle congruenze:

$$\begin{aligned} &\textbf{(a)} \quad 15X \equiv 9 \pmod{25} \\ &\textbf{(b)} \quad 17X \equiv 14 \pmod{21} \\ &\textbf{(c)} \quad 3X \equiv 6 \pmod{9} \end{aligned}$$

[Suggerimento: **(a)** $\mathrm{MCD}(15, 25) = 5$, $5 \nmid 9$, non è risolubile.
(b) $\mathrm{MCD}(17, 21) = 1$, quindi la congruenza ha un'unica soluzione $\pmod{21}$ data da $17^* \cdot 14$ dove $17^* \equiv 5 \pmod{21}$ e quindi $5 \cdot 14 = 70 \equiv 7 \pmod{21}$.
(c) $\mathrm{MCD}(3, 9) = 3 \mid 6$, quindi la congruenza ha 3 soluzioni che sono precisamente: $x_0 = 2, \quad x_1 = 2 + 3 = 5, \quad x_2 = 2 + 2 \cdot 3 = 8 \pmod{9}$.]

2.2. Metodo ricorsivo per la risoluzione di una congruenza lineare in una indeterminata
Siano $a, b, n \in \mathbb{Z}$ con a ed n interi positivi e $\mathrm{MCD}(a, n) = 1$.
(a) Mostrare che se $x \in \mathbb{Z}$ è la soluzione della congruenza:

$$aX \equiv b \pmod{n}, \tag{$*$}$$

allora x è anche soluzione della congruenza:

$$rX \equiv -bq \pmod{n}, \tag{$*'$}$$

dove $n = a \cdot q + r$ con $q, r \in \mathbb{Z}$ ed $0 < r \leqslant a - 1$.
(b) Mostrare che, se si può iterare la procedura descritta in **(a)**, dopo un numero finito di passi la soluzione di $(*)$ è anche soluzione di una congruenza del tipo:

$$X \equiv c \pmod{n}, \tag{$**$}$$

per un qualche $c \in \mathbb{Z}$.
(c) Risolvere, con il metodo sopra descritto, la congruenza

$$6X \equiv 7 \pmod{23}.$$

[Suggerimento: **(a)** Si noti che se $ax \equiv b \pmod{n}$ allora:
$rx = nx - aqx \equiv -bq \pmod{n}$.
(b) È ovvia perché se $a \neq 1$ allora $0 < r < a$.
(c) Si noti che $23 = 6 \cdot 3 + 5$ e quindi:
- da $23 = 6 \cdot 3 + 5$ passiamo a $5X \equiv -7 \cdot 3 \equiv 2 \pmod{23}$;
- da $23 = 5 \cdot 4 + 3$ passiamo a $3X \equiv -2 \cdot 4 \equiv 15 \pmod{23}$;
- da $23 = 3 \cdot 7 + 2$ passiamo a $2X \equiv -15 \cdot 7 \equiv 10 \pmod{23}$;
- da $23 = 2 \cdot 11 + 1$ passiamo a $X \equiv -10 \cdot 11 \equiv 5 \pmod{23}$.]

2.3. Determinare tutte le eventuali soluzioni delle seguenti equazioni diofantee lineari in due indeterminate:
(a) $2X + 5Y = 11$;
(b) $21X - 14Y = 147$;
(c) $14X + 2Y = 9$.
[Soluzioni:**(a)** $x = 3 + 5t, y = 1 - 2t, t \in \mathbb{Z}$.
(b) $x = 7 - (14/7)t, y = -(21/7)t, t \in \mathbb{Z}$.
(c) Non ha soluzioni.]

2.4. (Sylvester, 1884)
Siano a, b, n tre interi positivi con $\mathrm{MCD}(a,b) = 1$. Mostrare che:
(a) Per ogni $c > ab$, l'equazione

$$aX + bY = c \qquad (*_c)$$

ha soluzioni $(x, y) \in \mathbb{N}^+ \times \mathbb{N}^+$.
(b) Posto $g = g(a,b) := ab - a - b$, per ogni $c > g$, l'equazione $(*_c)$ ha soluzioni $(x, y) \in \mathbb{N} \times \mathbb{N}$. Il numero $g(a,b)$ è detto *numero di Frobenius*.
(c) Se $c = ab$, l'equazione $(*_c)$ non ha soluzioni in $\mathbb{N}^+ \times \mathbb{N}^+$.
(d) Se $c = g(a,b)$, l'equazione $(*_c)$ non ha soluzioni in $\mathbb{N} \times \mathbb{N}$.
(e) Se $c_1, c_2 \in \mathbb{N}$ e se $(*_{c_1})$ e $(*_{c_2})$ sono risolubili in $\mathbb{N}^+ \times \mathbb{N}^+$ (rispettivamente, in $\mathbb{N} \times \mathbb{N}$), allora $(*_{c_1+c_2})$ è risolubile in $\mathbb{N}^+ \times \mathbb{N}^+$ (rispettivamente, in $\mathbb{N} \times \mathbb{N}$).
(f) $g(a,b)$ è sempre dispari.
(g) Esattamente per $\dfrac{(g(a,b)+1)}{2}$ elementi c, con $0 \leqslant c \leqslant g(a,b)$, l'equazione $(*_c)$ è risolubile in $\mathbb{N} \times \mathbb{N}$.

Data l'equazione

$$5X + 7Y = c \qquad (**)$$

(h) Determinare una soluzione in $\mathbb{N} \times \mathbb{N}$ di $(**)$, quando $c = 24$.
(i) Determinare tutti i valori di c, con $0 \leqslant c \leqslant 23$, per i quali $(**)$ è risolubile in $\mathbb{N} \times \mathbb{N}$.
[Suggerimento: Innanzitutto, utilizzando il Teorema 2.5 e scegliendo opportunamente il parametro $t \in \mathbb{Z}$, è possibile trovare $u, v \in \mathbb{N}^+$ in modo tale che:

$$au - bv = 1.$$

(a) Si noti che $auc - bvc = c > ab$, dunque $\frac{uc}{b} - \frac{vc}{a} > 1$ quindi esiste $s \in \mathbb{N}$ tale che $\frac{uc}{b} > s > \frac{vc}{a}$. Si vede che $(x := uc - bs,\ y := as - vc) \in \mathbb{N}^+ \times \mathbb{N}^+$ è una soluzione di $(*_c)$.
(b) Se $ab \geqslant c > ab - a - b$, allora $c' := c + a + b > ab$, quindi $(*_{c'})$ ha una soluzione $(x', y') \in \mathbb{N}^+ \times \mathbb{N}^+$. È subito visto che $(x' - 1, y' - 1) \in \mathbb{N} \times \mathbb{N}$ è una soluzione di $(*_c)$.
(c) Se $ax + by = ab$, allora si perviene facilmente ad un assurdo utilizzando il Lemma di Euclide.
(d) segue facilmente da **(c)**.
(e) È immediato che se (x_i, y_i) è soluzione di $(*_{c_i})$, allora $(x_1 + x_2, y_1 + y_2)$ è soluzione di $(*_{c_1+c_2})$.
(f) Non potendo essere a e b entrambi pari (perché relativamente primi), è subito visto che, in ogni caso, $ab - a - b \equiv 1 \pmod 2$.
(g) Si noti che se c varia tra 0 e g anche $g - c$ varia tra 0 e g e quindi l'applicazione

$$\{c : 0 \leqslant c \leqslant g\} \longrightarrow \{c : 0 \leqslant c \leqslant g\} \quad c \longmapsto g - c$$

è una biiezione. Inoltre, se $(*_c)$ è risolubile in $\mathbb{N} \times \mathbb{N}$, $(*_{g-c})$ non può essere risolubile in $\mathbb{N} \times \mathbb{N}$, altrimenti (per il punto **(e)**) $(*_{g=c+(g-c)})$ sarebbe risolubile in $\mathbb{N} \times \mathbb{N}$. Quindi, il numero $n = n(a,b)$ dei valori di c, per $0 \leq c \leq g$, è al più uguale alla metà del numero degli elementi dell'insieme $\{c : 0 \leqslant c \leqslant g\}$, cioè $n \leq (g+1)/2$.

Per mostrare che vale l'uguaglianza, procediamo nella maniera seguente. Determiniamo il numero $\nu = \nu(a,b)$ dei valori di c, per $0 \leq c \leq ab$, per i quali l'equazione $(*_c)$ *non* ha soluzioni in $\mathbb{N} \times \mathbb{N}$. Poiché, per ogni c, con $g+1 \leq c\,(\leq ab)$, sappiamo che l'equazione $(*_c)$ ha soluzioni in $\mathbb{N} \times \mathbb{N}$ (punto **(b)**), allora ν deve necessariamente coincidere con il numero dei valori di c, con $0 \leq c \leq g\,(< ab)$, per i quali $(*_c)$ non ha soluzioni in $\mathbb{N} \times \mathbb{N}$, cioè $\nu = g + 1 - n$. Se mostriamo che $\nu \leq (g+1)/2$, allora potremo dedurre da quanto sopra che $\nu = n = (g+1)/2$.
Per mostrare che $\nu \leq (g+1)/2$ facciamoci aiutare dall'intuizione geometrica.
Chiamiamo con ℓ_c la retta del piano cartesiano definita dall'equazione $(*_c)$. Tracciamo nel piano cartesiano l'insieme R dei punti a coordinate intere (x,y), con $0 \leq x \leq b$, $0 \leq y \leq a$. Notiamo che R conta $r := (a+1)(b+1)$ punti. Quando $c = ab$, la retta ℓ_{ab} passa soltanto per i punti $(b,0)$ e $(0,a)$ di R e suddivide l'insieme R in due insiemi "triangolari" formati da $t := (r-2)/2$ punti ciascuno. Denotiamo con T il sottoinsieme "triangolare" di R che si trova "al di sotto" della retta ℓ_{ab}.
Se $0 \leq c \leq 2ab$, allora è facile assicurarsi che l'equazione $(*_c)$ ha soluzioni in $\mathbb{N} \times \mathbb{N}$ se e soltanto se la retta ℓ_c passa per almeno un punto di R.
Si noti, poi, che se $c \neq ab$ e se la retta ℓ_c passa per un punto di R, allora passa soltanto per tale punto di R. Infatti, se $(x,y), (x',y')$ sono due punti di R che soddisfano alla stessa equazione $(*_c)$ allora $a(x-x') = b(y'-y)$. Essendo $\mathrm{MCD}(a,b) = 1$, si ricava che $x - x' = kb$ e $y' - y = ka$, per qualche intero k. Essendo $(x,y), (x',y') \in R$, si ricava immediatamente che $|k| = 1$.
Notiamo, poi, che:
• i punti di T sono in numero di $t = ((a+1)(b+1) - 2)/2 = (ab + a + b - 1)/2$;
• per ogni punto $(x,y) \in T$ passa la retta ℓ_c, dove $c = ax + by$ e risulta $0 \leq c < ab$.
Pertanto, il numero ν è al più uguale al numero ottenuto dalla differenza tra il numero dei valori possibili per c, quindi $0 \leq c < ab$, (cioè, ab), meno il numero dei valori descritti da $c = ax + by$, quando (x,y) varia in T, (cioè, t). Quindi, $\nu \leq ab - ((a+1)(b+1) - 2)/2 = (ab - a - b + 1)/2 = (g+1)/2$.
(h) In questo caso $u = 3, v = 2$, quindi $\dfrac{3 \cdot 24}{7} > 10 > \dfrac{2 \cdot 24}{5}$ dunque $(2 = 3 \cdot 24 - 7 \cdot 10, 2 = 5 \cdot 10 - 2 \cdot 24)$ è una soluzione di $(**)$ per $c = 24$.
(i) Si noti che $g = g(5,7) = 23$ e, quindi, $(g+1)/2 = 12$. I 12 valori di c richiesti sono i seguenti: $c = 0, 5, 7, 10, 12, 14, 15, 17, 19, 20, 21, 22$.]

2.5. (a) Sia $m \geqslant 2$ e siano $a_1, \ldots, a_m$ interi non tutti nulli. Scelto $b \in \mathbb{Z}$ e posto $d := \mathrm{MCD}(a_1, \ldots, a_m)$, verificare che l'equazione diofantea:

$$a_1X_1 + a_2X_2 + \cdots + a_mX_m = b$$

è risolubile se, e soltanto se, $d \mid b$.
(b) Metodo algoritmico per la risoluzione della equazione diofantea lineare:

$$a_1X_1 + \cdots + a_mX_m = b \qquad (*)$$

dove $b, a_i \in \mathbb{Z}, a_i \neq 0$ per $1 \leqslant i \leqslant m$.

I Riduzione. Non è restrittivo limitarsi al caso in cui $a_i \in \mathbb{N}^+$ per ogni i. Infatti se $a_i < 0$, basta sostituire tali coefficienti con $-a_i$ e cambiare segno alla indeterminata X_i.

II Riduzione. Non è restrittivo supporre che $a_i \neq a_j$ se $i \neq j$. Perché se ad esempio $a_1 = a_2$, ponendo $X := X_1 + X_2$, abbiamo la seguente equazione diofantea:

$$a_1 X + a_3 X_3 + \cdots + a_m X_m = b. \qquad (**)$$

Una soluzione $(x_1, \cdots, x_m)$ di $(*)$ determina una soluzione di $(**)$ $(x_1 + x_2, x_3, \cdots, x_m)$. Mentre, una soluzione $(x, x_3, \cdots, x_m)$ determina infinite soluzioni di $(*)$, ottenute ponendo $x_2 := x - x_1$ e facendo variare comunque $x_1 \in \mathbb{Z}$.

Procedimento ricorsivo di risoluzione. Supponiamo che $a_i \in \mathbb{N}^+$ e che $a_i \neq a_j$, per $1 \leqslant i \neq j \leqslant m$, e supponiamo inoltre, per fissare le idee, che $a_1 = \max\{a_1, \cdots, a_m\}$. Dunque, dividendo a_1 per a_2, otteniamo la seguente relazione:

$$a_1 = a_2 q + r \quad \text{con} \quad 0 \leqslant r < a_2 (< a_1), \quad q \in \mathbb{Z}.$$

Poniamo

$$X_1' := q X_1 + X_2, \quad X_2' := X_1, \quad a_1' := a_2, \quad a_2' := r.$$

Dunque $(*)$ diventa:

$$a_1' X_1' + a_2' X_2' + a_3 X_3 + \cdots + a_m X_m = b. \qquad (*')$$

Una soluzione $(x_1, \cdots, x_m)$ di $(*)$ determina canonicamente una soluzione di $(*')$: $(q x_1 + x_2, x_1, x_3, \cdots, x_m)$. Viceversa, la soluzione $(x_1', x_2', x_3, \cdots, x_m)$ di $(*')$ determina la soluzione $(x_2', x_1' - q x_2', x_3, \cdots, x_m)$ di $(*)$.
Pertanto, ci siamo ricondotti ad una nuova equazione diofantea lineare $(*')$ per la quale $\max\{a_1', a_2', a_3, \cdots, a_m\} < \max\{a_1, a_2, a_3, \cdots, a_m\}$.

Dimostrare che questo processo conduce, dopo un numero finito di passi, ad una equazione in due indeterminate (per la quale sappiamo descrivere tutte le soluzioni) oppure ad un'equazione in cui almeno uno dei coefficienti è uguale ad 1.
Si noti che, se uno dei coefficienti, ad esempio a_i, è uguale ad 1, allora ovviamente $(*)$ è risolubile. Tutte le soluzioni di $(*)$ si ottengono ponendo

$$x_i := b - (a_1 x_1 + \cdots + a_{i-1} x_{i-1} + a_{i+1} x_{i+1} + \cdots + a_m x_m)$$

e facendo variare comunque $x_1, x_2, \cdots, x_{i-1}, x_{i+1}, \cdots, x_m \in \mathbb{Z}$.

[Osservazioni **(b)** . (1) Notiamo che, se esiste un coefficiente a_i, per $2 \leqslant i \leqslant m$, tale che $a_i \mid a_1$, conviene dividere a_1 per a_i. Infatti, in tal caso, $a_1 = q a_i + r$ con $r = 0$ e, quindi, nell'equazione diofantea $(*')$, determinata in questo modo da $(*)$, appariranno già al più $m - 1$ indeterminate.
(2) È subito visto che se $(*)$ è risolubile e se $(\mathring{x}_1, \cdots, \mathring{x}_m)$ è una soluzione di $(*)$, allora $(x_1, \cdots, x_m)$ con

$$x_i = \mathring{x}_i + a_m t_i \qquad 1 \leqslant i \leqslant m-1$$
$$x_m = \mathring{x}_m - \sum_{i=1}^{m-1} a_i t_i$$

è ancora una soluzione di $(*)$, al variare comunque di $t_1, \cdots, t_{m-1} \in \mathbb{Z}$. Non è vero, in generale, che tutte le soluzioni di $(*)$ siano del tipo sopra descritto.

Ad esempio, se consideriamo l'equazione diofantea $2X + 4Y = 6$, allora $(1, 1)$ è una soluzione. Però $(3, 0)$, che è un'altra soluzione di tale equazione, non si trova nell'insieme infinito di soluzioni $(1 + 4t, 1 - 2t)$, descritto al variare di $t \in \mathbb{Z}$. (Si osservi che ciò -ovviamente- non contraddice il Teorema 2.5.)]

(c) Risoluzione di un'equazione diofantea lineare in tre indeterminate
Si consideri l'equazione diofantea lineare in tre indeterminate

$$aX + bY + cZ = d \quad \text{con } \mathrm{MCD}(a, b, c) \mid d. \tag{$*$}$$

Sotto tale condizione $(*)$ è risolubile. Per determinare le sue soluzioni associamo a $(*)$ due equazioni diofantee lineari ciascuna in due indeterminate:

$$aX_1 + \mathrm{MCD}(b, c)X_2 = d, \tag{$*_1$}$$
$$bY_1 + cY_2 = \mathrm{MCD}(b, c) \tag{$*_2$}$$

Essendo $\mathrm{MCD}(a, \mathrm{MCD}(b, c)) = \mathrm{MCD}(a, b, c)$, è evidente che $(*)$ è risolubile se e soltanto se $(*_1)$ è risolubile. Inoltre, è noto che se $(\mathring{x}_1, \mathring{x}_2)$ è una soluzione di $(*_1)$ allora tutte le soluzioni di $(*_1)$ sono descritte da:

$$x_1 = \mathring{x}_1 + (\frac{\mathrm{MCD}(b, c)}{\mathrm{MCD}(a, b, c)})t$$
$$x_2 = \mathring{x}_2 - (\frac{a}{\mathrm{MCD}(a, b, c)})t$$

al variare comunque di $t \in \mathbb{Z}$.
Sappiamo che $(*_2)$ è sempre risolubile (Teorema 2.5). Sia $(\mathring{y}_1, \mathring{y}_2)$ una sua soluzione. Mostrare che tutte le soluzioni di $(*)$ sono descritte da:

$$x = \mathring{x}_1 + (\frac{\mathrm{MCD}(b, c)}{\mathrm{MCD}(a, b, c)})t$$
$$y = \mathring{y}_1\mathring{x}_2 - \mathring{y}_1\,(\frac{a}{\mathrm{MCD}(a, b, c)})t + (\frac{c}{\mathrm{MCD}(b, c)})s$$
$$z = \mathring{y}_2\mathring{x}_2 - \mathring{y}_2\,(\frac{a}{\mathrm{MCD}(a, b, c)})t - (\frac{b}{\mathrm{MCD}(b, c)})s$$

al variare di $t, s \in \mathbb{Z}$.
[Suggerimento: **(c)** notiamo che:
$d = aX_1 + \mathrm{MCD}(b, c)X_2 = aX_1 + (bY_1 + cY_2)X_2 = aX_1 + bY_1X_2 + cY_2X_2$, ed essendo anche $d = aX + bY + cZ$, allora, per la validità della uguaglianza formale precedente, dobbiamo avere:

$$X = X_1\,, \quad Y = Y_1X_2\,, \quad Z = Y_2X_2\,,$$

e se $b = b'\mathrm{MCD}(b, c)$ e $c = c'\mathrm{MCD}(b, c)$, con $\mathrm{MCD}(b', c') = 1$, dobbiamo avere anche:

$$X_2 = b'Y + c'Z\,.$$

Da ciò ricaviamo che ogni soluzione (x, y, z) di $(*)$ si può esprimere nella forma seguente $(x_1, \mathring{y}_1x_2, \mathring{y}_2x_2)$, dove (x_1, x_2) è una soluzione di $(*_1)$ ed $(\mathring{y}_1, \mathring{y}_2)$ è una qualche soluzione di $(*_2)$.

Dal momento che, quando $(\mathring{y}_1, \mathring{y}_2)$ varia tra le soluzioni $bY_1 + cY_2 = \mathrm{MCD}(b,c)$, $(\mathring{y}_1 x_2, \mathring{y}_2 x_2)$ varia tra le soluzioni di

$$bY + cZ = \mathrm{MCD}(b,c)x_2, \qquad (**_2)$$

allora l'insieme $\{(\mathring{y}_1 x_2, \mathring{y}_2 x_2) : (\mathring{y}_1, \mathring{y}_2)$ varia tra le soluzioni di $(*_2)\}$ coincide con l'insieme $\{(y,z) : (y,z)$ è una soluzione di $(**_2)\}$.
Poichè $(\mathring{y}_1 x_2, \mathring{y}_2 x_2)$ è una soluzione di $(**_2)$, allora una qualunque soluzione di $(**_2)$ è data da:

$$y = \mathring{y}_1 x_2 + (\frac{c}{\mathrm{MCD}(b,c)})s$$
$$z = \mathring{y}_2 x_2 - (\frac{b}{\mathrm{MCD}(b,c)})s$$

al variare di $s \in \mathbb{Z}$.
In conclusione, una qualunque soluzione di $(*)$ è del tipo:

$$x = x_1 = \mathring{x}_1 + \frac{\mathrm{MCD}(b,c)}{\mathrm{MCD}(a,b,c)})t$$
$$y = \mathring{y}_1 x_2 + (\frac{c}{\mathrm{MCD}(b,c)})s = \mathring{y}_1 \mathring{x}_2 - \mathring{y}_1\ (\frac{a}{\mathrm{MCD}(a,b,c)})t + (\frac{c}{\mathrm{MCD}(b,c)})s$$
$$z = \mathring{y}_2 x_2 - (\frac{b}{\mathrm{MCD}(b,c)})s = \mathring{y}_2 \mathring{x}_2 - \mathring{y}_2\ (\frac{a}{\mathrm{MCD}(a,b,c)})t - (\frac{b}{\mathrm{MCD}(b,c)})s$$

al variare di $t, s \in \mathbb{Z}$.]

(d) Determinare tutte le soluzioni dell'equazione diofantea:

$$6X - 4Y + 8Z = 12.$$

[Soluzione. **(d)** Dal momento che $2 = \mathrm{MCD}(6,-4,8) \mid 12$ e che $\mathrm{MCD}(-4,8) = 4$, allora consideriamo le seguenti equazioni diofantee lineari in due indeterminate:

$$6X_1 + 4X_2 = 12 \quad \text{ovvero} \quad 3X_1 + 2X_2 = 6 \qquad (*_1)$$
$$-4Y_1 + 8Y_2 = 4 \quad \text{ovvero} \quad Y_1 - 2Y_2 = -1 \qquad (*_2)$$

È subito visto che $(1,1)$ è una soluzione della seconda equazione e $(2,0)$ è una soluzione della prima. Pertanto, le soluzioni dell'equazione diofantea assegnata sono date da:

$$x = 2 + 2t$$
$$y = \left(\frac{-6}{2}\right)t + \left(\frac{8}{4}\right)s = -3t + 2s$$
$$z = \left(\frac{-6}{2}\right)t + \left(\frac{4}{4}\right)s = -3t + s$$

al variare comunque di $t, s \in \mathbb{Z}$.
Quindi, ad esempio, per $s = t = 0$, abbiamo $(2,0,0)$; per $t = -1$ ed $s = 0$, abbiamo $(0,3,3)$; per $t = 0$ ed $s = 1$ abbiamo $(2,2,1)$; per $t = 1$ ed $s = 0$ abbiamo $(4,-3,-3)$; per $t = 1$ ed $s = 1$ abbiamo $(4,-1,-2)$.]

2.6. Mostrare che la congruenza $aX + bY \equiv c \pmod{n}$ è risolubile se e soltanto se $d := \mathrm{MCD}(a, b, n) \mid c$. In tal caso ha esattamente dn soluzioni incongruenti.
[Soluzione. La prima affermazione discende dal fatto che $aX + bY \equiv c \pmod{n}$ è risolubile se e soltanto se è risolubile l'equazione diofantea in tre indeterminate $aX + bY - nZ = c$.
Per quanto riguarda la seconda affermazione, notiamo che se $\widetilde{d} := \mathrm{MCD}(b, n)$, per ogni $x \pmod{n}$ che risolve la congruenza $aX \equiv c \pmod{\widetilde{d}}$ allora la congruenza $bY \equiv c - ax \pmod{n}$ è risolubile ed ha esattamente $\widetilde{d}$ soluzioni. D'altro lato, poiché $\mathrm{MCD}(a, \widetilde{d}) = \mathrm{MCD}(a, b, n) = d$, la congruenza $aX \equiv c \pmod{\widetilde{d}}$ è risolubile ed ha d soluzioni $\pmod{\widetilde{d}}$, siano esse $\{x_1, \ldots, x_d\}$.
"Solleviamo" gli elementi x_i determinati $\pmod{\widetilde{d}}$ in elementi $\pmod{n}$: cioè, se k è quell'intero tale che $\widetilde{d}k = n$, allora gli elementi $\{x_i + h\widetilde{d} : 1 \leqslant i \leqslant d,\ 0 \leqslant h \leqslant k - 1\}$ sono gli elementi non congrui $\pmod{n}$ che verificano la congruenza $aX \equiv c \pmod{\widetilde{d}}$.
Per ciascuno dei dk elementi $x \in \{x_i + h\widetilde{d} : 1 \leqslant i \leqslant d,\ 0 \leqslant h \leqslant k - 1\}$, come abbiamo già osservato, la congruenza $bY \equiv c - ax \pmod{n}$ è risolubile ed ammette $\widetilde{d}$ soluzioni. In conclusione, la congruenza assegnata ammette $dk\widetilde{d} = dn$ soluzioni(x, y) non congrue $\pmod{n}$.]

2.7. Determinare tutte le soluzioni della congruenza

$$2X + 4Y \equiv 6 \pmod{8}$$

[Soluzione. $\mathrm{MCD}(2, 4, 8) = 2 \mid 6$ quindi la congruenza è risolubile. Consideriamo la congruenza

$$2X \equiv 6 \pmod{\mathrm{MCD}(4, 8)}$$

Poiché $4 = \mathrm{MCD}(4, 8)$ e $\mathrm{MCD}(2, 4) = 2 \mid 6$, quest'ultima congruenza è risolubile ed ammette 2 soluzioni $\pmod{4}$, che sono $x_1 = 1$ ed $x_2 = 3$.
Gli elementi $x_i + 4h$, $0 \leqslant h \leqslant 1$, sono gli elementi non congrui $\pmod{8}$ che verificano la congruenza $2X \equiv 6 \pmod{4}$. Per ciascuno di tali elementi x (e cioè $x \in \{5, 1, 7, 3\}$) la congruenza $4Y \equiv 6 - 2x \pmod{8}$ è risolubile ed ammette 4 soluzioni non congrue. Precisamente:

$$\begin{aligned} x = 1 \quad &\Rightarrow \quad y = 1, 3, 5, 7 \\ x = 3 \quad &\Rightarrow \quad y = 0, 2, 4, 6 \\ x = 5 \quad &\Rightarrow \quad y = 1, 3, 5, 7 \\ x = 7 \quad &\Rightarrow \quad y = 0, 2, 4, 6 \end{aligned}$$

In tal caso abbiamo 16 coppie (x, y) che sono tutte e sole le soluzioni della congruenza data $\pmod{n}$.]

2.8. Determinare le soluzioni della congruenza:

$$2X + 3Y \equiv 1 \pmod{7}$$

[Soluzione. $(0, 5), (1, 2), (2, 6), (3, 3), (4, 0), (5, 4), (6, 1) \pmod{7}$.]

2.9. (a) Siano $n, c, a_1, \ldots, a_r \in \mathbb{Z}, n > 0$. Posto $d :=\mathrm{MCD}(n, a_1, \ldots, a_r)$, dimostrare che la congruenza:

$$a_1X_1 + \cdots + a_rX_r \equiv c \pmod{n}$$

è risolubile se, e soltanto se, $d \mid c$.
(b) Se la congruenza considerata in (a) è risolubile, allora ammette dn^{r-1} soluzioni distinte.
[Suggerimento. Per **(a)** cfr. Esercizio 2.5 (a), osservando che la congruenza data è risolubile se e soltanto se l'equazione diofantea in $(r+1)$ indeterminate:

$$a_1X_1 + \cdots + a_rX_r + nX_{r+1} = c$$

è risolubile.
Per **(b)** si procede per induzione su r. Se $r = 1$, il risultato è già noto (Teorema 2.2). Il caso $r = 2$ è trattato nell'Esercizio 2.6, il quale indica come procedere nel passo induttivo da $r-1$ ad r indeterminate.]

2.10. Sia $S^* := \{a_1, \ldots, a_{\varphi(n)}\}$ un sistema ridotto di residui (modulo n).
(a) Verificare che se $a \in \mathbb{Z}$ e $\mathrm{MCD}(a, n) = 1$, allora $T^* := \{aa_1, \ldots, aa_{\varphi(n)}\}$ è ancora un sistema ridotto di residui (modulo n).
(b) È vero che, scelto $b \in \mathbb{Z}, \{a_1 + b, \ldots, a_{\varphi(n)} + b\}$ è ancora un sistema ridotto di residui (modulo n)?
[Suggerimento. **(a)** Elementi distinti di S^* sono certo incongruenti $\pmod n$; inoltre risulta $\mathrm{MCD}(aa_i, n) = 1, 1 \leqslant i \leqslant \varphi(n)$; dedurre che ogni elemento di T^* è congruente $\pmod n$ ad un elemento di S^*. **(b)** No: porre ad esempio $n = 4$, $b = 1, S^* = \{1, 3\}$.]

2.11. (a) Siano $a_1, \ldots, a_t, n \in \mathbb{Z}$ tali che $n > 0, t := \varphi(n)$, $\mathrm{MCD}(a_i, n) = 1$ e $a_i \not\equiv a_j \pmod n$, presi comunque i, j tali che $1 \leqslant i, j \leqslant t$ e $i \neq j$. Verificare che $\{a_1, \ldots, a_t\}$ è un sistema ridotto di residui (modulo n).
(b) Provare, con opportuni esempi, che $\varphi(n)$ interi a 2 a 2 incongruenti $(\mathrm{mod}\ n)$ possono non costituire un sistema ridotto di residui (modulo n).
[Suggerimento. Se $a_i = nq_i + l_i$, con $q_i, l_i \in \mathbb{Z}$ e $1 \leqslant l_i \leqslant n-1$, allora $\{l_1, \ldots, l_t\}$ è l'insieme S^* definito nella Proposizione 2.6, cioè il sistema ridotto di residui minimo positivo. Per ogni $a \in \mathbb{Z}$ tale che $\mathrm{MCD}(a, n) = 1$, risulta $a = nq + l$ con $l, q \in \mathbb{Z}$ ed $l \in S^*$. Da ciò segue facilmente **(a)**. Per **(b)**, si prenda $n = 4$, quindi $\varphi(n) = 2$; l'insieme $\{2, 3\}$ non forma un sistema ridotto di residui $\pmod 4$, anche se $2 \not\equiv 3 \pmod 4$. In tal caso si noti che $\mathrm{MCD}(2, 4) \neq 1$.]

2.12. Siano n, m interi positivi relativamente primi. Sia $S^* := \{x_1, \ldots, x_{\varphi(n)}\}$ (rispettivamente, $T^* := \{y_1, \ldots, y_{\varphi(m)}\}$) un sistema ridotto di residui (modulo n) (rispettivamente, (modulo m)). Dimostrare che

$$V^* := \{mx_i + ny_i,\ 1 \leqslant i \leqslant \varphi(n),\ 1 \leqslant j \leqslant \varphi(m)\}$$

è un sistema ridotto di residui (modulo nm).
[Suggerimento. Facendo uso del Lemma di Euclide, si può facilmente verificare che, se $mx_i + ny_j \equiv mx_h + ny_k \pmod{nm}$, allora $x_i \equiv x_h \pmod n$, $y_j \equiv y_k \pmod m$ e dunque $x_i = x_h$ e $y_j = y_k$. Questo assicura che gli elementi di V^* sono tutti distinti (modulo nm) e sono in numero di $\varphi(n)\varphi(m)$. Se poi $z \in \mathbb{Z}$ e $\mathrm{MCD}(z, mn) = 1$, allora necessariamente $\mathrm{MCD}(z, n) = 1$ e $\mathrm{MCD}(z, m) = 1$. Pertanto, utilizzando l'Esercizio 2.10 (a), possiamo trovare un unico i, $1 \leqslant i \leqslant \varphi(n)$, ed un unico j, $1 \leqslant j \leqslant \varphi(m)$, in modo tale che $z \equiv mx_i \pmod n$ e $z \equiv ny_j \pmod m$. Da ciò segue facilmente che $z \equiv mx_i + ny_j \pmod n$ e $z \equiv mx_i + ny_j \pmod m$, dunque $z \equiv mx_i + ny_j \pmod{nm}$.]

2.13. **(a)** Mostrare che se n ed m sono interi positivi e $\mathrm{MCD}(n,m) = 1$, allora $\varphi(nm) = \varphi(n)\varphi(m)$.
(b) Se p è primo ed $e \geqslant 1$, mostrare che:

$$\varphi(p^e) = p^e - p^{e-1} = p^e \left(1 - \frac{1}{p}\right).$$

(c) Se $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ con p_i primo, $e_i \geqslant 1, p_i \neq p_j$ se $1 \leqslant i \neq j \leqslant r$, allora

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

[Suggerimento. **(a)** È una conseguenza immediata dell'Esercizio 2.12. **(b)** Basta notare che gli interi tra 1 e p^e che sono divisibili per p sono del tipo kp, con k che varia in tutti i modi possibili tra 1 e p^{e-1}. **(c)** Discende da (a) e (b).]

2.14. Siano $a, b, c, d, e, f, n \in \mathbb{Z}$ con $n \geqslant 2$. Poniamo

$$\Delta := ad - bc.$$

Consideriamo il seguente sistema di due congruenze lineari in due incognite:

$$\begin{cases} aX + bY & \equiv e \pmod{n} \\ cX + dY & \equiv f \pmod{n} \end{cases} \qquad (*_n)$$

Se $\mathrm{MCD}(\Delta, n) = 1$ e se Δ^* è l'inverso aritmetico di $\Delta \pmod{n}$, allora mostrare che tale sistema ha un'unica soluzione $(\mathrm{mod}\ n)$ data da:

$$x \equiv \Delta^*(de - bf) \pmod{n},$$
$$y \equiv \Delta^*(af - ce) \pmod{n}.$$

[Suggerimento. Innanzitutto, se $\mathrm{MCD}(\Delta, n) = 1$ allora necessariamente deve essere $\mathrm{MCD}(a, b, n) = 1 = \mathrm{MCD}(c, d, n)$, quindi entrambe le congruenze del sistema sono risolubili ed ammettono ciascuna n soluzioni. Consideriamo il caso generale e supponiamo, quindi, che a, b, c e d non siano congrui a zero $(\mathrm{mod}\ n)$. (Se ad esempio b è congruo a zero $(\mathrm{mod}\ n)$, allora $\mathrm{MCD}(a, n) = 1$, quindi si risolve la prima congruenza e poi si sostituisce alla X, nella seconda congruenza, la soluzione della prima congruenza; si procede poi a risolvere la seconda congruenza rispetto ad Y.) Si moltiplichi la prima congruenza del sistema per d e la seconda per b e, poi, si sottragga la seconda congruenza dalla prima congruenza. Si ottiene:

$$\Delta X \equiv (de - bf) \pmod{n}.$$

In modo analogo, moltiplicando la prima congruenza per c e la seconda per a e sottraendo la prima dalla seconda, si ottiene:

$$\Delta Y \equiv (af - ce) \pmod{n}.$$

Si noti che se $\mathrm{MCD}(\Delta, n) \neq 1$, allora può accadere tanto che il sistema non sia

risolubile quanto che sia risolubile ed abbia più di una soluzione (mod n). Ad esempio:

$$\begin{cases} 2X & \equiv 2 \pmod 4 \\ X+2Y & \equiv 3 \pmod 4 \end{cases} \qquad (*')$$

ha come soluzioni $(1,0)$, $(1,2)$, $(3,0)$ e $(3,2)$, mentre il sistema:

$$\begin{cases} 2X & \equiv 1 \pmod 4 \\ X+2Y & \equiv 3 \pmod 4 \end{cases} \qquad (*'')$$

non ha soluzioni (perché la prima congrenza del sistema non è risolubile).
Si noti anche che, nel caso $\mathrm{MCD}(\Delta, n) \neq 1$, se si pone $\alpha := de - bf, \beta := af - ce$, allora il seguente sistema:

$$\begin{cases} \Delta X & \equiv \alpha \pmod n \\ \Delta Y & \equiv \beta \pmod n \end{cases} \qquad (\Delta_n)$$

non è detto che sia equivalente al sistema assegnato $(*_n)$ (cioè, non è detto che ammetta lo stesso insieme di soluzioni di $(*_n)$), perché la moltiplicazione per d, per b, per a o per c (se questi elementi non sono invertibili (mod n)) può portare alla creazione di "nuove soluzioni". Precisamente, se (x, y) è una soluzione del sistema $(*_n)$, allora (x, y) è anche una soluzione del sistema (Δ_n), ma non è vero il viceversa, a meno che a, b, c e d non possiedano un inverso aritmetico (mod n). Ad esempio, dato il sistema:

$$\begin{cases} Y & \equiv 0 \pmod 4 \\ 2X+2Y & \equiv 2 \pmod 4 \end{cases} \qquad (*_4)$$

ha come soluzioni $(1,0)$ e $(3,0)$, mentre "il sistema (Δ_4) associato" è il sistema:

$$\begin{cases} 2X & \equiv 2 \pmod 4 \\ 2Y & \equiv 0 \pmod 4 \end{cases} \qquad (*_4)$$

che ha come soluzioni $(1,0)$, $(3,0)$, $(1,2)$ e $(3,2)$.]

2.15. Siano $a, b, c, d, e, f, p \in \mathbb{Z}$ con p primo. Consideriamo il seguente sistema di due congruenze lineari in due incognite:

$$\begin{cases} aX+bY & \equiv e \pmod p \\ cX+dY & \equiv f \pmod p \end{cases} \qquad (*_p)$$

Sia $\Delta := ad - bc, \alpha := de - bf, \beta := af - ce$. Supponiamo che $\mathrm{MCD}(a, b, p) = 1$ e $1 = \mathrm{MCD}(c, d, p)$. Mostrare che:
(a) Se $\Delta \equiv 0 \pmod p$ e se $\alpha \equiv \beta \equiv 0 \pmod p$ allora il sistema $(*)$ ha p soluzioni.
(b) Se $\Delta \equiv 0 \pmod p$ e se $\alpha \not\equiv 0 \pmod p$ oppure $\beta \not\equiv 0 \pmod p$ allora il sistema

$(*)$ non è risolubile.
(c) Se $\Delta \not\equiv 0 \pmod p$, allora il sistema $(*)$ ha un'unica soluzione.
[Suggerimento. **(a)** e **(b)** Osservare che se $(*)$ è risolubile e $\Delta \equiv 0 \pmod p$ allora necessariamente $\alpha \equiv \beta \equiv 0 \pmod p$, dal momento che $\Delta X \equiv \alpha \pmod p$ e $\Delta Y \equiv \beta \pmod p$. Inoltre se $\Delta \equiv \alpha \equiv \beta \equiv 0 \pmod p$ allora si vede facilmente che $c \equiv ta \pmod p, d \equiv tb \pmod p, f \equiv te \pmod p$, per qualche $t \not\equiv 0 \pmod p$, e quindi le soluzioni di $(*)$ coincidono con le soluzioni di $aX + bY \equiv e \pmod p$, che sono in numero di p (cfr. l'Esercizio 2.6). **(c)** È un caso particolare del precedente Esercizio 2.14.
Si noti che se $\mathrm{MCD}(a, b, p) \neq 1$ o $\mathrm{MCD}(c, d, p) \neq 1$ allora $\mathrm{MCD}(a, b, p) = p$ o $\mathrm{MCD}(c, d, p) = p$ e quindi il sistema dato assumerebbe una forma degenere $(\mathrm{mod}\ p)$.]

2.16. Trovare, al variare tra gli interi del parametro λ $(0 \leqslant \lambda \leqslant 4)$ le soluzioni del seguente sistema di congruenze lineari:

$$\begin{cases} 4X + \lambda Y & \equiv 2 \pmod 5 \\ 2X + 3Y & \equiv 3 \pmod 5 \end{cases}$$

[Soluzione. $\Delta \equiv 0 \pmod 5$ se e soltanto se $\lambda \equiv 1 \pmod 5$.
Se $\lambda = 0$, il sistema ha un'unica soluzione: $(3, 4)$.
Se $\lambda = 2$, il sistema ha un'unica soluzione: $(0, 6)$.
Se $\lambda = 3$, il sistema ha un'unica soluzione: $(2, 3)$.
Se $\lambda = 4$, il sistema ha un'unica soluzione: $(1, 2)$.
Se $\lambda = 1$ il sistema non è risolubile.]

2.17. Trovare, al variare tra gli interi del parametro λ $(0 \leqslant \lambda \leqslant 6)$ le soluzioni del seguente sistema di congruenze lineari:

$$\begin{cases} 2X + 3Y & \equiv 5 \pmod 7 \\ X + \lambda Y & \equiv 6 \pmod 7 \end{cases}$$

[Soluzione. $\Delta \equiv 0 \pmod 7$ se, e soltanto se, $\lambda \equiv 5 \pmod 7$. Per $\lambda = 5$, le soluzioni del sistema sono: $(0, 4), (1, 1), (2, 5), (3, 2), (4, 6), (5, 3), (6, 0)$. Se $\lambda \in \{0, 1, 2, 3, 4\}$, il sistema ha un'unica soluzione: $(6, 0)$.]

2.18. Trovare, al variare tra gli interi del parametro λ, le soluzioni del seguente sistema di congruenze lineari:

$$\begin{cases} 2X + Y & \equiv \lambda \pmod 3 \\ X + 2Y & \equiv 1 \pmod 3 \end{cases}$$

[Soluzione. $\Delta \equiv 0 \pmod 3, \alpha_\lambda := de - bf = 2\lambda - 1, \beta_\lambda := af - ce = 2 - \lambda$.
Se $\lambda = 2, \alpha_\lambda \equiv 0 \pmod 3, \beta_\lambda \equiv 0 \pmod 3$. In tal caso, il sistema ha come soluzioni $(1, 0), (0, 2), (2, 1)$.
Se $\lambda = 0$ o se $\lambda = 1$, il sistema non ha soluzioni.]

2.19. Siano $A = (a_{ij}), B = (b_{ij})$ due matrici $r \times s$ ad entrate, a_{ij} e b_{ij}, intere e sia $n > 0$. Si dice che $A \equiv B \pmod n$, se $a_{ij} \equiv b_{ij} \pmod n$ presi comunque $1 \leqslant i \leqslant r,\ 1 \leqslant j \leqslant s$.
Si dice che una *matrice quadrata* M, *ad entrate intere è invertibile* $(\mathrm{mod}\ n)$ se esiste

una matrice $\widetilde{M}$ tale che $M\widetilde{M} \equiv I \equiv \widetilde{M}M \pmod{n}$, dove I è la matrice identità. Si vede senza difficoltà che se una matrice M è invertibile (mod n), allora la sua inversa $\widetilde{M}$ è determinata univocamente (mod n).
(a) Mostrare che se C è una matrice $s \times t$ ad entrate intere e se $A \equiv B \pmod{n}$ allora $AC \equiv BC \pmod{n}$.
(b) Sia A una matrice quadrata ad entrate intere, sia A^{agg} la matrice aggiunta di A ad entrate intere e sia $\Delta := det(A)$. Mostrare che se $\text{MCD}(\Delta, n) = 1$, allora l'inversa della matrice $A \pmod{n}$ è data da $\widetilde{A} := \Delta^* \cdot A^{\text{agg}}$, dove Δ^* è un inverso aritmetico (mod n) di Δ.
(c) Si consideri un sistema di congruenze lineari in r equazioni ed r incognite:

$$\begin{cases} \sum_{j=1}^{r} a_{ij} X_j \equiv b_i \pmod{n} \\ 1 \leqslant i \leqslant r \end{cases}$$

che scriviamo in forma compatta matriciale nella seguente maniera:

$$AX \equiv B \pmod{n}$$

dove $A = (a_{ij})$ è una matrice $r \times r$, $X = (X_j)$ e $B = (b_j)$ sono due matrici $r \times 1$.
Sia $\Delta := det(A)$. Mostrare che, se $\text{MCD}(\Delta, n) = 1$, allora il sistema ammette un'unica soluzione (scritta in forma matriciale) $x = (x_j) \pmod{n}$ che può essere espressa nella maniera seguente:

$$x \equiv \Delta^* \cdot A^{\text{agg}} \cdot B \pmod{n}$$

dove Δ^* è un inverso aritmetico di $\Delta \pmod{n}$.
[Suggerimento: rivisitazione del Teorema di G. Cramér (mod n).]