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* $(\text{mod } n)$ 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 $(\text{mod } n)$ 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 $(\text{mod } n)$":*
$a \equiv a \pmod{n}$, per ogni $a \in \mathbb{Z}$;
(2) *Proprietà simmetrica della "congruenza $(\text{mod } n)$":*
$a \equiv b \pmod{n} \iff b \equiv a \pmod{n}$;
(3) *Proprietà transitiva della "congruenza $(\text{mod } n)$":*
$a \equiv b \pmod{n}, b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$;
(4) *Proprietà di compatibilità con la somma della "congruenza $(\text{mod } n)$":*
$a \equiv b \pmod{n}, c \equiv d \pmod{n} \Rightarrow a + c \equiv b + d \pmod{n}$;
(5) *Proprietà di compatibilità con il prodotto della "congruenza $(\text{mod } n)$":*
$a \equiv b \pmod{n}$, $c \equiv d \pmod{n}$, $\Rightarrow ac \equiv bd \pmod{n}$;
(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*

$$\frac{a}{d} \equiv \frac{b}{d} \qquad \left(\mathrm{mod}\ \frac{n}{d}\right).$$

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:

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

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* $\pmod n$.
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*, $\pmod n$.
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:

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

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

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:

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

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*

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

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.]