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).]

3 Il "piccolo" Teorema di Fermat

Pierre de Fermat, francese, giudice presso il tribunale di Tolosa, è considerato uno dei padri fondatori della moderna teoria dei numeri. L'interesse per questa teoria fu suscitato in lui dalla lettura della traduzione (commentata) in latino dell'*Arithmetica* di Diofanto di Alessandria (matematico greco vissuto nel III secolo d. C.), pubblicata nel 1621 a cura di C. Bachet de Méziriac.
Una delle caratteristiche dell'attività matematica di Fermat fu quella di non scrivere esplicitamente le dimostrazioni dei suoi risultati. Egli si limitava di solito a semplici annotazioni (celebri sono quelle a margine della copia dell'*Arithmetica* di Diofanto) e le diffondeva attraverso una fitta corrispondenza che aveva stabilito con vari altri cultori della matematica suoi contemporanei (tra i quali principalmente il religioso M. Mersenne).
Nel 1640, ad esempio, Fermat comunicò a B. Frénicle de Bessy che, se p è un numero primo ed a un qualunque intero non divisibile per p, allora $a^{p-1} - 1$ è divisibile per p. La prima dimostrazione completa di tale risultato fu pubblicata nel 1736, quasi cento anni più tardi, da Euler.

Teorema 3.1. *(**"Piccolo" Teorema di Fermat**) Sia p un numero primo ed $a \in \mathbb{Z}$. Se $p \nmid a$, allora $a^{p-1} \equiv 1 \pmod{p}$.*

Dimostrazione (Ivory, 1806). Poiché $p \nmid a$, $S = \{0, a, 2a, \ldots, (p-1)a\}$ è un sistema completo di residui (modulo p) (cfr. anche Esercizio 1.4). Quindi, dalla Proposizione 1.3 (5) si ricava che:

$$a \cdot 2a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p},$$

ovvero

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

Poiché $p \nmid (p-1)!$, necessariamente $p \mid (a^{p-1} - 1)$ e da ciò segue la tesi. □

Corollario 3.2. *Sia p un numero primo. Per ogni $a \in \mathbb{Z}$ si ha:*

$$a^p \equiv a \pmod{p}. \qquad \square$$

Il "Piccolo" Teorema di Fermat non si inverte, in generale. Innanzitutto, mostriamo che: se un intero n $(n \geqslant 2)$ è tale che $a^{n-1} \equiv 1 \pmod{n}$, per qualche $a \in \mathbb{Z}$ e $\mathrm{MCD}(a, n) = 1$, allora n *non* è necessariamente primo.
Proveremo questo fatto con un controesempio, cui premettiamo il seguente lemma tecnico.

Lemma 3.3. *Siano p e q due numeri primi distinti ed $a \in \mathbb{Z}$ in modo tale che:*

$$a^q \equiv a \pmod{p} \quad e \quad a^p \equiv a \pmod{q}.$$

Allora:

$$a^{pq} \equiv a \pmod{pq}.$$

Dimostrazione. Applicando il Corollario 3.2 ad a^q, si ha che $(a^q)^p \equiv a^q \pmod{p}$ e dunque $a^{pq} \equiv a \pmod{p}$. In modo analogo si ottiene che $a^{pq} \equiv a \pmod{q}$. Essendo ovviamente $\mathrm{MCD}(p,q) = 1$, la tesi segue facilmente (cfr. Esercizio 1.2). $\square$

Veniamo al controesempio annunciato. Sia $n = 341 = 11 \cdot 31$ ed $a = 2$. Mostriamo che $2^{340} \equiv 1 \pmod{341}$ pur non essendo 341 un numero primo. È facile vedere che $2^{11} \equiv 2 \pmod{31}$ (infatti $2^{11} = 2 \cdot 2^{10} = 2 \cdot 1024 = 2(31 \cdot 33 + 1)$) e che $2^{31} \equiv 2 \pmod{11}$ (infatti $2^{31} = 2 \cdot (2^{10})^3 \equiv 2 \cdot 1^3 \pmod{11}$). Perciò, utilizzando il Lemma 3.3, $2^{341} = 2^{11 \cdot 31} \equiv 2 \pmod{341}$, da cui $2^{340} \equiv 1 \pmod{341}$, mentre 341 non è primo.

Osservazione 3.4. L'esempio precedente ci porta a considerare numeri naturali del tipo $2^n - 2$, i quali hanno un notevole interesse storico, testimoniato dal fatto che si attribuisce (anche se in maniera controversa) agli antichi matematici cinesi dell'epoca di Confucio (VI - V secolo a. C.) la seguente questione:

$$\text{un intero } n \text{ è primo} \iff n \mid (2^n - 2) \ ?$$

Per maggiori dettagli storici su tale problematica rinviamo a [R, pag. 85]. Tale questione ha una risposta positiva per $n \leqslant 340$, ma l'esempio precedente (che è dovuto a Sarrus e risale al 1819) mostra che, in generale, la risposta è negativa. Ciò ha portato alla seguente definizione:

Definizione 3.5. Si chiama *numero pseudoprimo (in base* 2) ogni intero non primo n tale che $n \mid (2^n - 2)$.

Si noti che, se n è dispari, allora:

$$n \text{ è pseudoprimo (in base 2)} \iff 2^{n-1} \equiv 1 \pmod{n}.$$

I numeri pseudoprimi $n < 10^3$ sono $341, 561 = 3 \cdot 11 \cdot 17$ e $645 = 3 \cdot 5 \cdot 43$. Il più piccolo numero pseudoprimo pari è $2 \cdot 73 \cdot 1103 = 161038$ ed è stato scoperto da Lehmer nel 1950. Nel 1938 Poulet ha determinato tutti i numeri pseudoprimi dispari $\leqslant 10^8$. Si può inoltre dimostrare che i numeri pseudoprimi sono infiniti (cfr. Esercizio 3.15) ed anzi, di più, Beeger nel 1951 ha dimostrato che i numeri pseudoprimi pari sono infiniti.

La nozione di numero pseudoprimo può essere "rafforzata" nella maniera seguente, determinando un "tipo più raro" di numeri, la cui esistenza dimostra che il "Piccolo" Teorema di Fermat non si inverte.

Definizione 3.6. Si chiama *numero di Carmichael* ogni intero non primo n tale che, per ogni intero a, relativamente primo con n, risulti:

$$a^{n-1} \equiv 1 \pmod{n}.$$

Si può dimostrare facilmente che un intero non primo n è di Carmichael se, e soltanto se, per ogni $a \in \mathbb{Z}$ risulta che $n \mid (a^n - a)$. Dunque ogni numero di Carmichael è pseudoprimo. Il viceversa è falso, in quanto, ad esempio 341 non è un numero di Carmichael (infatti si vede che $31 \nmid (11^{341} - 11)$ e dunque $341 \nmid (11^{341} - 11)$). Si dimostra invece che 561 è un numero di Carmichael (dunque è il più piccolo numero di Carmichael. Il successivo numero di Carmichael è $1105 = 5 \cdot 13 \cdot 17$). Nel 1993 Alford, Granville e Pomerance hanno dimostrato che esistono infiniti numeri di Carmichael.

Nel 1760, 24 anni dopo la dimostrazione del "Piccolo" Teorema di Fermat, Euler dimostrò la seguente generalizzazione di tale teorema:

Teorema 3.7. *(**Teorema di Euler - Fermat**) Siano $a, n \in \mathbb{Z}, n > 0$. Se* $\mathrm{MCD}(a, n) = 1$, *allora:*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Dimostrazione. Sia $S^* := \{k_1, \ldots, k_{\varphi(n)}\}$ un sistema ridotto di residui (modulo n) (cfr. Definizione 2.7). Poiché $\mathrm{MCD}(a, n) = 1$, anche $T^* := \{ak_1, \ldots, ak_{\varphi(n)}\}$ è un sistema ridotto di residui (modulo n) (cfr. Esercizio 2.10 (a)) e quindi:

$$a^{\varphi(n)} \cdot k_1 \cdot k_2 \cdot \ldots \cdot k_{\varphi(n)} = ak_1 \cdot ak_2 \cdot \ldots \cdot ak_{\varphi(n)} \equiv k_1 \cdot k_2 \cdot \ldots \cdot k_{\varphi(n)} \pmod{n}.$$

Poiché $\mathrm{MCD}(k_1 \cdot k_2 \cdot \ldots \cdot k_{\varphi(n)}, n) = 1$, dal Corollario 1.11 (a) segue la tesi. □

Osservazione 3.8. **(a)** Il Teorema 3.7 generalizza il Teorema 3.1, in quanto, per ogni primo p, si ha $\varphi(p) = p - 1$.
(b) Si noti che, in generale, $a^{\varphi(n)} \not\equiv 1 \pmod{n}$ (ad esempio, $n = 4, a = 2$, allora $2^2 \not\equiv 1 \pmod{4}$) e quindi anche $a^{\varphi(n)+1} \not\equiv a \pmod{n}$.
(c) Si noti che, se $\mathrm{MCD}(a, n) = 1$, allora $a^{\varphi(n)-1}$ è un inverso aritmetico (mod n) di a.

Passiamo ora a dare alcune applicazioni (conseguenze o risultati collegati) del Teorema di Euler - Fermat e della nozione di inverso aritmetico.

I APPLICAZIONE:
Formula risolutiva delle congruenze lineari.
Tutte e sole le soluzioni distinte della congruenza

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

con $n > 0$ e $\mathrm{MCD}(a, n) =: d \mid b$, sono date da:

$$x_k := \left(\frac{a}{d}\right)^{\varphi\left(\frac{n}{d}\right)-1} \cdot \left(\frac{b}{d}\right) + k\left(\frac{n}{d}\right), \quad 0 \leqslant k \leqslant d - 1.$$

Dimostrazione. Basta applicare il Teorema 2.2 ed il Teorema 3.7. □

Il seguente celebre risultato verrà utilizzato tra poco per fornire una ulteriore applicazione del "Piccolo" Teorema di Fermat, e precisamente nella risoluzione delle congruenze quadratiche del tipo $X^2 \equiv -1 \pmod{p}$, dove p è un numero primo dispari.

Teorema 3.9. *(**Teorema di Wilson**) Sia p un numero primo. Allora:*

$$(p-1)! \equiv -1 \pmod{p}.$$

Dimostrazione. Se $p = 2, 3$ il risultato è ovvio.
Supponiamo dunque che $p \geqslant 5$ e consideriamo il sistema ridotto di residui (modulo p) $S^* := \{1, 2, \ldots, p-1\}$. Gli elementi a di S^* coincidenti con l'inverso aritmetico (cfr. Definizione 1.13) sono esattamente 1 e $p-1$. Infatti

$$a^2 \equiv 1 \pmod{p} \iff (a-1)(a+1) \equiv 0 \pmod{p} \iff$$

$$\iff a \equiv 1 \pmod{p} \text{ oppure } a \equiv -1 \equiv p-1 \pmod{p} \iff$$

$$\iff a = 1 \text{ oppure } a = p-1.$$

I restanti elementi $2, 3, \ldots, p-2$ non coincidono con il loro inverso aritmetico in S^* e, dunque, possono essere ripartiti in paia $\{a, a'\}, a \neq a'$, tali che $aa' \equiv 1 \pmod{p}$. Si ottiene allora:

$$(p-2)! = 2 \cdot 3 \cdot \ldots \cdot (p-2) \equiv 1 \pmod{p}$$

e, moltiplicando ambo i membri per $p-1$:

$$(p-1)! \equiv p-1 \equiv -1 \pmod{p}. \qquad \square$$

Osservazione 3.10. **(a)** Il Teorema di Wilson fu enunciato nel 1770 da E. Waring sul suo *Meditationes Algebricae* e da Waring attribuito ad un suo studente, appunto J. Wilson. La prima dimostrazione completa di tale risultato viene generalmente attribuita a Lagrange nel 1771.
(b) Il Teorema di Wilson si inverte, infatti:

$$n \text{ è primo} \iff (n-1)! \equiv -1 \pmod{n}.$$

($\Leftarrow$) Se $d \mid n$ e $d \neq n$, allora $d \mid (n-1)!$. Poiché, per ipotesi, $n \mid (n-1)!+1$, allora $d \mid (n-1)!+1$, ma $d \mid (n-1)!$ e pertanto $d = 1$.
(c) Si osservi che, se $p \geq 5$ è un primo, allora $(p-3)!$ è un inverso aritmetico di $p-2 \pmod{p}$, essendo $1 \equiv (p-2)! = (p-2)(p-3)! \pmod{p}$. Più generalmente, si può osservare che, per ogni k, $1 \leq k \leq p-2$, l'intero $((p-2)!)/k$ è un inverso aritmetico di $k \pmod{p}$.

La problematica connessa con il teorema successivo è molto antica, infatti se ne trovano tracce in un manuale di aritmetica di Sun Tsu (matematico cinese del I secolo d.C.).

II APPLICAZIONE: Il Teorema Cinese dei Resti.
Siano $n_1, n_2, \ldots, n_r$ *interi positivi tali che* $\mathrm{MCD}(n_i, n_j) = 1$ *con* $1 \leqslant i, j \leqslant r$ *e* $i \neq j$. *Per ogni scelta di* $a_1, a_2, \ldots, a_r \in \mathbb{Z}$ *il sistema di congruenze lineari:*

$$\begin{cases} X \equiv a_i \pmod{n_i} \\ 1 \leqslant i \leqslant r \end{cases}$$

è risolubile ed ha un'unica soluzione modulo $n_1 \cdot n_2 \cdot \ldots \cdot n_r$.

Dimostrazione. Sia $n := n_1 \cdot n_2 \cdot \ldots \cdot n_r$ ed $N_i := \dfrac{n}{n_i}$ $(1 \leqslant i \leqslant r)$. Verifichiamo che l'intero:

$$x_0 := \sum_{i=1}^{r} a_i N_i^{\varphi(n_i)} \tag{1}$$

è soluzione del sistema assegnato. Infatti, per ogni indice $j \neq i$, risulta $N_j \equiv 0 \pmod{n_i}$ e dunque $x_0 \equiv a_i N_i^{\varphi(n_i)} \pmod{n_i}$. Poiché $\mathrm{MCD}(N_i, n_i) = 1$, allora $N_i^{\varphi(n_i)} \equiv 1 \pmod{n_i}$ (Teorema di Euler-Fermat). Da ciò segue che x_0 è soluzione del sistema.
Se $x' \in \mathbb{Z}$ è un'altra soluzione del sistema dato, risulta $x' \equiv x_0 \pmod{n_i}$. Poiché $\mathrm{MCD}(n_i, n_j) = 1$, in base all'Esercizio 1.2 (esteso per induzione al caso di r fattori relativamente primi a coppie), si ha $x_0 \equiv x' \pmod{n}$ e, quindi, la soluzione del sistema è unica (modulo n). $\square$

Si noti che la formula (1), che determina la soluzione (modulo n) del sistema di congruenze sopra considerato, può essere sostituita dalla formula:

$$x_0' := \sum_{i=1}^{r} a_i M_i \tag{1'}$$

dove $M_i := N_i N_i^*$, con N_i^* un inverso aritmetico di $N_i \pmod{n_i}$ per ogni i, $1 \leqslant i \leqslant r$. Ciò è conveniente, dal punto di vista computazionale, se risulta più semplice determinare esplicitamente N_i^* (possibilmente $N_i^* < N_i^{\varphi(n_i)-1}$), senza far ricorso al Teorema di Euler-Fermat.

III APPLICAZIONE:
Risoluzione di un sistema di congruenze lineari.
Si consideri il sistema di congruenze lineari:

$$\begin{cases} a_i X \equiv b_i \pmod{m_i} \\ 1 \leqslant i \leqslant r \end{cases} \tag{2}$$

con $\mathrm{MCD}(m_i, m_j) = 1$, *se* $i \neq j$. *Si ponga* $d_i := \mathrm{MCD}(a_i, m_i), a_i' := \dfrac{a_i}{d_i}$, $b_i' := \dfrac{b_i}{d_i}$ *ed* $n_i := \dfrac{m_i}{d_i}$ $(1 \leqslant i \leqslant r)$. *Se* $d_i \mid b_i$ *per ogni* i $(1 \leqslant i \leqslant r)$, *il sistema* (2) *è risolubile. In tal caso, le soluzioni di* (2) *si trovano considerando il seguente sistema:*

$$\begin{cases} X \equiv (a_i')^{\varphi(n_i)-1} b_i' \pmod{n_i} \\ 1 \leqslant i \leqslant r \end{cases} \tag{$2^{\#}$}$$

con $\mathrm{MCD}(n_i, n_j) = 1$, *se* $i \neq j$.
Precisamente, se $m := m_1 m_2 \cdot \ldots \cdot m_r, d := d_1 d_2 \cdot \ldots \cdot d_r, n := n_1 n_2 \cdot \ldots \cdot n_r$ *e se* $\mathring{x}$ *è l'unica soluzione di* $(2^{\#})$ *(modulo* n*), allora* $\mathring{x}$ *determina* d *soluzioni di* (2) *incongruenti (modulo* m*) che sono tutte le soluzioni di* (2)*:*

$$x_k := \mathring{x} + kn, \quad 0 \leqslant k \leqslant d - 1.$$

[Nota: *"Sollevando" in* $\mathbb{Z}$ *le soluzioni dei sistemi di congruenze* (2) *e* $(2^{\#})$, *abbiamo che l'insieme delle "soluzioni in* $\mathbb{Z}$*" del sistema* $(2^{\#})$ *è dato da* $\{\mathring{x} + tn : t \in \mathbb{Z}\}$ *e coincide con l'insieme delle "soluzioni in* $\mathbb{Z}$*" di* (2)*, che è dato da* $\{\mathring{x} + kn + sm : 0 \leqslant k \leqslant d - 1,\ s \in \mathbb{Z}\}$.]

Dimostrazione. È chiaro che $\mathrm{MCD}(n_i, n_j) = 1$ se $i \neq j$: dunque $(2^{\#})$ è risolubile. Poiché $\mathrm{MCD}(a_i', n_i) = 1$, per determinare le soluzioni del sistema $(2^{\#})$ (modulo n) basta applicare la formula risolutiva delle congruenze lineari (I Applicazione del Teorema di Euler-Fermat).
Se $\mathring{x}$ è una soluzione di $(2^{\#})$ (modulo n), allora non è difficile verificare che $\mathring{x}$ determina le seguenti d soluzioni del sistema (2), incongruenti (modulo m):

$$x_k := \mathring{x} + kn, \quad 0 \leqslant k \leqslant d - 1.$$

Infatti, per ogni i, $1 \leqslant i \leqslant r$

$$a_i'(\mathring{x} + kn) \equiv b_i' \pmod{n_i}$$

e quindi, moltiplicando per d_i ambo i membri, abbiamo che:

$$a_i(\mathring{x} + kn) \equiv b_i \pmod{m_i}.$$

Il fatto che le x_k siano tutte le soluzioni incongrue (mod n) di (2) discende dal fatto che, se x è una soluzione di (2), allora x è anche una soluzione di $(2^{\#})$ e, quindi, $x \equiv \mathring{x} \pmod{n}$. Da ciò si conclude facilmente. □

Esempio 3.11. Si consideri il seguente sistema:

$$\begin{cases} 2X \equiv 2 \pmod{4} \\ 2X \equiv 3 \pmod{5} \\ 14X \equiv 7 \pmod{21} \end{cases} \tag{3.11.1}$$

Tenendo presente che l'inverso aritmetico di 2 (mod 5) è 3 e l'inverso aritmetico di 2 (mod 3) è 2, al sistema (3.11.1) è associato il seguente sistema:

$$\begin{cases} X & \equiv 1 \pmod 2 \\ X & \equiv 4 \pmod 5 \\ X & \equiv 2 \pmod 3 \end{cases} \tag{3.11.2}$$

Il sistema (3.11.2) ha un'unica soluzione $\mathring{x} = 1 \cdot 15 + 4 \cdot 6^4 + 2 \cdot 10^2 \equiv -1 \pmod{30}$. Questa determina 14 soluzioni di (3.11.1) (modulo 420) date da:

$$x_k = -1 + k \cdot 30, \quad 0 \leqslant k \leqslant 13.$$

IV APPLICAZIONE: *Sia p un primo dispari. La congruenza:*

$$X^2 \equiv -1 \pmod p$$

è risolubile se, e soltanto se, $p \equiv 1 \pmod 4$. In tal caso $\mathring{x} := \left(\frac{(p-1)}{2}\right)!$ è una soluzione della congruenza data.

Dimostrazione. $(\Rightarrow)$. Sia $\mathring{x} \in \mathbb{Z}$ tale che $\mathring{x}^2 \equiv -1 \pmod p$. Allora $\mathring{x}^{p-1} = (\mathring{x}^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod p$ e, in base al "Piccolo" Teorema di Fermat (Teorema 3.1), $\mathring{x}^{p-1} \equiv 1 \pmod p$, quindi $(-1)^{\frac{p-1}{2}} \equiv 1 \pmod p$. Essendo $p \neq 2$, si ha che $1 = (-1)^{\frac{p-1}{2}}$ e pertanto $\frac{p-1}{2}$ è pari, cioè $p \equiv 1 \pmod 4$.
$(\Leftarrow)$. Sia $p \equiv 1 \pmod 4$. Dopo aver osservato che:

$$\{h : \frac{p-1}{2} + 1 \leqslant h \leqslant p-1\} = \{p-k : 1 \leqslant k \leqslant \frac{p-1}{2}\},$$

si vede subito che:

$$\begin{aligned} (p-1)! &= 1 \cdot 2 \cdot \cdots \cdot \frac{p-1}{2} \cdot (p-1)(p-2) \cdot \cdots \cdot \left[p - \left(\frac{p-1}{2}\right)\right] \\ &\equiv 1 \cdot 2 \cdot \cdots \cdot \frac{p-1}{2} \cdot (-1)(-2) \cdot \cdots \cdot \left[-\left(\frac{p-1}{2}\right)\right] \pmod p \\ &= (-1)^{\frac{p-1}{2}} \cdot 1^2 \cdot 2^2 \cdot \cdots \cdot \left(\frac{p-1}{2}\right)^2 \\ &= (-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2 \end{aligned}$$

Per ipotesi $\frac{p-1}{2}$ è pari e, dal Teorema di Wilson, si ricava:

$$-1 \equiv (p-1)! \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod p.$$

Pertanto $\mathring{x} = (\frac{p-1}{2})!$ è soluzione della congruenza in esame. $\square$

V APPLICAZIONE: *Sia n un intero tale che* $\mathrm{MCD}(n, 10) = 1$. *Allora n divide un intero le cui cifre sono tutte uguali ad* 1.

Dimostrazione. Dato che $\mathrm{MCD}(9, 10) = 1$, anche $\mathrm{MCD}(9n, 10) = 1$. Dal Teorema di Euler-Fermat, $10^{\varphi(9n)} \equiv 1 \pmod{9n}$, cioè esiste $k \in \mathbb{Z}$ tale che $9nk = 10^{\varphi(9n)} - 1$. Dunque $nk = (10^{\varphi(9n)} - 1)/9$, donde la conclusione. □

La dimostrazione del risultato precedente non determina un intero "minimale" con la proprietà enunciata. Infatti, se $n = 3$, allora per quanto sopra abbiamo:

$$3 \mid \left(\frac{10^{\varphi(27)} - 1}{9} \right) = \frac{10^{18} - 1}{9},$$

tuttavia è facile vedere anche che $3 \mid 111$.

VI APPLICAZIONE: *Siano $n, a \in \mathbb{Z}$, $n > 0$ tali che* $\mathrm{MCD}(a, n) = \mathrm{MCD}(a - 1, n) = 1$. *Allora:*

$$1 + a + a^2 + \cdots + a^{\varphi(n)-1} \equiv 0 \pmod{n}.$$

Dimostrazione. Si noti che:

$$a^{\varphi(n)} - 1 = (a - 1)(a^{\varphi(n)-1} + \cdots + a^2 + a + 1).$$

Dal Teorema di Euler-Fermat, $(a-1)(a^{\varphi(n)-1}+\cdots+a^2+a+1) \equiv 0 \pmod{n}$ e, poiché $\mathrm{MCD}(a - 1, n) = 1$, è lecito "semplificare" $(a - 1)$ dalla precedente congruenza: da cui la tesi. □

Si noti che, nella precedente applicazione, la condizione che $\mathrm{MCD}(a - 1, n)$ sia uguale ad 1 (oltre alla condizione $\mathrm{MCD}(a, n) = 1$) è essenziale, perché ad esempio se $n = 4$ ed $a = 5$, allora $\varphi(n) = 2$ e $1 + 5 \not\equiv 0 \pmod{4}$.

Come mostrano le applicazioni del Teorema di Euler-Fermat e, come vedremo meglio nello sviluppo della teoria delle congruenze, sovente è necessario calcolare grandi potenze di interi modulo un intero n fissato. È pertanto opportuno disporre di una tecnica per il calcolo della esponenziazione modulare.

Ad esempio, se vogliamo trovare il più piccolo intero positivo congruo a $3^{10} \pmod{11}$, senza usare il "Piccolo" Teorema di Fermat, possiamo procedere nella maniera seguente.

1° Passo. Esprimere l'esponente 10 in base 2:

$$10 = (1010)_2$$

2° Passo. Utilizzando il passo precedente, scrivere 3^{10} come prodotto di potenze di 3, con esponenti potenze di 2, fino alla piú grande potenza di 2 minore di 10:

$$3^{10} = 3^{2^3+2} = 3^8 \cdot 3^2$$

3° Passo. Calcolare il più piccolo intero positivo congruo a $3^{2^k} \pmod{11}$ per $k \leqslant 3$:

$$\begin{aligned} 3 &\equiv 3 && \pmod{11} \\ 3^2 &\equiv 9 && \pmod{11} \\ 3^4 &\equiv 81 \equiv 4 && \pmod{11} \\ 3^8 &\equiv 16 \equiv 5 && \pmod{11} \end{aligned}$$

Quindi, possiamo concludere facilmente che

$$3^{10} \equiv 5 \cdot 9 \equiv 1 \pmod{11}.$$

Metodo ricorsivo di calcolo per l'esponenziazione modulare. Siano dati b, N ed n interi positivi. Per calcolare il più piccolo intero positivo congruo a $b^N \pmod{n}$, si può procedere nella seguente maniera:

1° Passo. Esprimere l'esponente N in base 2:

$$N = (a_k a_{k-1} \ldots a_1 a_0)_2 \text{ con } a_i \in \{0, 1\}, 0 \leqslant i \leqslant k.$$

2° Passo. Scrivere b^N come prodotto di potenze del tipo b^{2^h} per $0 \leqslant h \leqslant k$:

$$b^N = b^{a_k 2^k + a_{k-1} 2^{k-1} + \cdots + a_0 2^0} = \prod_{h=0}^{k} b^{a_h 2^h} = \prod_{\substack{a_h \neq 0 \\ h=0}}^{k} b^{2^h}.$$

3° Passo. Calcolare il più piccolo intero positivo congruo a b^{2^h} (modulo n) per ogni h, $0 \leqslant h \leqslant k$:

$$b^{2^h} \equiv r_h \pmod{n}, \text{ con } 0 \leqslant r_h \leqslant n-1, \ 0 \leqslant h \leqslant k.$$

Si noti anche che $r_{h+1} \equiv (r_h)^2 \pmod{n}$, per $0 \leqslant h \leqslant k-1$.

Conclusione.

$$b^N \equiv \prod_{a_h \neq 0} r_h \equiv r \pmod{n}, \text{ con } 0 \leqslant r \leqslant n-1.$$

Esempio 3.12. Per calcolare il più piccolo intero positivo congruo a $2^{138} \pmod{23}$, scriviamo:

$$138 = (10001010)_2 = 2^7 + 2^3 + 2.$$

Poiché:

$$\begin{aligned} 2^{2^0} &\equiv 2 \pmod{23} & 2^{2^1} &\equiv 4 \pmod{23} \\ 2^{2^2} &\equiv 16 \equiv -7 \pmod{23} & 2^{2^3} &\equiv 49 \equiv 3 \pmod{23} \\ 2^{2^4} &\equiv 9 \pmod{23} & 2^{2^5} &\equiv 81 \equiv 12 \pmod{23} \\ 2^{2^6} &\equiv 144 \equiv 6 \pmod{23} & 2^{2^7} &\equiv 36 \equiv 13 \pmod{23}, \end{aligned}$$

dunque:

$$2^{138} = 2^{2^7} \cdot 2^{2^3} \cdot 2^2 \equiv 13 \cdot 3 \cdot 4 \equiv 18 \pmod{23}.$$

3. Esercizi e Complementi

3.1. Siano p e q due primi distinti. Provare che, per ogni $a \in \mathbb{Z}$:

$$pq \mid (a^{pq} - a^p - a^q + a).$$

[Suggerimento: risulta $a^{pq} - a^p \equiv 0 \equiv a^q - a \pmod{q}$ e $a^{pq} - a^q \equiv 0 \equiv a^p - a \pmod{p}$, cfr. Corollario 3.2.]

3.2. **(a)** Siano p e q due primi distinti. Provare che:

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

(b) Siano n ed m due interi positivi distinti e relativamente primi. Provare che:

$$n^{\varphi(m)} + m^{\varphi(n)} \equiv 1 \pmod{mn}.$$

[Suggerimento: basta provare **(b)**.
Risulta $n^{\varphi(m)} - 1 \equiv 0 \pmod{m}$ e $m^{\varphi(n)} - 1 \equiv 0 \pmod{n}$ (cfr. Teorema 3.7). Moltiplicando le due congruenze tra loro, segue l'asserto.]

3.3. Sia $n \geqslant 2$. Mostrare che:
(a) $\{k \in \mathbb{Z} : \text{MCD}(k,n) = 1,\ 1 \leqslant k \leqslant n\} = \{n - k : k \in \mathbb{Z},\ \text{MCD}(k,n) = 1,\ 1 \leqslant k \leqslant n\}$.
(b) Se $\{k_1, k_2, \ldots, k_{\varphi(n)}\}$ è il sistema ridotto di residui minimo positivo (modulo n), allora:

$$2(k_1 + k_2 + \cdots + k_{\varphi(n)}) = n\varphi(n).$$

[Suggerimento: **(b)** discende da **(a)** in quanto:

$$\sum_{i=1}^{\varphi(n)} k_i = \sum_{i=1}^{\varphi(n)} (n - k_i).]$$

3.4. Utilizzando il "Piccolo" Teorema di Fermat (cfr. Teorema3.1 o, meglio, il suo Corollario 3.2), mostrare che se p è primo e $a, b \in \mathbb{Z}$, allora:

$$(a + b)^p \equiv a^p + b^p \pmod{p}.$$

3.5. Mostrare che le seguenti proprietà sono equivalenti:
(i) l'enunciato del "Piccolo" Teorema di Fermat assieme all'enunciato del Teorema di Wilson;
(ii) per ogni primo p e per ogni $a \in \mathbb{Z}$, allora:

$$p \mid (a^p + (p-1)!a);$$

(iii) per ogni primo p e per ogni $a \in \mathbb{Z}$, allora:

$$p \mid ((p-1)!a^p + a).$$

[Suggerimento: **(i)** $\Rightarrow$ **(ii)** [rispettivamente **(i)** $\Rightarrow$ **(iii)**]. Si moltiplichi la congruenza $a^p \equiv a \pmod{p}$ per la congruenza $-1 \equiv (p-1)! \pmod{p}$ [rispettivamente $(p-1)! \equiv -1 \pmod{p}$]. **(ii)** [oppure **(iii)**] $\Rightarrow$ **(i)**. Posto $a = 1$, si ottiene $(p-1)! \equiv -1 \pmod{p}$. Dall'ipotesi, avendo già dimostrato che $(p-1)! \equiv -1 \pmod{p}$, si ottiene allora che $a^p \equiv a \pmod{p}$.]

3.6. Siano $n_1, \ldots, n_r$ interi positivi a due a due relativamente primi. Posto $n := \prod_{i=1}^{n} n_i$, verificare che l'applicazione canonica tra anelli:

$$\rho : \mathbb{Z}/n\mathbb{Z} \longrightarrow (\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_r\mathbb{Z}),$$

definita da $\rho(a + n\mathbb{Z}) := (a + n_1\mathbb{Z}, \ldots, a + n_r\mathbb{Z})$, è un isomorfismo di anelli.
[Suggerimento: se $a + n\mathbb{Z} \in \mathrm{Ker}(\rho)$, allora $a \in \cap n_i\mathbb{Z} = n\mathbb{Z}$, dove $n = \mathrm{mcm}(n_i \mid 1 \leqslant i \leqslant r)$. La suriettività di ρ è un'immediata conseguenza del Teorema Cinese dei Resti.]

3.7. Dimostrare che il seguente sistema di congruenze lineari:

$$\begin{cases} X \equiv a_i \pmod{n_i} \\ 1 \leqslant i \leqslant r \end{cases}$$

con $a_i, n_i, r \in \mathbb{Z}$, $r, n_i \geqslant 2$, è risolubile se, e soltanto se, $\mathrm{MCD}(n_i, n_j) \mid (a_i - a_j)$, presi comunque $i \neq j, 1 \leqslant i, j \leqslant r$. Nel caso in cui tale sistema sia risolubile, dimostrare che esso ammette un'unica soluzione (modulo $\mathrm{mcm}(n_1, n_2, \ldots, n_r)$).
[Suggerimento: si proceda per induzione su $r \geqslant 2$. Sia $r = 2$ e sia $x = a_1 + kn_1$ una soluzione della prima congruenza del sistema, per un qualche $k \in \mathbb{Z}$. Affinché x sia anche soluzione della seconda congruenza del sistema deve essere $x = a_2 + hn_2$, per un qualche $h \in \mathbb{Z}$. Dunque $a_1 - a_2 = hn_2 - kn_1$. Viceversa, se $d := \mathrm{MCD}(n_1, n_2)$, allora esistono $\alpha, \beta \in \mathbb{Z}$ in modo tale che $d = \alpha n_1 + \beta n_2$. Inoltre, per ipotesi deve esistere $t \in \mathbb{Z}$ in modo tale che $td = a_1 - a_2$, quindi $\mathring{x} := a_1 - t\alpha n_1 = a_2 + t\beta n_2$ è soluzione del sistema. Se y è un'altra soluzione del sistema e se

$$n_1' := \frac{n_1}{\mathrm{MCD}(n_1, n_2)}, \quad n_2' := \frac{n_2}{\mathrm{MCD}(n_1, n_2)},$$

allora in particolare $n_1' \mid (y - \mathring{x})$ e $n_2' \mid (y - \mathring{x})$. Essendo $\mathrm{MCD}(n_1', n_2') = 1$, allora $n_1' \cdot n_2' \mid (y - \mathring{x})$.]

3.8. Sia $p \geqslant 5$ un primo dispari, allora mostrare che:

$$2(p-3)! \equiv -1 \pmod{p}.$$

[Suggerimento: per il Teorema di Wilson:
$-1 \equiv (p-1)! = (p-3)!(p-2)(p-1) \equiv (p-3)! \cdot 2 \pmod{p}$.]

3.9. Per ogni $n \geqslant 2$ e per ogni $a \in \mathbb{Z}$ con $\mathrm{MCD}(a, n) = 1$, mostrare che:

$$a^n \equiv a^{n-\varphi(n)} \pmod{n}.$$

[Suggerimento: semplice conseguenza del Teorema di Euler-Fermat; notare che $n > \varphi(n)$ se $n \geqslant 2$ e moltiplicare ambo i membri della congruenza $a^{\varphi(n)} \equiv 1 \pmod{n}$ per $a^{n-\varphi(n)}$.]

3.10. Risolvere le seguenti congruenze utilizzando il Teorema di Euler-Fermat:

(a) $7X \equiv 12 \pmod{17}$;
(b) $3X \equiv 5 \pmod{16}$.

[Soluzioni: **(a)** $x \equiv 9 \pmod{17}$; **(b)** $x \equiv 7 \pmod{16}$.]

3.11. Risolvere il seguente sistema di congruenze:

$$\begin{cases} X \equiv 2 \pmod 3 \\ X \equiv 3 \pmod 5 \\ X \equiv 2 \pmod 7 \end{cases}$$

[Suggerimento: $n = 3 \cdot 5 \cdot 7 = 105, N_1 = \dfrac{n}{n_1} = 35, N_2 = \dfrac{n}{n_2} = 21, N_3 = \dfrac{n}{n_3} = 15$. La soluzione (modulo 105) è data da: $\mathring{x} = 2 \cdot 35^2 + 3 \cdot 21^4 + 2 \cdot 15^6 \equiv 23 \pmod{105}$.]

3.12. Se $n > 2$, mostrare che:
(a) $\varphi(n)$ è pari;
(b) se $\{k_1, \ldots, k_{\varphi(n)}\}$ è un sistema ridotto di residui (modulo n), allora:

$$k_1 + \cdots + k_{\varphi(n)} \equiv 0 \pmod n.$$

[Suggerimento: **(a)** se $n = 2^k \cdot m$ con $k \geqslant 2$ e $2 \nmid m$, allora $\varphi(n) = \varphi(2^k)\varphi(m) = (2^k - 2^{k-1})\varphi(m)$. Se $n = p^k \cdot m$ con $k \geqslant 1$ e p primo dispari e $p \nmid m$, allora $\varphi(n) = \varphi(p^k)\varphi(m) = (p^k - p^{k-1})\varphi(m) = p^{k-1}(p-1)\varphi(m)$. **(b)** segue da **(a)** e dall'Esercizio 3.3 (b).]

3.13. Mostrare che 63 non è primo, verificando che $2^{63} \not\equiv 2 \pmod{63}$.
[Suggerimento: $63 = 6 \cdot 10 + 3$, $2^{63} = (2^6)^{10} \cdot 2^3 = 64^{10} \cdot 2^3 \equiv 1^{10} \cdot 2^3 = 8 \pmod{63}$.]

3.14. Mostrare che $91 \mid (3^{91} - 3)$, pur essendo 91 un numero non primo.
[Suggerimento: $91 = 7 \cdot 13 = (1011011)_2 = 2^6 + 2^4 + 2^3 + 2^1 + 2^0$, $3^{91} = 3^{(2^6)} \cdot 3^{(2^4)} \cdot 3^{(2^3)} \cdot 3^2 \cdot 3$, con $3^2 \equiv 9 \pmod{91}$ $3^{(2^3)} \equiv (3^{(2^2)})^2 = 81^2 \equiv 9 \pmod{91}$, $3^{(2^4)} \equiv 81 \pmod{91}$, $3^{(2^5)} \equiv 9 \pmod{91}$, $3^{(2^6)} \equiv 81 \pmod{91}$, dunque $3^{91} \equiv 81 \cdot 81 \cdot 9 \cdot 9 \cdot 3 \equiv 9 \cdot 9 \cdot 9 \cdot 3 = 81 \cdot 27 \equiv 3 \pmod{91}$.]

3.15. Mostrare che, se n è un numero pseudoprimo (in base 2) dispari, allora anche $N := 2^n - 1$ è un numero pseudoprimo (in base 2) dispari.
Dunque, esistono infiniti numeri pseudoprimi (in base 2) dispari.
[Suggerimento: Sia $n = r \cdot s$ con $2^n - 2 = kn$, con $1 < r, s < n$ e $k \geqslant 1$. L'intero N è composto, in quanto $(2^r - 1) \mid (2^n - 1) = N$; infatti $(2^n - 1) = (2^r - 1)(2^{s(r-1)} + 2^{s(r-2)} + \cdots + 2^s + 1)$. Inoltre,

$$2^{N-1} = 2^{2^n - 2} = 2^{kn}$$

Poiché $N = (2^n - 1) \mid (2^{kn} - 1)$, abbiamo che $N \mid (2^{N-1} - 1)$ cioè $2^{N-1} \equiv 1 \pmod N$.]

4 Generalità sulle congruenze polinomiali, Teorema di Lagrange e Teorema di Chevalley

Sia $f(X)$ un polinomio non nullo a coefficienti interi ed n un intero positivo. Ci occuperemo ora della ricerca delle (eventuali) soluzioni della congruenza polinomiale:

$$f(X) \equiv 0 \pmod{n}. \tag{1}$$

Vale in proposito il seguente risultato:

Teorema 4.1. *Sia $n = p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$, con p_i primo, $e_i \geqslant 1$ ed $r \geqslant 1$. Le soluzioni della congruenza (1) coincidono con le soluzioni del sistema di congruenze:*

$$\begin{cases} f(X) \equiv 0 \pmod{p_i^{e_i}} \\ 1 \leqslant i \leqslant r\ . \end{cases} \tag{2}$$

Dimostrazione. Se $\mathring{x}$ è una soluzione di (1), ovviamente $\mathring{x}$ è anche soluzione di ogni congruenza del sistema (2). Viceversa, se $\mathring{x}$ è soluzione di (2), allora $p_i^{e_i} \mid f(\mathring{x})$ per ogni i, e, poiché $\mathrm{MCD}(p_i^{e_i}, p_j^{e_j}) = 1$ (se $i \neq j$), possiamo concludere che $n = p_1^{e_1} \ldots p_r^{e_r} \mid f(\mathring{x})$ (cfr. Esercizio 1.2). $\square$

Osservazione 4.2. Supponiamo che, fissato i, con $1 \leq i \leq r$, $f(X) \equiv 0 \pmod{p_i^{e_i}}$ ammetta s_i soluzioni distinte, che denotiamo con y_{ij_i} $(1 \leqslant j_i \leqslant s_i)$. Posto $s := \prod_{i=1}^{r} s_i$, al variare di i, $1 \leqslant i \leqslant r$, per ogni scelta di y_{ij_i} con $1 \leqslant j_i \leqslant s_i$ si ottiene un sistema di congruenze lineari del tipo:

$$\begin{cases} X \equiv y_{ij_i} \pmod{p_i^{e_i}} \\ 1 \leqslant i \leqslant r\ . \end{cases}$$

In base al Teorema Cinese dei Resti ed al Teorema 4.1, ciascuno di tali s sistemi di congruenze fornisce una sola soluzione alla congruenza (1) ed è evidente che sistemi diversi forniscono soluzioni incongruenti (modulo n); dunque (2) ammette $s = \prod_{i=1}^{r} s_i$ soluzioni distinte.
Dal precedente ragionamento discende che, se denotiamo con $\boldsymbol{N}(f(X), n)$ il numero delle soluzioni della congruenza (1) e se $n = hk$ con $\mathrm{MCD}(h, k) = 1$, allora:

$$\boldsymbol{N}(f(X), n) = \boldsymbol{N}(f(X), h) \cdot \boldsymbol{N}(f(X), k).$$

Ad esempio le soluzioni della congruenza:

$$X^2 + 3X + 2 \equiv 0 \pmod{6}$$

sono le stesse del sistema di congruenze:

$$\begin{cases} X^2 + 3X + 2 \equiv 0 \pmod 2 \\ X^2 + 3X + 2 \equiv 0 \pmod 3 \end{cases}$$

ovvero:

$$\begin{cases} X^2 + X \equiv 0 \pmod 2 \\ X^2 + 2 \equiv 0 \pmod 3 \,. \end{cases}$$

La prima congruenza del sistema ha soluzioni $\{y_{11} = 0, y_{12} = 1\} \pmod 2$, la seconda congruenza ha soluzioni $\{y_{21} = 1, y_{22} = 2\} \pmod 3$. Le soluzioni dei quattro sistemi seguenti, ottenuti variando $i, 1 \leqslant i \leqslant 2$, e $j, 1 \leqslant j \leqslant 2$,

$$\begin{cases} X \equiv y_{1i} \pmod 2 \\ X \equiv y_{2j} \pmod 3 \end{cases}$$

sono date da $x = 4,\ 1,\ 2,\ 5 \pmod 6$. Questi valori di x sono, dunque, tutte le soluzioni della congruenza data (mod 6).

Dalle considerazioni precedenti discende anche che il problema della risoluzione di (2) può essere ricondotto allo studio di due problemi.

I PROBLEMA: Determinare le soluzioni di un sistema di congruenze lineari del tipo:

$$\begin{cases} X \equiv a_i \pmod{m_i} \\ 1 \leqslant i \leqslant r \end{cases}$$

con $a_i \in \mathbb{Z}$ e $\mathrm{MCD}(m_i, m_j) = 1$ se $i \neq j$.

II PROBLEMA: Determinare le soluzioni di una congruenza polinomiale del tipo:

$$f(X) \equiv 0 \pmod{p^e}$$

con $f(X) \in \mathbb{Z}[X], f(X) \neq 0$, p primo ed $e \geqslant 1$.

Al I Problema dà completa risposta il Teorema Cinese dei Resti (cfr. Paragrafo 3). Un metodo di approccio al II Problema consiste in un procedimento di tipo induttivo:

II PROBLEMA (A): Determinare le soluzioni di una congruenza polinomiale del tipo:

$$f(X) \equiv 0 \pmod p$$

con $f(X) \in \mathbb{Z}[X], f(X) \neq 0$ e p primo.

II PROBLEMA (B): Supponendo di aver determinato le soluzioni di una congruenza polinomiale del tipo:

$$f(X) \equiv 0 \pmod{p^n},$$

determinare le soluzioni della congruenza:

$$f(X) \equiv 0 \pmod{p^{n+1}},$$

con $f(X) \in \mathbb{Z}[X], f(X) \neq 0$, p primo ed $n \geqslant 1$.

In altri termini, una soluzione di $f(X) \equiv 0 \pmod{p^e}$ per $e \geqslant 2$ è determinata per successive approssimazioni (a meno di potenze di p) a partire dalle soluzioni di $f(X) \equiv 0 \pmod{p}$. L'algoritmo che descriveremo è ispirato al cosiddetto metodo di Newton utilizzato in analisi.

Affrontiamo dapprima il II Problema (B). A tale scopo richiamiamo alcune proprietà formali dei polinomi.

Definizione 4.3. Sia $f(X) = \sum_{i=0}^{m} a_i X^i \in \mathbb{Z}[X]$. Si chiama *polinomio derivato di* $f(X)$ il polinomio:

$$(f(X))' := a_1 + 2a_2 X + \cdots + m a_m X^{m-1} = \sum_{i=1}^{m} i a_i X^{i-1}.$$

Per comodità di notazione il polinomio $(f(X))'$ verrà denotato in seguito anche con $f'(X)$, o semplicemente con f', se non ci saranno pericoli di ambiguità.
In generale, si chiama *k-esimo polinomio derivato di* $f(X)$ (con $k \geqslant 1$) il polinomio $f^{(k)} := f^{(k)}(X) := (f^{(k-1)}(X))'$.
Si conviene di porre $f(X) =: f^{(0)}(X)$.

Il seguente risultato è di dimostrazione immediata:

Lemma 4.4. *Siano $f, g \in \mathbb{Z}[X]$ ed $a \in \mathbb{Z}$. Allora:*
(a) $(f+g)' = f' + g'$;
(b) $(af)' = af'$;
(c) $(fg)' = f'g + fg'$. $\square$

Vale, inoltre, il seguente risultato "formale" analogo alla formula di Taylor:

Lemma 4.5. *Sia $f(X) = \sum_{i=0}^{m} a_i X^i \in \mathbb{Z}[X]$, con $m := \deg(f(X))$. Per ogni $\alpha \in \mathbb{Z}$ si ha:*

$$f(X+\alpha) = f(X) + \frac{f'(X)}{1!}\alpha + \frac{f''(X)}{2!}\alpha^2 + \cdots + \frac{f^{(m)}(X)}{m!}\alpha^m.$$

Inoltre, per ogni k tale che $0 \leqslant k \leqslant m$, risulta:

$$\frac{f^{(k)}(X)}{k!} \in \mathbb{Z}[X].$$

Dimostrazione. In base al Lemma 4.4 (a), (b) (cioè, per "la proprietà di linearità" della derivazione), è sufficiente limitarsi al caso in cui $f(X) = X^i$. In tal caso, $f^{(k)}(X) = i(i-1)\ldots(i-k+1)X^{i-k}$, per ogni k, con $0 \leq k \leqslant i$. Si ha allora, in base alla Definizione 4.3 ed alla nota formula del binomio di Newton[1]:

$$\begin{aligned} f(X+\alpha) = (X+\alpha)^i &= \sum_{k=0}^{i} \binom{i}{k} X^{i-k}\alpha^k = \\ &= \sum_{k=0}^{i} \frac{i(i-1)\ldots(i-k+1)}{k!} X^{i-k}\alpha^k = \\ &= \sum_{k=0}^{i} f^{(k)}(X)\frac{1}{k!}\alpha^k. \end{aligned}$$

L'ultima affermazione del lemma è ovvia, in quanto, in generale per

$$f(X) = \sum_{i=0}^{m} a_i X^i,$$

risulta:

$$\frac{f^{(k)}(X)}{k!} = \sum_{i=k}^{m} \binom{i}{k} a_i X^{i-k},$$

dove $\binom{i}{k}$, per $0 \leqslant k \leqslant i$, è un intero essendo uguale a $\frac{i!}{k!(i-k)!}$. □

Osservazione 4.6. Sia $f(X) \in \mathbb{Z}[X]$ come nel lemma precedente, se calcoliamo tale polinomio in un intero $\mathring{x} \in \mathbb{Z}$ e se poniamo $x := \mathring{x} + \alpha$ allora dal lemma precedente otteniamo la ben nota uguaglianza:

$$f(x) = f(\mathring{x}) + \frac{f'(\mathring{x})}{1!}(x-\mathring{x}) + \frac{f''(\mathring{x})}{2!}(x-\mathring{x})^2 + \cdots + \frac{f^{(m)}(\mathring{x})}{m!}(x-\mathring{x})^m.$$

Al Problema II (B) fornisce una risposta completa il seguente teorema:

Teorema 4.7. *Sia $f(X) \in \mathbb{Z}[X], f(X) \neq 0$; sia p un primo ed $n \in \mathbb{Z}, n > 0$. Supponiamo che la congruenza:*

$$f(X) \equiv 0 \pmod{p^n} \qquad (*_n)$$

[1]Presi comunque $\alpha, \beta \in \mathbb{Z}[X]$ (ovvero, più generalmente, presi in un qualunque anello con caratteristica 0), si dimostra facilmente per induzione su $r \geqslant 1$ che:

$$(\alpha+\beta)^r = \sum_{k=0}^{r} \binom{r}{k} \alpha^{r-k}\beta^k$$

sia risolubile e che, di questa congruenza, siano note le soluzioni $\{y_1, \ldots, y_r\}$ $(\mathrm{mod}\ p^n)$. *Consideriamo la congruenza:*

$$f(X) \equiv 0 \pmod{p^{n+1}} \qquad (*_{n+1})$$

Le (eventuali) soluzioni di $(*_{n+1})$ $(\mathrm{mod}\ p^{n+1})$ *sono della forma:*

$$x_t := y + tp^n,$$

dove y *è una soluzione di* $(*_n)$ *e* $t \in \mathbb{Z}$, $0 \leqslant t \leqslant p-1$. *Precisamente si presentano tre casi:*

I Caso. *Se* $f'(y) \not\equiv 0 \pmod{p}$, x_t *è soluzione di* $(*_{n+1})$ *se, e soltanto se, risulta:*

$$t \equiv -\frac{f(y)}{p^n}(f'(y))^{p-2} \pmod{p}.$$

II Caso. *Se* $f'(y) \equiv 0 \pmod{p}$ *e* $f(y) \equiv 0 \pmod{p^{n+1}}$, *allora* x_t *è soluzione di* $(*_{n+1})$, *per ogni* t, *con* $0 \leqslant t \leqslant p-1$.

III Caso. *Se* $f'(y) \equiv 0 \pmod{p}$ *e* $f(y) \not\equiv 0 \pmod{p^{n+1}}$, x_t *non è soluzione di* $(*_{n+1})$, *per nessun valore di* t, *con* $0 \leqslant t \leqslant p-1$.

Conseguentemente, la soluzione y *di* $(*_n)$, $y \in \{y_1, \ldots, y_r\}$, *determina:*

- *nel* I Caso, *una ed una sola soluzione di* $(*_{n+1})$ $(\mathrm{mod}\ p^{n+1})$, *e cioè:*

$$x := y - f(y)(f'(y))^{p-2};$$

- *nel* II Caso, p *soluzioni distinte di* $(*_{n+1})$ $(\mathrm{mod}\ p^{n+1})$, *e cioè:*

$$x_t = y + tp^n, \quad 0 \leqslant t \leqslant p-1;$$

- *nel* III Caso, *nessuna soluzione di* $(*_{n+1})$ $(\mathrm{mod}\ p^{n+1})$.

[Nel I Caso, y è detta *soluzione non singolare* di $(*_n)$, mentre negli altri casi, y è detta *soluzione singolare* di $(*_n)$.]

Dimostrazione. Una (eventuale) soluzione di $(*_{n+1})$ è ovviamente soluzione di $(*_n)$ e dunque $x \equiv y \pmod{p^n}$, per un qualche y soluzione di $(*_n)$, cioè $y \in \{y_1, \ldots, y_r\}$, ovvero $x = y + kp^n$, dove k è un intero opportuno. Poiché la soluzione x deve essere determinata $(\mathrm{mod}\ p^{n+1})$, allora dividendo k per p, abbiamo $k = qp + t$, dove $0 \leqslant t \leqslant p-1$. Quindi:

$$x = x_t := y + tp^n\,, \ \ 0 \leqslant t \leqslant p-1\ .$$

Si noti che $f(y) \equiv 0 \pmod{p^n}$, quindi $f(y)/p^n \in \mathbb{Z}$.
In base al Lemma 4.5, posto $m := \deg(f(X))$, si ha:

$$f(x_t) = f(y + tp^n) = f(y) + \frac{f'(y)}{1!}tp^n + \cdots + \frac{f^{(m)}(y)}{m!}(tp^n)^m.$$

Poiché $n+1 \leqslant 2n < \cdots < n \cdot m$, si ha $0 \equiv p^{2n} \equiv \cdots \equiv p^{nm} \pmod{p^{n+1}}$ e quindi, dall'uguaglianza precedente, si ottiene:

$$f(x_t) \equiv f(y) + f'(y)tp^n \pmod{p^{n+1}}.$$

Pertanto $x_t = y + tp^n$ è soluzione di $(*_n)$ se, e soltanto se, esiste t, con $0 \leqslant t \leqslant p-1$, tale che:

$$0 \equiv f(y) + f'(y)tp^n \pmod{p^{n+1}},$$

ovvero, "cancellando" p^n (cfr. Proposizione 1.9):

$$f'(y)t \equiv -\frac{f(y)}{p^n} \pmod{p}.$$

In conclusione, per ogni y soluzione di $(*_n)$, poniamo:

$$a = a(y) := f'(y), \quad b = b(y) := -\frac{f(y)}{p^n}.$$

Allora, per risolvere $(*_{n+1})$ ci siamo ricondotti a discutere della risolubilità della congruenza lineare in una nuova indeterminata (denotata T) con coefficienti $a = a(y)$, $b = b(y)$ che dipendono da y, al variare di y tra le soluzioni di $(*_n)$:

$$aT \equiv b \pmod{p} \qquad (\bullet_y)$$

Per tale congruenza $(\bullet_y)$, distinguiamo tre casi:
I Caso. Se $a \not\equiv 0 \pmod{p}$, per ogni $y \in \{y_1, \ldots, y_r\}$, la congruenza lineare $(\bullet_y)$ ha una ed una sola soluzione $t \equiv a^* \cdot b \equiv a^{p-2}b \pmod{p}$.
In tal caso, $x_t = y + p^n t \equiv y - p^n \frac{f(y)}{p^n}(f'(y))^{p-2} = y - f(y)(f'(y))^{p-2} \pmod{p^{n+1}}$ è l'unica soluzione di $(*_{n+1}) \pmod{p^{n+1}}$ determinata dalla soluzione y di $(*_{n+1})$.
II Caso. Se $a \equiv b \equiv 0 \pmod{p}$, la congruenza $(\bullet_y)$ degenera, cioè è soddisfatta per ogni t, con $0 \leqslant t \leqslant p-1$.
In tal caso, per ogni $y \in \{y_1, \ldots, y_r\}$, le soluzioni distinte di $(*_{n+1})$ (cioè non congruenti modulo p^{n+1}) sono esattamente p, e sono date da:

$$x_t = y + tp^n, \quad 0 \leqslant t \leqslant p-1.$$

III Caso. Se $a \equiv 0 \pmod{p}$ e $b \not\equiv 0 \pmod{p}$, allora $(\bullet_y)$ non è risolubile. Quindi, $x_t = y + tp^n$ non è mai soluzione di $(*_{n+1})$, comunque si prenda t, con $0 \leqslant t \leqslant p-1$. Cioè, in altri termini, la soluzione $y \in \{y_1, \ldots, y_r\}$ di $(*_n)$ non determina alcuna soluzione di $(*_{n+1})$. $\square$

Vogliamo illustrare il risultato precedente con quattro esempi.

Esempio 4.8. Consideriamo la congruenza:

$$X^4 - 1 \equiv 0 \pmod{25}.$$

Notiamo, innanzitutto, che $X^4 - 1 \equiv 0 \pmod 5$, per il "Piccolo" Teorema di Fermat, ha quattro soluzioni: $y_1 = 1, y_2 = 2, y_3 = 3, y_4 = 4$.
Se $f(X) := X^4 - 1$ allora $f'(X) = 4X^3$. Essendo $f'(y_i) \not\equiv 0 \pmod 5$ per ogni $1 \leqslant i \leqslant 4$, allora ciascuna y_i determina un'unica soluzione di $f(X) \equiv 0 \pmod{25}$ data da:

$$x_i := y_i + \bar{t}_i \cdot 5,$$

dove $\bar{t}_i$ è l'unica soluzione $\pmod 5$ della seguente congruenza lineare nella indeterminata T associata ad y_i (che denotiamo semplicemente con $(\bullet_i)$ invece che con $(\bullet_{y_i})$):

$$a(y_i)T \equiv b(y_i) \pmod 5 \qquad (\bullet_i)$$

dove $a(y_i) := f'(y_i)$ e $b(y_i) := -\frac{f(y_i)}{5}$, per $1 \leqslant i \leqslant 4$.
Per $i = 1$, $a(1) = 4$, $b(1) = 0$, quindi la congruenza:

$$4T \equiv 0 \pmod 5 \qquad (\bullet_1)$$

ha come soluzione $\bar{t}_1 = 0$, dunque $x_1 = y_1 = 1 \pmod{25}$.
Per $i = 2$, $a(2) = 32$, $b(2) = -3$, quindi la congruenza:

$$2T \equiv -3 \pmod 5 \qquad (\bullet_2)$$

ha come soluzione $\bar{t}_2 = 1$, dunque $x_2 = 2 + 1 \cdot 5 = 7 \pmod{25}$.
Per $i = 3$, $a(3) = 108$, $b(3) = -16$, quindi la congruenza:

$$3T \equiv -1 \pmod 5 \qquad (\bullet_3)$$

ha come soluzione $\bar{t}_3 = 3$, dunque $x_3 = 3 + 3 \cdot 5 = 18 \pmod{25}$.
Per $i = 4$, $a(4) = 256$, $b(4) = -51$, quindi la congruenza:

$$T \equiv -1 \pmod 5 \qquad (\bullet_4)$$

ha come soluzione $\bar{t}_4 = -1$, dunque $x_4 = 4 - 5 = -1 \equiv 24 \pmod{25}$.

Può essere utile riassumere il procedimento precedente nella seguente tabella:

p	n	$p^n \rightsquigarrow p^{n+1}$	$f(X)$	$f'(X)$
5	1	$5 \rightsquigarrow 25$	$X^4 - 1$	$4X^3$

$\bmod p^n$	$\bmod p$				$\bmod p^{n+1}$
y	$f'(y)$	$\frac{f(y)}{p^n}$	$f'(y)T \equiv \frac{-f(y)}{p^n}$	t	$x_t = y + tp^n$
1	4	0	$4T \equiv 0$	0	1
2	32	3	$2T \equiv -3$	1	7
3	108	16	$3T \equiv -1$	3	18
4	256	51	$T \equiv -1$	4	24

Il precedente esempio può essere generalizzato nella maniera seguente:

Esempio 4.9. Sia p un primo ed e un intero $\geqslant 1$. La congruenza:

$$f(X) := X^{p-1} - 1 \equiv 0 \pmod{p^e}$$

ha esattamente $p-1$ soluzioni distinte.
Infatti, se $e = 1$, tale risultato è un'ovvia conseguenza del "Piccolo" Teorema di Fermat. Sia $e \geqslant 2$ e sia y una soluzione di $f(X) \equiv 0 \pmod{p^{e-1}}$. È subito visto che $f'(y) = (p-1)y^{p-2} \not\equiv 0 \pmod{p}$ (essendo $y^{p-1} \equiv 1 \pmod{p}$) e, dunque, si è nel I Caso del Teorema 4.7.

Esempio 4.10. Consideriamo la congruenza:

$$X^{10} - 1 \equiv 0 \pmod{25}.$$

Notiamo innanzitutto che la congruenza

$$X^{10} - 1 \equiv 0 \pmod{5}$$

ha due soluzioni: $y_1 = 1, y_2 = 4$.
Infatti $X^{10} = (X^4)^2X^2$, dunque $X^{10} - 1 \equiv (X^4)^2X^2 - 1 \pmod{5}$. Dal momento che, per il "Piccolo" Teorema di Fermat, $x^4 \equiv 1 \pmod{5}$, per ogni x non congruo a $0 \pmod{5}$, allora le soluzioni di $X^{10} - 1 \equiv 0 \pmod{5}$ coincidono con le soluzioni di $X^2 - 1 \equiv 0 \pmod{5}$, che sono appunto $y_1 = 1$ ed $y_2 = 4$ (per maggiori dettagli, cfr. anche la successiva Definizione 4.12 (e)).
Se $f(X) := X^{10} - 1$, allora $f'(X) = 10X^9$ e quindi $f'(y_i) \equiv 0 \pmod{5}$ per $i = 1, 2$. Inoltre, $f(y_i) \equiv 0 \pmod{25}$, per $i = 1, 2$ (ciò è ovvio per $y_1 = 1$, per $y_2 = 4$ è subito visto che $4^5 \equiv -1 \pmod{25}$. Infatti, $4^2 \equiv -9 \pmod{25}, 4^4 \equiv 81 \equiv 6 \pmod{25}, 4^5 \equiv 24 \equiv -1 \pmod{25}$, dunque $4^{10} \equiv (-1)^2 = 1 \pmod{25}$. Pertanto, y_1 determina le seguenti 5 soluzioni della congruenza data:

$$x_{1,t} := 1 + t \cdot 5, \quad \text{per} \quad 0 \leqslant t \leqslant 4.$$

Analogamente, y_2 determina le seguenti 5 soluzioni della congruenza data:

$$x_{2,t} := 4 + t \cdot 5, \quad \text{per} \quad 0 \leqslant t \leqslant 4.$$

In conclusione, la congruenza assegnata ha 10 soluzioni $\pmod{25}$. Può essere utile riassumere il procedimento precedente nella seguente tabella:

p	n	$p^n \rightsquigarrow p^{n+1}$	$f(X)$	$f'(X)$
5	1	$5 \rightsquigarrow 25$	$X^{10}-1$	$10X^9$

mod p^n	mod p				mod p^{n+1}
y	$f'(y)$	$\frac{f(y)}{p^n}$	$f'(y)T \equiv \frac{-f(y)}{p^n}$	t	$x_t = y + tp^n$
1	0	0	$\curvearrowright$	$0,1,2,3,4$	$1,6,11,16,21$
4	0	0	$\curvearrowright$	$0,1,2,3,4$	$74,9,14,19,24$

L'esempio precedente si generalizza nella forma seguente:

Esempio 4.11. Sia p un primo dispari. La congruenza:

$$f(X) = X^{p\frac{p-1}{2}} - 1 \equiv 0 \pmod{p^2} \qquad (*_2)$$

ammette $\frac{p(p-1)}{2}$ soluzioni distinte.
Si verifica preliminarmente che la congruenza $f(X) \equiv 0 \pmod{p}$ ammette esattamente $\frac{p-1}{2}$ soluzioni distinte.
Osserviamo, innanzitutto, che le soluzioni di:

$$f(X) = X^{p\frac{p-1}{2}} - 1 \equiv 0 \pmod{p} \qquad (*_1)$$

sono le stesse di quelle della congruenza:

$$g(X) = X^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$$

dal momento che la congruenza $X^p \equiv X \pmod{p}$ ha come soluzioni tutti gli elementi di un sistema completo di residui (cfr. per maggiori dettagli la successiva Definizione 4.12 (e)).
Mostriamo, poi, che $g(X) \equiv 0 \pmod{p}$ ha esattamente $\frac{p-1}{2}$ soluzioni $\pmod{p}$. Per questo, abbiamo bisogno del seguente

Lemma 4.12. *Sia p un primo dispari. Le due congruenze:*

$$X^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p} \qquad (*)$$

$$X^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p} \qquad (**)$$

ammettono ciascuna $\frac{p-1}{2}$ soluzioni distinte (modulo p). L'unione di tali insiemi di soluzioni costituisce un sistema ridotto di residui (modulo p).

Dimostrazione. Certamente $x = 0$ non è soluzione nè di $(*)$ nè di $(**)$ e le due congruenze non possono ammettere soluzioni comuni perché $p > 2$. Considerato il sistema ridotto di residui $S^* = \{1, 2, \ldots, p-1\}$, basterà allora provare che (almeno) $\frac{p-1}{2}$ elementi di S^* verificano $(*)$ e che (almeno) altrettanti verificano $(**)$.
Osserviamo innanzitutto che gli interi

$$1^2, 2^2, \ldots, \left[\frac{p-1}{2}\right]^2$$

sono primi con p e, a due a due incongruenti (modulo p).
Infatti se h, k sono interi tali che $1 \leqslant h, k \leqslant \frac{p-1}{2}$ e $h^2 \equiv k^2 \pmod{p}$, allora, $h^2 - k^2 = (h+k)(h-k) \equiv 0 \pmod{p}$ e quindi, $h \equiv k \pmod{p}$ (da cui $h = k$), oppure $h \equiv -k \pmod{p}$, cioè $h \equiv p-k \pmod{p}$, e perciò $h = p-k$, il che è assurdo.
Pertanto è possibile costruire un sistema ridotto di residui (modulo p), diciamo U^*, scegliendo opportunamente altri $\frac{p-1}{2}$ interi, che denotiamo con $t_1, \ldots, t_{\frac{p-1}{2}}$, nella maniera seguente:

$$U^* := \{1^2, 2^2, \ldots, \left[\frac{p-1}{2}\right]^2, t_1, \ldots, t_{\frac{p-1}{2}}\}.$$

Confrontando S^* con U^*, è chiaro che, per $\frac{p-1}{2}$ elementi $a \in S^*$, risulta $a \equiv h^2 \pmod{p}$ (con $1 \leqslant h \leqslant \frac{p-1}{2}$), mentre per altri $\frac{p-1}{2}$ elementi $a \in S^*$ risulta $a \equiv t_i \pmod{p}$ (con $1 \leqslant i \leqslant \frac{p-1}{2}$).
I Caso: Sia $a \equiv h^2 \pmod{p}$, con $1 \leqslant h \leqslant \frac{p-1}{2}$. Allora $a^{\frac{p-1}{2}} \equiv h^{p-1} \equiv 1 \pmod{p}$ (infatti $p \nmid h$ e, dunque, è applicabile il Teorema 3.1): pertanto a è soluzione di $(*)$.
II Caso: Sia $a \in S^*$ tale che $a \equiv t_i \pmod{p}$. Per ogni $k \in S^*$, l'insieme $T^* := \{k, 2k, \ldots, (p-1)k\}$ è ancora un sistema ridotto di residui (modulo p) (cfr. Esercizio 2.10) e, dunque, esiste un unico elemento $k' \in S^*$ tale che $kk' \equiv a \pmod{p}$. L'elemento k' è detto *associato di k relativamente ad a* $\pmod{p}$ e, per ipotesi, è distinto da k. Infatti, se fosse $k = k'$, allora $a \equiv k^2 \equiv (p-k)^2 \pmod{p}$ e uno dei due interi $k, p-k$ dovrebbe essere minore o uguale a $\frac{p-1}{2}$. Ciò è escluso, in quanto stiamo supponendo $a \equiv t_i \pmod{p}$ (con $1 \leqslant i \leqslant \frac{p-1}{2}$).
Allora, fissato $a \in S^*$ con $a \equiv t_i \pmod{p}$, gli elementi di S^* si ripartiscono in due sottoinsiemi (disgiunti) di elementi non associati, cioè:

$$S^* : \{h_1, \ldots, h_{\frac{p-1}{2}}\} \sqcup \{h'_1, \ldots, h'_{\frac{p-1}{2}}\}$$

in modo che:

$$h_j h'_j \equiv a \pmod{p},\ 1 \leqslant j \leqslant \frac{p-1}{2}.$$

Ne segue che:

$$(p-1)! = h_1 h'_1 \ldots h_{\frac{p-1}{2}} h'_{\frac{p-1}{2}} \equiv \underbrace{a \cdot a \cdot \cdots \cdot a}_{(p-1)/2 \text{ volte}} = a^{\frac{p-1}{2}} \pmod{p}$$

e dunque, in base al Teorema di Wilson:

$$(p-1)! \equiv -1 \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

In tal caso, a è soluzione di $(**)$ e la tesi è così dimostrata. $\square$

Esempio 4.10 (seguito). Abbiamo visto sopra che le soluzioni di $(*_1)$ coincidono con quelle di $(*)$. Sia y una delle $\frac{p-1}{2}$ soluzioni distinte di

$$X^{p\left(\frac{p-1}{2}\right)} - 1 \equiv 0 \pmod{p}.$$

allora: $f'(y) = p\left(\frac{p-1}{2}\right) \cdot y^{p\left(\frac{p-1}{2}\right)-1} \equiv 0 \pmod{p}$. Inoltre, si vede facilmente che $f(y) \equiv 0 \pmod{p^2}$. Infatti $y^{p\left(\frac{p-1}{2}\right)} - 1 = kp$ per qualche k, elevando al quadrato abbiamo che

$$k^2p^2 = (y^{p\left(\frac{p-1}{2}\right)} - 1)^2 = y^{p(p-1)} + 1 - 2y^{p\left(\frac{p-1}{2}\right)} \qquad (\diamondsuit)$$

Inoltre, $\varphi(p^2) = p(p-1)$ e quindi per il Teorema di Euler:

$$z^{p(p-1)} \equiv 1 \pmod{p^2}$$

per ogni z relativamente primo con p^2. Dunque, per $z = y$, da $(\diamondsuit)$ abbiamo che:

$$0 \equiv 2 - 2y^{p\left(\frac{p-1}{2}\right)} \pmod{p^2}$$

e dunque che

$$y^{p\left(\frac{p-1}{2}\right)} - 1 \equiv 0 \pmod{p^2}.$$

Dunque siamo nella condizione del II Caso del Teorema 4.7 e ciò permette di concludere quanto enunciato nell'Esempio 4.11.

Veniamo ora al Problema II (A). Non esiste un procedimento teorico generale per determinare se una congruenza del tipo:

$$f(X) \equiv 0 \pmod{p},$$

con p primo e $f(X) \in \mathbb{Z}[X]$, ammetta soluzioni e, nel caso affermativo, per calcolarle esplicitamente. Ci limiteremo qui a svolgere semplici considerazioni generali tendenti a semplificare il problema e che, comunque, saranno utili nel seguito per la risoluzione delle congruenze quadratiche (modulo p), cioè congruenze del tipo $f(X) \equiv 0 \pmod{p}$, dove $f(X) \in \mathbb{Z}[X]$ e $\deg(f) = 2$.

Cominciamo con la seguente definizione che estende ai polinomi a coefficienti in $\mathbb{Z}$ la nozione di congruenza (mod n):

Definizione 4.13. Sia $n \in \mathbb{Z}, n > 0$ e siano

$$f = \sum_{i=0}^{r} a_i X^i, \quad g = \sum_{j=0}^{s} b_j X^j \in \mathbb{Z}[X].$$

(a) Si dice che il polinomio f è *identicamente congruo a zero modulo* n (in simboli, $f(X) \equiv_X 0 \pmod{n}$) se $a_i \equiv 0 \pmod{n}$ preso comunque $1 \leqslant i \leqslant r$.

(b) Si dice che f è *identicamente congruo a g modulo n* (e si scrive $f \equiv_X g \pmod{n}$) se $f - g$ è identicamente congruo a zero modulo n (cioè se risulta $a_i \equiv b_i \pmod{n}$, per ogni i tale che $0 \leqslant i \leqslant \min(r,s)$ e se ad esempio $r = \min(r,s) < s$ allora $b_j \equiv 0 \pmod{n}$, per ogni j, con $r+1 \leqslant j \leqslant s$).

(c) Se $f(X) \not\equiv_X 0 \pmod{n}$, si chiama *grado di f modulo n* (e si scrive $\deg_n(f)$) il massimo intero m tale che $a_m \not\equiv 0 \pmod{n}$.

(d) Si dice che f *divide g modulo n* (e si scrive $f \mid g \pmod{n}$) se esiste $h \in \mathbb{Z}[X]$ tale che $fh \equiv_X g \pmod{n}$.

(e) Si dice inoltre che $f(X)$ è *equivalente a $g(X)$ modulo n*, (in simboli $f(X) \sim g(X) \pmod{n}$) se, per ogni $a \in \mathbb{Z}$, $f(a) \equiv g(a) \pmod{n}$.

Se $f(X) \sim g(X) \pmod{n}$, allora le congruenze:

$$f(X) \equiv 0 \pmod{n} \quad \text{e} \quad g(X) \equiv 0 \pmod{n}$$

hanno le stesse soluzioni (modulo n).

Osservazione 4.14. **(1)** Si consideri l'omomorfismo suriettivo tra anelli di polinomi:

$$\bar{\varphi}_n : \mathbb{Z}[X] \longrightarrow (\mathbb{Z}/n\mathbb{Z})[X],\ f \mapsto \bar{f},$$

che estende in modo naturale l'omomorfismo canonico suriettivo

$$\varphi_n : \mathbb{Z} \longrightarrow (\mathbb{Z}/n\mathbb{Z}),$$

(cioè $\bar{\varphi}_n$ è così definito:
per ogni $f := \sum_{i=0}^{m} a_i X^i \in \mathbb{Z}[X]$, $\bar{\varphi}_n(f) = \bar{f} := \sum_{i=0}^{m} \bar{a}_i X^i$, con $\bar{a}_i := a_i + n\mathbb{Z} =: \varphi_n(a)$).
È del tutto evidente che:
(a′) $f \equiv_X 0 \pmod{n} \iff \bar{f} = 0$ (in $(\mathbb{Z}/n\mathbb{Z})[X]$);
(b′) $f \equiv_X g \pmod{n} \iff \bar{f} = \bar{g}$ (in $(\mathbb{Z}/n\mathbb{Z})[X]$);
(c′) $\deg_n(f) = \deg(\bar{f})$;
(d′) $f \mid g \pmod{n} \iff \bar{f} \mid \bar{g}$ (in $(\mathbb{Z}/n\mathbb{Z})[X]$).
(2) Si noti che, per ogni intero $n \geqslant 0$, se $f \equiv_X g \pmod{n}$, allora $\deg_n(f) = \deg_n(g)$. Si noti, inoltre, che se p è un numero primo e $f, g \in \mathbb{Z}[X]$ sono due polinomi non identicamente congrui a 0 (mod p), allora $\deg_p(fg) = \deg_p(f) + \deg_p(g)$. Una uguaglianza di tale tipo in generale non vale (mod n), se n non è un primo: ad esempio se $f = 2X - 1$, $g = 2X + 1$ e se $n = 4$, allora $\deg_n(fg) = 0$ mentre $\deg_n(f) = \deg_n(g) = 1$.

Proposizione 4.15. *Siano $a, n \in \mathbb{Z}$, $n > 0$ ed $f, g \in \mathbb{Z}[X]$. Risulta:*
(a) $(X - a) \mid f \pmod{n}$ *se, e soltanto se,* $f(a) \equiv 0 \pmod{n}$.
(b) *Se* $f \equiv_X g \pmod{n}$, *allora* $f \sim g \pmod{n}$. *In particolare, quindi, le congruenze:*

$$f(X) \equiv 0 \pmod{n} \quad e \quad g(X) \equiv 0 \pmod{n}$$

hanno le stesse soluzioni.

Dimostrazione. Semplice esercizio. □

Osservazione 4.16. La prima affermazione della Proposizione 4.15 (b) non si inverte, in generale. Ad esempio posto $f(X) = X$, $g(X) = X^p$ con p primo, si ha che $f \not\equiv_X g \pmod p$ (cfr. Definizione 4.13 (b)), mentre $f(a) \equiv g(a) \pmod p$, per ogni $a \in \mathbb{Z}$, cioè $f \sim g \pmod p$ (cfr. Corollario 3.2).

Corollario 4.17. *Sia $n \in \mathbb{Z}, n > 0$, e sia $f := \sum_{i=0}^{m} a_i X^i \in \mathbb{Z}[X]$. Posto $\hat{f}(X) := \sum_{i=0}^{m} \hat{a}_i X^i$ con $a_i \equiv \hat{a}_i \pmod n, 0 \leqslant \hat{a}_i \leqslant n-1$ e $0 \leqslant i \leqslant m$, allora $\deg_n(f) = \deg(\hat{f})$ ed inoltre:*

$$f(X) \equiv_X \hat{f}(X) \pmod n. \qquad \square$$

Corollario 4.18. *Sia p primo ed $f(X) \in \mathbb{Z}[X]$. Esiste un polinomio $\widetilde{f}(X) \in \mathbb{Z}[X]$ di grado $\leqslant p-1$, eventualmente uguale al polinomio nullo, tale che:*

$$f(X) \sim \widetilde{f}(X) \pmod p.$$

Dimostrazione. Sia $f(X) := \sum_{i=0}^{m} a_i X^i$ con $m := \deg_p(f(X))$.
Se $m \leqslant p-1$, si pone $\widetilde{f} := f$.
Se invece $m \geqslant p$, si pone:

$$\widetilde{f} := \sum_{i=0}^{p-1} a_i X^i + \sum_{j=p}^{m} a_j X^{r_j},$$

dove r_j, con $1 \leqslant r_j \leqslant p-1$, è il "resto" del seguente "tipo particolare" di divisione di j per $p-1$:

$$j = q_j(p-1) + r_j, \text{ (con } p \leqslant j \leqslant m).$$

In altri termini sostituiamo X^p con X, essendo $X^p \sim X$, X^{p+1} con X^2, essendo $X^{p+1} \sim X^2$, etc.. Utilizzando il "Piccolo" Teorema di Fermat, si verifica subito che:
$f(a) - \widetilde{f}(a) \equiv 0 \pmod p$ per ogni $a \in \mathbb{Z}$ e da ciò segue la tesi. □

Per illustrare il Corollario 4.18, si noti che se p è un primo dispari e $f(X) := X^{p\left(\frac{p-1}{2}\right)} - 1$ allora $\widetilde{f}(X) = X^{\frac{p-1}{2}} - 1$. Abbiamo già notato sopra (Esempio 4.11) che:

$$f(X) \sim \widetilde{f}(X) \pmod p.$$

Teorema 4.19. (**Teorema di Lagrange**)
Sia p un primo ed $f \in \mathbb{Z}[X]$ tale che $\deg_p(f) = m \geqslant 1$. La congruenza:

$$f(X) \equiv 0 \pmod p$$

ammette al più m soluzioni distinte (cioè incongruenti modulo p).

Dimostrazione. Si procede per induzione su $m \geqslant 1$.
Se $m = 1$, allora $f(X) \equiv a_0 + a_1 X \equiv 0 \pmod{p}$, con $\mathrm{MCD}(a_1, p) = 1$. In tal caso è ben noto (cfr. Lemma 2.3) che la congruenza ammette un'unica soluzione (modulo p).
Sia $m \geqslant 2$ ed assumiamo che il teorema sia vero per ogni polinomio di grado positivo $\leqslant m-1$ (modulo p). Se la congruenza in esame non ha soluzioni, la tesi è ovvia; se viceversa $a \in \mathbb{Z}$ ne è una soluzione, si divide $f(X)$ per $X - a$ ottenendo un polinomio $q(X) \in \mathbb{Z}[X]$ tale che:

$$f(X) = (X - a)q(X) + f(a).$$

Da ciò segue che $f(X) \equiv_X (X - a)q(X) \pmod{p}$ e pertanto le congruenze:

$$f(X) \equiv 0 \pmod{p} \quad \text{e} \quad (X - a)q(X) \equiv 0 \pmod{p}$$

hanno lo stesso insieme di soluzioni (mod p). Se ora $b \in \mathbb{Z}$ è un'altra soluzione della prima congruenza e se $b \not\equiv a \pmod{p}$, allora $(b - a)q(b) \equiv 0 \pmod{p}$ e quindi, essendo p primo, $q(b) \equiv 0 \pmod{p}$.
Tenendo presente che $\deg_p(q) \leqslant m - 1$, la tesi discende immediatamente dalla ipotesi induttiva applicata alla congruenza $q(X) \equiv 0 \pmod{p}$. □

Corollario 4.20. *Siano f, p ed m come nel Teorema 4.19 e sia $\widetilde{f}$ in $\mathbb{Z}[X]$ come nel Corollario 4.18 (cioè $f \sim \widetilde{f} \pmod{p}$ e $\deg_p(\widetilde{f}) \leqslant p - 1$), allora la congruenza $f(X) \equiv 0 \pmod{p}$ ha al più $\widetilde{m}$ soluzioni distinte* (mod p)*, dove $\widetilde{m} := \deg_p(\widetilde{f}) \leqslant \deg_p(f)$.*

Dimostrazione. Semplice conseguenza del Teorema 4.19, applicato ad $\widetilde{f}$, dal momento che le congruenze

$$f(X) \equiv 0 \pmod{p} \quad \text{e} \quad \widetilde{f}(X) \equiv 0 \pmod{p}$$

hanno le stesse soluzioni (modulo p). □

Esempio 4.21. Sia $p = 3$, $f(X) = X^5 + X + 1$. Allora $\deg_3(f) = 5$, $X^5 \sim X^3 \sim X \pmod{3}$, quindi $\widetilde{f} := X + X + 1 = 2X + 1$. Pertanto le soluzioni della congruenza $X^5 + X + 1 \equiv 0 \pmod{3}$ sono al più tante quante le soluzioni di $2X + 1 \equiv 0 \pmod{3}$, cioè una. Precisamente, $\widetilde{f}(X) \equiv 0 \pmod{3}$ (e $f(X) \equiv 0 \pmod{3}$) hanno un'unica soluzione, che è data da $x \equiv 1 \pmod{3}$.

Osservazione 4.22. Il Teorema di Lagrange non vale, in generale, per congruenze modulo un intero non primo. Ad esempio, la congruenza:

$$X^2 - 1 \equiv 0 \pmod{8}$$

ammette quattro soluzioni distinte (e cioè $1, 3, 5, 7$), pur essendo il polinomio di secondo grado, $\deg_8(X^2 - 1) = 2$. Per un'estensione di questo esempio rinviamo al successivo Esercizio 4.4.

Corollario 4.23. *Conservando le notazioni ed ipotesi del Teorema 4.19 e denotando con $a_1, a_2, \ldots, a_t$ $(0 \leqslant t \leqslant m)$ le soluzioni distinte di $f(X) \equiv 0 \pmod p$, si ha:*

$$f(X) \equiv_X g(X)(X-a_1)^{e_1}(X-a_2)^{e_2} \cdot \cdots \cdot (X-a_t)^{e_t} \pmod p$$

dove $e_1, e_2, \ldots, e_t$ sono interi positivi tali che $\sum_{i=1}^{t} e_i \leqslant m$ e dove $g(X)$ in $\mathbb{Z}[X]$, $\deg_p(g) \geqslant 0$ e la congruenza $g(X) \equiv 0 \pmod p$ non è risolubile.

Dimostrazione. Basta iterare l'argomentazione usata nella dimostrazione del Teorema 4.19. □

Proposizione 4.24. *Sia p primo, $f \in \mathbb{Z}[X]$ e t il numero delle soluzioni distinte della congruenza:*

$$f(X) \equiv 0 \pmod p.$$

Risulta:

$$t = \deg_p(f) \iff f \mid (X^p - X) \pmod p.$$

Dimostrazione. Notiamo innanzitutto che, per il Corollario 4.23,

$$X^p - X \equiv_X X(X-1)(X-2) \cdot \cdots \cdot (X-(p-1)) \pmod p$$

$(\Rightarrow)$ Se $t = \deg_p(f)$, allora per il Corollario 4.23

$$f(X) \equiv_X (X-a_1)(X-a_2) \cdot \cdots \cdot (X-a_t) \pmod p$$

con $\{a_1, a_2, \ldots, a_t\} \subseteq \{0, 1, \ldots, p-1\}$.
Dunque è ovvio che $f(X) \mid (X^p - X) \pmod p$.
$(\Leftarrow)$ Se $f(X)g(X) \equiv_X X^p - X \pmod p$ per un qualche $g(X) \in \mathbb{Z}[X]$, allora per l'Osservazione 4.13 (2) $\deg_p(f(X)g(X)) = \deg_p(f(X)) + \deg_p(g(X)) = \deg_p(X^p - X) = p$ ed inoltre le seguenti congruenze:

$$X^p - X \equiv 0 \pmod p$$
$$f(X)g(X) \equiv 0 \pmod p \qquad (*_{fg})$$

hanno le stesse soluzioni. Poiché la prima congruenza ha p soluzioni, anche la seconda congruenza deve avere p soluzioni.
Osserviamo che le soluzioni della congruenza $(*_{fg})$ sono le soluzioni di almeno una delle seguenti due congruenze:

$$f(X) \equiv 0 \pmod p \qquad (*_f)$$
$$g(X) \equiv 0 \pmod p. \qquad (*_g)$$

Per il Teorema di Lagrange $(*_f)$ ha al più $\deg_p(f)$ soluzioni e $(*_g)$ ha al più $\deg_p(g)$ soluzioni, quindi $(*_{fg})$ ha al più $\deg_p(f(X)) + \deg_p(g(X)) = p$ soluzioni. Pertanto, affinché accada che $(*_{fg})$ abbia esattamente p soluzioni distinte, deve accadere che tanto $(*_f)$ quanto $(*_g)$ abbiano ciascuna il massimo numero di soluzioni distinte possibili e cioè, rispettivamente, $\deg_p(f)$ e $\deg_p(g)$ (inoltre, le soluzioni di $(*_f)$ debbono essere distinte da quelle di $(*_g)$). □

Osservazione 4.25. **(1)** Utilizzando la definizione di divisibilità di polinomi (mod n) si definisce facilmente anche un MCD di due polinomi $f, g \in \mathbb{Z}[X]$ (mod n) essendo un polinomio $h \in \mathbb{Z}[X]$ che verifica le seguenti due proprietà:

- $h \mid f$ e $h \mid g \pmod{n}$;
- $h' \mid f$ e $h' \mid g \pmod{n} \Rightarrow h' \mid h \pmod{n}$.

È subito visto che se esiste un MCD (mod n) di due polinomi f, g questo è "essenzialmente unico" a meno di congruenze (mod n) ed è denotato brevemente con $\mathrm{MCD}_n(f, g)$. Se poi $n = p$ è un numero primo, allora si dimostra che, presi comunque due polinomi non identicamente congrui a 0 (mod p), esiste sempre $\mathrm{MCD}_p(f, g)$.

(2) La Proposizione 4.23 è un semplice corollario del seguente risultato più generale:

Siano $p, f(X)$ e t come nella Proposizione 4.24. Sia $h \in \mathbb{Z}[X]$ il massimo comun divisore dei polinomi f e $X^p - X \pmod{p}$. Risulta allora:

$$t = \deg_p(h).$$

Dimostrazione. Con le notazioni del Corollario 4.23, ricordiamo che possiamo scrivere $f \equiv_X g \cdot (X - a_1)^{e_1} \cdot (X - a_2)^{e_2} \cdot \cdots \cdot (X - a_t)^{e_t}$ ed inoltre $X^p - X \equiv_X X(X-1) \cdot \cdots \cdot (X - (p-1)) \pmod{p}$ (cfr. Corollario 3.2). Da ciò segue facilmente che $\mathrm{MCD}_p(f, X^p - X)$ esiste ed è dato da $h := (X - a_1)(X - a_2) \cdot \cdots \cdot (X - a_t)$ e dunque che $\deg_p(h) = t$. □

Terminiamo questo paragrafo con un teorema dimostrato da C. Chevalley e che riguarda polinomi in più indeterminate.

Sia $f \in \mathbb{Z}[X_1, \ldots, X_r]$, dunque possiamo rappresentare f nella maniera seguente:

$$f = \sum_{0 \leqslant i_1, \ldots, i_r \leqslant t} a_{i_1, i_2, \ldots, i_r} \, X_1^{i_1} \, X_2^{i_2} \, \ldots \, X_r^{i_r},$$

con $a_{i_1, i_2, \ldots, i_r} \in \mathbb{Z}$ e $i_1, i_2, \ldots, i_r \geqslant 0$.
Poniamo, per semplicità di notazione, $f = \sum_{\boldsymbol{i}} a_{\boldsymbol{i}} \boldsymbol{X}^{\boldsymbol{i}}$, dove $\boldsymbol{i} := (i_1, \ldots, i_r)$ è un multi-indice e $\boldsymbol{X}^{\boldsymbol{i}} := X_1^{i_1} X_2^{i_2} \ldots X_r^{i_r}$. L'intero $i_1 + i_2 + \cdots + i_r$ si chiama *grado (complessivo)* del monomio $a_{i_1, i_2, \ldots, i_r} X_1^{i_1} X_2^{i_2} \ldots X_r^{i_r}$. Il massimo dei gradi dei monomi del polinomio f si dice *grado (complessivo)* di f e viene denotato con $\deg(f)$. Se $n \geqslant 0$ si denota con $\deg_n(f)$ il massimo dei gradi (complessivi), $i_1 + i_2 + \cdots + i_r$, dei monomi del polinomio f per i quali $a_{i_1, i_2, \ldots, i_r} \not\equiv 0 \pmod{n}$.

Definizione 4.26. Sia $f := \sum_{\boldsymbol{i}} a_{\boldsymbol{i}} \boldsymbol{X}^{\boldsymbol{i}} \in \mathbb{Z}[X_1, X_2, \ldots, X_r]$ e sia $n \geqslant 0$. Diremo che il polinomio f è *identicamente congruo a zero (modulo n)*, in simboli $f \equiv_{\boldsymbol{X}} 0 \pmod{n}$, se $a_{\boldsymbol{i}} \equiv 0 \pmod{n}$ per ciascun multi-indice $\boldsymbol{i}$.
Se $f, g \in \mathbb{Z}[X_1, X_2, \ldots, X_r]$, diremo che f è *identicamente congruo a g (modulo n)*, in simboli $f \equiv_{\boldsymbol{X}} g \pmod{n}$, se $f - g \equiv_{\boldsymbol{X}} 0 \pmod{n}$.

Diremo che f è *equivalente a g (modulo n)*, in simboli $f \sim g \pmod{n}$, se preso comunque $(a_1, \ldots, a_r) \in \mathbb{Z}^r$,

$$f(a_1, \ldots, a_r) \equiv g(a_1, \ldots, a_r) \pmod{n}$$

È ovvio che, se $f \equiv_{\boldsymbol{X}} g \pmod{n}$, allora $\deg_n(f) = \deg_n(g)$. Inoltre:

$$f \equiv_{\boldsymbol{X}} g \pmod{n} \Rightarrow f \sim g \pmod{n}.$$

Abbiamo già osservato per polinomi in una indeterminata che non è vero il viceversa.

Proposizione 4.27. *Sia $f \in \mathbb{Z}[X_1, X_2, \ldots, X_r]$, sia m il grado complessivo di f e sia p un numero primo.*
Esiste un polinomio $\widetilde{f} \in \mathbb{Z}[X_1, X_2, \ldots, X_r]$, eventualmente nullo, con il grado di $\widetilde{f}$ in ciascuna indeterminata $\leqslant p-1$, tale che

$$f \sim \widetilde{f} \pmod{p}.$$

Dimostrazione. Per ogni $k \geqslant p-1$, si consideri una divisione con il "resto" di k rispetto a $(p-1)$, del "tipo particolare" seguente:

$$k = q \cdot (p-1) + r \quad \text{con } 1 \leqslant r \leqslant p-1.$$

È ovvio che, per ogni $1 \leqslant i \leqslant r$, se $k = q \cdot (p-1) + r$ allora:

$$X_i^k \sim X_i^r \pmod{p}.$$

Applicando questa "trasformazione" ad ogni indeterminata X_i ed ad ogni esponente $\geqslant p-1$, si ottiene un polinomio $\widetilde{f}$ che soddisfa alla proprietà enunciata. □

Proposizione 4.28. *Siano $f, g \in \mathbb{Z}[X_1, X_2, \ldots, X_r]$ sia p un primo fissato e siano $\widetilde{f}, \widetilde{g} \in \mathbb{Z}[X_1, X_2, \ldots, X_r]$ come nella Proposizione 4.27.*

$$\widetilde{f} \sim \widetilde{g} \pmod{p} \iff \widetilde{f} \equiv_{\boldsymbol{X}} \widetilde{g} \pmod{p}$$

Dimostrazione. ($\Rightarrow$) Passando al polinomio $f-g$, basta dimostrare che se $h \in \mathbb{Z}[X_1, X_2, \ldots, X_r]$, con grado di $h \leqslant p-1$ in ogni indeterminata, allora:

$$h \sim 0 \pmod{p} \Rightarrow h \equiv_{\boldsymbol{X}} 0 \pmod{p}.$$

Si proceda per induzione sul numero delle indeterminate r.
Se $r = 1$, un polinomio di grado $\leqslant p-1$ con p radici distinte deve essere identicamente congruo a zero (modulo p) per il Teorema di Lagrange.
Sia $(x_2, \ldots, x_r) \in \mathbb{Z}^{r-1}$, poniamo:

$$w(X_1) := h(X_1, x_2, \ldots, x_r) = \sum_{j=0}^{p-1} h_j(x_2, \ldots, x_r) X_1^j \in \mathbb{Z}[X_1]\,.$$

Riapplicando il Teorema di Lagrange a $w(X_1)$ abbiamo che:

$$w \equiv_{X_1} 0 \pmod{p}, \text{ cioè } h_j \sim 0 \pmod{p}, \text{ per ogni } j.$$

Dunque, per ipotesi induttiva, h_j è identicamente congruo a 0 (modulo p) per ogni j, e quindi $h \equiv_{\boldsymbol{X}} 0 \pmod{p}$.
($\Leftarrow$) È banale. $\square$

Nel 1935 E. Artin congetturò che una congruenza polinomiale priva di termine noto (modulo p), con p primo, ha sempre una soluzione non banale se il numero delle indeterminate del polinomio è maggiore del grado (complessivo) del polinomio. Ad esempio, se $a, b, c \in \mathbb{Z}$, con $abc \not\equiv 0 \pmod{p}$,

$$aX^2 + bY^2 + cZ^2 \equiv 0 \pmod{p}$$

ha sempre almeno una soluzione non banale. Tale congettura fu dimostrata nel 1936 da C. Chevalley.

Teorema 4.29. (C. Chevalley)
Sia p un primo e siano $f, g \in \mathbb{Z}[X_1, X_2, \ldots, X_r]$ due polinomi ciascuno con grado (complessivo) $\leqslant r - 1$.
(a) *Se la congruenza*

$$f(X_1, X_2, \ldots, X_r) \equiv 0 \pmod{p} \tag{3}$$

è risolubile, allora ha almeno due soluzioni.
(b) *Se g è un polinomio privo di termine noto (ad esempio un polinomio omogeneo non costante), allora la congruenza*

$$g(X_1, X_2, \ldots, X_r) \equiv 0 \pmod{p} \tag{4}$$

ha sempre una soluzione non banale.

Dimostrazione. (b) segue immediatamente da (a), in quanto la congruenza (4) possiede sempre la soluzione banale $(0, 0, \ldots, 0)$.
(a) Supponiamo che (3) possieda un'unica soluzione:

$$(a_1, a_2, \ldots, a_r) \pmod{p}.$$

Consideriamo il polinomio

$$h(X_1, X_2, \ldots, X_r) := 1 - f(X_1, X_2, \ldots, X_r)^{p-1}$$

Siano $x_1, x_2 \ldots, x_r \in \mathbb{Z}$, è ovvio che:

$$h(x_1, \ldots, x_r) \equiv \begin{cases} 1 \pmod{p}, & \text{se } x_i \equiv a_i \pmod{p}, \text{ per ogni } i \\ 0 \pmod{p}, & \text{altrimenti .} \end{cases}$$

Sia $\widetilde{h}$ un polinomio di grado $\leqslant p-1$ in ciascuna indeterminata tale che $h \sim \widetilde{h}$ (mod p) (cfr. Proposizione 4.27).
Si consideri, poi, il seguente polinomio:

$$h^*(X_1, X_2, \ldots, X_r) := \prod_{i=1}^{r} \left(1 - (X_i - a_i)^{p-1}\right)$$

È subito visto che $h^* \sim h \pmod{p}$ e dunque $h^* \sim \widetilde{h} \pmod{p}$. Quindi, per la Proposizione 4.28, $h^* \equiv_{\boldsymbol{X}} \widetilde{h} \pmod{p}$. Questo è impossibile perchè $\deg_p(h^*) = (p-1)\cdot r$, mentre $\deg_p(\widetilde{h}) \leqslant \deg_p(h) = (p-1)\deg_p(f) < (p-1)\cdot r$. Pertanto la congruenza (3) non può possedere un'unica soluzione. $\square$

4. Esercizi e Complementi

4.1. Siano p un primo ed e, d due interi positivi. Mostrare che:
(a) Se la congruenza $f(X) \equiv 0 \pmod{p}$ ammette s soluzioni distinte e tutte non singolari, lo stesso è vero per la congruenza $f(X) \equiv 0 \pmod{p^e}$, per ogni $e \geqslant 1$.
(b) Se $d \mid (p-1)$, la congruenza $X^d - 1 \equiv 0 \pmod{p^e}$ ha esattamente d soluzioni per ogni $e \geqslant 1$.
[Suggerimento. **(a)**. Sia y una soluzione non singolare della congruenza

$$f(X) \equiv 0 \pmod{p^n} \qquad (*_n)$$

e sia $x = y + \bar{t}p^n$ l'unica soluzione della congruenza

$$f(X) \equiv 0 \pmod{p^{n+1}} \qquad (*_{n+1})$$

con $1 \leqslant n \leqslant e-1$. Utilizzando il Lemma 4.5 per il polinomio $f'(X)$ calcolato in x, abbiamo che

$$f'(x) = f'(y) + \bar{t}\, p^n\, f''(y) + \ldots \equiv f'(y) \pmod{p}\,.$$

(b). Se $y^d \equiv 1 \pmod{p}$, allora $dy^{d-1} \not\equiv 0 \pmod{p}$. L'asserto discende da (a) e dalla Proposizione 4.24 (cfr. anche il successivo Lemma 5.11).]

4.2. **(a)** Verificare le seguenti congruenze polinomiali modulo un primo p dispari:
(1) $X^{p-1} - 1 \equiv_X (X-1)(X-2)\cdot\ldots\cdot[X-(p-1)] \pmod{p}$;
(2) $X^{p-2} + X^{p-3} + \cdots + X + 1 \equiv_X (X-2)(X-3)\cdot\ldots\cdot[X-(p-1)] \pmod{p}$.
(b) Utilizzando la (1) di (a), ridimostrare il Teorema di Wilson.
[Suggerimento. **(a)**(1) Si osservi che $(X-k) \mid (X^{p-1}-1) \pmod{p}$, per ogni k $(1 \leqslant k \leqslant p-1)$.
(2) segue da (1) e dal fatto che $X^{p-1} - 1 = (X-1)(X^{p-2} + X^{p-3} + \cdots + X + 1)$.
(b) Basta porre $X = p$ in (1).]

4.3. Sia $f(X) \in \mathbb{Z}[X]$ con $\deg(f) \geqslant 1$. Dimostrare che esistono infiniti primi p tali che la congruenza $f(X) \equiv 0 \pmod{p}$ è risolubile.
[Suggerimento. Se $f(X) = a_0 + a_1X + \cdots + a_nX^n$, allora $f(a_0X) = a_0(1 + Xg(X))$, con $g(X) \in \mathbb{Z}[X]$.
Questa osservazione permette di ricondurci al caso in cui $a_0 = 1$ ovvero $f(X) = 1 + Xg(X)$. Supponiamo, per assurdo, che $f(X) \equiv 0$ sia risolubile soltanto $(\mathrm{mod}\, p_i)$ per $i = 1, 2, \ldots, t$. Poniamo $N := p_1p_2\cdot\ldots\cdot p_t$. Dal momento che $\lim_{x\to+\infty} |f(x)| = +\infty$, è ovviamente possibile trovare $h >> 0$ in modo tale che, per $M := N^h$, $|f(M)| \neq 1$. Poiché $f(M) = 1 + Mg(M)$, allora deve essere $\mathrm{MCD}(f(M), M) = 1$. Pertanto se $p \mid M$ allora $p \nmid f(M)$ e quindi perveniamo ad un assurdo.]

4.4. Mostrare che, per ogni $s > 0$, esiste un intero $N > 0$ tale che la congruenza $X^2 \equiv 1 \pmod{N}$ ha più di s soluzioni.
[Suggerimento. Se p è un primo dispari, $X^2 \equiv 1 \pmod{p}$ ha le due soluzioni $1, p-1$. Quindi, se $p_1, p_2, \ldots, p_r$ sono primi distinti, $X^2 \equiv 1 \pmod{p_1p_2\cdot\ldots\cdot p_r}$ ha esattamente 2^r soluzioni distinte. Basta trovare r tale che $2^r > s$ e porre $N = p_1p_2\cdot\ldots\cdot p_r$.]

4.5. Verificare che il Corollario 4.18 non è più valido se si sostituiscono p e $p-1$ rispettivamente con n e $\varphi(n)$ (con $n \in \mathbb{Z}, n \geqslant 2$).
[Suggerimento. Si scelga, ad esempio, $n = 4$ e $f(X) = X^3 - X$.]

4.6. Siano $p, f(X)$ e t definiti come nella Proposizione 4.24.
Posto $F := \mathrm{MCD}(f, X^p - X)$, massimo comun divisore calcolato in $\mathbb{Z}[X]$, è vero che $t = \deg_p(F)$?
[Suggerimento. La risposta è negativa: si ponga $p = 5$ ed $f(X) = (X+2)(X+1)^2$ da cui $t = 2$ e $F(X) = X + 1$, perché

$$\begin{aligned} X^5 - X = X(X^4 - 1) = \\ = X(X^2 - 1)(X^2 + 1) = \\ = X(X + 1)(X - 1)(X^2 + 1). \end{aligned}$$

4.7. (Teorema di Warning) Sia $f \in \mathbb{Z}[X_1, \ldots, X_r]$, con $\deg(f) < r$, e sia p un numero primo. La congruenza $f \equiv 0 \pmod{p}$ ha un numero di soluzioni (in $\mathbb{Z}^r$) divisibile per p.
[Suggerimento. Seguire un'argomentazione simile a quella utilizzata per dimostrare il Teorema di Chevalley. Precisamente se $\boldsymbol{a}_i = (a_{i1}, a_{i2}, \ldots, a_{ir})$, per $i = 1, 2, \ldots, s$, sono le soluzioni della congruenza data, considerare il polinomio:

$$h^*(X_1, X_2, \ldots, X_r) := \sum_{i=1}^{s} \prod_{j=1}^{r} \left(1 - (X_j - a_{ij})^{p-1}\right).]$$

4.8. Determinare le soluzioni della congruenza:

$$f(X) := X^2 + X + 7 \equiv 0 \pmod{27}.$$

[Soluzione. La congruenza:

$$X^2 + X + 7 \equiv 0 \pmod{3} \qquad (*_1)$$

ha un'unica soluzione $y \equiv 1 \pmod{3}$.
Consideriamo la congruenza:

$$X^2 + X + 7 \equiv 0 \pmod{3^2}. \qquad (*_2)$$

Osserviamo che $f'(X) = 2X + 1$, quindi $f'(y) \equiv 0 \pmod{3}$. Inoltre, $f(1) \equiv 0 \pmod{9}$, dunque gli elementi $y_1 = 1,\ y_2 = 1 + 3 = 4,\ y_3 = 1 + 2 \cdot 3 = 7$ sono le soluzioni di $(*_2)$.
Per calcolare le soluzioni della congruenza data:

$$X^2 + X + 7 \equiv 0 \pmod{3^3} \qquad (*_3)$$

osserviamo che:

$$\begin{aligned} f'(y_1) = 3 \equiv 0 \pmod{3} \qquad & f(y_1) = 9 \equiv 9 \pmod{27} \\ f'(y_2) = 9 \equiv 0 \pmod{3} \qquad & f(y_2) = 27 \equiv 0 \pmod{27} \\ f'(y_3) = 15 \equiv 0 \pmod{3} \qquad & f(y_3) = 63 \equiv 9 \pmod{27}. \end{aligned}$$

Quindi, y_1 non determina soluzioni di $(*_3)$ (cioè non esiste nessuna soluzione t della congruenza

$$3T \equiv -\frac{9}{9} = -1 \pmod{3} \qquad (\bullet_1)$$

e quindi nessun intero $x = y_1 + t \cdot 3^2$ è tale che $f(x) \equiv 0 \pmod{27}$). Mentre, y_2 determina tre soluzioni di $(*_3)$ date da:

$$x_{2,1} = y_2 + 0 \cdot 3^2 = 4,\ x_{2,2} = y_2 + 1 \cdot 3^2 = 13,\ x_{2,3} = y_2 + 2 \cdot 3^2 = 22 \pmod{27}$$

(dal momento che la congruenza

$$9T \equiv -\frac{27}{9} = -3 \pmod{3} \qquad (\bullet_2)$$

è risolubile per $t = 0, 1, 2 \pmod{3}$).
Infine, y_3 non determina soluzioni di $(*_3)$ (in quanto la congruenza

$$15T \equiv -\frac{63}{9} = -7 \equiv -1 \pmod{3} \qquad (\bullet_3)$$

non è risolubile).
In definitiva, le soluzioni della congruenza assegnata sono: $x = 4, 13, 22 \pmod{27}$.]

5 Radici primitive dell'unità e congruenze del tipo $X^m \equiv a \pmod{n}$

Oggetto di questo paragrafo è lo studio della risolubilità di congruenze del tipo:

$$X^m \equiv a \pmod{n}$$

con $m, n, a \in \mathbb{Z}$ ed $m, n > 0$. Per l'effettiva ricerca delle soluzioni di tali congruenze svilupperemo, in modo essenziale, la teoria delle radici primitive dell'unità e la teoria degli indici.

I risultati qui esposti sono stati in gran parte ottenuti da Gauss, che li ha trattati (più o meno nella forma in cui essi sono stati qui presentati) nel suo celebre *Disquisitiones Arithmeticae* (cfr. [G]). Tuttavia, alcuni teoremi furono congetturati e in parte dimostrati precedentemente: ad esempio il Teorema dell'esistenza di radici primitive modulo un primo fu congetturato da Lambert nel 1769 e dimostrato da Legendre nel 1785. Il termine *radice primitiva* fu introdotto da Euler nel 1773.

Definizione 5.1. Siano $a, n \in \mathbb{Z}$ tali che $n > 0$ e $\mathrm{MCD}(a, n) = 1$. Si chiama *ordine di* $a \pmod{n}$ (e si scrive $\mathrm{ord}_n(a)$) il minimo intero positivo k per cui risulti

$$a^k \equiv 1 \pmod{n}.$$

Osservazione 5.2. È bene sottolineare che la *definizione precedente ha senso se, e soltanto se,* $\mathrm{MCD}(a, n) = 1$.
Infatti, se $\mathrm{MCD}(a, n) \neq 1$ la congruenza $aX \equiv 1 \pmod{n}$ non è risolubile (cfr. Teorema 2.2) e quindi $a^k \not\equiv 1 \pmod{n}$ per ogni $k \geqslant 1$; viceversa, se $\mathrm{MCD}(a, n) = 1$ l'asserto è immediata conseguenza del Teorema di Euler-Fermat (cfr. Teorema 3.7).

D'ora in poi, quindi, nel considerare l'ordine $\pmod{n}$ *di un elemento* a, $\mathrm{ord}_n(a)$, *supporremo sempre tacitamente che* $\mathrm{MCD}(a, n) = 1$.

Vale, innanzi tutto, il seguente risultato (di immediata verifica):

Proposizione 5.3. *Siano* $a, b, n \in \mathbb{Z}, n > 0$. *Se* $a \equiv b \pmod{n}$, *allora* $\mathrm{ord}_n(a) = \mathrm{ord}_n(b)$. □

Si noti che il viceversa dell'enunciato precedente è falso: ad esempio $\mathrm{ord}_5(2) = 4 = \mathrm{ord}_5(3)$ e $2 \not\equiv 3 \pmod{5}$.

Proposizione 5.4. *Siano* $a, b, n, m \in \mathbb{Z}, n > 0$ *e* $m > 0$. *Risulta:*

(1) $a^m \equiv 1 \pmod{n} \iff \mathrm{ord}_n(a) \mid m$;

(2) $\mathrm{ord}_n(a) \mid \varphi(n)$ *(cfr. Definizione 2.9);*

(3) $\mathrm{ord}_n(a^m) = \mathrm{ord}_n(a)/\mathrm{MCD}(m, \mathrm{ord}_n(a))$. *Ne segue che:*
$\mathrm{ord}_n(a^m) = \mathrm{ord}_n(a) \iff \mathrm{MCD}(m, \mathrm{ord}_n(a)) = 1$;

(4) $\mathrm{ord}_n(a) = \mathrm{ord}_n(a^*)$, *dove* a^* *è un inverso aritmetico di* $a \pmod n$;

(5) $\mathrm{MCD}(\mathrm{ord}_n(a), \mathrm{ord}_n(b)) = 1 \Rightarrow \mathrm{ord}_n(ab) = \mathrm{ord}_n(a) \cdot \mathrm{ord}_n(b)$.

Dimostrazione. (1) ($\Leftarrow$). È ovvio.
($\Rightarrow$). Si ponga $h := \mathrm{ord}_n(a)$ e si operi la divisione euclidea:

$$m = qh + r, \quad 0 \leqslant r < h.$$

Allora, $1 \equiv a^m = (a^h)^q \cdot a^r \equiv a^r \pmod n$ (in quanto $a^h \equiv 1 \pmod n$); per la minimalità dell'ordine, deve risultare $r = 0$ e dunque $h \mid m$.
(2) È un'immediata conseguenza di (1) e del Teorema 3.7.
(3) Si ponga $h := \mathrm{ord}_n(a)$ e $d := \mathrm{MCD}(m, h)$. Se k è un intero positivo, da (1) si ha:

$$(a^m)^k = a^{mk} \equiv 1 \pmod n \iff h \mid mk \iff \frac{h}{d} \mid \frac{m}{d} \cdot k.$$

Poiché $\mathrm{MCD}(h/d, m/d) = 1$, allora $(h/d) \mid k$; quindi h/d è il minimo intero positivo k per cui $(a^m)^k \equiv 1 \pmod n$, cioè $\mathrm{ord}_n(a^m) = h/d$.
(4) Si ponga $h := \mathrm{ord}_n(a)$ e $h^* := \mathrm{ord}_n(a^*)$. Si ha:

$$(a^*)^h = 1 \cdot (a^*)^h \equiv a^h \cdot (a^*)^h = (aa^*)^h \equiv 1 \pmod n$$

e dunque, in base a (1), $h^* \mid h$. Procedendo in modo analogo, si prova che $h \mid h^*$ e dunque: $h = h^*$.
(5) Si ponga $h_1 := \mathrm{ord}_n(a)$ e $h_2 := \mathrm{ord}_n(b)$ e $h := \mathrm{ord}_n(ab)$. Poiché $(ab)^{h_1 h_2} \equiv 1 \pmod n$, in base al punto (1), si ha che $h \mid h_1 h_2$. D'altra parte:

$$a^h b^h = (ab)^h \equiv 1 \pmod n \text{ e quindi } a^h \equiv (b^h)^* \pmod n.$$

Da (4) segue che $\mathrm{ord}_n(a^h) = \mathrm{ord}_n(b^h)$ e quindi da (3):

$$\frac{h_1}{\mathrm{MCD}(h_1, h)} = \frac{h_2}{\mathrm{MCD}(h_2, h)}.$$

Poiché, per ipotesi, $\mathrm{MCD}(h_1, h_2) = 1$, si ha che:

$$h_1 \mid \mathrm{MCD}(h_1, h) \quad \text{e} \quad h_2 \mid \mathrm{MCD}(h_2, h).$$

Pertanto $h_1 \mid h$ e $h_2 \mid h$ e, quindi, $h_1 h_2 \mid h$. □

È immediato verificare che l'enunciato **(5)** della proposizione precedente vale, più in generale, per $r \geqslant 2$ interi i cui ordini siano a due a due relativamente primi.

Corollario 5.5. *Siano $a, n, i, j, N \in \mathbb{Z}$ con $n, i, j, N > 0$ e* $\mathrm{MCD}(a, n) = 1$. *Allora:*

$$a^i \equiv a^j \pmod{n} \iff i \equiv j \pmod{\mathrm{ord}_n(a)}.$$

In particolare,

$$a^N \equiv a^r \pmod{n}$$

dove r è il resto della divisione di N per $\mathrm{ord}_n(a)$, *cioè* $N = q \cdot \mathrm{ord}_n(a) + r$, *con* $0 \leqslant r \leqslant \mathrm{ord}_n(a) - 1$.

Dimostrazione. Sia $h := \mathrm{ord}_n(a)$.
($\Leftarrow$). Se $i - j = th$ per qualche $t \in \mathbb{Z}$, poiché $a^h \equiv 1 \pmod{n}$, allora:

$$a^i = a^{j+th} = a^j (a^h)^t \equiv a^j \pmod{n}.$$

($\Rightarrow$). Supponiamo per fissare le idee che $j \geqslant i$, con $a^i \equiv a^j \pmod{n}$. Dal momento che $\mathrm{MCD}(a, n) = 1$ allora anche $\mathrm{MCD}(a^i, n) = 1$. Inoltre:

$$a^j = a^i a^{j-i} \equiv a^i \pmod{n}.$$

Moltiplicando ambo i membri della congruenza per l'inverso aritmetico di $a^i \pmod{n}$, otteniamo che

$$a^{j-i} \equiv 1 \pmod{n},$$

quindi $h \mid (j - i)$, cioè $i \equiv j \pmod{h}$. □

Ad esempio $3^{14} \equiv 3^2 \equiv 4 \pmod{5}$, perché $\mathrm{ord}_5(3) = 4$ e $14 \equiv 2 \pmod{4}$.

Il seguente risultato approfondisce i legami tra l'ordine e la funzione φ di Euler (cfr. Proposizione 5.4 (2)) ed introduce la successiva definizione di radice primitiva dell'unità.

Lemma 5.6. *Siano $a, n \in \mathbb{Z}, n > 0$. Le seguenti affermazioni sono equivalenti:*

(i) $\mathrm{ord}_n(a) = \varphi(n)$;

(ii) $\{1, a, a^2, \ldots, a^{\varphi(n)-1}\}$ *è un sistema ridotto di residui (modulo n).*

Dimostrazione. **(i)** $\Rightarrow$ **(ii)**. Certamente $\mathrm{MCD}(a^k, n) = 1$, per ogni k tale che $0 \leqslant k \leqslant \varphi(n) - 1$.
Inoltre, se $a^h \equiv a^k \pmod{n}$ con $0 \leqslant h < k \leqslant \varphi(n) - 1$, si avrebbe $a^{k-h} \equiv 1 \pmod{n}$ con $1 \leqslant k - h \leqslant \varphi(n) - 1$ e ciò è assurdo. La tesi è dunque ovvia (cfr. anche l'Esercizio 2.11(a)).
(ii) $\Rightarrow$ **(i)**. Ovviamente $a^{\varphi(n)} \equiv 1 \pmod{n}$ (cfr. Teorema 3.7); inoltre, per ipotesi, $a^k \not\equiv 1 \pmod{n}$ per ogni k tale che $1 \leqslant k \leqslant \varphi(n) - 1$. Dunque $\mathrm{ord}_n(a) = \varphi(n)$. □

Definizione 5.7. Sia $n \in \mathbb{Z}, n > 0$. Si chiama *radice primitiva dell'unità (modulo n)* un intero a verificante una delle due condizioni (equivalenti) del Lemma 5.6.

Ad esempio, per $n = 5$, allora 2 è una radice primitiva (modulo 5), in quanto $\{2, 2^2, 2^3, 2^4\}$ è un sistema ridotto di residui (modulo 5), ovvero $\mathrm{ord}_5(2) = 4 = \varphi(5)$.
Se $n = 8$, si può verificare direttamente che *non* esistono radici primitive (modulo 8).

Proposizione 5.8. *Sia n un intero positivo tale che esiste (almeno) una radice primitiva (modulo n). Allora, esistono esattamente $\varphi(\varphi(n))$ radici primitive distinte* (modulo n) *(cioè, non congruenti (modulo n)).*

Dimostrazione. Sia a una radice primitiva (mod n).
Poiché $S^* := \{a, a^2, \ldots, a^{\varphi(n)}\}$ è un sistema ridotto di residui (mod n), ogni radice primitiva (mod n) è congrua ad un (ed un solo) elemento di S^* e, inoltre, $a^k \in S^*$ è una radice primitiva (mod n) se e soltanto se si ha che $\mathrm{ord}_n(a^k) = \varphi(n) = \mathrm{ord}_n(a)$. In base alla Proposizione 5.4 (3), le radici primitive (mod n) sono in corrispondenza biunivoca con gli interi k tali che $1 \leqslant k \leqslant \varphi(n)$ e $\mathrm{MCD}(k, \varphi(n)) = 1$, cioè sono in numero di $\varphi(\varphi(n))$. □

Osservazione 5.9. Sia $n \in \mathbb{Z}, n > 0$ ed U_n il gruppo (moltiplicativo) delle unità dell'anello $\mathbb{Z}/n\mathbb{Z}$ (cfr. anche Osservazione 2.8). È chiaro che:

$$U_n = \{\bar{k} = k + n\mathbb{Z} \mid k \in \mathbb{Z} \text{ e } \mathrm{MCD}(k, n) = 1\},$$

e dunque $\#(U_n) = \varphi(n)$. Invitiamo il lettore a tradurre le nozioni introdotte in questo paragrafo nel linguaggio gruppale, con riferimento al gruppo moltiplicativo U_n.

Ci occuperemo ora del problema dell'esistenza di radici primitive (modulo n), esaminando dapprima il caso in cui $n = p$ sia un numero primo. Vale in proposito il seguente risultato:

Teorema 5.10. *Se p è un numero primo, esiste sempre una radice primitiva (modulo p). Più precisamente, esistono esattamente $\varphi(p-1)$ radici primitive (modulo p), non congruenti (modulo p).*

Del Teorema 5.10 daremo due differenti dimostrazioni. Ad esse premettiamo alcuni risultati utili per il seguito.

Lemma 5.11. *Sia p un primo e d un intero positivo tale che $d \mid (p-1)$. La congruenza:*

$$X^d \equiv 1 \pmod{p}$$

ha esattamente d soluzioni non congruenti (modulo p).

Dimostrazione. Verifichiamo, innanzitutto, che $(X^d - 1) \mid (X^p - X)$.
Per ipotesi esiste $k \in \mathbb{Z}, k > 0$ tale che $dk = p - 1$. Dunque, è subito visto che:

$$X^p - X = X(X^{dk} - 1) = X(X^d - 1)(X^{d(k-1)} + X^{d(k-2)} + \cdots + X^d + 1).$$

La conclusione discende dalla Proposizione 4.24. Alla conclusione si può pervenire utilizzando direttamente il Teorema di Lagrange. Infatti, le congruenze (mod p), associate a ciascuno dei polinomi a secondo membro della precedente decomposizione di $X^p - X$, hanno ciascuna un numero di soluzioni minore od uguale del grado del polinomio. Poiché $X^p - X \equiv 0 \pmod{p}$ ha esattamente p soluzioni allora, in particolare, $X^d - 1 \equiv 0 \pmod{p}$ non può avere meno di d soluzioni (mod p). $\square$

Osservazione 5.12. (a). Se $d \nmid (p-1)$, la congruenza $X^d \equiv 1 \pmod{p}$ (che è sempre banalmente risolubile) ammette un numero di soluzioni distinte inferiori a d.
Ad esempio, posto $d = 4$ e $p = 7$, si verifica subito che $X^4 \equiv 1 \pmod{7}$ ha soltanto due soluzioni (cioè 1 e 6) (mod 7).
Più precisamente, se $t := \mathrm{MCD}(d, p-1)$ le soluzioni distinte della congruenza in questione sono esattamente t; tale fatto può essere provato utilizzando la Proposizione 4.24 oppure come semplice conseguenza di un successivo teorema (cfr. Teorema 5.18).
(b) Se $d \nmid (p-1)$, nessun intero ha ordine d (modulo p); infatti $\mathrm{ord}_p(a) \mid \varphi(p) = p - 1$ (cfr. Proposizione 5.4 (2)).

Teorema 5.13. *Sia p un primo e d un intero positivo tale che si abbia: $d \mid (p-1)$. Allora, esistono esattamente $\varphi(d)$ interi non congruenti* (mod p) *ed aventi ordine d* (mod p).

Dimostrazione. Sia $S^* = \{1, 2, \ldots, p-1\}$ il sistema ridotto di residui minimo positivo (mod p) e, per ogni intero positivo d tale che $d \mid (p-1)$, si ponga:

$$\psi(d) := \#\{k \in S^* \ : \ \mathrm{ord}_p(k) = d\}.$$

Vogliamo dimostrare che $\varphi(d) = \psi(d)$.
Poiché l'ordine di ogni elemento di S^* è un divisore di $\varphi(p) = p - 1$, è chiaro che:

$$p - 1 = \sum_{d \mid (p-1)} \psi(d). \tag{1}$$

Consideriamo ora, per ogni intero positivo d tale che $d \mid (p-1)$, i seguenti insiemi:

$$S_d^* := \{k \in S^* : \mathrm{MCD}(k, p-1) = d\}$$
$$\tilde{S}_d := \{k' \in \mathbb{Z} : 1 \leqslant k' \leqslant \frac{p-1}{d} \text{ e } \mathrm{MCD}(k', \frac{p-1}{d}) = 1\}.$$

È chiaro che la famiglia $\{S_d^* : d \mid (p-1)\}$ costituisce una partizione di S^* ed è altresì chiaro che S_d^* e $\tilde{S}_d$ sono equipotenti (l'applicazione $f : S_d^* \longrightarrow \tilde{S}_d$ tale che $f(k) = k/d$ è certamente biiettiva).
Ne segue che:

$$\#(S_d^*) = \#(\tilde{S}_d) = \varphi\left(\frac{p-1}{d}\right)$$

e, dunque, che

$$p - 1 = \sum_{d|(p-1)} \varphi\left(\frac{p-1}{d}\right) = \sum_{d|(p-1)} \varphi(d) \tag{2}$$

(L'ultima uguaglianza sussiste perché $(p-1)/d$ descrive, al variare di d, l'insieme di tutti i divisori di $p-1$, cioè:

$$\{d : d \mid (p-1), 1 \leqslant d \leqslant p-1\} = \{(p-1)/d : d \mid (p-1), 1 \leqslant d \leqslant p-1\}.)$$

Confrontando (2) con (1) si ha:

$$\sum_{d|(p-1)} \psi(d) = \sum_{d|(p-1)} \varphi(d)$$

e, quindi, per dimostrare che $\psi(d) = \varphi(d)$, basta verificare che, per ogni divisore d di $p-1$, si abbia $\psi(d) \leqslant \varphi(d)$.
Supponiamo che $\psi(d) > 0$, per ogni d tale che $d \mid (p-1)$, (altrimenti la diseguaglianza è ovvia) e dunque sia $a \in S^*$ tale che $\mathrm{ord}_p(a) = d$. L'insieme $T := \{a, a^2, \ldots, a^d\}$ è costituito da d interi non congrui $\pmod p$ che sono soluzioni della congruenza:

$$X^d \equiv 1 \pmod p$$

(infatti, $(a^h)^d = (a^d)^h \equiv 1 \pmod p$, per ogni h tale che $1 \leqslant h \leqslant d$).
Il Lemma 5.11 ci assicura che la congruenza in questione ha esattamente d soluzioni non congruenti $\pmod p$: quindi ogni intero di S^* di ordine $d \pmod p$ è necessariamente congruente $\pmod p$ ad un elemento di T. Dunque (cfr. Proposizione 5.4(3)):

$$\begin{aligned}\psi(d) &\leqslant \#\{a^k \in T \ : \ \mathrm{ord}(a^k) = d\} = \#\{a^k \in T \ : \ \mathrm{MCD}(k,d) = 1\} = \\ &= \#\{k \in \mathbb{Z} \ : \ 1 \leqslant k \leqslant d \ \text{ e } \ \mathrm{MCD}(k,d) = 1\} = \varphi(d) \quad \square\end{aligned}$$

I Dimostrazione del Teorema 5.10. È una conseguenza immediata del Teorema 5.13 (per $d = p-1$). $\square$

II Dimostrazione del Teorema 5.10 (senza far uso del Teorema 5.13). In base alla Proposizione 5.8, basta dimostrare che esiste una radice primitiva $\pmod p$.
Se $p = 2$, ogni intero dispari è una radice primitiva $\pmod 2$.

Sia quindi p dispari e supponiamo che $p-1$ ammetta la seguente fattorizzazione in numeri primi:

$$p-1 = q_1^{e_1} \cdots q_r^{e_r} \quad (\text{con } e_i \geqslant 1,\ 1 \leqslant i \leqslant r).$$

In base alla Proposizione 5.4 (5), basta verificare che per ogni i, con $1 \leqslant i \leqslant r$, esiste un intero a_i, tale che $\mathrm{ord}_p(a_i) = q_i^{e_i}$; in tal caso, infatti, l'intero $\prod_{i=1}^{r} a_i$ ha ordine $p-1$ ed è quindi una radice primitiva (mod p).

Per semplicità di notazione, fissato comunque $i, 1 \leqslant i \leqslant r$, poniamo $q_i = q, e_i = e$. Poiché $q^e \mid (p-1)$ e quindi anche $q^{e-1} \mid (p-1)$, le congruenze:

$$X^{q^e} \equiv 1 \pmod{p} \quad \text{e} \quad X^{q^{e-1}} \equiv 1 \pmod{p}$$

ammettono rispettivamente q^e e q^{e-1} soluzioni distinte (cfr. Lemma 5.11). Dunque, essendo $q^{e-1} < q^e$, è possibile determinare $a \in \mathbb{Z}$ che sia soluzione della prima congruenza ma non della seconda, cioè:

$$a^{q^e} \equiv 1 \pmod{p} \quad \text{e} \quad a^{q^{e-1}} \not\equiv 1 \pmod{p}.$$

Si tratta ora di verificare che $\mathrm{ord}_p(a) = q^e$ e cioè che $a^k \not\equiv 1 \pmod{p}$ per ogni k tale che $1 \leqslant k \lneqq q^e$. Per assurdo, sia $h := \mathrm{ord}_p(a)$, $h < q^e$. Allora $h \mid q^e$ e quindi $h = q^f$, con $0 \leqslant f < e$; pertanto $q^{e-1} = q^{e-1-f}h$ e quindi

$$a^{q^{e-1}} = (a^h)^{q^{e-1-f}} \equiv 1 \pmod{p}$$

il che è assurdo. $\square$

Osservazione 5.14. La seconda dimostrazione del Teorema 5.10 ha il vantaggio, rispetto alla prima, di suggerire un metodo operativo per la ricerca delle radici primitive. Tale metodo tuttavia non è in generale di un effettivo aiuto pratico: infatti, se p è grande, non ci sono metodi pratici per determinare la decomposizione in fattori primi di $p-1$. Tuttavia, le idee sopra esposte permettono spesso di semplificare i termini del problema, come è suggerito dal seguente esempio.

Esempio 5.15. Sia $p = 23$. Ci proponiamo di calcolare le radici primitive (mod 23), che, in base al Teorema 5.10, sono in numero di $\varphi(22) = 10$.
Per ogni intero a tale che $23 \nmid a$, $\mathrm{ord}_{23}(a) \mid 22$ e dunque $\mathrm{ord}_{23}(a)$ può assumere uno dei seguenti valori: $1, 2, 11, 22$.
Verifichiamo che 21 è una radice primitiva (mod 23). Infatti, si ha:

$$2^1 \not\equiv 1 \pmod{23},\ 2^2 \not\equiv 1 \pmod{23},\ 2^{2^2} = 16 \equiv -7 \not\equiv 1 \pmod{23},$$

$$2^{2^3} \equiv 49 \equiv 3 \not\equiv 1 \pmod{23},\ 2^{11} = 2^{2^3} \cdot 2^2 \cdot 2 \equiv 3 \cdot 4 \cdot 2 \equiv 1 \pmod{23}$$

e $(-1)^1 \not\equiv 1 \pmod{23}$, $(-1)^2 \equiv 1 \pmod{23}$.
Ne segue che $\mathrm{ord}_{23}(2) = 11$ e $\mathrm{ord}_{23}(-1) = \mathrm{ord}_{23}(22) = 2$ e quindi, essendo $\mathrm{MCD}(11, 2) = 1$, allora (cfr. Proposizione 5.4 (5)) si ha:

$$\mathrm{ord}_{23}(21) = \mathrm{ord}_{23}(-2) = \mathrm{ord}_{23}(-1) \cdot \mathrm{ord}_{23}(2) = 2 \cdot 11 = 22.$$

Le radici primitive (mod 23) sono quindi date (a meno della congruenza (mod 23)) dall'insieme:

$$\{(-2)^k | 1 \leqslant k \leqslant 22,\ \mathrm{MCD}(k, 22) = 1\} =$$

$$= \{(-2)^k | k = 1, 3, 5, 7, 9, 13, 15, 17, 19, 21\},$$

e cioè (come si verifica con semplici calcoli):

$$\{21, 15, 14, 10, 17, 19, 7, 5, 20, 11\}.$$

Il metodo precedente per determinare una radice primitiva (modulo 23) è suggerito dalla II dimostrazione del Teorema 5.10. Poiché $22 = 2 \cdot 11$, basta determinare una soluzione di $X^2 \equiv 1 \pmod{23}$ che *non* sia soluzione di $X \equiv 1 \pmod{23}$ (ad esempio, -1) ed una soluzione di $X^{11} \equiv 1 \pmod{23}$ che *non* sia soluzione di $X^k \equiv 1 \pmod{23}$, con $1 \leqslant k \leqslant 10$, (ad esempio, 2). Dunque $a = (-1) \cdot 2 = -2 \equiv 21 \pmod{23}$ è una radice primitiva $\pmod{23}$.

Il calcolo di una radice primitiva (mod p), con p primo, può essere effettuato efficacemente con un metodo algoritmico semplice indicato da Gauss [G, Art. 73 e 74].

Algoritmo di Gauss per il calcolo di una radice primitiva modulo un intero primo p

Passo 1. Scegliere un intero a, $2 \leqslant a \leqslant p-1$, e calcolare $\mathrm{ord}_p(a)$. Se $\mathrm{ord}_p(a) = p-1$, allora a è una radice primitiva $\pmod{p}$.

Passo 2. Se $d := \mathrm{ord}_p(a) \neq p-1$, allora scegliere un intero b, con $2 \leqslant b \leqslant p-1, b \not\equiv a^i$ per ogni $i, 1 \leqslant i \leqslant d$.
Calcolare $t := \mathrm{ord}_p(b)$ e mostrare che $t \nmid d$.
Se $t = p-1$, allora b è una radice primitiva $\pmod{p}$.

Passo 3. Se $t \neq p-1$, sia $d_1 := \mathrm{mcm}(d, t)$. Allora $d_1 > d$ e possiamo scrivere $d_1 = d't'$ con $d' \mid d, t' \mid t$ e $\mathrm{MCD}(d', t') = 1$.
Se $\alpha \equiv a^{\frac{d}{d'}} \pmod{p}$ e $\beta \equiv b^{\frac{t}{t'}} \pmod{p}$ allora $a_1 := \alpha\beta$ è tale che $\mathrm{ord}_p(a_1) = d_1$ (perché $\mathrm{ord}_p(\alpha) = d'$ e $\mathrm{ord}_p(\beta) = t'$).
Se $d_1 = p-1$, allora a_1 è una radice primitiva.
Se $d_1 \neq p-1$, allora si ritorna al Passo 2.
Il procedimento termina dopo un numero finito di passi e permette di trovare una radice primitiva $\pmod{p}$ che non è necessariamente la più piccola radice primitiva positiva.

Esempio 5.16. Si prenda $p = 41, a = 10, b = 9$. È subito visto che $\mathrm{ord}_{41}(10) = 5$. Sia $b = 9$, si verifica direttamente che $b \not\equiv 10^i$ per ogni $1 \leqslant i \leqslant 5$. Si vede che $\mathrm{ord}_{41}(9) = 4$. Dunque $d = 5$, $t = 4$ e quindi $d_1 = \mathrm{mcm}(5, 4) = 20$. Pertanto $20 = 5 \cdot 4$ con $\mathrm{MCD}(5, 4) = 1$, quindi $d' = d = 5$,

$t' = t = 4$. Da ciò segue che $\alpha = a = 10$, $\beta = b = 9$ e dunque $a_1 = 10 \cdot 9 \equiv 8 \pmod{41}$, con $\mathrm{ord}_{41}(8) = 5 \cdot 4 = 20$.
Ripetiamo il Passo 2. Sia $b_1 = 3$ con $3 \not\equiv 8^i$, per ogni $1 \leqslant i \leqslant 20$. Si vede facilmente che $\mathrm{ord}_{41}(3) = 8$. Essendo $\mathrm{mcm}(20, 8) = 40 = 5 \cdot 8$ con $\mathrm{MCD}(5, 8) = 1$, allora i nuovi α e β sono dati da $8^{\frac{20}{5}}$ e $3^{\frac{8}{8}}$. Quindi $8^4 \cdot 3 \equiv 29 \pmod{41}$ con $\mathrm{ord}_{41}(29) = \mathrm{ord}_{41}(8^4) \cdot \mathrm{ord}_{41}(3) = 5 \cdot 8 = 40$, cioè 29 è una radice primitiva $\pmod{41}$.
Si noti che 29 non è la più piccola radice primitiva $\pmod{41}$, infatti si verifica facilmente che 6 è la più piccola radice primitiva positiva $\pmod{41}$.

Come vedremo tra breve, l'esistenza di una radice primitiva (modulo n) permette di risolvere facilmente congruenze del tipo:

$$X^m \equiv a \pmod{n}, \quad \text{con } \mathrm{MCD}(a, n) = 1 \tag{$\bullet$}$$

D'altra parte, in virtù di quanto esposto nel Paragrafo 4, lo studio di congruenze di tipo ($\bullet$) può essere ricondotto a quello di congruenze del tipo:

$$X^m \equiv a \pmod{p} \tag{$\star$}$$

con p primo, $p \mid n$ e $p \nmid a$. Dunque, tramite tale riduzione, l'esistenza di radici primitive modulo un primo sarà sufficiente per la soluzione di congruenze del tipo ($\bullet$), in quanto daremo un metodo effettivo di risoluzione di ogni congruenza del tipo ($\star$), facendo uso di una radice primitiva $\pmod{p}$.
Per completezza, tuttavia, desideriamo anche accennare al problema della esistenza di radici primitive modulo un intero positivo arbitrario. Vale in proposito il seguente risultato:

Teorema 5.17. (Gauss, 1801). *Sia n un intero positivo. Esiste una radice primitiva $\pmod{n}$ se, e soltanto se, n è uno dei seguenti interi:*

$$2, 4, p^k, 2p^k$$

con $k \geqslant 1$ e p primo dispari.

Dimostrazione. Cfr. Esercizio 5.15 e seguenti $\square$

Pertanto, dal teorema precedente discende che $8, 12, 15$ e 16 sono i soli interi $n < 20$ che non possiedono radici primitive.

Veniamo ora al risultato centrale di questo paragrafo.

Teorema 5.18. *Sia p un numero primo, m un intero positivo ed a un intero tale che $p \nmid a$; sia inoltre r una radice primitiva (mod p) ed h l'intero tale che:*

$$r^h \equiv a \pmod{p}, \quad 1 \leqslant h \leqslant p - 1$$

(h è univocamente determinato da a ed r ed è detto indice di a rispetto ad r*; in simboli* $\mathrm{ind}_r(a) := h$*). Posto* $d := \mathrm{MCD}(m, p-1)$*, allora la congruenza*

$$X^m \equiv a \pmod{p} \qquad (\star)$$

è risolubile se, e soltanto se, $d \mid h$.
In questo caso, la congruenza $(\star)$ *ha esattamente* d *soluzioni distinte* $\{x_i : 1 \leqslant i \leqslant d\}$ *che sono univocamente determinate dalle* d *soluzioni* $\{y_i : 1 \leqslant i \leqslant d\}$ *della congruenza lineare* $mY \equiv h \pmod{p-1}$*, ponendo* $x_i = r^{y_i}$*, per* $1 \leqslant i \leqslant d$.

Dimostrazione. Poichè $p \nmid a$, ogni (eventuale) soluzione x di $(\star)$ non può essere divisibile per p e, dunque, è congruente (mod p) a:

$$r^y, \text{ per un qualche intero } y, \text{ con } 1 \leqslant y \leqslant p-1.$$

Dunque $(\star)$ è risolubile se, e soltanto se, esiste un intero y $(1 \leqslant y \leqslant p-1)$ che risolve la congruenza:

$$r^{my} \equiv r^h \pmod{p},$$

Pertanto, per il Corollario 5.5, $(\star)$ è risolubile se, e soltanto se, $my \equiv h \pmod{\mathrm{ord}_p(r)}$, cioè se, e soltanto se, la congruenza lineare

$$mY \equiv h \pmod{p-1}$$

è risolubile.
La conclusione discende immediatamente dal Teorema 2.2. □

Il seguente criterio può essere attribuito ad Euler anche se la dimostrazione originaria riguardava il caso $m = 2$, (cfr. la successiva Proposizione 6.5).

Corollario 5.19. (Criterio di Euler). *Con le notazioni ed ipotesi del Teorema 5.18, la congruenza* $(\star)$ *è risolubile se, e soltanto se, risulta:*

$$a^{\frac{p-1}{d}} \equiv 1 \pmod{p}.$$

Dimostrazione. Siano r, h come nell'enunciato del Teorema 5.18. Risulta:

$$a^{\frac{p-1}{d}} \equiv 1 \pmod{p} \iff r^{\frac{h(p-1)}{d}} \equiv 1 \pmod{p} \iff$$
$$\iff \frac{h(p-1)}{d} \equiv 0 \pmod{p-1}.$$

L'ultima condizione è ovviamente equivalente al fatto che $d \mid h$ e dunque la tesi discende immediatamente dal Teorema 5.18. □

Corollario 5.20. *Sia p un primo ed m un intero positivo. La congruenza:*

$$X^m \equiv a \pmod{p} \qquad (\star)$$

è risolubile esattamente per $1 + \left[\frac{(p-1)}{\mathrm{MCD}(m,\, p-1)}\right]$ *valori distinti* (mod p) *di a. In particolare, $(\star)$ è sempre risolubile (qualunque sia a) se, e soltanto se,* $\mathrm{MCD}(m, p-1) = 1$.

Dimostrazione. Sia $a \not\equiv 0 \pmod{p}$ ed r una radice primitiva (modulo p). Tenuto conto del Teorema 5.18, gli interi a distinti (mod p) per i quali $(\star)$ è risolubile corrispondono agli esponenti h tali che $d := \mathrm{MCD}(m, p-1) \mid h$ e $1 \leqslant h \leqslant p-1$. Tali interi sono esattamente

$$d, 2d, \ldots, sd \quad \text{con } sd = p-1$$

e pertanto sono in numero di $\frac{p-1}{d}$.
Se $a \equiv 0 \pmod{p}$ allora la congruenza $(\star)$ è risolubile (avendo come soluzione la soluzione banale $x = 0$): dunque complessivamente $(\star)$ è risolubile per $1 + \left[\frac{(p-1)}{d}\right]$ valori distinti (mod p) di a.
L'ultima asserzione è, ormai, del tutto ovvia. $\square$

La tecnica dimostrativa del Teorema 5.18 può essere applicata anche, e *direttamente*, per la soluzione di congruenze del tipo:

$$X^m \equiv a \pmod{n}, \text{ con } \mathrm{MCD}(a, n) = 1 \qquad (\bullet)$$

dove n è un intero positivo per il quale esista una radice primitiva (mod n). A tale scopo è opportuno premettere la definizione ed alcune proprietà elementari degli "indici".

Definizione 5.21. Sia n un intero positivo tale che esista una radice primitiva $r \pmod{n}$ (cfr. Teorema 5.17). Si verifica immediatamente che l'insieme $S^* := \{r, r^2, \ldots, r^{\varphi(n)}\}$ è un sistema ridotto di residui (mod n) e, dunque, per ogni $a \in \mathbb{Z}$ tale che $\mathrm{MCD}(a, n) = 1$ esiste un unico $r^h \in S^*$ $(1 \leqslant h \leqslant \varphi(n))$ tale che $r^h \equiv a \pmod{n}$. L'intero h (univocamente determinato (mod $\varphi(n)$) da a, fissato r) è detto *indice di a relativamente ad r* (in simboli, $\mathrm{ind}_r(a) := h$).

Proposizione 5.22. *Sia n un intero positivo tale che esista una radice primitiva $r \pmod{n}$. Presi comunque $a, b \in \mathbb{Z}$ tali che* $\mathrm{MCD}(a, n) = 1 = \mathrm{MCD}(b, n)$ *e preso comunque $k > 0$, si ha:*

(a) $a \equiv b \pmod{n} \iff \mathrm{ind}_r(a) = \mathrm{ind}_r(b)$;

(b) $\mathrm{ind}_r(ab) \equiv \mathrm{ind}_r(a) + \mathrm{ind}_r(b) \pmod{\varphi(n)}$;

(c) $\mathrm{ind}_r(a^k) \equiv k \cdot \mathrm{ind}_r(a) \pmod{\varphi(n)}$;

(d) $\mathrm{ind}_r(r) = 1$;

(e) $\mathrm{ind}_r(1) = \varphi(n)$ $(\equiv 0 \pmod{\varphi(n)})$;

(f) *se* a^* *è un inverso aritmetico di* $a \pmod n$, *risulta:* $\mathrm{ind}_r(a^*) \equiv -\mathrm{ind}_r(a) \pmod{\varphi(n)}$;

(g) *se* $\bar r$ *è un'altra radice primitiva* $\pmod n$, *risulta:* $\mathrm{ind}_{\bar r}(a) \equiv \mathrm{ind}_{\bar r}(r) \cdot \mathrm{ind}_r(a) \pmod{\varphi(n)}$.

Dimostrazione. Le semplici verifiche sono lasciate al lettore.
Ad esempio, per **(b)** basta osservare che:

$$r^{\mathrm{ind}_r(ab)} \equiv r^{\mathrm{ind}_r(a)+\mathrm{ind}_r(b)} \pmod n$$

ed applicare il Corollario 5.5.
Analogamente per **(g)** basta osservare che:

$$\bar r^{\mathrm{ind}_{\bar r}(a)} \equiv a \equiv r^{\mathrm{ind}_r(a)} \equiv \left(\bar r^{\mathrm{ind}_{\bar r}(r)}\right)^{\mathrm{ind}_r(a)} \equiv \bar r^{\mathrm{ind}_{\bar r}(r)\cdot\mathrm{ind}_r(a)} \pmod n. \ \square$$

Veniamo ora alla risoluzione di congruenze del tipo $(\bullet)$.

Teorema 5.23. *Sia* n *un intero positivo tale che esista una radice primitiva* $r \pmod n$. *Siano* a, m *interi tali che* $m > 0$ *e* $\mathrm{MCD}(a, n) = 1$.
Posto $d := \mathrm{MCD}(\varphi(n), m)$, *la congruenza:*

$$X^m \equiv a \pmod n \qquad (\bullet)$$

è risolubile se, e soltanto se, $d \mid \mathrm{ind}_r(a)$.
In tal caso la congruenza $(\bullet)$ *ha esattamente* d *soluzioni distinte.*

Dimostrazione. Procedendo come nella dimostrazione del Teorema 5.18, si verifica che risolvere $(\bullet)$ equivale a risolvere la congruenza lineare:

$$mY \equiv \mathrm{ind}_r(a) \pmod{\varphi(n)}$$

dove $Y = \mathrm{ind}_r(X)$.
La conclusione segue subito dal Teorema 2.2. $\square$

Corollario 5.24. (Criterio di Gauss). *Con le notazioni ed ipotesi del Teorema 5.23, la congruenza* $(\bullet)$ *è risolubile se, e soltanto se, risulta:*

$$a^{\frac{\varphi(n)}{d}} \equiv 1 \pmod n.$$

Dimostrazione. Applicando le proprietà dell'indice, si ha:

$$\begin{aligned} a^{\frac{\varphi(n)}{d}} \equiv 1 \pmod n &\iff \mathrm{ind}_r(a^{\frac{\varphi(n)}{d}}) = \mathrm{ind}_r(1) \\ &\iff \left(\frac{\varphi(n)}{d}\right) \cdot \mathrm{ind}_r(a) \equiv 0 \pmod{\varphi(n)} \\ &\iff d \mid \mathrm{ind}_r(a). \ \square \end{aligned}$$

Osservazione 5.25. **(1)** È chiaro che il Teorema 5.18 e il Criterio di Euler (Corollario 5.19) sono casi particolari rispettivamente del Teorema 5.23 e del criterio di Gauss (Corollario 5.24).
(2) Particolarmente importante è il caso di congruenze del tipo (•) tali che $m = 2$ e $n = p$ è primo dispari. In tal caso risulta $\mathrm{MCD}(2, p-1) = 2$ e dunque la congruenza

$$X^2 \equiv a \pmod{p}$$

è risolubile se, e soltanto se, $\mathrm{ind}_r(a)$ è pari. Sulla risoluzione di tali congruenze (quadratiche) torneremo ampiamente nel paragrafo successivo.
(3) Il Corollario 5.24 vale, assumendo come si è fatto che n possieda una radice primitiva. Se tale ipotesi non è soddisfatta si possono dare controesempi (cfr. il punto successivo e l'Osservazione 6.11).
(4) Si noti che una congruenza del tipo $X^m \equiv a \pmod{n}$ può essere risolubile anche nel caso in cui n non possieda una radice primitiva, ovvero nel caso in cui n possieda una radice primitiva, ma si verifichi che $\mathrm{MCD}(a, n) \neq 1$. Ad esempio se $n = 8$, la congruenza $X^2 \equiv 1 \pmod{8}$ è risolubile; se $n = 6$, la congruenza $X^2 \equiv 4 \pmod{6}$ è risolubile; se $n = 12$, la congruenza $X^3 \equiv 8 \pmod{12}$ è risolubile.

I risultati precedenti, relativi alla risoluzione di congruenze del tipo (•), hanno il difetto di rinviare a priori al calcolo di una radice primitiva e, come già osservato (cfr. Osservazione 5.14), non esistono metodi generali veramente efficaci per il calcolo di radici primitive. Sono però disponibili delle tavole, calcolate sperimentalmente, che forniscono esplicitamente le radici primitive $\pmod{n}$ per valori anche molto grandi di n. Ci limitiamo qui a presentare la seguente tavola in cui g_p denota la minima radice primitiva $\pmod{p}$, per ogni primo $p < 100$.

p	2	3	5	7	11	13	17	19	23	29	31	37	41
g_p	1	2	2	3	2	2	3	2	5	2	3	2	6
p	43	47	53	53	61	67	71	73	79	83	89	97	
g_p	3	5	2	2	2	2	7	5	3	2	3	5	

Osservazione 5.26. **(a)** Una tra le prime raccolte di tavole è contenuta nel famoso *Canon Arithmeticus* di C. Jacobi del 1839 (ristampa del 1956). Jacobi è riuscito ad elencare tutte le soluzioni (a, b) della congruenza

$$g_p^a \equiv b \pmod{p}$$

dove $1 \leqslant a, b \leqslant p-1$ e g_p è la radice primitiva minima $\pmod{p}$ e con $p < 1000$. Naturalmente oggi esistono delle tavole molto più esaurienti che possono essere ulteriormente estese progressivamente con il miglioramento delle prestazioni dei mezzi di calcolo (cfr. ad esempio A. E. Western - J. C. Miller, Tables of indices and primitive roots, Royal Society Math. Tables,

Cambridge University Press, 1968).
(b) Nel 1944 S. Pillai ha dimostrato che

$$\limsup_{p \longrightarrow +\infty} g_p = +\infty$$

più precisamente, per infiniti primi p, risulta

$$g_p > c \cdot \log(\log(p)),$$

dove c è una costante positiva.

Il risultato precedente è stato migliorato da Friedlander nel 1949 che ha dimostrato che, per un'infinità di primi p,

$$g_p > C \cdot \log p$$

(dove C è una costante positiva opportuna).

D'altra parte è stato dimostrato da Burgers nel 1962 che g_p non cresce "troppo in fretta", poiché per p sufficientemente grande

$$g_p \leqslant C \cdot p^{\frac{1}{4}+\varepsilon},$$

dove C è una costante positiva ed $\varepsilon > 0$.

Ricordiamo inoltre che Kearnes nel 1984 ha dimostrato il seguente risultato congetturato da Powell nel 1983: preso comunque un intero N esistono infiniti primi p tali che

$$N < g_p < p - N.$$

Segnaliamo infine due classiche congetture non ancora risolte:

(1) Esistono infiniti primi p tali che $g_p = 2$?

(2) (Gauss). Esistono infiniti primi p tali che ammettano 10 come radice primitiva?

Queste congetture sono state riformulate nel 1927 da E. Artin nella seguente forma più generale:

(3) Sia a un intero non nullo, non quadrato perfetto e distinto da 1 e -1. È vero che a è una radice primitiva per infiniti primi?

Più precisamente, la congettura di Artin è la seguente.

(3′) Se $N_a(x) := \#\{p : p \text{ primo} \leqslant x \text{ tale che } a \text{ è una radice primitiva } (\mathrm{mod}\ p)\}$ allora:

$$N_a(x) \sim A\frac{x}{\log x}$$

dove A dipende soltanto da a?

Da segnalare, comunque, che risultati parziali importanti sulla congettura di Artin sono stati ottenuti da C. Hooley nel 1965 (la congettura di Artin vale se vale l'ipotesi di Riemann generalizzata) e, successivamente, da R. Gupta e M. Ram Murthy (1984) e D.R. Heath-Brown (1985), dai quali si può dedurre che uno almeno tra 2, 3 e 5 è una radice primitiva mod p, per infiniti numeri primi p.
Le restrizioni su a nella congettura di Artin si giustificano in questo modo. Se $a = \pm 1$, allora $a^2 = 1$ e quindi $a = \pm 1$ non è radice primitiva $\pmod p$ per $p - 1 > 2$. Se $a = x^2$ e se p è primo dispari tale che $p \nmid x$, applicando il "Piccolo" Teorema di Fermat (cfr. Teorema 3.1) si ha:

$$a^{\frac{p-1}{2}} = x^{p-1} \equiv 1 \pmod p$$

e, dunque, a non è radice primitiva (mod p). Ne segue che, in tal caso, i primi che ammettono a come radice primitiva sono al più in numero finito.

Vogliamo concludere il paragrafo con alcuni esempi di risoluzioni di congruenze di tipo $(\star)$.

Esempio 5.27. Vogliamo studiare le congruenze:

$$X^5 \equiv a \pmod 7, \quad \text{con } 1 \leqslant a \leqslant 6. \tag{$*$}$$

Si noti che $m = 5, p = 7$ e quindi $\mathrm{MCD}(m, p-1) = 1$. È facile verificare che esistono $\varphi(\varphi(7)) = \varphi(6) = 2$ radici primitive distinte (mod 7) che sono, a calcoli fatti, $r = 3$ ed $s = 5$. Calcoliamo l'indice di ogni intero a $(1 \leqslant a \leqslant 6)$ relativamente ad r ed s. Si ha:

a	1	2	3	4	5	6
$\mathrm{ind}_r(a)$	6	2	1	4	5	3

a	1	2	3	4	5	6
$\mathrm{ind}_s(a)$	6	4	5	2	1	3

Ogni congruenza $(*)$ si trasforma in:

$$5 \cdot \mathrm{ind}_r(X) \equiv \mathrm{ind}_r(a) \pmod 6 \quad \text{oppure} \quad 5 \cdot \mathrm{ind}_s(X) \equiv \mathrm{ind}_s(a) \pmod 6,$$

e poiché $\mathrm{MCD}(5,6) = 1$, entrambe le congruenze sono risolubili per ogni valore di a. A tale conclusione si poteva arrivare anche utilizzando il Criterio di risolubilità di Euler. Infatti $p = 7, m = 5, d = \mathrm{MCD}(5,6) = 1$ e quindi $a^6 \equiv 1 \pmod 7$ per ogni a, tale che $p \nmid a$.
Le congruenze (mod 6) sopra considerate ammettono, fissato a, un'unica soluzione (la quale determina un'unica soluzione x per la congruenza $(*)$). Precisamente si ha:

a	1	2	3	4	5	6	(mod 7)
$\mathrm{ind}_r(a)$	0	2	1	4	5	3	(mod 6)
$\mathrm{ind}_r(x)$	0	4	5	2	1	3	(mod 6)
x	1	4	5	2	3	6	(mod 7)

a	1	2	3	4	5	6	(mod 7)
$\mathrm{ind}_s(a)$	0	4	5	2	1	3	(mod 6)
$\mathrm{ind}_s(x)$	0	2	1	4	5	3	(mod 6)
x	1	4	5	2	3	6	(mod 7)

Esempio 5.28. Vogliamo studiare le congruenze:

$$X^3 \equiv a \pmod{13}, \quad \text{con } 1 \leqslant a \leqslant 12. \tag{$**$}$$

In base al Criterio di Euler (cfr. Corollario 5.19), le congruenze $(**)$ sono risolubili se, e soltanto se, $a^{\frac{12}{d}} \equiv 1 \pmod{13}$ e cioè (essendo $d = \mathrm{MCD}(3,12) = 3$) se, e soltanto se, $a^4 \equiv 1 \pmod{13}$. Poiché risulta:

(mod 13) a	1	2	3	4	5	6	7	8	9	10	11	12
(mod 13) a^4	1	3	3	9	1	9	9	1	9	3	3	1

le $(**)$ sono risolubili per $a = 1, 5, 8, 12$.
Essendo $2^6 = 2^3 \cdot 2^3 = 8 \cdot 8 \equiv -1 \pmod{13}$, si verifica subito che $r = 2$ è una radice primitiva (mod 13) e gli indici relativamente ad $r = 2$ sono i seguenti:

a	1	2	3	4	5	6	7	8	9	10	11	12
$\mathrm{ind}_2(a)$	12	1	4	2	9	5	11	3	8	10	7	6

Pertanto, le soluzioni delle quattro congruenze $(**)$ risolubili sono ottenute risolvendo le quattro congruenze lineari:

$$3Y \equiv \mathrm{ind}_2(a) \pmod{12},$$

con $a \equiv 1, 5, 8, 12 \pmod{13}$ e, quindi, $\mathrm{ind}_2(a) = 12, 9, 3, 6$, dove $Y = \mathrm{ind}_2(X)$. Ciascuna di esse ammette tre soluzioni (mod 12), che si ottengono dall'unica soluzione della congruenza

$$Y \equiv \frac{\mathrm{ind}_2(a)}{3} \pmod{4}$$

dove $3 \mid \mathrm{ind}_2(a)$, per $a \equiv 1, 5, 8, 12 \pmod{13}$.
Pertanto, le soluzioni sono:

$$y \equiv \frac{\mathrm{ind}_2(a)}{3} + 4k \pmod{12},\ k = 0, 1, 2.$$

Precisamente, si ha:

(mod 13) a	(mod 12) $\mathrm{ind}_2(a)$	(mod 12) $y = \mathrm{ind}_2(x)$	(mod 13) x
1	12	4	3
		8	9
		12	1
5	9	3	8
		7	11
		11	7
8	3	1	2
		5	6
		9	5
12	6	2	4
		6	12
		10	10

5. Esercizi e Complementi

5.1. Siano $a, n \in \mathbb{Z}, n \geqslant 2$. Mostrare che:
(a) se $h, k \in \mathbb{Z}, k, h > 0$ e $\mathrm{ord}_n(a) = hk$, allora $\mathrm{ord}_n(a^h) = k$;
(b) se p è un primo dispari, $k \in \mathbb{Z}, k > 0$ e $\mathrm{ord}_p(a) = 2k$, allora $a^k \equiv -1 \pmod{p}$;
(c) se $\mathrm{ord}_n(a) = n-1$, allora n è primo (e quindi a è una radice primitiva $\pmod{n}$);
(d) se p è primo e $\mathrm{ord}_p(a) = 3$, allora $\mathrm{ord}_p(a+1) = 6$.
[Suggerimento: **(a)** è evidente. Per **(b)** si osservi che se $a^k \equiv b \not\equiv 1 \pmod{p}$ allora da $b^2 \equiv 1 \pmod{p}$ e $b \not\equiv 1 \pmod{p}$ si ricava che $b \equiv -1 \pmod{p}$. Per **(c)** basta ricordare che $\mathrm{ord}_n(a) \mid \varphi(n)$ e $\varphi(n) \leqslant n-1$. Per **(d)** si osservi che $a^2 + a + 1 \equiv 0 \pmod{p}$ e dunque $(a+1)^2 \equiv a \pmod{p}, (a+1)^3 \equiv -1 \pmod{p}$.]

5.2. Sia p un primo dispari ed r una radice primitiva $(\mathrm{mod}\ p)$. Mostrare che:
(a) $r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$;
(b) se r' è un'altra radice primitiva $(\mathrm{mod}\ p)$ (cioè $r' \not\equiv r \pmod{p}$), allora rr' non è mai una radice primitiva $(\mathrm{mod}\ p)$;
(c) se $a \in \mathbb{Z}$ è tale che $ar \equiv 1 \pmod{p}$, allora a è una radice primitiva $(\mathrm{mod}\ p)$;
(d) se $p \geqslant 5$, l'insieme delle radici primitive $(\mathrm{mod}\ p)$ può essere ripartito in paia di elementi distinti di tipo $\{r, r'\}$ con $rr' \equiv 1 \pmod{p}$;
(e) se $p \equiv 1 \pmod{4}$, $-r$ è una radice primitiva $(\mathrm{mod}\ p)$;
(f) se $p \equiv 3 \pmod{4}$, $\mathrm{ord}_p(-r) = \frac{p-1}{2}$.
[Suggerimento: **(a)** $r^{\frac{p-1}{2}}$ è soluzione di $X^2 \equiv 1 \pmod{p}$ (Si tenga presente anche l'Esercizio 5.1 (b)). **(b)** segue immediatamente da **(a)**. **(c)** è una conseguenza della Proposizione 5.4 (4). **(d)** basta porre $r' = r^{p-2}$. **(e)**, **(f)** si calcoli $(-r)^{\frac{p-1}{2}}$.]

5.3. Se p è un primo dispari ed n un intero positivo, allora:

$$1^n + 2^n + \cdots + (p-1)^n \equiv \begin{cases} 0 \pmod{p} & \text{se } (p-1) \nmid n, \\ -1 \pmod{p} & \text{se } (p-1) \mid n. \end{cases}$$

[Suggerimento: se r è una radice primitiva $(\mathrm{mod}\ p)$, la somma in questione è congruente $(\mathrm{mod}\ p)$ a $1 + r^n + r^{2n} + \cdots + r^{(p-2)n}$. Se $(p-1) \mid n$, l'asserto è evidente dal momento che l'espressione precedente è congrua a $p-1 \pmod{p}$; se $(p-1) \nmid n$, poiché $(r^{(p-2)n} + \cdots + r^n + 1) \cdot (r^n - 1) = (r^{(p-1)n} - 1) \equiv 0 \pmod{p}$ e $r^n - 1 \not\equiv 0 \pmod{p}$, si ricava che $1 + r^n + r^{2n} + \cdots + r^{(p-2)n} \equiv 0 \pmod{p}$.]

5.4. Se p è un primo dispari ed r è una radice primitiva $(\mathrm{mod}\ p^n)$ con $n \geqslant 2$, allora r è una radice primitiva $(\mathrm{mod}\ p)$.
[Suggerimento: se $h := \mathrm{ord}_p(r)$, risulta $r^{hp} \equiv 1 \pmod{p^2}$. Infatti $p \mid (r^h - 1)$ e $p \mid (r^{p(h-1)} + r^{p(h-2)} + \cdots + r + 1)$ (poiché $p \mid (r^{(h-1)} + r^{(h-2)} + \cdots + r + 1)$ e $p \nmid (r-1)$). Quindi, per induzione su n, si dimostra che $r^{hp^{n-1}} \equiv 1 \pmod{p^n}$. Ne segue che $\varphi(p^n) \mid p^{n-1}h$, da cui discende l'asserto.]

5.5. Sia p un primo dispari ed r una radice primitiva $(\mathrm{mod}\ p)$. Mostrare che $\mathrm{ind}_r(-1) = \mathrm{ind}_r(p-1) = \frac{p-1}{2}$.
[Suggerimento: $0 \equiv (r^{p-1} - 1) = (r^{\frac{p-1}{2}} - 1) \cdot (r^{\frac{p-1}{2}} + 1) \pmod{p}$, da cui si ricava che $r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ e quindi che $\mathrm{ind}_r(-1) = \frac{p-1}{2}$.]

5.6. (a) Un metodo algoritmico per il calcolo delle potenze di un intero a (mod n).

Calcolare dapprima tutti i prodotti $a, 2a, \ldots, (n-1)a \pmod n$. Procedere poi induttivamente: se $h \geqslant 1$ e se $a^h \equiv j \pmod n$, allora $a^{h+1} \equiv ja \pmod n$.
(b) Calcolare la potenza dodicesima di 3 (mod 21). [Soluzione (b) : $3^{12} \equiv 15 \pmod{21}$.]

5.7. Stabilire se la congruenza $X^4 \equiv 4 \pmod{17}$ è risolubile. In caso affermativo determinare le soluzioni.
[Suggerimento: $r = 3$, $\mathrm{ind}_3(4) = 12$. La congruenza $4 \cdot Y \equiv 12 \pmod{16}$ ha quattro soluzioni $y \equiv 3, 7, 11, 15 \pmod{16}$, da cui segue che le soluzioni cercate sono, rispettivamente, $x \equiv 10, 11, 7, 6 \pmod{17}$.]

5.8. Mostrare che se r è una radice primitiva (mod n), allora:

$$1 + r + r^2 + \cdots + r^{\varphi(n)-1} \equiv 0 \pmod n.$$

[Suggerimento: si usi l'Esercizio 3.12 (b).]

5.9. Determinare per quali valori di a la congruenza nell'indeterminata X

$$7^X \equiv a \pmod{17}$$

è risolubile. Per ogni valore di a, per il quale la congruenza è risolubile, determinare le soluzioni (mod 16).
[Suggerimento: la radice primitiva minima positiva (mod 17) è $r = 3$. La tabella degli indici è la seguente:

(mod 17) a	1	2	3	4	5	6	7	8
(mod 16) $\mathrm{ind}_3(a)$	16	14	1	12	5	15	11	10
(mod 17) a	9	10	11	12	13	14	15	16
(mod 16) $\mathrm{ind}_3(a)$	2	3	7	13	4	9	6	8

Quindi la congruenza precedente diviene:

$$X \,\mathrm{ind}_3(7) \equiv \mathrm{ind}_3(a) \pmod{16}$$

cioè

$$11X \equiv \mathrm{ind}_3(a) \pmod{16}.$$

Poiché $\mathrm{MCD}(11, 16) = 1$. Tale congruenza è risolubile per ogni a ed ha un'unica soluzione data da $x \equiv 3 \cdot \mathrm{ind}_3(a) \pmod{16}$.]

5.10. Determinare per quali valori di a la congruenza

$$8X^5 \equiv a \pmod{17}$$

è risolubile. Per ogni valore di a per il quale la congruenza è risolubile determinare le soluzioni (mod 17).
[Suggerimento: se r è una radice primitiva (mod 17) la congruenza data si riconduce alla congruenza

$$5Y \equiv \mathrm{ind}_r(a) - \mathrm{ind}_r(8) \pmod{16}, \text{ con } Y := \mathrm{ind}_r(X).$$

Dal momento che $\mathrm{MCD}(5, 16) = 1$. La congruenza data è risolubile per ogni valore di a ed ammette per ogni a un'unica soluzione.
Per $r = 3$ abbiamo, pertanto, la seguente tabella:

(mod 17)	a	1	2	3	4	5	6	7	8
(mod 16)	$\mathrm{ind}_3(a)$	16	14	1	12	5	15	11	10
(mod 16)	$\mathrm{ind}_3(a)$ - $\mathrm{ind}_3(8)$	6	4	7	2	11	5	1	16
(mod 16)	y	14	4	11	10	15	1	13	16
(mod 17)	x	2	13	7	8	6	3	12	11

.]

(mod 17)	a	9	10	11	12	13	14	15	16
(mod 16)	$\mathrm{ind}_3(a)$	2	3	7	13	4	9	6	8
(mod 16)	$\mathrm{ind}_3(a)$ - $\mathrm{ind}_3(8)$	8	9	13	3	10	15	12	14
(mod 16)	y	8	5	9	7	2	3	12	6
(mod 17)	x	16	5	14	11	9	10	4	15

5.11. Determinare per quali valori di a la congruenza

$$X^6 \equiv a \pmod{23}$$

è risolubile e determinare, per ciascun valore di a per il quale è risolubile, le soluzioni (mod 23).
[Suggerimento: la radice primitiva minima in valore assoluto (mod 23) è $r = -2$ (Esempio 5.15). Essendo $\mathrm{MCD}(6, 22) = 2$, la congruenza $6Y \equiv \mathrm{ind}_{-2}(a) \pmod{22}$ è risolubile se e soltanto se, $\mathrm{ind}_{-2}(a)$ è pari ed in tal caso ha due soluzioni:

(mod 23)	a	1	2	3	4	5	6	7	8
(mod 22)	$\mathrm{ind}_r(a)$	22	12	8	2	17	20	15	14
(mod 22)	$\mathrm{ind}_r(x)$	11, 22	2, 13	5, 16	4, 15	-	7, 18	-	6, 17
(mod 23)	x	22, 1	4, 19	14, 9	16, 7	-	10, 13	-	18, 5

(mod 23)	a	9	10	11	12	13	14	15	16
(mod 22)	$\mathrm{ind}_r(a)$	16	7	21	10	18	5	3	4
(mod 22)	$\mathrm{ind}_r(x)$	10, 21	-	-	9, 20	3, 14	-	-	8, 19
(mod 23)	x	12, 11	-	-	17, 6	15, 8	-	-	3, 20

(mod 23)	a	17	18	19	20	21	22
(mod 22)	$\mathrm{ind}_r(a)$	9	6	13	19	1	11
(mod 22)	$\mathrm{ind}_r(x)$	-	1, 12	-	-	-	-
(mod 23)	x	-	21, 2	-	-	-	-

.]

5.12. Sia p un primo e $a \in \mathbb{Z}$ con $p \nmid a$. Mostrare che se $\mathrm{ord}_p(a) = n \cdot m$ con $\mathrm{MCD}(n, m) = 1$, allora esistono $b, c \in \mathbb{Z}$ con $\mathrm{ord}_p(b) = n$, $\mathrm{ord}_p(c) = m$ e $b \cdot c \equiv a \pmod{p}$.
[Suggerimento: innanzitutto (Teorema 2.5) è possibile trovare due interi $u, v > 0$ tali che $nu - mv = 1$. Si ponga $c := a^{nu}, b := (a^*)^{mv}$ dove a^* è inverso aritmetico di $a \pmod{p}$.]

5.13. Determinare le eventuali soluzioni della congruenza:

$$2^X \equiv X \pmod{13}.$$

[Suggerimento: si vede facilmente che $r = 2$ è una radice primitiva (mod 13). Il problema della risoluzione della congruenza data si trasforma nel problema della risoluzione della congruenza:

$$X \mathrm{ind}_2(2) \equiv \mathrm{ind}_2(X) \pmod{12}$$

ovvero $X - \mathrm{ind}_2(X) \equiv 0 \pmod{12}$.
Pertanto, le soluzioni della congruenza data sono le soluzioni del sistema:

$$\begin{cases} X \equiv a \pmod{13} \\ X \equiv \mathrm{ind}_2(a) \pmod{12}\,. \end{cases}$$

Essendo:

(mod 13)	a	1	2	3	4	5	6	7	8	9	10	11	12
(mod 12)	$\mathrm{ind}_2(a)$	12	1	4	2	9	5	11	3	8	10	7	6

le soluzioni non congrue (mod $12 \cdot 13 = 156$) sono in tutto 12 e sono date da $x = 10, 16, 57, 59, 90, 99, 115, 134, 144, 145, 149, 152 \pmod{12 \cdot 13}$.]

5.14. Determinare per quali valori di a la congruenza:

$$9X^8 \equiv a \pmod{14}$$

è risolubile. Per ciascuno dei valori di a per il quale la congruenza è risolubile, determinare le soluzioni della congruenza.
[Suggerimento: $n = 14, \varphi(n) = 6$. Si vede che $r = 3$ è una radice primitiva (mod 14).
Le soluzioni, *per quegli interi a che soddisfano alla condizione* $\mathrm{MCD}(a, 14) = 1$, si ottengono facilmente nella seguente maniera:

(mod 14)	a, con $\mathrm{MCD}(a, 14) = 1$	1	3	5	9	11	13
(mod 6)	$\mathrm{ind}_3(a)$	0	1	5	2	4	3
(mod 6)	$\mathrm{ind}_3(a) - 2$	4	5	3	0	2	1

per tali valori di a, la congruenza:

$$8\mathrm{ind}_3(X) \equiv \mathrm{ind}_3(a) - 2 \pmod{6}$$

è risolubile se e soltanto se $\mathrm{MCD}(8, 6) = 2 \mid (\mathrm{ind}_3(a) - 2)$, quindi se e soltanto se $a \equiv 1, 9, 11 \pmod{14}$.
Le soluzioni sono: per $a \equiv 1$, $x \equiv 5, 9 \pmod{14}$; per $a \equiv 9$, $x \equiv 1, 13 \pmod{14}$; per $a \equiv 11$, $x \equiv 3, 11 \pmod{14}$.
Tuttavia, la congruenza potrebbe essere risolubile anche per valori di a non necessariamente primi con 14.
Per determinare quindi *tutte* le soluzioni, posto $f(X) := 9X^8 - a$, si debbono determinare le soluzioni del sistema di congruenze:

$$\begin{cases} f(X) \equiv 0 \pmod{2} \\ f(X) \equiv 0 \pmod{7} \end{cases} \quad \text{ovvero} \quad \begin{cases} X - a \equiv 0 \pmod{2} \\ 2X^2 - a \equiv 0 \pmod{7} \end{cases} \qquad (\diamond)$$

La seconda congruenza del sistema è risolubile se e soltanto se $(4a)^3 \equiv 1 \pmod{7}$ cioè per $a \equiv 1, 2, 4 \pmod{7}$, mentre la prima congruenza è risolubile per qualsiasi valore di $a \pmod{2}$.
In definitiva, le soluzioni della congruenza data si ottengono per a che soddisfa uno qualunque dei seguenti sistemi (mod 14):

$$\begin{cases} a \equiv 0 \pmod{2} \\ a \equiv 1 \pmod{7} \end{cases} \quad \begin{cases} a \equiv 0 \pmod{2} \\ a \equiv 2 \pmod{7} \end{cases} \quad \begin{cases} a \equiv 0 \pmod{2} \\ a \equiv 4 \pmod{7} \end{cases}$$

$$\begin{cases} a \equiv 1 \pmod{2} \\ a \equiv 1 \pmod{7} \end{cases} \quad \begin{cases} a \equiv 1 \pmod{2} \\ a \equiv 2 \pmod{7} \end{cases} \quad \begin{cases} a \equiv 1 \pmod{2} \\ a \equiv 4 \pmod{7} \end{cases}$$

e cioè $a \equiv 8, 2, 4, 1, 9, 11 \pmod{14}$. In corrispondenza di ciascuno di tali valori di a, si deve risolvere il sistema $(\diamond)$, il quale
per $a \equiv 8$ ha come soluzioni $x \equiv 2, 12 \pmod{14}$;
per $a \equiv 2$ ha come soluzioni $x \equiv 6, 8 \pmod{14}$;
per $a \equiv 4$ ha come soluzioni $x \equiv 4, 10 \pmod{14}$;
per $a \equiv 1$ ha come soluzioni $x \equiv 5, 9 \pmod{14}$;
per $a \equiv 9$ ha come soluzioni $x \equiv 1, 13 \pmod{14}$;
per $a \equiv 11$ ha come soluzioni $x \equiv 3, 11 \pmod{14}$.]

5.15. Mostrare che, se $n = 2^k$, con $k \geqslant 3$, non esiste una radice primitiva $\pmod{n}$.

5.16. Se $r, s \geqslant 3$ e se $\mathrm{MCD}(r, s) = 1$, allora mostrare che:
(a) non esiste una radice primitiva $\pmod{r \cdot s}$;
(b) se $n = p \cdot q$ ed p e q sono primi dispari, allora non esiste una radice primitiva $\pmod{n}$;
(c) se $n = 2^e p^k$ con $e \geqslant 2, k \geqslant 1$, p primo dispari, allora non esiste una radice primitiva $\pmod{n}$.

5.17. Se p è un primo dispari, mostrare che:
(a) esiste sempre una radice primitiva $r \pmod{p}$ tale che:

$$r^{p-1} \not\equiv 1 \pmod{p^2};$$

(b) se r è una radice primitiva $\pmod{p}$, allora r oppure $r+p$ è una radice primitiva $\pmod{p^2}$;
(c) se r è una radice primitiva $\pmod{p}$ e se

$$r^{p-1} \not\equiv 1 \pmod{p^2}$$

allora:

$$r^{(p-1)p^{k-2}} \not\equiv 1 \pmod{p^k}$$

per ogni $k \geqslant 2$;
(d) se r è una radice primitiva $\pmod{p}$ e se

$$r^{(p-1)p^{k-2}} \not\equiv 1 \pmod{p^k}$$

allora r è una radice primitiva $\pmod{p^k}$.

5.18. Sia p un primo dispari e $k \geqslant 1$. Mostrare che:
(a) esiste sempre una radice primitiva $r \pmod{p^k}$ con $r \equiv 1 \pmod{2}$;
(b) se r è una radice primitiva $\pmod{p^k}$, e se $r \equiv 1 \pmod{2}$ allora r è anche una radice primitiva $\pmod{2 \cdot p^k}$.

6 Congruenze quadratiche e legge di reciprocità

Il punto centrale di questo paragrafo è la dimostrazione della Legge di Reciprocità Quadratica (abbreviata LRQ). La prima dimostrazione completa di tale legge risale a Gauss, che la terminò nell'aprile del 1796 (e successivamente lo stesso Gauss ne ha dato almeno altre otto dimostrazioni differenti). Il primo a congetturare la validità della LQR era stato comunque Euler (nel 1745), che ne aveva poi dato anche una dimostrazione (sbagliata) nel 1783, nel suo *Opuscula Analytica*. Infine, A.M. Legendre nel suo lavoro *Recherches d'Analyse Indéterminée* (1785) dapprima, e poi nel volume *Essai sur la Théorie des Nombres* (1798), aveva ridimostrato la LRQ (in forma però incompleta), introducendo una nuova notazione (cioè, il *simbolo di Legendre*), che ne permetteva una formulazione più elegante.

Questa pluralità di contributi doveva quindi scatenare un'accesa disputa tra Euler, Legendre e Gauss, per l'attribuzione di priorità e meriti nella dimostrazione della LRQ. Informazioni più precise al riguardo si trovano in un libro di Bachmann [B], che si è ispirato ad un famoso articolo di Kronecker [K] del 1875.

La teoria delle congruenze quadratiche, cioè delle congruenze del tipo:

$$aX^2 + bX + c \equiv 0 \pmod{p} \tag{1}$$

con $a, b, c \in \mathbb{Z}$ e p primo, è certamente più complessa della teoria delle congruenze lineari, sviluppata nel Paragrafo 2 (ricordiamo che l'ipotesi che p sia primo non è restrittiva, perché possiamo sempre ricondurci a tale caso in base a quanto esposto nel Paragrafo 4). In effetti, la congruenza (1) può non essere risolubile e, se è risolubile, può non essere facile calcolarne le soluzioni. In questo paragrafo illustreremo un procedimento che permetterà di stabilire se (1) è o non è risolubile, ma non forniremo alcun metodo specifico pratico, veramente efficace, per il calcolo delle soluzioni, rinviando per questo alle tecniche generali del paragrafo precedente.

Nel considerare (1) possiamo senz'altro supporre che $p \nmid a$ (in caso contrario, (1) è una congruenza lineare) e che $p \neq 2$ (se $p = 2$, la ricerca delle soluzioni di (1) si riduce ad una banale verifica, cfr. anche il successivo Esercizio 6.1). In tali ipotesi $p \nmid 4a$ e, dunque, (1) è equivalente alla congruenza:

$$4a(aX^2 + bX + c) = (2aX + b)^2 - (b^2 - 4ac) \equiv 0 \pmod{p}.$$

Ponendo $Y := 2aX + b$ e $d := b^2 - 4ac$, (1) è equivalente a

$$Y^2 \equiv d \pmod{p}. \tag{2}$$

La risoluzione di (1) si riduce alla risoluzione di (2) e successivamente, nel caso in cui y_0 sia soluzione di (2), alla risoluzione della congruenza lineare:

$$2aX + b \equiv y_0 \pmod{p}.$$

Si noti che tale congruenza, fissato y_0 ha un'unica soluzione (mod p) data da:

$$x_0 := \frac{p+1}{2}\, a^*(y_0 - b),$$

essendo a^* un inverso aritmetico di $a \pmod p$ e $\frac{p+1}{2}$ un inverso aritmetico di $2 \pmod p$.

Nella prima parte di questo paragrafo ci occuperemo di congruenze quadratiche della forma:

$$X^2 \equiv a \pmod p \tag{3}$$

con p primo dispari ed a intero tale che $\mathrm{MCD}(a,p) = 1$.

Proposizione 6.1. *Se la congruenza* (3) *è risolubile, allora essa ha due soluzioni distinte (cioè incongruenti* (mod p)*).*

Dimostrazione. Il Teorema di Lagrange (cfr. Teorema 4.19) assicura che (3) ha al più due soluzioni. Se x_0 è una soluzione di (3), anche $p - x_0 =: x_1$ è soluzione di (3) (infatti $(p - x_0)^2 \equiv x_0^2 \equiv a \pmod p$).
Inoltre $x_0 \not\equiv x_1 \pmod p$ (altrimenti risulterebbe $p - x_0 \equiv x_0 \pmod p$, da cui $2x_0 \equiv 0 \pmod p$, mentre $p \nmid 2$ e $p \nmid x_0$, perché $p \nmid a$). □

Definizione 6.2. Sia p un primo dispari ed a un intero tale che si abbia $\mathrm{MCD}(a,p) = 1$. Se la congruenza (3) è risolubile, si dirà che a è un *residuo quadratico* di p; in caso contrario, si dirà che a è un *non residuo quadratico* di p.

Proposizione 6.3. *Sia p un primo dispari ed a un intero tale che si abbia* $\mathrm{MCD}(a,p) = 1$. *Allora a è un residuo quadratico di p se, e soltanto se, a è congruente* (mod p) *ad uno dei seguenti interi:*

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2.$$

Quindi, tra gli interi $1, 2, \ldots, p-1$, esattamente $\frac{p-1}{2}$ sono residui quadratici di p, mentre gli altri $\frac{p-1}{2}$ non lo sono.

Dimostrazione. È sufficiente osservare che, se a è un residuo quadratico di p, una delle due soluzioni della congruenza (3) è congruente ad uno degli interi $1, 2, \ldots, \frac{p-1}{2}$ (ciò segue immediatamente dalla dimostrazione della Proposizione 6.1). L'implicazione inversa è ovvia.

Per quanto concerne l'ultima affermazione, basta verificare che gli interi $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ sono a due a due incongruenti (mod p) (cfr. anche la dimostrazione del Lemma 4.12). □

Per caratterizzare quando un intero a è un residuo quadratico di p è conveniente introdurre la seguente notazione, dovuta a Legendre:

Definizione 6.4. Sia p un primo dispari ed a un intero tale che si abbia $\mathrm{MCD}(a,p)=1$. Si chiama *simbolo di Legendre* il simbolo così definito:

$$\left(\frac{a}{p}\right) := \begin{cases} 1, & \text{se } a \text{ è un residuo quadratico di } p \\ -1, & \text{se } a \text{ non è un residuo quadratico di } p \end{cases}$$

Se $p=2$ e se a è dispari, allora si pone:

$$\left(\frac{a}{2}\right) = \left(\frac{1}{2}\right) := 1\,.$$

A volte, per avere una definizione valida per ogni intero a, si pone $(\frac{a}{p}) := 0$ se $p \mid a$.

Un primo importante risultato, che otteniamo riformulando il Corollario 5.19, per $m=2$, è il seguente:

Proposizione 6.5. (Criterio di Euler). *Sia p un primo dispari ed a un intero tale che* $\mathrm{MCD}(a,p)=1$. *Risulta:*

$$\left(\frac{a}{p}\right) = 1 \iff a^{\frac{p-1}{2}} \equiv 1 \pmod{p}. \quad \square$$

Proposizione 6.6. *Sia p un primo dispari ed siano $a,b \in \mathbb{Z}$ tali che si abbia* $\mathrm{MCD}(a,p)=1=\mathrm{MCD}(b,p)$. *Allora:*

(a) $a \equiv b \pmod{p} \Rightarrow (\frac{a}{p}) = (\frac{b}{p})$;

(b) $(\frac{a^2}{p}) = 1$;

(c) $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod{p}$;

(d) $(\frac{a}{p}) = (-1)^{\mathrm{ind}_r(a)}$, *dove r è una radice primitiva* $\pmod{p}$;

(e) $(\frac{ab}{p}) = (\frac{a}{p}) \cdot (\frac{b}{p})$;

(f) $(\frac{1}{p}) = 1$;

(g) $(\frac{a}{p}) = (\frac{a^*}{p})$, *dove a^* è un inverso aritmetico di a* $\pmod{p}$;

(h) $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{se } p \equiv 1 \pmod 4, \\ -1 & \text{se } p \equiv 3 \pmod 4; \end{cases}$

(i) $(\frac{ab^2}{p}) = (\frac{a}{p})$.

Dimostrazione. **(a)**: è del tutto ovvio. **(b)**: basta osservare che a è soluzione della congruenza $X^2 \equiv a^2 \pmod{p}$. **(c)**: dal "Piccolo" Teorema di Fermat segue che $(a^{\frac{p-1}{2}})^2 \equiv 1 \pmod{p}$ e dunque $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. Per concludere basta utilizzare il Criterio di Euler (cfr. Proposizione 6.5). **(d)**: è un'immediata conseguenza del Teorema 5.23 ovvero dell'Osservazione 5.25(2). Infatti, $X^2 \equiv a \pmod{p}$ è risolubile se e soltanto se $2 = \mathrm{MCD}(2, p-1) \mid \mathrm{ind}_r(a)$. **(e)**: risulta $(\frac{ab}{p}) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv (\frac{a}{p}) \cdot (\frac{b}{p}) \pmod{p}$. Poiché il simbolo di Legendre assume soltanto valori ± 1 e $p > 2$, la congruenza $(\frac{ab}{p}) \equiv (\frac{a}{p}) \cdot (\frac{b}{p}) \pmod{p}$ è un'uguaglianza. **(f)**: è immediata. **(g)**: risulta: $(\frac{a}{p}) \cdot (\frac{a^*}{p}) = (\frac{aa^*}{p}) = (\frac{1}{p}) = 1$. Da ciò segue l'asserto. **(h)**: da (c) segue che $(\frac{-1}{p}) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$. Ragionando come in (e), essendo $p > 2$, si ha l'uguaglianza. Infine, si osservi che $\frac{p-1}{2}$ è pari (rispettivamente dispari) se, e soltanto se, $p \equiv 1 \pmod{4}$ (rispettivamente, $p \equiv 3 \pmod{4}$). **(i)**: risulta $(\frac{ab^2}{p}) = (\frac{a}{p}) \cdot (\frac{b^2}{p}) = (\frac{a}{p})$. □

Si noti che l'affermazione **(a)** della proposizione precedente non si inverte. Infatti $2 \not\equiv 3 \pmod{5}$, mentre $X^2 \equiv 2 \pmod{5}$ e $X^2 \equiv 3 \pmod{5}$ non sono risolubili, quindi:

$$\left(\frac{2}{5}\right) = \left(\frac{3}{5}\right) = -1.$$

Oppure, $1 \not\equiv 4 \pmod{5}$, però come è subito visto:

$$\left(\frac{1}{5}\right) = \left(\frac{4}{5}\right) = 1.$$

Corollario 6.7. *Nella situazione della Proposizione 6.6, si ha:*

$$\left(\frac{-a^2}{p}\right) = 1 \iff p \equiv 1 \pmod{4}$$

In altre parole la congruenza $X^2 + a^2 \equiv 0 \pmod{p}$ *è risolubile se, e soltanto se,* $p \equiv 1 \pmod{4}$. □

Corollario 6.8. *Sia* p *un primo dispari ed* a *un intero tale che* $\mathrm{MCD}(a, p) = 1$. *La congruenza:*

$$aX^2 + bX + c \equiv 0 \pmod{p} \tag{1}$$

è risolubile se, e soltanto se, l'intero $b^2 - 4ac$ *è un residuo quadratico di* p *oppure è congruente a zero* $\pmod{p}$. □

Dimostrazione. L'enunciato segue dalla "riduzione" discussa all'inizio del paragrafo. □

Corollario 6.9. *Sia p un primo dispari ed $a = \pm p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$ un intero tale che* $\mathrm{MCD}(a,p) = 1$. *Allora:*

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right) \cdot \left(\frac{p_1}{p}\right)^{e_1} \cdot \left(\frac{p_2}{p}\right)^{e_2} \cdot \ldots \cdot \left(\frac{p_r}{p}\right)^{e_r}. \quad \square$$

Dal precedente corollario discende che per calcolare $(\frac{a}{p})$ è sufficiente saper calcolare i simboli di Legendre del tipo $(\frac{\pm 1}{p})$ e $(\frac{q}{p})$, con p, q primi distinti. La Legge di Reciprocità Quadratica, come vedremo, riguarderà il calcolo del simbolo $(\frac{q}{p})$, nel caso in cui p, q siano primi distinti *entrambi dispari*.

Corollario 6.10. *Sia p un primo dispari ed r una radice primitiva (modulo p). I residui quadratici di p sono congruenti alle potenze pari di r. Quindi:*

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0.$$

Dimostrazione. La prima affermazione è una conseguenza immediata della Proposizione 6.6(d) e la seconda della Proposizione 6.3. $\square$

Osservazione 6.11. Siano a, n interi tali che $n > 2$ e $\mathrm{MCD}(a,n) = 1$. In analogia con quanto esposto sopra, diremo che a è un *residuo quadratico* di n se la congruenza $X^2 \equiv a \pmod{n}$ è risolubile. Si verifica facilmente (utilizzando il Teorema di Euler - Fermat) che se a è un residuo quadratico di n, allora $a^{\frac{\varphi(n)}{2}} \equiv 1 \pmod{n}$. L'affermazione reciproca è però falsa, in generale. Infatti, se $n = 8$ e $a = 3$, si ha $\varphi(8) = 4$ e $3^2 \equiv 1 \pmod{8}$ mentre la congruenza $X^2 \equiv 3 \pmod{8}$ non è risolubile. (Questo fatto non è in disaccordo con il Corollario 5.24: infatti $n = 8$ è un intero che non ammette radici primitive!)

La maggior parte delle numerose differenti dimostrazioni della LRQ utilizza il seguente risultato, noto come "Lemma di Gauss".

Teorema 6.12. (Lemma di Gauss). *Sia p un primo dispari ed a un intero tale che* $\mathrm{MCD}(a,p) = 1$. *Consideriamo il sistema completo di residui minimo in valore assoluto (modulo p):*

$$\Sigma := \{-\frac{p-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{p-1}{2}\}$$

e l'insieme

$$S(a) := \{a, 2a, 3a, \ldots, \left(\frac{p-1}{2}\right) a\}.$$

Indicato con $\nu = \nu(a)$ il numero degli elementi di $S(a)$ congruenti (modulo p) agli interi negativi di Σ, si ha:

$$\left(\frac{a}{p}\right) = (-1)^{\nu(a)}.$$

Dimostrazione. Osserviamo dapprima che, se h e k sono interi tali che $1 \leqslant h < k \leqslant \frac{p-1}{2}$, allora $ha \not\equiv \pm ka \pmod{p}$. Infatti, se fosse $ha \equiv \pm ka \pmod{p}$, allora $h \equiv \pm k \pmod{p}$ e ciò è assurdo in base alle ipotesi fatte su h e k. Per ogni k tale che $1 \leqslant k \leqslant \frac{p-1}{2}$, esiste un unico $r_k \in \Sigma$ tale che $r_k \equiv ka \pmod{p}$ e, per quanto osservato sopra, l'insieme $\{r_1, \ldots, r_{\frac{p-1}{2}}\}$ è costituito da interi a due a due differenti in valore assoluto (cioè $|r_h| \neq |r_k|$ se $h \neq k$). Ne segue che gli insiemi $\{1, 2, \ldots, \frac{p-1}{2}\}$ e $\{|r_1|, \ldots, |r_{\frac{p-1}{2}}|\}$ coincidono e quindi, in base alla definizione di ν, si ha:

$$\prod_{i=1}^{\frac{p-1}{2}} r_i = (-1)^{\nu} \prod_{i=1}^{\frac{p-1}{2}} |r_i| = (-1)^{\nu} \left(\frac{p-1}{2}\right)!.$$

D'altra parte, essendo $r_k \equiv ka \pmod{p}$ $(1 \leqslant k \leqslant \frac{p-1}{2})$, si ha:

$$\left(\frac{p-1}{2}\right)! \, a^{\frac{p-1}{2}} \equiv \prod_{i=1}^{\frac{p-1}{2}} r_i = (-1)^{\nu} \left(\frac{p-1}{2}\right)! \pmod{p}$$

e pertanto, poichè $p \nmid \left(\frac{p-1}{2}\right)!$, applicando la Proposizione 6.6(c), si ha:

$$(-1)^{\nu} \equiv a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p},$$

da cui (essendo $p > 2$) segue la tesi. $\square$

Osservazione 6.13. Confrontando la Proposizione 6.6 (d) con il Teorema 6.12, si ha $(-1)^{\nu(a)} = (-1)^{\mathrm{ind}_r(a)}$ e dunque $\nu(a) \equiv \mathrm{ind}_r(a) \pmod{2}$. Non è detto però che $\nu(a) = \mathrm{ind}_r(a)$: ad esempio, ponendo $p = 7, r = 5$ e $a = 2$ si verifica che $\nu(2) = 2$ e $\mathrm{ind}_5(2) = 4$. (Infatti, in tal caso si ha che: $\Sigma = \{-3, -2, -1, 0, 1, 2, 3\}$, $S(2) = \{2, 4, 6\}$, $\nu(2) = 2$; inoltre, $5, 5^2 \equiv 4 \pmod{7}, 5^3 \equiv 6 \pmod{7}, 5^4 \equiv 2 \pmod{7}$ dunque $\mathrm{ind}_5(2) = 4$.)

Ci proponiamo, ora, di applicare il Lemma di Gauss per calcolare $(\frac{2}{p})$ e $(\frac{3}{p})$.

Corollario 6.14. *Sia p un primo dispari. Allora:*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{se, e soltanto se, } p \equiv 1 \text{ oppure } p \equiv 7 \pmod{8}, \\ -1 & \text{se, e soltanto se, } p \equiv 3 \text{ oppure } p \equiv 5 \pmod{8}. \end{cases}$$

Ne segue che:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Dimostrazione. Per calcolare $\nu(2)$ basta osservare che gli elementi del tipo $2k \in S(2)$ congruenti (modulo p) agli interi negativi di Σ verificano la diseguaglianza

$$\frac{p+1}{2} \leqslant 2k \leqslant p-1 \quad \text{e cioè} \quad \frac{p+1}{4} \leqslant k \leqslant \frac{p-1}{2}.$$

Dividendo p per 8, restano individuati $m, r \in \mathbb{N}$ tali che:

$$p = 8m + r, \quad \text{con } 0 \leqslant r \leqslant 7$$

e dunque, si ha:

$$2m + \frac{r+1}{4} \leqslant k \leqslant 4m + \frac{r-1}{2}.$$

Poichè p è dispari, r assume i valori $1, 3, 5, 7$.
Se quindi $r = 1$, risulta $2m + \frac{1}{2} \leqslant k \leqslant 4m$ e, dunque, $2m + 1 \leqslant k \leqslant 4m$. Ne segue che $\nu(2) = 4m - (2m+1) + 1 = 2m$.
Procedendo in modo analogo, si ha:
se $r = 3$, $2m + 1 \leqslant k \leqslant 4m + 1$ e quindi $\nu = 2m + 1$,
se $r = 5$, $2m + 2 \leqslant k \leqslant 4m + 2$ e quindi $\nu = 2m + 1$,
se $r = 7$, $2m + 2 \leqslant k \leqslant 4m + 3$ e quindi $\nu = 2m + 2$.
Pertanto $\nu(2)$ è pari se, e soltanto se, $r = 1, 7$ cioè $p \equiv 1, 7 \pmod 8$.

Relativamente all'ultima parte dell'enunciato, basta verificare che:
se $p \equiv 1, 7 \pmod 8$, allora $\frac{p^2-1}{8}$ è pari, mentre se $p \equiv 3, 5 \pmod 8$, allora $\frac{p^2-1}{8}$ è dispari. $\square$

Corollario 6.15. *Sia p un primo, $p \geqslant 5$. Allora:*

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \textit{se, e soltanto se, } p \equiv 1, 11 \pmod{12}, \\ -1 & \textit{se, e soltanto se, } p \equiv 5, 7 \pmod{12}. \end{cases}$$

Dimostrazione. Procedendo in modo analogo alla dimostrazione precedente, si vede che $\nu = \nu(3)$ coincide con il numero degli interi k tali che

$$\frac{p+1}{2} \leqslant 3k \leqslant p \quad \text{e cioè} \quad \frac{p+1}{6} \leqslant k \leqslant \frac{p}{3}.$$

Dividendo p per 12, per le restrizioni poste su p si ha che:

$$p = 12m + r \quad \text{con } r = 1, 5, 7, 11,$$

($r \neq 3, 9$ perché altrimenti p sarebbe divisibile per 3).
Pertanto, si ha:
se $r = 1$, $2m + 1 \leqslant k \leqslant 4m$ e, quindi, $\nu = 2m$,
se $r = 5$, $2m + 1 \leqslant k \leqslant 4m + 1$ e, quindi, $\nu = 2m + 1$,
se $r = 7$, $2m + 2 \leqslant k \leqslant 4m + 2$ e, quindi, $\nu = 2m + 1$,
se $r = 11$, $2m + 2 \leqslant k \leqslant 4m + 3$ e, quindi, $\nu = 2m + 2$.
Da ciò discende la tesi. $\square$

Osservazione 6.16. Riotterremo il risultato precedente come semplice applicazione della LRQ (cfr. il successivo Esempio 6.24). Questa dimostrazione risulterà quindi superflua, ma ci sembra, comunque, particolarmente istruttiva in vista della dimostrazione della LRQ.

Richiamiamo, ora, alcuni concetti e proprietà che saranno utili per dimostrare la LRQ.

Definizione 6.17. Sia α un numero reale. Si chiama *parte intera di* α (e si denota $[\alpha]$) il più grande intero $\leqslant \alpha$. Si chiama *parte residuale di* α il numero reale $\alpha_1 := \alpha - [\alpha]$ (ovviamente $0 \leqslant \alpha_1 < 1$ e $\alpha = [\alpha] + \alpha_1$).

Proposizione 6.18. *Siano α, β numeri reali tali che $\alpha \leqslant \beta$. Allora:*
(a) *il numero degli interi k tali che $\alpha \leqslant k \leqslant \beta$ è uguale a $[\beta]-[\alpha]$, se $\alpha \notin \mathbb{Z}$, oppure a $[\beta]-[\alpha]+1$ se $\alpha \in \mathbb{Z}$;*
(b) *per ogni intero n, $[n+\beta] = n + [\beta]$;*
(c) *siano n_1, n_2 interi tali che $n_1 \leqslant n_2$. Si ponga:*

$$\nu := \#\{k \in \mathbb{Z}; 2n_1 + \alpha \leqslant k \leqslant 2n_2 + \beta\} \quad e$$

$$\mu := \#\{h \in \mathbb{Z} : \alpha \leqslant h \leqslant \beta\}.$$

Allora:

$$\mu \equiv \nu \pmod 2.$$

Dimostrazione. **(a)**: gli interi cercati sono $[\alpha]+1, [\alpha]+2, \ldots, [\beta]$ e dunque sono esattamente $[\beta]-[\alpha]$ se $\alpha \notin \mathbb{Z}$; se $\alpha \in \mathbb{Z}$, agli interi sopra elencati si deve aggiungere $[\alpha] = \alpha \in \mathbb{Z}$. **(b)**: sia $\beta_1 := \beta - [\beta]$. Allora $n + \beta = (n + [\beta]) + \beta_1$ ed $n + [\beta]$ è un intero. Da ciò segue la tesi. **(c)**: da (a) e (b) segue che $\nu = [2n_2 + \beta] - [2n_1 + \alpha] = 2n_2 + [\beta] - 2n_1 - [\alpha] = 2(n_2 - n_1) + \mu$ se $\alpha \notin \mathbb{Z}$. Ad analoga conclusione si perviene se $\alpha \in \mathbb{Z}$. $\square$

Proposizione 6.19. *Siano p un primo dispari ed a un intero anch'esso dispari tale che* $\mathrm{MCD}(a,p) = 1$. *Allora*

$$\left(\frac{a}{p}\right) = (-1)^{\sigma_{a,p}} \quad con \quad \sigma_{a,p} := \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right]$$

Dimostrazione. Come nel Teorema 6.12, sia $S(a) := \{ka : 1 \leqslant k \leqslant \frac{p-1}{2}\}$. Dividendo gli elementi di $S(a)$ per p, si ottiene:

$$ka = q_k p + t_k \quad \text{con} \quad q_k, t_k \in \mathbb{N} \quad \text{e} \quad 1 \leqslant t_k \leqslant p-1.$$

Ne segue che $\frac{ka}{p} = q_k + \frac{t_k}{p}$ e quindi $\left[\frac{ka}{p}\right] = q_k$; pertanto si ha:

$$ka = \left[\frac{ka}{p}\right] \cdot p + t_k, \quad 1 \leqslant k \leqslant \frac{p-1}{2}.$$

Si denoti con $\{s_1, \ldots, s_\mu\}$ l'insieme $\{t_k : \text{con } 1 \leqslant t_k \leqslant \frac{p-1}{2}$, al variare di k e con $1 \leqslant k \leqslant \frac{p-1}{2}\}$ e con $\{r_1, \ldots, r_\nu\}$ l'insieme $\{t_k : \text{e con } \frac{p+1}{2} \leqslant t_k \leqslant p-1$, al variare di k e con $1 \leqslant k \leqslant \frac{p-1}{2}\}$. Si noti che ν è lo stesso intero, $\nu(a)$, considerato nel Lemma di Gauss (cfr. Teorema 6.12).
Vogliamo verificare che l'insieme $\{s_1, \ldots, s_\mu, p-r_1, \ldots, p-r_\nu\}$ coincide con l'insieme $\{1, 2, \ldots, \frac{p-1}{2}\}$. A tale scopo basta provare che $s_{i'} \not\equiv p - r_{j'} \pmod{p}$ (con $1 \leqslant i' \leqslant \mu$ e $1 \leqslant j' \leqslant \nu$). Se infatti $s_{i'} \equiv ia \pmod{p}$ e $r_{j'} \equiv ja \pmod{p}$; dove $1 \leqslant i \neq j \leqslant \frac{p-1}{2}$), allora $(i+j)a \equiv s_{i'} + r_{j'} \pmod{p}$; se, per assurdo, fosse $s_{i'} \equiv p - r_{j'} \pmod{p}$, allora $(i+j)a \equiv 0 \pmod{p}$ e dunque $i + j \equiv 0 \pmod{p}$, il che è ovviamente assurdo.
Si ha allora:

$$\sum_{k=1}^{\frac{p-1}{2}} k = \sum_{i=1}^{\mu} s_i + \sum_{j=1}^{\nu} (p - r_j) = p\nu + \sum_{i=1}^{\mu} s_i - \sum_{j=1}^{\nu} r_j$$

ed anche:

$$\sum_{k=1}^{\frac{p-1}{2}} ka = \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right] \cdot p + \sum_{i=1}^{\mu} s_i + \sum_{j=1}^{\nu} r_j$$

da cui, sottraendo la prima uguaglianza dalla seconda, si ottiene:

$$(a-1) \sum_{k=1}^{\frac{p-1}{2}} k = p(\sigma_{a,p} - \nu) + 2 \sum_{j=1}^{\nu} r_j.$$

Tenendo presente che $p \equiv a \equiv 1 \pmod{2}$, si ha $0 \equiv \sigma_{a,p} - \nu \pmod{2}$ e dunque, applicando il Teorema 6.12, si ha la tesi. □

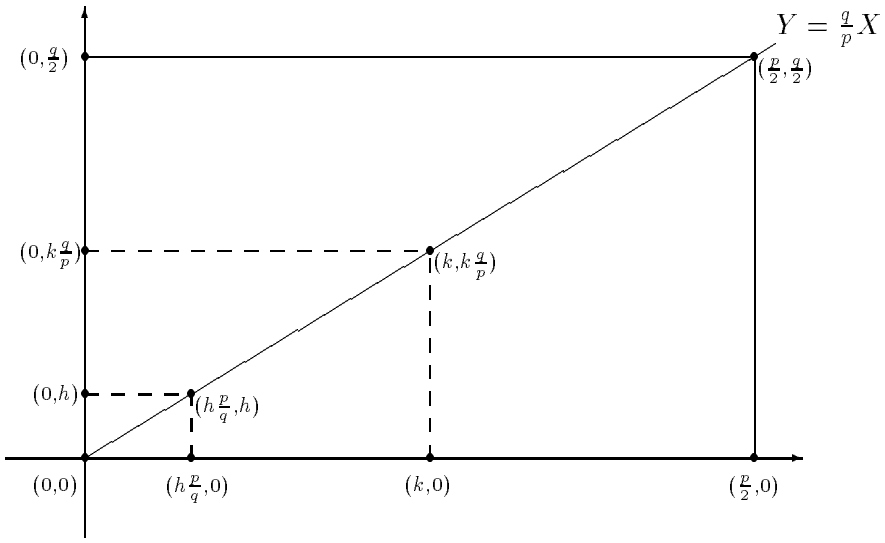
Veniamo finalmente alla LRQ. La dimostrazione che ne daremo è dovuta a F. G. Eisenstein (allievo di Gauss) ed è, in pratica, una semplificazione di una delle varie dimostrazioni che Gauss dette di tale legge.

Osservazione 6.20. Si noti che ormai la prima dimostrazione di Gauss, scritta "in a very repulsive form", come scrisse H. J. Smith, è stata rivisitata e riscritta in maniera estremamente chiara da E. Brown (cfr. Amer. Math. Montly, **88** (1981), 257-263). Altre semplici dimostrazioni sono state date da M. Gersternhaber (cfr. Amer. Math. Montly, **70** (1963), 397-398) e da J.S. Frame (cfr. Amer. Math. Montly, **85** (1978), 818-819).
Per un esame comparativo di varie dimostrazioni classiche della LRQ va infine segnalato un articolo di Frobenius del 1914 (cfr. Gesamm. Abh., **3** (1914), 628-647; Springer, 1968).

Teorema 6.21. (Legge di Reciprocità Quadratica). *Siano p, q due primi dispari distinti. Allora:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Dimostrazione. Nel piano cartesiano consideriamo il rettangolo di vertici $(0,0), (\frac{p}{2},0), (0,\frac{q}{2}), (\frac{p}{2},\frac{q}{2})$.



e denotiamo con R l'interno di tale rettangolo. L'idea della dimostrazione consiste nel contare, in due modi distinti, i punti a coordinate intere giacenti in R.

Sia (n,m) un punto del piano a coordinate intere: è chiaro che $(n,m) \in R$ se, e soltanto se, risulta

$$1 \leqslant n \leqslant \frac{p-1}{2} \quad \text{e} \quad 1 \leqslant m \leqslant \frac{q-1}{2}$$

essendo $\frac{p-1}{2} = \left[\frac{p}{2}\right]$ e $\frac{q-1}{2} = \left[\frac{q}{2}\right]$. Pertanto i punti cercati sono in numero di $\left(\frac{p-1}{2}\right) \cdot \left(\frac{q-1}{2}\right)$.

Procediamo, ora, al calcolo degli stessi punti seguendo un altro metodo. La diagonale del rettangolo (condotta dal vertice $(0,0)$) ha equazione:

$$Y = \frac{q}{p}X$$

e si verifica subito che nessun punto di R a coordinate intere (n,m) giace su tale diagonale. In caso contrario, risulterebbe $m = \frac{q}{p}n$, dunque $pm = qn$ e pertanto $p \mid n$ e $q \mid m$. Ciò è in contrasto con le limitazioni $1 \leqslant n \leqslant \frac{p-1}{2}$ e $1 \leqslant m \leqslant \frac{q-1}{2}$.
Se denotiamo allora con T_1 (rispettivamente T_2) il sottoinsieme triangolare di R giacente al di sotto (rispettivamente al di sopra) della diagonale, è evidente che i punti cercati sono quelli giacenti in T_1 più quelli giacenti in

T_2. Ora, se k è un intero tale che $1 \leqslant k \leqslant \frac{p-1}{2}$, il numero degli interi y tali che $0 < y < \frac{qk}{p}$ è dato da $[qk/p]$ e pertanto i punti di T_1 a coordinate intere e con ascissa k sono esattamente $[qk/p]$. Ne segue che i punti a coordinate intere in T_1 sono:

$$\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{qk}{p}\right].$$

Analogamente, i punti a coordinate intere in T_2 sono:

$$\sum_{h=1}^{\frac{q-1}{2}} \left[\frac{ph}{q}\right].$$

In definitiva, abbiamo:

$$\left(\frac{p-1}{2}\right)\cdot\left(\frac{q-1}{2}\right) = \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{qk}{p}\right] + \sum_{h=1}^{\frac{q-1}{2}} \left[\frac{ph}{q}\right].$$

Applicando due volte la Proposizione 6.19, abbiamo:

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = (-1)^{\sum_{h=1}^{\frac{q-1}{2}}\left[\frac{ph}{q}\right]}\cdot(-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{qk}{p}\right]} = (-1)^{(\frac{p-1}{2})\cdot(\frac{q-1}{2})}. \quad \square$$

Corollario 6.22. *Siano p, q due primi dispari distinti. Allora:*

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{se} \quad p \equiv 1 \pmod 4 \quad \text{o/e} \quad q \equiv 1 \pmod 4, \\ -1 & \text{se} \quad p \equiv q \equiv 3 \pmod 4. \end{cases}$$

Dimostrazione. Basta osservare che $(\frac{p-1}{2})\cdot(\frac{q-1}{2})$ è pari se, e soltanto se, almeno uno dei due primi p, q è congruente a 1 (mod 4). $\square$

Corollario 6.23. *Siano p, q due primi dispari distinti. Allora:*

$$\left(\frac{p}{q}\right) = \begin{cases} (\frac{q}{p}) & \text{se} \quad p \equiv 1 \pmod 4 \quad \text{o/e} \quad q \equiv 1 \pmod 4, \\ -(\frac{q}{p}) & \text{se} \quad p \equiv q \equiv 3 \pmod 4. \end{cases}$$

Dimostrazione. Basta moltiplicare per $(\frac{q}{p})$ ambo i membri dell'uguaglianza del Corollario 6.22, tenendo conto del fatto che $(\frac{q}{p})^2 = 1$ $\square$

Algoritmo per il calcolo del simbolo di Legendre. A questo punto è opportuno chiarire come i risultati precedenti possono essere utilizzati per calcolare $(\frac{a}{p})$, dove p è un primo dispari ed a un intero tale che $\mathrm{MCD}(a, p) = 1$. Se $a = \pm 2^{e_0} p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}$ (con $p_1, \ldots, p_r$ primi dispari distinti), dal Corollario 6.9 segue che:

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right)\left(\frac{2}{p}\right)^{e_0}\left(\frac{p_1}{p}\right)^{e_1}\left(\frac{p_2}{p}\right)^{e_2}\cdot\ldots\cdot\left(\frac{p_r}{p}\right)^{e_r}.$$

La LRQ permette di ricondurre il calcolo di ogni $(\frac{p_i}{p})$ al calcolo di $(\frac{p}{p_i})$ (nel caso in cui $p_i < p$), rinviando quindi al calcolo del simbolo di Legendre con "denominatore" più piccolo di quello di partenza. Dividendo p per p_i si ha:

$$p = h_i p_i + r_i, \text{ con } h_i, r_i \in \mathbb{N} \quad \text{e} \quad 1 \leqslant r_i \leqslant p_i,$$

dunque $p \equiv r_i \pmod{p_i}$ e pertanto $(\frac{p}{p_i}) = (\frac{r_i}{p_i})$. A questo punto si fattorizza r_i nel prodotto di primi e si itera il procedimento sopra esposto. In questo modo, per il calcolo di un qualsiasi simbolo di Legendre $(\frac{p_i}{p})$, ci si riduce, in ultima analisi, al calcolo di simboli di Legendre del tipo:

$$\left(\frac{1}{q}\right), \quad \left(\frac{-1}{q}\right), \quad \left(\frac{2}{q}\right) \ ,$$

dove q è un qualunque primo dispari; i valori di tali simboli di Legendre sono stati già calcolati.

Esemplifichiamo le considerazioni ora svolte.

Esempio 6.24. Calcolo di $(\frac{3}{p})$ con p primo dispari, $p > 3$.
Si ha, ponendo $r \equiv p \pmod{3}, 1 \leqslant r \leqslant 2$:

$$\begin{aligned}
\left(\frac{3}{p}\right) &= \begin{cases} (\frac{p}{3}) = (\frac{r}{3}) & \text{se } p \equiv 1 \pmod 4, \\ -(\frac{p}{3}) = -(\frac{r}{3}) & \text{se } p \equiv 3 \pmod 4, \end{cases} \\
&= \begin{cases} (\frac{1}{3}) = 1 & \text{se } p \equiv 1 \pmod 4 \text{ e } p \equiv 1 \pmod 3, \\ -(\frac{1}{3}) = -1 & \text{se } p \equiv 3 \pmod 4 \text{ e } p \equiv 1 \pmod 3, \\ (\frac{2}{3}) = -1 & \text{se } p \equiv 1 \pmod 4 \text{ e } p \equiv 2 \pmod 3, \\ -(\frac{2}{3}) = 1 & \text{se } p \equiv 3 \pmod 4 \text{ e } p \equiv 2 \pmod 3, \end{cases} \\
&= \begin{cases} 1 & \text{se } p \equiv 1, 11 \pmod{12}, \\ -1 & \text{se } p \equiv 5, 7 \pmod{12}. \end{cases}
\end{aligned}$$

Esempio 6.25. Calcolo di $(\frac{4}{p})$ con p primo dispari.
Risulta, ovviamente:

$$\left(\frac{4}{p}\right) = \left(\frac{2}{p}\right)^2 = 1.$$

Esempio 6.26. Calcolo di $(\frac{5}{p})$ con p dispari, $p \neq 5$.
Se $p = 3$, $(\frac{5}{3}) = (\frac{2}{3}) = -1$. Sia $p > 5$: in tal caso $(\frac{5}{p}) = (\frac{p}{5})$ e risulta:

$$p = 5k + r \text{ con } k, r, \in \mathbb{N} \quad \text{e} \quad 1 \leqslant r \leqslant 4.$$

Pertanto:

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{r}{5}\right) = \begin{cases} (\frac{1}{5}) = 1 & \text{se } p \equiv 1 \pmod 5, \\ (\frac{2}{5}) = -1 & \text{se } p \equiv 2 \pmod 5, \\ (\frac{3}{5}) = (\frac{5}{3}) = (\frac{2}{3}) = -1 & \text{se } p \equiv 3 \pmod 5, \\ (\frac{4}{5}) = (\frac{2}{5})^2 = 1 & \text{se } p \equiv 4 \pmod 5, \end{cases}$$

$$= \begin{cases} 1 & \text{se } p \equiv 1, 4 \pmod 5, \\ -1 & \text{se } p \equiv 2, 3 \pmod 5. \end{cases}$$

Esempio 6.27. Calcolo di $(\frac{6}{p})$ con $p \geqslant 5$, p primo.
Poiché $(\frac{6}{p}) = (\frac{2}{p}) \cdot (\frac{3}{p})$, allora, $(\frac{6}{p}) = -1$ se, e soltanto se, uno soltanto tra i simboli $(\frac{2}{p})$ e $(\frac{3}{p})$ vale -1. A partire dai valori già noti di $(\frac{2}{p})$ e $(\frac{3}{p})$ si ottiene facilmente che:

$$\left(\frac{6}{p}\right) = \begin{cases} 1 & \text{se } p \equiv 1, 5, 19, 23 \pmod{24}, \\ -1 & \text{se } p \equiv 7, 11, 13, 17 \pmod{24}. \end{cases}$$

Esempio 6.28. Calcolo di $(\frac{7}{p})$ con p primo dispari, $p \neq 7$.
Se $p = 3$, $(\frac{7}{3}) = (\frac{1}{3}) = 1$; se $p = 5$, $(\frac{7}{5}) = (\frac{2}{5}) = -1$. Sia ora $p > 7$; in tal caso si ha:

$$\left(\frac{7}{p}\right) = \begin{cases} (\frac{p}{7}) & \text{se } p \equiv 1 \pmod 4, \\ -(\frac{p}{7}) & \text{se } p \equiv 3 \pmod 4. \end{cases}$$

Ora, $p = 7k + r$ con $k, r \in \mathbb{N}$ e $1 \leqslant r \leqslant 6$; conseguentemente:

$$\left(\frac{p}{7}\right) = \begin{cases} (\frac{1}{7}) = 1 & \text{se } p \equiv 1 \pmod 7, \\ (\frac{2}{7}) = 1 & \text{se } p \equiv 2 \pmod 7, \\ (\frac{3}{7}) = -1 & \text{se } p \equiv 3 \pmod 7, \\ (\frac{4}{7}) = 1 & \text{se } p \equiv 4 \pmod 7, \\ (\frac{5}{7}) = -1 & \text{se } p \equiv 5 \pmod 7, \\ (\frac{6}{7}) = -1 & \text{se } p \equiv 6 \pmod 7. \end{cases}$$

Ne segue che:

$$\left(\frac{7}{p}\right) = \begin{cases} 1 & \text{se } p \equiv 1, 3, 9, 19, 25, 27 \pmod{28}, \\ -1 & \text{se } p \equiv 5, 11, 13, 15, 17, 23 \pmod{28}. \end{cases}$$

Concludiamo questo paragrafo studiando la risolubilità di congruenze quadratiche di tipo:

$$X^2 \equiv a \pmod n \tag{4}$$

dove n è un intero arbitrario $\geqslant 2$ ed a un intero tale che $\mathrm{MCD}(a,n)=1$. Tenuto conto delle considerazioni svolte all'inizio del Paragrafo 4 e supposto che n ammetta la seguente fattorizzazione in numeri primi distinti:

$$n = 2^{e_0} p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_r^{e_r},$$

la risolubilità di (4) equivale alla risolubilità del sistema:

$$\begin{cases} X^2 \equiv a \pmod{2^{e_0}}, \\ X^2 \equiv a \pmod{p_i^{e_i}}, \\ 1 \leqslant i \leqslant r \end{cases}$$

Ci occuperemo quindi separatamente dei seguenti problemi:

I Problema: studio della risolubilità di congruenze del tipo:

$$X^2 \equiv a \pmod{p^e}$$

con p primo dispari, $e \geqslant 1$ ed a intero tale che $\mathrm{MCD}(a,p)=1$.

II Problema: studio della risolubilità di congruenze del tipo:

$$X^2 \equiv a \pmod{2^e}$$

con $e \geqslant 1$ ed a intero dispari.

Veniamo al I Problema:

Teorema 6.29. *Sia p primo dispari ed a un intero tale che* $\mathrm{MCD}(a,p)=1$. *Allora la congruenza:*

$$X^2 \equiv a \pmod{p^e} \text{ con } e \geqslant 1 \tag{5}$$

è risolubile se, e soltanto se, $\left(\frac{a}{p}\right)=1$.

Dimostrazione. Se la congruenza (5) è risolubile, ogni sua soluzione risolve anche la congruenza $X^2 \equiv a \pmod{p}$: dunque $\left(\frac{a}{p}\right)=1$.

Viceversa, assumiamo che $\left(\frac{a}{p}\right)=1$ e procediamo per induzione su e. Il caso $e=1$ è assunto per ipotesi. Sia $e \geqslant 2$ e supponiamo che la congruenza $X^2 \equiv a \pmod{p^{e-1}}$ sia risolubile. Se y ne è una soluzione, esiste $b \in \mathbb{Z}$ tale che $y^2 = a + bp^{e-1}$. Poiché $\mathrm{MCD}(p,2y)=1$, la seguente congruenza lineare nell'indeterminata T:

$$2yT \equiv -b \pmod{p} \tag{$\bullet_y$}$$

ammette un'unica soluzione t. (Osserviamo che, a meno di un ovvio adattamento di notazione relativo all'esponente, tale congruenza lineare coincide

con quella considerata nella dimostrazione del Teorema 4.6; cfr. anche la successiva Osservazione 6.30.) Poniamo allora

$$x := x_t := y + tp^{e-1} .$$

Già sappiamo che x è soluzione di (5) (cf. dimostrazione del Teorema 4.6). Infatti, ripetendo il ragionamento già fatto (Teorema 4.6) si ha:

$$x^2 = a + bp^{e-1} + 2ytp^{e-1} + t^2p^{2e-2} \equiv a + bp^{e-1} - bp^{e-1} \pmod{p^e}$$

in quanto $2ytp^{e-1} \equiv -bp^{e-1} \pmod{p^e}$ e $2e - 2 \geqslant e$, per $e \geqslant 2$. □

Osservazione 6.30. Si noti che il Teorema 4.7 permette di ottenere la seconda implicazione del teorema precedente. Sia infatti $f(X) := X^2 - a$ e y una soluzione di $f(X) \equiv 0 \pmod{p^{e-1}}$, quindi se $y^2 = a + bp^{e-1}$ allora $f(y)/p^{e-1} = b$. Poichè p è dispari, si dimostra per induzione su $e \geqslant 2$ che $f'(y) = 2y \not\equiv 0 \pmod{p}$ dunque si è nella situazione descritta nel I Caso del Teorema 4.7 (cioè che y è una soluzione non singolare; cfr. anche Esercizio 4.1). Ne segue che (5) è risolubile.
Si noti che questo ragionamento non si può ripetere nel caso del successivo Teorema 6.32(3), per il quale sarà necessario sviluppare una dimostrazione "ad hoc".

Corollario 6.31. *Con le notazioni del Teorema 6.29, se la congruenza* (5) *è risolubile, essa ammette esattamente due soluzioni distinte (cioè non congruenti* $\pmod{p^e}$*).*

Dimostrazione. Alla conclusione si può pervenire (ragionando come nella Osservazione 6.30), applicando il Teorema 4.7. Diamo, comunque, una dimostrazione esplicita (ispirata a quella del Teorema 4.7), che poi tornerà utile per dimostrare il successivo Corollario 6.34.
Se x_0 è una soluzione di (5), è chiaro che x_0 e $x_1 := p - x_0$ sono due soluzioni distinte di (5). Proviamo, per induzione su e, che (5) ammette soltanto due soluzioni distinte. Se $e = 1$, l'asserto è vero (cfr. Proposizione 6.1). Supponiamo che $e \geqslant 2$ e che la congruenza:

$$X^2 \equiv a \pmod{p^{e-1}} \tag{6}$$

ammetta soltanto due soluzioni y_0, y_1. Dalla dimostrazione del Teorema 6.29 segue che y_i $(0 \leqslant i \leqslant 1)$ determina la soluzione $x_i := y_i + t_ip^{e-1}$ di (5), dove $y_i^2 = a + b_ip^{e-1}$ per un qualche $b_i \in \mathbb{Z}$ e t_i è la soluzione della congruenza lineare $2y_iT \equiv -b_i \pmod{p}$.

Per concludere basta verificare che se x è una soluzione della congruenza (5), allora $x \equiv x_0 \pmod{p^e}$ oppure $x \equiv x_1 \pmod{p^e}$. Poiché x è una soluzione di (6), allora $x \equiv y_i \pmod{p^{e-1}}$, con $i = 0$ oppure $i = 1$. Posto

$x = y_i + \tau p^{e-1}$ per un qualche $\tau \in \mathbb{Z}$, dalla congruenza $x^2 \equiv a \equiv (x_i)^2 \pmod{p^e}$ discende che:

$$y_i^2 + 2y_i\tau p^{e-1} + \tau^2 p^{2e-2} \equiv y_i^2 + 2y_i t_i p^{e-1} + t_i^2 p^{2e-2} \pmod{p^e}.$$

Da ciò di ricava facilmente che $\tau \equiv t_i \pmod{p}$ e quindi si conclude che $x \equiv x_i \pmod{p^e}$. $\square$

Veniamo ora al II Problema:

Teorema 6.32. *Sia a un intero dispari. Allora:*

(1) *La congruenza $X^2 \equiv a \pmod 2$ è sempre risolubile;*

(2) *La congruenza $X^2 \equiv a \pmod 4$ è risolubile se, e soltanto se, $a \equiv 1 \pmod 4$;*

(3) *La congruenza $X^2 \equiv a \pmod{2^e}$, $e \geqslant 3$ è risolubile se, e soltanto se, $a \equiv 1 \pmod 8$.*

Dimostrazione. (1). È del tutto ovvio. **(2).** Sia $x_0 \in \mathbb{Z}$ una soluzione della congruenza $X^2 \equiv a \pmod 4$. Essendo a dispari, anche x_0 è dispari e poiché il quadrato di ogni intero dispari è congruente ad 1 (mod 4), si ha $a \equiv x_0^2 \equiv 1 \pmod 4$. Viceversa, se $a \equiv 1 \pmod 4$, allora 1 e 3 sono soluzioni della congruenza in questione. **(3).** È facile verificare che il quadrato di ogni intero dispari è congruente ad 1 (mod 8) (cfr. Esercizio 1.3 (b)). Se, quindi, la congruenza $X^2 \equiv a \pmod{2^e}$ ($e \geqslant 3$) è risolubile, anche la congruenza $X^2 \equiv a \pmod 8$ è risolubile e pertanto, procedendo come sopra, si ottiene che $a \equiv 1 \pmod 8$. Viceversa, assumiamo che $a \equiv 1 \pmod 8$ e procediamo per induzione su e. Se $e = 3$, la congruenza $X^2 \equiv a \pmod 8$ è certamente risolubile (ed ha quattro soluzioni 1, 3, 5, 7 (mod 8)). Supponiamo ora che $e \geqslant 4$ e che $X^2 \equiv a \pmod{2^{e-1}}$ sia risolubile. Se y ne è una soluzione, si ha $y^2 = a + b2^{e-1}$, per un qualche $b \in \mathbb{Z}$. Poichè a è dispari, anche y è dispari e, pertanto, la seguente congruenza lineare nell'indeterminata T:

$$yT \equiv -b \pmod 2$$

ammette un'unica soluzione $t \pmod 2$. Si pone allora:

$$x := x_t := y + t2^{e-2}$$

e si verifica, facilmente, che x è una soluzione della congruenza $X^2 \equiv a \pmod{2^e}$. Infatti, si ha $yt2^{e-1} \equiv -b \cdot 2^{e-1} \pmod{2^e}$, $2e - 4 \geqslant e$ e dunque $x^2 = a + b2^{e-1} + yt2^{e-1} + t^2 2^{2e-4} \equiv a \pmod{2^e}$. $\square$

Osservazione 6.33. Si noti che nella dimostrazione del punto (3) del Teorema 6.32 si ha che se b è pari allora risulta $t \equiv 0 \pmod 2$; se b è dispari, $t \equiv 1 \pmod 2$. Ne primo caso $x = y$ e nel secondo $x = y + 2^{e-2}$.

Corollario 6.34. *Sia a un intero dispari. Allora:*

(1) *La congruenza $X^2 \equiv a \pmod 2$ ha un'unica soluzione;*

(2) *Se la congruenza $X^2 \equiv a \pmod 4$ è risolubile, allora ha esattamente due soluzioni distinte (cioè incongruenti (modulo 4));*

(3) *Se la congruenza $X^2 \equiv a \pmod{2^e}$, $e \geqslant 3$ è risolubile, allora ha esattamente quattro soluzioni distinte (cioè incongruenti (modulo 2^e)).*

Dimostrazione. **(1)** e **(2)** sono del tutto evidenti. Dimostriamo **(3)** seguendo la linea dimostrativa del Corollario 6.31.

Innanzitutto, se x_0 è una soluzione di

$$X^2 \equiv a \pmod{2^e} \quad e \geqslant 3, \tag{7}$$

si verifica subito che:

$$x_0, \quad -x_0, \quad x_0 + 2^{e-1}, \quad -x_0 + 2^{e-1}$$

sono quattro soluzioni distinte di (7). Proviamo, per induzione su e, che (7) ammette soltanto quattro soluzioni distinte. Se $e = 3$, allora possiamo porre $a = 1$ (in quanto, $a \equiv 1 \pmod 8$, cfr. Teorema 6.32 (3)), ed è evidente che $X^2 \equiv 1 \pmod 8$ ha soltanto quattro soluzioni distinte (cioè: $1, 3, 5, 7 \pmod 8$). Sia $e \geqslant 4$ e supponiamo che l'asserto sia vero per l'esponente $e - 1$. Denotiamo con y_0, y_1, y_2, y_3 le quattro soluzioni distinte di

$$X^2 \equiv a \pmod{2^{e-1}} \tag{8}$$

Procedendo come nel Teorema 6.32, y_i $(0 \leqslant i \leqslant 3)$ determina la soluzione di (7):

$$x_i := y_i + t_i 2^{e-2},$$

dove si è posto $y_i^2 = a + b_i 2^{e-1}$ $(b_i \in \mathbb{Z})$ e t_i soluzione della congruenza $y_i T \equiv -b_i \pmod 2$. A partire da una qualsiasi scelta di i, con $0 \leqslant i \leqslant 3$, gli interi $x_i, -x_i, x_i + 2^{e-1}, -x_i + 2^{e-1}$ sono quattro soluzioni distinte di (7) (cfr. anche Osservazione 6.33). Per concludere basta verificare che se x è una soluzione di (7), allora x è congruente (modulo 2^e) ad una di tali soluzioni. Poiché x è anche soluzione di (8), esiste un unico intero i $(0 \leqslant i \leqslant 3)$ tale che $x \equiv y_i \pmod{2^{e-1}}$. Inoltre non è restrittivo assumere che $1 \leqslant x < 2^e$ e $1 \leqslant y_i < 2^{e-1}$ e quindi risulta necessariamente $x = y_i$ oppure $x = y_i + 2^{e-1}$. Nel primo caso, $y_i^2 \equiv a \pmod{2^e}$, quindi si vede facilmente che $x_i = y_i$ e, pertanto, $x \equiv x_i \pmod{2^e}$. Nel secondo caso si hanno due alternative:

(a) se $x_i = y_i$, allora $x \equiv x_i + 2^{e-1} \pmod{2^e}$;

(b) se $x_i = y_i + 2^{e-2}$, allora dal fatto che $x^2 \equiv (x_i)^2 \pmod{2^e}$ si ricava facilmente che $y_i \equiv 0 \pmod 2$ e ciò è assurdo in quanto a (e, quindi, y_i) è dispari. $\square$

Osservazione 6.35. Vogliamo commentare la dimostrazione del teorema precedente, anche alla luce del Teorema 4.7.
Innanzitutto, osserviamo che, con le notazioni sopra introdotte, per ogni j fissato, con $0 \leqslant j \leqslant 3$, risulta:

$$\{x_j, -x_j, x_j+2^{e-1}, -x_j+2^{e-1}\} = \{x_i, -x_i, x_i+2^{e-1}, -x_i+2^{e-1} : 0 \leqslant i \leqslant 3\}.$$

Inoltre, notiamo che $\{x_0, x_1, x_2, x_3\}$ è un sottoinsieme dell'insieme sopra considerato $\{x_j, -x_j, x_j + 2^{e-1}, -x_j + 2^{e-1}\}$ di tutte le soluzioni distinte di $X^2 \equiv a \pmod{2^e}$ ed, in generale, non coincide con quest'ultimo.
Per esemplificare quanto osservato sopra, descriviamo più dettagliatamente, il passaggio dalla congruenza $X^2 \equiv a \pmod 8$ alla congruenza $X^2 \equiv a \pmod{16}$.
Nel caso risolubile, cioè $a \equiv 1 \pmod 8$, denotiamo con $\{y_0 = 1, y_1 = 3, y_2 = 5, y_3 = 7\}$ le soluzioni della congruenza $X^2 \equiv 1 \pmod 8$. Quindi se $a \equiv 1 \pmod 8$ abbiamo due congruenze risolubili $\pmod{16}$.

Caso 1: $X^2 \equiv 1 \pmod{16}$.
Conserviamo le notazioni della dimostrazione del Corollario 6.34. Allora, $b_0 = 0, b_1 = 1, b_2 = 3, b_3 = 6$, quindi $t_0 = 0, t_1 = 1, t_2 = 1, t_3 = 0$, pertanto $x_0 = 1, x_1 = 7, x_2 = 9, x_3 = 7$. Mentre l'insieme delle soluzioni distinte $X^2 \equiv 1 \pmod{16}$ è dato da:

$$\{1, -1, 9, -9\} = \{1, 15, 9, 7\} = \{x_j, -x_j, x_j + 8, -x_j + 8\}$$

per ogni scelta di j, con $0 \leqslant j \leqslant 3$. Inoltre, esaminando il problema con l'ottica del Teorema 4.7, abbiamo che $y_0 = 1$ e $y_3 = 7$ sono anche soluzioni della congruenza $\pmod{2^4}$ e quindi ciascuna di queste determina due soluzioni $\pmod{2^4}$ date da:

$$y_0 = 1, y_0 + 2^3 = 8, y_1 = 7, y_1 + 2^3 = 15$$

(II Caso del Teorema 4.7). Mentre $y_1 = 3$ e $y_2 = 5$ non sono soluzioni della congruenza $\pmod{2^4}$ e, quindi, non determinano alcuna soluzione della congruenza $\pmod{2^4}$ (III Caso del Teorema 4.7).

Caso 2: $X^2 \equiv 9 \pmod{16}$.
In questo caso, $b_0 = 1, b_1 = 0, b_2 = 2, b_3 = 5$, quindi $t_0 = 1, t_1 = 0, t_2 = 0, t_3 = 1$, pertanto $x_0 = 5, x_1 = 3, x_2 = 5, x_3 = 11$. Mentre l'insieme delle soluzioni distinte $X^2 \equiv 9 \pmod{16}$ è dato da:

$$\{3, -3, 11, -11\} = \{3, 13, 11, 5\} = \{x_j, -x_j, x_j + 8, -x_j + 8\}$$

per ogni scelta di j, con $0 \leqslant j \leqslant 3$. Inoltre le soluzioni $y_1 = 3$ e $y_2 = 5$ della congruenza $X^2 \equiv 1 \pmod 8$ determinano ciscuna due soluzioni della congruenza $X^2 \equiv 9 \pmod{16}$ e cioè

$$y_1 = 3, y_1 + 2^3 = 11, y_2 = 5, y_2 + 2^3 = 13.$$

Mentre le soluzioni y_0 e y_3 non determinano soluzioni della congruenza $X^2 \equiv 9 \pmod{16}$.

Possiamo riassumere nel seguente teorema i risultati sopra ottenuti.

Teorema 6.36. *Sia n un intero $\geqslant 2$ che ammette la seguente fattorizzazione in primi distinti:*

$$n = 2^{e_0} p_1^{e_1} p_2^{e_2} \cdot \ldots \cdot p_r^{e_r}.$$

Sia a un intero tale che $\mathrm{MCD}(a, n) = 1$. *Allora, la congruenza*

$$X^2 \equiv a \pmod{n} \tag{4}$$

è risolubile se, e soltanto se, le seguenti due condizioni sono soddisfatte:
(1) $(\frac{a}{p_1}) = \cdots = (\frac{a}{p_r}) = 1$;

(2) $\begin{cases} a \text{ dispari}, & \text{se } e_0 = 1; \\ a \equiv 1 \pmod 4, & \text{se } e_0 = 2 \text{ (cioè se } 4 \mid n \text{ e } 8 \nmid n); \\ a \equiv 1 \pmod 8, & \text{se } e_0 \geqslant 3 \text{ (cioè se } 8 \mid n). \end{cases}$

Dimostrazione. È una semplice congruenza dei Teoremi 4.1, 6.29, 6.32. □

Corollario 6.37. *Con le notazioni del Teorema 6.36, se la congruenza* (4) *è risolubile, il numero delle sue soluzioni distinte (cioè, incongruenti* (mod n)*) è dato da:*

$$\begin{cases} 2^r & \text{se } e_0 \leqslant 1, \\ 2^{r+1} & \text{se } e_0 = 2, \\ 2^{r+2} & \text{se } e_0 \geqslant 3. \end{cases}$$

Dimostrazione. È una semplice conseguenza dell'Osservazione 4.2 e dei Corollari 6.31 e 6.34. □

Osservazione 6.38. Come applicazione del Teorema 6.36, vogliamo studiare la risolubilità dell'equazione diofantea in due indeterminate X e Y:

$$aX^2 + bY + c = 0 \quad \text{con } a, b, c \in \mathbb{Z} \tag{9}$$

Se $a = 0$ (e $b \neq 0$), (9) è risolubile se, e soltanto se, $b \mid c$; se $b = 0$ (e $a \neq 0$), (9) è risolubile se, e soltanto se, $\frac{-c}{a}$ è il quadrato di un numero intero. Supponiamo, ora, che $a \neq 0$ e $b \neq 0$. In tal caso (9) è risolubile se, e soltanto se,

$$aX^2 \equiv -c \pmod{b} \tag{10}$$

è risolubile.
Supponiamo allora che la congruenza quadratica (10) sia risolubile e poniamo $d :=\mathrm{MCD}(a, b)$. Allora risulta che $d \mid c$ e perciò, indicati con $\bar{a}, \bar{b}, \bar{c}$ gli interi tali che

$$a = \bar{a}d, \qquad b = \bar{b}d, \qquad c = \bar{c}d,$$

è immediato che la risolubilità di (9) equivale alla risolubilità di:

$$\bar{a}X^2 + \bar{b}Y + \bar{c} = 0 \quad \text{con MCD}(\bar{a}, \bar{b}) = 1. \tag{11}$$

In tal caso, la risolubilità di (11) equivale alla risolubilità della congruenza: $\bar{a}X^2 \equiv -\bar{c} \pmod{\bar{b}}$. Denotiamo, allora, con $\bar{a}^*$ un inverso aritmetico di $\bar{a}$ $(\text{mod } \bar{b})$ e posto $-\bar{c} \cdot \bar{a}^* =: e$, questa ultima congruenza è equivalente alla congruenza:

$$X^2 \equiv e \pmod{\bar{b}} \tag{12}$$

e per stabilire se (12) è risolubile basta applicare il Teorema 6.36.

In particolare, l'equazione diofantea:

$$X^2 \pm pY - c = 0,$$

con p primo dispari e $c \in \mathbb{Z}$, è risolubile se, e soltanto se, $(\frac{c}{p}) = 1$. Ad esempio, quindi, l'equazione diofantea $X^2 \pm 3Y + 1 = 0$ non è risolubile; mentre $X^2 \pm pY - 5 = 0$ è risolubile per un primo p dispari se e soltanto se, $p \equiv 1, 4 \pmod 5$.

"Geometricamente" questo fatto si traduce nell'esistenza di parabole del piano che non contengono alcun punto a coordinate intere (ad esempio $X^2 \pm 3Y - 5 = 0$) oppure che ne contengono infiniti (ad esempio $X^2 \pm 11Y - 5 = 0$).

Il matematico tedesco C.G. Jacobi (1804 - 1851) ha introdotto un simbolo (noto come simbolo di Jacobi) che generalizza il simbolo di Legendre e ne estende alcune proprietà.

Definizione 6.39. Siano a, n interi tali che $n > 1$ e $\text{MCD}(a, n) = 1$. Posto $n = p_1 p_2 \cdot \ldots \cdot p_r$, con $p_1, p_2, \ldots, p_r$ primi non necessariamente a due a due distinti, si chiama *simbolo di Jacobi* il simbolo così definito:

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right) \cdot \ldots \cdot \left(\frac{a}{p_r}\right)$$

dove $(\frac{a}{p_i})$ per $1 \leqslant i \leqslant r$ è l'usuale simbolo di Legendre.

Proposizione 6.40. *Siano n, m interi dispari tali che $n > 1, m > 1$; siano inoltre a, b interi relativamente primi con n e con m. Risulta:*

(a) $a \equiv b \pmod n \Rightarrow (\frac{a}{n}) = (\frac{b}{n})$;

(b) $(\frac{ab}{n}) = (\frac{a}{n}) \cdot (\frac{b}{n})$;

(c) $(\frac{a}{nm}) = (\frac{a}{n}) \cdot (\frac{a}{m})$;

(d) $(\frac{a}{n^2}) = (\frac{a^2}{n}) = 1$;

(e) $(\frac{1}{n}) = 1$;

(f) $(\frac{-1}{n}) = (-1)^{\frac{n-1}{2}}$;

(g) $(\frac{2}{n}) = (-1)^{\frac{n^2-1}{8}}$. *In particolare,* $(\frac{2}{n}) = 1$ *se, e soltanto se* $n \equiv \pm 1 \pmod 8$.

(h) (Legge di Reciprocità Quadratica; forma generalizzata). *Siano* n, m *interi dispari tali che* $n > 1, m > 1$ *e* $\mathrm{MCD}(n, m) = 1$. *Allora:*

$$\left(\frac{m}{n}\right) \cdot \left(\frac{n}{m}\right) = (-1)^{\frac{n-1}{2} \cdot \frac{m-1}{2}}.$$

Dimostrazione. Per verificare **(a), ... , (e)** basta utilizzare la definizione del simbolo di Jacobi e le proprietà del simbolo di Legendre.
(f). Sia $n = p_1 p_2 \cdot \ldots \cdot p_r$. Tenuto conto della Proposizione 6.6 (h), basta verificare che

$$\frac{n-1}{2} \equiv \frac{p_1 - 1}{2} + \frac{p_2 - 1}{2} + \cdots + \frac{p_r - 1}{2} \pmod 2.$$

Infatti, risulta $n = [(p_1 - 1) + 1][(p_2 - 1) + 1] \cdot \ldots \cdot [(p_r - 1) + 1] = 4k + 1 + (p_1 - 1) + \cdots + (p_r - 1)$ per un qualche $k \in \mathbb{N}$, perché $4 \mid (p_i - 1)(p_j - 1))$, con $1 \leqslant i, j \leqslant r$. Da ciò segue banalmente la congruenza voluta. **(g)**. Si procede come in (f). Tenuto conto del Corollario 6.14, basta verificare che:

$$\frac{n^2 - 1}{8} \equiv \frac{p_1^2 - 1}{8} + \cdots + \frac{p_r^2 - 1}{8} \pmod 2.$$

Infatti $n^2 = [(p_1^2 - 1) + 1] \ldots [(p_r^2 - 1) + 1] = 16h + 1 + (p_1^2 - 1) + \cdots + (p_r^2 - 1)$ per un qualche $h \in \mathbb{N}$, perché $4 \mid (p_i^2 - 1)$ e quindi $16 \mid (p_i^2 - 1)(p_j^2 - 1)$, con $1 \leqslant i, j \leqslant r$. Da ciò segue l'asserto. **(h)**. Sia $n = p_1 p_2 \cdot \ldots \cdot p_r$ e $m = q_1 q_2 \cdot \ldots \cdot q_s$. Tenuto conto del Teorema 6.21, si ha:

$$\begin{aligned}
\left(\frac{n}{m}\right) \cdot \left(\frac{m}{n}\right) &= \prod_{j=1}^{s} \prod_{i=1}^{r} \left(\frac{p_i}{q_j}\right) \cdot \prod_{i=1}^{r} \prod_{j=1}^{s} \left(\frac{q_j}{p_i}\right) = \prod_{i=1}^{r} \prod_{j=1}^{s} \left(\frac{p_i}{q_j}\right) \cdot \left(\frac{q_j}{p_i}\right) = \\
&= \prod_{i=1}^{r} \prod_{j=1}^{s} (-1)^{(\frac{p_i - 1}{2} \cdot \frac{q_j - 1}{2})} = \\
&= (-1)^{\sum_{i=1}^{r} \sum_{j=1}^{s} (\frac{p_i - 1}{2} \cdot \frac{q_j - 1}{2})} = \\
&= (-1)^{(\sum_{i=1}^{r} (\frac{p_i - 1}{2})) \cdot (\sum_{j=1}^{s} (\frac{q_j - 1}{2}))}.
\end{aligned}$$

Per concludere basta osservare (cfr. dimostrazione di **(f)**) che:

$$\sum_{i=1}^{r} (\frac{p_i - 1}{2}) \equiv \frac{n-1}{2} \pmod 2 \quad \text{e} \quad \sum_{j=1}^{s} (\frac{q_j - 1}{2}) \equiv \frac{m-1}{2} \pmod 2. \square$$

Osservazione 6.41. Si consideri la congruenza:

$$X^2 \equiv a \pmod{n} \tag{13}$$

con n dispari, $n > 1$ e $\mathrm{MCD}(a, n) = 1$. È chiaro che (cfr. Teorema 6.36) se (13) è risolubile, allora $(\frac{a}{n}) = 1$. Il viceversa è invece falso (anche se n è un intero per il quale esiste una radice primitiva dell'unità). Basta porre $n = 9$ (cfr. Teorema 5.17) ed osservare che $(\frac{2}{9}) = (\frac{2}{3^2}) = 1$, mentre $X^2 \equiv 2 \pmod{9}$ non è risolubile (in quanto $(\frac{2}{3}) = -1$, cfr. Teorema 6.29).

Si noti la parziale analogia tra queste considerazioni e quelle svolte nell'Osservazione 6.11.

Possiamo, ora, applicare il simbolo di Jacobi e le sue proprietà per dimostrare il seguente risultato:

Proposizione 6.42. (S. Chowla). *L'equazione diofantea quadratica in una indeterminata X*

$$X^2 = a, \quad \textit{con } a \in \mathbb{Z} \tag{14}$$

è risolubile se, e soltanto se, per ogni primo p la congruenza

$$X^2 \equiv a, \pmod{p} \tag{15}$$

è risolubile.

Dimostrazione. È chiaro che se (14) è risolubile, ogni (15) è risolubile. Viceversa, ammettiamo per assurdo che $a \neq b^2$, per ogni $b \in \mathbb{Z}$. Verificheremo che esiste un intero dispari n tale che $(\frac{a}{n}) = -1$ (e, dunque, che esiste un primo dispari p con $p \mid n$ e tale che $(\frac{a}{p}) = -1$).

Distinguiamo tre casi, che insieme coprono tutte le possibilità per le quali a non è quadrato:

(a) Sia $a = \pm 2^e b$, con b, e interi positivi dispari. Sia n una soluzione del sistema:

$$\begin{cases} X \equiv 5 \pmod{8} \\ X \equiv 1 \pmod{b} \end{cases}$$

Si verifica con facilità che $(\frac{\pm 2}{n}) = -1$ (Proposizione 6.40 (f) e (g)), $(\frac{2^{e-1}}{n}) = 1$ e $(\frac{b}{n}) = (\frac{n}{b}) = (\frac{1}{b}) = 1$. Allora $(\frac{a}{n}) = -1 \cdot 1 \cdot 1 = -1$.

(b) Sia $a = \pm 2^{2h} q^k b$, con q, k, b interi dispari, q primo e $q \nmid b$. Sia n una soluzione del sistema:

$$\begin{cases} X \equiv 1 \pmod{4b} \\ X \equiv c \pmod{q} \end{cases}$$

dove c è un intero tale che $(\frac{c}{q}) = -1$. Allora si ha: $(\frac{\pm 1}{n}) = 1$, $(\frac{2^{2h}}{n}) = 1$, $(\frac{b}{n}) = (\frac{n}{b}) = 1$, $(\frac{q^k}{n}) = (\frac{q}{n}) = (\frac{n}{q}) = (\frac{c}{q}) = -1$ e pertanto $(\frac{a}{n}) = -1$.

(c) sia $a = -b^2$, con b intero dispari. Scelto $n \equiv 3 \pmod 4$ tale che $\mathrm{MCD}(a, n) = 1$, è chiaro che $(\frac{a}{n}) = (\frac{-1}{n}) = -1$. □

Osservazione 6.43. Più generalmente, si dimostra che *l'equazione diofantea $X^n = a$ è risolubile se, e soltanto se, $X^n \equiv a \pmod{p^k}$ è risolubile per ogni p primo e per ogni $k \geqslant 1$.* Anzi, più precisamente è noto che *se $X^n \equiv a \pmod p$ è risolubile per ogni p primo, due casi sono possibili:*

1. *Se $8 \nmid n$, allora $X^n = a$ è risolubile;*

2. *Se $8 \mid n$, allora $X^n = a$ è risolubile, oppure $2^{\frac{n}{2}} X^n = a$ è risolubile.*

Il secondo caso, nell'enunciato precedente, si presenta effettivamente, come mostra il seguente esempio: $X^8 \equiv 16 \pmod p$ è risolubile, per ogni primo p, però l'equazione diofantea $X^8 = 16$ non è risolubile, mentre è ovviamente risolubile $2^4 X^8 = 16$.

Per maggiori dettagli si veda: E. Trost, Niew Arch. Wisk. **18** (1934), 58-61 od, anche, N.C. Ankeny - C.A. Rogers, Ann. Math. **53** (1951), 541-550. Una prova più algebrica di un caso particolare di tale risultato è stata data più recentemente da J. Kraft e M. Rosen, Amer. Math. Montly, **88** (1981), 269-270.

6. Esercizi e Complementi

6.1. Siano $a, b, c \in \mathbb{Z}, a \equiv 1 \pmod 2$. Determinare quando la congruenza $aX^2 + bX + c \equiv 0 \pmod 2$ è risolubile.
[Soluzione. La tabella seguente descrive i vari casi possibili:

b	c	x
0	0	0
0	1	1
1	0	0, 1
1	1	–

.]

6.2. Verificare che, per ogni primo p, la congruenza $X^2 \equiv 0 \pmod p$ ha un'unica soluzione $(\mathrm{mod}\ p)$.

6.3. Sia a un intero positivo che scriviamo nella forma $a = b^2 d$, con $b, d \in \mathbb{Z}$ e d privo di fattori quadratici. Mostrare che, per ogni p primo dispari tale che $p \nmid a$, risulta $(\frac{a}{p}) = (\frac{d}{p})$.

6.4. (a). Se q è un primo dispari ed r è una radice primitiva $(\mathrm{mod}\ q)$, si ha $(\frac{r}{q}) = -1$.
(b). Siano p, q primi dispari tali che $q = 2p + 1$ e si consideri l'insieme $T := \{a \in \mathbb{Z} : 1 \leqslant a \leqslant q - 1 \text{ e } (\frac{a}{q}) = -1\}$. Verificare che $\#(T) = p$, che $p - 1$ elementi di T sono radici primitive $(\mathrm{mod}\ q)$ e infine che $2p$ è l'unico elemento di T che non è radice primitiva $(\mathrm{mod}\ q)$.
(c). Utilizzando (b), calcolare le radici primitive modulo $7, 11, 23, 47$.
(Si noti che 11 e 23 sono gli unici primi q, tra 7 e 47, del tipo $q = 2p + 1$, con p primo.)
(d). Con le notazioni di (b), dimostrare che $2(-1)^{\frac{p-1}{2}}$ è una radice primitiva $(\mathrm{mod}\ q)$.
(e). Verificare che 2 è una radice primitiva modulo $11, 59$, e 107, mentre -2 è una radice primitiva modulo $7, 23, 47, 159$ e 167.
[Suggerimento. **(a)** segue dalle Proposizioni 6.6 (d) e 5.22 (d). **(b)** Il primo asserto è conseguenza della Proposizione 6.3 e del fatto che $\frac{q-1}{2} = p$. Per il secondo, cfr. (a) e la Proposizione 5.8. Infine, per il terzo si verifichi che, necessariamente, $q \equiv 3 \pmod 4$ da cui segue che $(\frac{q-1}{q}) = -1$ e $\mathrm{ord}_q(q-1) = 2$. **(c)** Se $q = 7$, $T = \{3, 5, 6\}$, $r = 3, 5$. Se $q = 11$, $T = \{2, 6, 7, 8, 10\}$, $r = 2, 6, 7, 8$. Se $q = 23$, $T = \{5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22\}$, $r = 5, 7, 10, 11, 14, 15, 17, 19, 20, 21$. Se $q = 47$, $T = \{5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 38, 39, 40, 41, 43, 44, 45, 46\}$, $r = 5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 38, 39, 40, 41, 43, 44, 45$. **(d)** Se $p \equiv 1 \pmod 4$, $\frac{p-1}{2}$ è pari e bisogna quindi provare che $\mathrm{ord}_q(2) = 2p$. A priori, $\mathrm{ord}_q(2) = 1, 2, p, 2p$ e bisogna pertanto escludere le prime tre eventualità. Per le prime due è ovvio essendo $q \geqslant 7$, per la terza, si ha $2^p = 2^{\frac{q-1}{2}} \equiv (\frac{2}{q}) \pmod q$ e, essendo $p \equiv 1 \pmod 4$ allora $q \equiv 3 \pmod 8$, dunque $2^p \equiv -1 \pmod q$. Se invece $p \equiv 3 \pmod 4$, bisogna provare che $\mathrm{ord}_q(-2) = 2p$. Procedendo come sopra, essendo $q \equiv 7 \pmod 8$, si ha: $(-2)^p \equiv (\frac{-2}{q}) = (\frac{-1}{q}) \cdot (\frac{2}{q}) \equiv -1 \pmod q$, e da ciò segue l'asserto. **(e)** È una semplice conseguenza di (d).]

6.5. Sia p un primo dispari ed a un intero tale che $\mathrm{MCD}(a,p)=1$. Se $(\frac{a}{p})=1$, allora

$$\left(\frac{p-a}{p}\right)=\begin{cases}1 & \text{se } p\equiv 1 \pmod 4,\\ -1 & \text{se } p\equiv 3 \pmod 4.\end{cases}$$

[Suggerimento: $(\frac{p-a}{p})\equiv (p-a)^{\frac{p-1}{2}}\equiv (-a)^{\frac{p-1}{2}}\equiv (-1)^{\frac{p-1}{2}} \pmod p$.]

6.6. Sia p un primo dispari ed a un intero tale che $\mathrm{MCD}(a,p)=1$. Mostrare che:

$$(p-1)!\equiv -\left(\frac{a}{p}\right)a^{\frac{p-1}{2}} \pmod p.$$

[Suggerimento. Dal Criterio di Eulero segue che $(\frac{a}{p})\equiv a^{\frac{p-1}{2}} \pmod p$, quindi $(\frac{a}{p})a^{\frac{p-1}{2}}\equiv 1 \pmod p$; la conclusione è conseguenza del Lemma di Wilson.]

6.7. Sia p un primo dispari e siano $a,b\in\mathbb{Z}$ tali che $\mathrm{MCD}(a,p)=\mathrm{MCD}(b,p)=1$. Se $(\frac{a}{p})=(\frac{b}{p})$, allora $aX^2\equiv b \pmod p$ è risolubile (e viceversa).
[Suggerimento. Se a^* è l'inverso aritmetico di $a \pmod p$, allora $X^2\equiv a^*b \pmod p$ è risolubile $\iff$ $(\frac{a^*b}{p})=1 \iff (\frac{a}{p})=(\frac{b}{p})$.]

6.8. Mostrare che esistono infiniti primi di tipo $4k+1$.
[Suggerimento. Per assurdo, siano $p_1,\ldots,p_n$ i soli primi di tipo $4k+1$. L'intero dispari $N:=4(p_1p_2\cdot\ldots\cdot p_n)^2+1$ è divisibile per un primo dispari p. Utilizzando la Proposizione 6.6 (h), si verifica che $p\equiv 1 \pmod 4$ e che da ciò segue un assurdo.]

6.9. Mostrare che esistono infiniti primi di tipo $8k-1$.
[Suggerimento. Per assurdo, siano $p_1,\ldots,p_n$ i soli primi di tipo $8k-1$. L'intero $N:=(4p_1\cdot\ldots\cdot p_n)^2-2$ ammette certamente un divisore primo p dispari. Ne segue che $(\frac{2}{p})=1$, quindi $p\equiv 1,7 \pmod 8$. Se tutti i divisori primi dispari di N fossero della forma $8k+1$, siccome N è pari risulterebbe $N\equiv 2 \pmod{16}$, mentre $N\equiv -2 \pmod{16}$. Se invece fosse $p\equiv 7\equiv -1 \pmod 8$, allora $p\mid (N-(4p_1p_2\cdot\ldots\cdot p_n)^2)=2$ e ciò è ugualmente assurdo.]

6.10. Mostrare che esistono infiniti primi del tipo:

(a) $8k+3$;

(b) $8k+5$;

(c) $8k+7$;

(d) $6k+1$.

[Suggerimento. Per ciascuna parte si assuma che esistano un numero finito di primi del tipo indicato. Per la parte **(a)** prendere in esame $N:=(4p_1p_2\cdot\ldots\cdot p_n)^2-2$; per la parte **(b)** prendere in esame $N:=(p_1p_2\cdot\ldots\cdot p_n)^2+2$; per la parte **(d)** $N:=(2p_1p_2\cdot\ldots\cdot p_n)^2+3$. Per **(c)** si noti che $8k+7\equiv 8k-1 \pmod 8$ (cfr. Esercizio 6.9).]

6.11. Sia n un intero dispari ed a un intero tale che $\mathrm{MCD}(a,n)=1$. Mostrare che la risolubilità della congruenza $aX^2+bX+c\equiv 0 \pmod n$ può essere ricondotta alla risolubilità di una congruenza del tipo: $Y^2\equiv d \pmod n$.
[Suggerimento. Si proceda come già fatto all'inizio del Paragrafo 6 per ogni fattore primo p (necessariamente dispari) di n e si tenga conto del Teorema 6.36.]

6.12. Determinare se le seguenti congruenze sono risolubili:

(a) $2X^2 - 5X + 7 \equiv 0 \pmod{21}$

(b) $X^2 + X - 2 \equiv 0 \pmod{35}$

[Soluzione. **(a)** Sia $a = 2, b = -5, c = 7, d = b^2 - 4ac = -31, Y = 2aX + b = 4X - 5$. Poiché $21 = 3 \cdot 7$ è dispari, allora le soluzioni della congruenza data si determinano dalle soluzioni della congruenza

$$Y^2 \equiv -31 \pmod{21} \quad \text{cioè} \quad Y^2 \equiv 11 \pmod{21}.$$

Poiché $(\frac{11}{21}) = (\frac{21}{11}) = (\frac{10}{11}) = (\frac{2}{11})(\frac{5}{11}) = -(\frac{11}{5}) = -(\frac{1}{5}) = -1$, $Y^2 \equiv 11 \pmod{21}$ non è risolubile, pertanto non è risolubile la congruenza data. **(b)** In tal caso $d = 9, Y = 2X + 1, Y^2 \equiv 9 \pmod{35}$ è risolubile in quanto $(\frac{9}{5}) = 1$ e $(\frac{9}{7}) = 1$. Precisamente le soluzioni sono $x = 1, 8, 26, 33 \pmod{35}$.]

6.13. Sia p primo, $p \neq 3$ ed a un intero tale che $\text{MCD}(a, p) = 1$. Mostrare che la congruenza: $aX^3 + bX^2 + cX + d \equiv 0 \pmod{p}$ può essere ricondotta ad una congruenza del tipo: $Y^3 + eY + f \equiv 0 \pmod{p}$.
[Suggerimento. Si moltiplichi la congruenza assegnata per a^* e si ponga $X = Y - 3^* a^* b$.]

6.14. Mostrare che p è un qualsiasi primo dispari, allora:

$$\left(\frac{2}{p}\right) = \left(\frac{8-p}{p}\right) = \left(\frac{p}{p-8}\right) = \left(\frac{2}{p-8}\right).$$

[Suggerimento. Utilizzando la Proposizione 6.40 si ha: $(\frac{8-p}{p}) = (\frac{8}{p}) = (\frac{2 \cdot 4}{p}) = (\frac{2}{p})$, $(\frac{p}{p-8}) = (\frac{8}{p-8}) = (\frac{2}{p-8})$, $(\frac{2}{p}) = (\frac{2}{p-8})$ perché $p \equiv 8 \pmod{p-8}$.]

6.15. Sia $k \geqslant 2$ e sia $p = 4k + 3$ un numero primo. Mostrare che:

(a) $2p + 1$ è primo $\iff 2^p \equiv 1 \pmod{(2p+1)}$.

(b) Se $2p+1$ è primo, il numero $M_p := 2^p - 1$ (detto *p-esimo numero di Mersenne*) è composto.

[Suggerimento. **(a, $\Rightarrow$)**. Basta osservare che $2^p = 2^{\frac{2p+1-1}{2}} \equiv (\frac{2}{2p+1}) = 1$ (modulo $2p + 1$) per il Criterio di Euler, essendo $2p + 1 \equiv 7 \pmod{8}$. **(a, $\Leftarrow$)**. Poniamo $n := 2p + 1$. Se $2^p \equiv 1 \pmod{n}$, allora necessariamente $p = \text{ord}_n(2)$ e quindi $p \mid \varphi(n)$. Se $n = p_1^{e_1} \cdots p_r^{e_r}$ allora $p \mid \left(\prod_{i=1}^r p_i^{e_i - 1} \cdot (p_i - 1)\right)$. Poiché si vede subito che $p \nmid p_i$, per ogni i, allora $p \mid (p_i - 1)$, per qualche i. D'altro lato $2p + 1 = p_i \cdot n'$ dove $n' := \frac{n}{p_i}$. Se $n' > 1$, allora è subito visto che deve essere $n' > 2$, e quindi si avrebbe che $p \nmid (p_i - 1)$, poiché avremmo che $p > p_i - 1$, e ciò è assurdo. Pertanto $n' = 1$, cioè $2p + 1 = p_i$ è un primo. **(b)**. È una semplice conseguenza di (a).]

6.16. Sia p un primo dispari. Mostrare che $X^4 \equiv -4 \pmod{p}$ è risolubile se e soltanto se $p \equiv 1 \pmod{4}$.
[Suggerimento. Si noti che $X^4 + 4 = ((X+1)^2 + 1)((X-1)^2 + 1)$. Pertanto $X^4 \equiv -4 \pmod{p}$ è risolubile se e soltanto se almeno una delle congruenze $((X+1)^2 + 1) \equiv 0 \pmod{p}$ oppure $((X-1)^2 + 1) \equiv 0 \pmod{p}$ è risolubile. È subito che entrambe sono risolubili se e soltanto se $(\frac{-1}{p}) = 1$.]

6.17. Calcolare i seguenti simboli di Jacobi:

$$\textbf{(a)}\ \left(\frac{713}{1009}\right); \qquad \textbf{(b)}\ \left(\frac{111}{991}\right); \qquad \textbf{(c)}\ \left(\frac{313}{367}\right).$$

[Soluzione. **(a)** Si noti che $1009 \equiv 1 \pmod 4$ ed è primo e che $713 = 23 \cdot 31$.

$$\begin{aligned}\left(\frac{23}{1009}\right) &= \left(\frac{1009}{23}\right) = \left(\frac{20}{23}\right) = \\ &= \left(\frac{4}{23}\right)\left(\frac{5}{23}\right) = \left(\frac{23}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1, \\ \left(\frac{31}{1009}\right) &= \left(\frac{1009}{31}\right) = \left(\frac{17}{31}\right) = \left(\frac{31}{17}\right) = \left(\frac{14}{17}\right) = \\ &= \left(\frac{2}{17}\right)\left(\frac{7}{17}\right) = \left(\frac{7}{17}\right) = \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) = \\ &= -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1\end{aligned}$$

quindi $(\frac{713}{1009}) = 1$. **(b)**: -1. **(c)**: 1.]

6.18. Determinare il numero delle soluzioni della congruenza

$$X^2 \equiv 4 \pmod{105}.$$

[Soluzione. Poiché $105 = 3 \cdot 5 \cdot 7$ e ciascuna delle congruenze $X^2 \equiv 4 \pmod 3, X^2 \equiv 4 \pmod 5, X^2 \equiv 4 \pmod 7$ ha due soluzioni, allora la congruenza data ha 2^3 soluzioni (mod 105): $2, 23, 37, 47, 58, 68, 82, 103$.]

6.19. (Gauss). Sia p un primo dispari. Siano $n, n+1$ due interi consecutivi nel sistema ridotto di residui $S^* := \{1, 2, \ldots, p-1\}$. Denotiamo con (RR) (rispettivamente: (RN); (NR); (NN)) il numero delle coppie di interi consecutivi $(n, n+1)$ di S^* tali che $(\frac{n}{p}) = 1$ e $(\frac{n+1}{p}) = 1$ (rispettivamente: $(\frac{n}{p}) = 1$ e $(\frac{n+1}{p}) = -1$; $(\frac{n}{p}) = -1$ e $(\frac{n+1}{p}) = 1$; $(\frac{n}{p}) = -1$ e $(\frac{n+1}{p}) = -1$). I seguenti enunciati mostrano che la distribuzione dei residui e dei non residui quadratici è essenzialmente casuale, in quanto ciascuna delle quattro possibilità si presenta con una frequenza pressoché uguale (cioè, frequenza uguale a circa $\left[\frac{1}{4}(p-1)\right]$).
Poniamo $\varepsilon := (-1)^{\frac{p-1}{2}} = (\frac{-1}{p}) = (\frac{p-1}{p})$. Mostrare che:

(1) (RR) + (RN) = $\frac{1}{2}(p-2-\varepsilon)$;

(2) (NR) + (NN) = $\frac{1}{2}(p-2+\varepsilon)$;

(3) (RR) + (NR) = $\frac{1}{2}(p-1)-1 = \frac{1}{2}(p-3)$;

(4) (RN) + (NN) = $\frac{1}{2}(p-1)$;

(5) $\sum_{n=1}^{p-2}(\frac{n(n+1)}{p}) = -1$;

(6) (RR) + (NN) - (RN) - (NR) = -1;

(7) (RR) + (NN) = $\frac{1}{2}(p-3)$;

(8) (RR) - (NN) = $-\frac{1}{2}(1+\varepsilon)$;

(9) (RR) $= \frac{1}{4}(p-4-\varepsilon)$;

(10) (NN) $= \frac{1}{4}(p-2+\varepsilon)$;

(11) (RN) + (NR) $= \frac{1}{2}(p-1)$;

(12) (RN) - (NR) $= 1-\frac{1}{2}(1+\varepsilon) = \frac{1}{2}(1-\varepsilon)$;

(13) (RN) $= \frac{1}{4}(p-\varepsilon)$;

(14) (NR) $= \frac{1}{4}(p-2+\varepsilon)$.

[Suggerimento. **(1)** Il numero (RR) + (RN) è il numero delle coppie $(n, n+1)$ per cui n è un residuo quadratico, dove n varia tra 1 e $p-2$. Quindi tale numero dipende dal valore di

$$\left(\frac{p-1}{p}\right) = \left(\frac{-1}{p}\right) = \varepsilon.$$

Se $p-1$ è un non residuo quadratico, cioè se $\varepsilon = -1$, allora i residui quadratici sono tutti tra gli interi $\{1, 2, \ldots, p-2\}$ e quindi (RR) + (RN) $= \frac{1}{2}(p-1)$. Se $p-1$ è un residuo quadratico, cioè $\varepsilon = 1$, allora i residui quadratici tra gli interi $\{1, 2, \ldots, p-2\}$ sono $\frac{1}{2}(p-1)-1 = \frac{1}{2}(p-3)$.
Similmente si dimostrano **(2)**, **(3)** e **(4)**.
(5) Se n^* è un inverso aritmentico di n allora:

$$n(n+1) = n^2 + n \equiv n^2(1+n^*) \pmod{p}$$

e quindi

$$\sum_{n=1}^{p-2}\left(\frac{n(n+1)}{p}\right) = \sum_{n=1}^{p-2}\left(\frac{1+n^*}{p}\right) = \sum_{n=2}^{p-1}\left(\frac{n}{p}\right).$$

Poichè

$$\sum_{n=1}^{p-1}\left(\frac{n}{p}\right) = 0,$$

allora

$$\sum_{n=2}^{p-1}\left(\frac{n}{p}\right) = -\left(\frac{1}{p}\right) = -1.$$

(6) segue da (5).
(7) e **(8)** sono semplici conseguenze di (6), (1), e (2).
(9) e **(10)** seguono da (7) e (8).
(11) e **(12)** seguono da (3) e (4) e dal fatto che (RN) - (NR) + (NN) - (RR) =1.
(13) e **(14)** seguono immediatamente da (11) e (12).]