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 $\pmod{2 \cdot p^k}$.