1. *Verificare che* $x^K \equiv 1 \mod n$, *implica* $x^K \equiv 1 \mod p$, *per ogni divisore primo* p *di* n. *Vale anche il viceversa? (dimostrarlo o esibire un controesempio).*

Sol. Sia $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ la decomposizione di n in fattori primi. Osserviamo che $\gcd(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$, per ogni $i \neq j$. Dal Teorema Cinese del Resto, abbiamo che

$$x^K \equiv 1 \mod n \quad \Leftrightarrow \quad \begin{cases} x^K \equiv 1 \mod p_1^{\alpha_1} \\ \vdots \\ x^K \equiv 1 \mod p_k^{\alpha_k} \end{cases} \quad \Rightarrow \quad \begin{cases} x^K \equiv 1 \mod p_1 \\ \vdots \\ x^K \equiv 1 \mod p_k. \end{cases}$$

L'ultima implicazione non ha viceversa:
consideriamo ad esempio

$$x^2 \equiv 1 \mod 200 \quad \Leftrightarrow \quad \begin{cases} x^2 \equiv 1 \mod 2^3 \\ x^2 \equiv 1 \mod 5^2 \end{cases} \quad \Rightarrow \quad \begin{cases} x^2 \equiv 1 \mod 2 \\ x^2 \equiv 1 \mod 5. \end{cases}$$

Si verifica facilmente che $x = 11$ soddisfa il sistema di congruenze modulo 2 e modulo 5, ma non la congruenza iniziale.

Un'interpretazione di questi fatti è la seguente:
Se l'ordine di $\bar{x}$ in $\mathbb{Z}_n^*$ divide K, allora l'ordine di $\bar{x}$ in $\mathbb{Z}_p^*$ divide K, per ogni divisore primo p di n.

2. *Verificare che* $\gcd(x^K - 1, n) = 1$, *implica* $x^K \not\equiv 1 \mod p$, *per ogni divisore primo* p *di* n.

Sol. Se $\gcd(x^K - 1, n) = 1$, allora per ogni divisore primo p di n si ha che p non divide $x^K - 1$. In particolare, $x^K \not\equiv 1 \mod p$.
In altre parole: l'ordine di $\bar{x}$ in $\mathbb{Z}_p^*$ non divide K.

3. *Sia* $p \in \mathbb{N}$ *primo. Sia* $y \in \mathbb{Z}_p^*$ *tale che*

$$\begin{cases} y^{l^a} \equiv 1 \mod p \\ y^{l^{a-1}} \not\equiv 1 \mod p, \end{cases} \qquad \textit{con } l \textit{ primo.}$$

Verificare che:
(a) L'ordine di y *in* $\mathbb{Z}_p^*$ *è uguale a* l^a.
(b) Vale $p \equiv 1 \mod l^a$.

Sol. (a) Osserviamo innanzitutto che per questo particolare tipo di potenze vale la seguente relazione

$$(y^{l^b})^{l^c} = y^{l^b \cdot l^c} = y^{l^{b+c}}. \qquad (*)$$

(in generale $x^n = 1 \mod p$ implica $x^{n+1} = x^n x = x \mod p$; dunque NON implica $x^{n+1} = 1 \mod p$!!!)
Se $y^{l^a} \equiv 1 \mod p$, allora l'ordine di y in $\mathbb{Z}_p^*$ divide l^a. Poiché l è primo, l'ordine di y in $\mathbb{Z}_p^*$ è necessariamente una potenza di l, cioè l^b, con $b \leq a$.
Supponiamo per assurdo che l'ordine di y in $\mathbb{Z}_p^*$ sia minore di l^a, cioè sia l^b, con $b < a - 1$. Ma questo insieme alla relazione (*) contraddice il fatto che $y^{l^{a-1}} \not\equiv 1 \mod p$. Dunque l'ordine di y in $\mathbb{Z}_p^*$ è uguale ad l^a.
(b) Poiché Z_p^* è un gruppo ciclico di ordine $p - 1$, e l'ordine di un elemento necessariamente divide l'ordine del gruppo, $l^a \mid p - 1$. Il che equivale a $p \equiv 1 \mod l^a$.

• Sia $p = 13$. Allora $\mathbb{Z}_p^*$ è un gruppo ciclico di ordine $p - 1 = 12 = 2^2 \cdot 3$ e per ogni divisore d di 12 esistono $\varphi(d)$ elementi di ordine d.

In particolare esiste elemento di ordine $2^2 = 4$: ed infatti vale $13 \equiv 1 \mod 4$.

• Sia $p = 17$. Allora $\mathbb{Z}_p^*$ è un gruppo ciclico di ordine $p - 1 = 16 = 2^4$ e per ogni divisore d di 16 esistono $\varphi(d)$ elementi di ordine d.
In particolare esistono elemento di ordine 2, un elemento di ordine 4, un elemento di ordine 8 ed un elemento di ordine 16: ed infatti vale $17 \equiv 1 \mod 2,\ 4,\ 8,\ 16$.

4. *Sia $n \in \mathbb{Z}$. Supponiamo che esista $x \in \mathbb{Z}_n$ per cui valgono*

$$\begin{cases} x^M \equiv 1 \mod n \\ \gcd(x^{M/l} - 1, n) = 1, \end{cases} \qquad \text{con } l \text{ divisore primo di } M.$$

Verificare che per ogni divisore primo p di n, valgono

$$\begin{cases} x^M \equiv 1 \mod p \\ x^{M/l} \not\equiv 1 \mod p. \end{cases}$$

Sol: - Se $x^M \equiv 1 \mod n$ allora $x^M \equiv 1 \mod p$, per ogni divisore primo p di n (vedi Esercizio 1).
- Supponiamo che $\gcd(x^{M/l} - 1, n) = 1$. Allora per ogni divisore primo p di n, si ha che p *non divide* $x^{M/l} - 1$, ossia $x^{M/l} \not\equiv 1 \mod p$ (vedi Esercizio 2).

5. *(Criterio di Pocklington) Sia n un intero. Sia M un intero con la seguente proprietà: per ogni divisore primo l di M, esiste $x \in \mathbb{Z}_n$ tale che*

$$\begin{cases} x^M \equiv 1 \mod n \\ \gcd(x^{M/l} - 1, n) = 1. \end{cases} \qquad (*)$$

Verificare che:
(a) Per ogni divisore primo p di n vale $p \equiv 1 \mod M$.
(b) Se $M > \sqrt{n}$, allora n è primo.

Sol. Le condizioni (*) implicano

$$\begin{cases} x^M \equiv 1 \mod p \\ \gcd(x^{M/l} - 1, p) = 1 \end{cases}, \quad \forall p \text{ divisore primo di } n \qquad (**)$$

(vedi Esercizio 1);
le condizioni (**) implicano

$$\begin{cases} x^M \equiv 1 \mod p \\ x^{M/l} \not\equiv 1 \mod p, \end{cases}, \quad \forall p \text{ divisore primo di } n \qquad (***)$$

(vedi Esercizio 4).
Sia p un qualunque divisore primo di n.
• A partire dalle (***), per ogni divisore primo l di M, siamo in grado di costruire un elemento y di ordine l^a in $\mathbb{Z}_p^*$, dove l^a è la massima potenza di l che divide M.

dim: Definiamo $y := x^{M/l^a}$ e verifichiamo che ha ordine l^a in $\mathbb{Z}_p^*$. Dalla prima equazione in (**)

$$y^{l^a} = (x^{M/l^a})^{l^a} = x^M \equiv 1 \mod p;$$

ne segue che $ord_p(Y)$ divide l^a e, poiché l è primo, $ord_p(Y) = l^b$, per $b \leq a$. Supponiamo per assurdo che sia $ord_p(Y) = l^b$, con $b < a$. Dalla seconda equazione in (***) abbiamo $b < a - 1$, in quanto $x^{M/l} \not\equiv 1 \mod p$ equivale a $y^{l^{a-1}} \not\equiv 1 \mod p$. Ma, come abbiamo osservato dell'Esercizio 3, se $y^{l^b} \equiv 1 \mod p$, allora per

ogni $\alpha > 0$, anche $y^{l^{b+\alpha}} = (y^{l^b})^{l^\alpha} \equiv 1 \mod p$. Questo contraddice la seconda equazione in (***) e dobbiamo concludere che $ord_p(Y) = l^a$, come richiesto.

L'esistenza di un elemento di ordine l^a in $\mathbb{Z}_p^*$ e il fatto che l'ordine di un elemento necessariamente divide l'ordine del gruppo, implica che $l^a \mid p-1$, ossia $p \equiv 1 \mod l^a$. Poiché ciò vale per ogni divisore primo l di $M = l_1^{a_1} \cdot \ldots \cdot l_k^{a_k}$, dal Teorema Cinese del Resto, abbiamo che

$$\begin{cases} p \equiv 1 \mod l_1^{a_1} \\ \vdots \quad \vdots \quad \vdots \\ p \equiv 1 \mod l_k^{a_k} \end{cases} \quad \Leftrightarrow \quad p \equiv 1 \mod M,$$

come richiesto.

(b) Supponiamo che $M > \sqrt{n}$. Allora $p - 1 = KM$, con $K \in \mathbb{Z}$, implica $p > M > \sqrt{n}$.

6. *(Criterio di Pocklington, caso speciale $M = Q$ primo) Sia $n >> 0$ un intero (pseudoprimo). Sia Q un primo con la seguente proprietà: esiste $x \in \mathbb{Z}_n$ tale che*

$$\begin{cases} x^Q \equiv 1 \mod n \\ \gcd(x-1, n) = 1. \end{cases}$$

Allora:
(a) Per ogni divisore primo p di n vale $p \equiv 1 \mod Q$.
(b) Se $Q > \sqrt{n}$, allora n è primo.

Osservazione. Sia $n \gg 0$ pseudoprimo. Vorremmo dimostrare che n è primo mediante il criterio di Pocklington. Il risultato del prossimo esercizio ci suggerisce come scegliere M per avere delle possibilità di porci nelle ipotesi del criterio.

8. *Sia n un intero. Sia M un intero con la seguente proprietà:*
per ogni divisore primo l di M, esiste $x \in \mathbb{Z}_n$ (possibilmente dipendente da l) per cui valgono le relazioni

$$\begin{cases} x^M \equiv 1 \mod n \\ \gcd(x^{M/l} - 1, n) = 1. \end{cases}$$

Allora esiste un elemento $z \in \mathbb{Z}_n^*$ di ordine M.

Se n è pseudoprimo, verosimilmente $\varphi(n) = n - 1$. Se esiste un elemento $z \in \mathbb{Z}_n^*$ di ordine M, allora M deve essere un divisore di $n - 1$.

Procediamo così:
Cerchiamo di fattorizzare almeno parzialmente $n - 1$ determinandone i fattori più piccoli. Sia Q il prodotto di tali fattori, per cui $n - 1 = Q \cdot R$.
Possono succedere tre cose:

(a) (quasi mai) $n - 1 = Q \cdot R$, con $Q > \sqrt{n}$.

(b) (probabilmente) $n - 1 = Q \cdot R$, con $Q < \sqrt{n}$ ed $R > \sqrt{n}$ non pseudoprimo e non fattorizzabile in tempo utile. In questo caso non siamo in grado di applicare il criterio.

(c) (a volte) $n - 1 = Q \cdot R$, con $Q < \sqrt{n}$ ed $R > \sqrt{n}$ pseudoprimo. In questo caso applichiamo il criterio ricorsivamente.

Teorema (Criterio di Pocklington). *Sia n un intero. Sia M un intero con la seguente proprietà: per ogni divisore primo l di M, esiste $x \in \mathbb{Z}_n$ tale che*

$$\begin{cases} x^M \equiv 1 \mod n \\ \gcd(x^{M/l} - 1, n) = 1. \end{cases}$$

Allora:

(a) Per ogni divisore primo p di n vale $p \equiv 1 \mod M$.

(b) Se $M > \sqrt{n}$, allora n è primo.

Osservazione. Le ipotesi del criterio di Pocklington implicano che per ogni divisore primo l di M, esiste $y \in \mathbb{Z}_n$ tale che

$$ord(y) = l^a, \quad \text{in } \mathbb{Z}_p^*, \text{ per ogni divisore primo } p \text{ di } n,$$

dove a è l'esponente massimo per cui $l^a | M$.

Dalla condizione $ord_p(y) = l^a$, segue che $l^a \mid p - 1$. Poiché questo vale per ogni divisore primo l di M, si ha che

$$M \mid p - 1.$$

Conclusione: per ogni divisore primo p di n vale $p \equiv 1 \mod M$, e di conseguenza $p > M$. Se $M > \sqrt{n}$, allora n è primo.

Teorema (Goldwasser-Kilian). *Sia $n \gg 0$ un intero (pseudoprimo). Sia $E(\mathbb{Z}_n)$ una "curva ellittica" su $\mathbb{Z}_n$ (cioè con discriminante $\Delta \in \mathbb{Z}_n^*$). Sia M un intero con la seguente proprietà: per ogni divisore primo l di M, esiste un punto al finito $P \in E(\mathbb{Z}_n)$ tale che*

$$\begin{cases} M \cdot P = \infty \in E(\mathbb{Z}_n) \\ M/l \cdot P \neq \infty \in E(\mathbb{Z}_p), \text{ per ogni } p \text{ divisore primo di } n. \end{cases}$$

(la seconda condizione può essere controllata anche senza conoscere p). Allora

(a) Per ogni divisore primo p di n vale $M \mid \#E(\mathbb{Z}_p)$.

(b) Se $M > (n^{1/4} + 1)^2$, allora n è primo.

Osservazione. Le ipotesi del Teorema di Golwasser-Kilian implicano che per ogni divisore primo l di M esiste un punto al finito $Y \in E(\mathbb{Z}_n)$ con

$$ord(Y) = l^a, \quad \text{in } E(\mathbb{Z}_p) \text{ per ogni divisore primo } p \text{ di } n,$$

dove a è l'esponente massimo per cui $l^a | M$.

Ne segue che M divide $\#E(\mathbb{Z}_p)$, per ogni divisore primo p di n.

Per il Teorema di Hasse, $M < (\sqrt{p} + 1)^2 = p + 1 + 2\sqrt{p}$. Se inoltre $M > (n^{1/4} + 1)^2$, allora

$$(n^{1/4} + 1)^2 < (\sqrt{p} + 1)^2,$$

da cui segue che $p > \sqrt{n}$, per ogni divisore primo di n. In particolare, n è primo.

Osservazione. Sia $Y \in E(\mathbb{Z}_n)$ un punto *al finito*, nel senso che è al finito su $E(\mathbb{Z}_p)$, per ogni divisore primo p di n. Abbiamo che $ord(Y) = l^a$ su $E(\mathbb{Z}_p)$, se $l^a \cdot Y = \infty$, ma $l^{a-1} \cdot Y \neq \infty$ su $E(\mathbb{Z}_p)$.

Diciamo che $l^a \cdot Y = \infty$ su $E(\mathbb{Z}_n)$, se $l^a \cdot Y = \infty$ su $E(\mathbb{Z}_p)$, per ogni divisore primo p di n. Ciò avviene precisamente quando il denominatore non invertibile d che si trova all'ultimo passo del calcolo soddisfa $\gcd(d, n) = n$ (e non solo $\gcd(d, n) > 1$). Abbiamo che $M/l \cdot P \neq \infty \in E(\mathbb{Z}_p)$, per ogni p divisore primo di n, precisamente quando calcolando $M/l \cdot P$ su $E(\mathbb{Z}_n)$, per ogni denominatore d che che dobbiamo invertire vale $\gcd(d, n) = 1$.

Nelle implementazioni del Teorema di Goldwasser-Kilian come test di primalità si usa per lo più il seguente caso speciale:

(Teorema di Goldwasser-Kilian, caso speciale $M = Q$ primo). *Sia $n \gg 0$ un intero (pseudoprimo). Sia $E(\mathbb{Z}_n)$ una "curva ellittica" su $\mathbb{Z}_n$ (cioè con discriminante $\Delta \in \mathbb{Z}_n^*$). Sia Q un primo con la seguente proprietà: esiste un punto al finito $P \in E(\mathbb{Z}_n)$ tale che*

$$Q \cdot P = \infty, \quad \text{in } E(\mathbb{Z}_n).$$

Allora

(a) Per ogni divisore primo p di n vale $Q \mid \#E(\mathbb{Z}_p)$.
(b) Se $Q > (n^{1/4} + 1)^2$, allora n è primo.

Sia $n \gg 0$ un intero (pseudoprimo),
sia $E(\mathbb{Z}_n)$ una "curva ellittica" random su $\mathbb{Z}_n$;
calcoliamo l'ordine della curva $m := \#E(\mathbb{Z}_n)$ (vedi Osservazione 1).

Supponiamo che m si fattorizzi come $m = r \cdot Q$, con Q primo, $Q > (n^{1/4} + 1)^2$;
costruiamo un punto $X_0 = (U_0, V_0)$ al finito su su $E(\mathbb{Z}_n)$ (vedi Osservazione 2);
sia $P := \frac{m}{Q} \cdot X_0$.

Calcoliamo $Q \cdot P$ su $E(\mathbb{Z}_n)$:
se $Q \cdot P = \infty$ su $E(\mathbb{Z}_n)$, con $\gcd(d, n) = n$ (dove d è il denominatore non-invertibile che si incontra nel calcolo), allora $Q \cdot P = \infty$ su $E(\mathbb{Z}_p)$ per ogni divisore primo p di n (vedi Osservazione 3).

Poiché Q è primo, possiamo concludere direttamente che $ord(P) = Q$ su $E(\mathbb{Z}_p)$ (e non solo $ord(P) \mid Q$)
e quindi che Q divide $\#E(\mathbb{Z}_p)$, per per ogni divisore primo p di n.

Dopodiché Q primo e $Q > (n^{1/4} + 1)^2$, implica n primo.

• La difficoltà sta nel fattorizzare l'ordine della curva $m := \#E(\mathbb{Z}_n)$:
in generale m (che ha l'ordine di grandezza di $n \gg 0$) non si riesce a fattorizzare;
nel caso in cui m non si riesce a fattorizzare completamente o non presenti una fattorizzazione parziale del tipo $m = r \cdot Q$, con $Q > (n^{1/4} + 1)^2$ primo o pseudoprimo (in quest'ultimo caso si applica il test a Q, etc...), si cambia curva.

Osservazione 1. Teoricamente, per calcolare $\#E(\mathbb{Z}_n)$ esiste l'algoritmo di Schoof che è deterministico e polinomiale in $\log n$ (n è pseudoprimo, ma lo trattiamo come se fosse primo). Nelle implementazioni, si usa una variante dell'agoritmo di Goldwasser-Kilian dovuta ad Atkin e Morain: invece che prendere una curva ellittica $E(\mathbb{Z}_n)$ random e contarne i punti, si usano curve ellittiche speciali, la cui cardinalità $\#E(\mathbb{Z}_n)$ è data da una formula.

Osservazione 2. Per costruire un punto X_0 su $E(\mathbb{Z}_n) : Y^2 = X^3 + AX + B$, si parte da U_0 random, si calcola $U_0^3 + AU_0 + B$, e se ne calcola la radice quadrata modulo n, usando Shanks-Tonelli (n è pseudoprimo, ma lo trattiamo come se fosse primo).

Osservazione 3. Se fosse $1 < \gcd(d, n) < n$, allora n sarebbe sicuramente composto.