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).

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

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

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

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

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

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

5. Sia n un intero e sia $x \in \mathbb{Z}_n$. Sia M un intero con la seguente proprietà: per ogni divisore primo l di M, valgono le relazioni

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

   Allora x ha ordine M in $\mathbb{Z}_n^*$.

6. (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

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

   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.

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

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

   Verificare che se $M > \sqrt{n}$, allora n è primo.