3. Sia n un numero naturale e sia $x \in \mathbf{Z}$ con $\mathrm{mcd}(x, n) = 1$. Sia a l'ordine di $x \in \mathbf{Z}_n^*$ e sia $k \in \mathbf{Z}$. Dimostrare che l'ordine di $x^k \in \mathbf{Z}_n^*$ è uguale a $a/\mathrm{mcd}(a, k)$.

2. (a) Supponiamo che $n \in \mathbf{Z}_{>1}$ ha la proprietà che $\mathrm{mcd}(n, 10) = 1$. Determinare la lunghezza del periodo dell'espansione decimale di $\frac{1}{n}$.
   (b) Determinare i numeri naturali $n \in \mathbf{Z}_{>1}$ con $\mathrm{mcd}(n, 10) = 1$ che hanno la proprietà che il periodo dell'espansione decimale di $\frac{1}{n}$ ha lunghezza ≤ 6.

4. Sia n un numero naturale dispari.
   (a) Dimostrare che $H = \{\overline{x} \in \mathbf{Z}_n^* : \overline{x}^2 = \overline{1}\}$ è un sottogruppo di $\mathbf{Z}_n^*$.
   (b) Dimostrare che $\#H = 2^d$ dove d è il numero di divisori primi di n.
   (c) Determinare H per $n = 91$.

1. (Numeri di Fermat) Per ogni numero naturale n, si definisce l'ennesimo numero di Fermat come $F_n = 2^{2^n} + 1$; Far vedere che ogni divisore primo p di F_n soddisfa $p \equiv 1 \pmod{2^{n+2}}$.

1. (Numeri di Mersenne) Per ogni numero naturale n, si definisce l'ennesimo numero di Mersenne come $M_n = 2^n - 1$; Far vedere che quando n è dispari, ogni divisore primo p di M_n soddisfa $p \equiv \pm 1 \pmod 8$.

9. Si p un numero primo dispari.
   (a) Dimostrare che per ogni $\overline{x} \in \mathbf{Z}_p^*$ la classe $\overline{x}^{(p-1)/2}$ è uguale a $\pm\overline{1}$.
   (b) Far vedere che $\overline{x} \in \mathbf{Z}_p^*$ è un *quadrato* se e solo se $\overline{x}^{(p-1)/2} = \overline{1}$.
   (c) Quanti quadrati ci sono in $\mathbf{Z}_p^*$?

10. Si p un numero primo e sia d un divisore di $p - 1$.
   (a) Sia $W = \{\overline{x} \in \mathbf{Z}_p^* : \overline{x}^d = \overline{1}\}$. Quanti elementi ci sono in W?
   (b) Dimostrare che per ogni $\overline{x} \in \mathbf{Z}_p^*$ la classe $\overline{x}^{(p-1)/d}$ è un elemento di W.
   (c) Far vedere che $\overline{x} \in \mathbf{Z}_p^*$ è una *d-esima potenza* se e solo se $\overline{x}^{(p-1)/d} = \overline{1}$.
   (d) Quante d-esime potenze ci sono in $\mathbf{Z}_p^*$?

4. Sia $p \equiv 3 \pmod 4$ un numero primo. Supponiamo che $a \in \mathbf{Z}$ sia un quadrato diverso da zero modulo p. Far vedere che:
   (a) vale $a^{(p-1)/2} \equiv 1 \pmod p$;
   (b) il numero $a^{(p+1)/4}$ è radice quadrata di a modulo p.

10. Sia p un numero primo dispari.
   (a) Far vedere che 2 è un quadrato modulo p per $p = 7, 17, 23, 31$, ma non è un quadrato modulo p per $p = 3, 5, 11, 19$.
   (b) Dimostrare che 2 è un quadrato modulo p se e solo se $p \equiv \pm 1 \pmod 8$.
   (Sugg. http://en.wikipedia.org/wiki/Gauss's_lemma_(number_theory))

PER IL SEGUENTE ESERCIZIO È UTILE UN COMPUTER.

9. (Esperimento fattorizzare usando il metodo "$p - 1$") Sia $M = 2^3 \cdot 3^2 \cdot 5 \cdot 7$
   (a) Sia $n = 95431706263$. Scegliere $\overline{a} \in \mathbf{Z}_n^*$ a caso. Calcolare $\overline{b} = \overline{a}^M \pmod n$. Calcolare il divisore $d = \mathrm{mcd}(b - 1, n)$ di n ed il cofattore n/d.
   (b) Sia $n = 57841557763361$. Scegliere $\overline{a} \in \mathbf{Z}_n^*$ a caso. Calcolare $\overline{b} = \overline{a}^M \pmod n$. Calcolare il divisore $d = \mathrm{mcd}(b - 1, n)$ di n ed il cofattore n/d.
   (c) Come mai l'algoritmo trova queste due fattorizzazioni?