1. Sia $n \in \mathbf{Z}$ e sia p un divisore primo di n^2+1. Dimostrare che $p = 2$ oppure $p \equiv 1 \pmod 4$.

2. Il *repunit* R_n è un numero naturale, la cui espansione decimale consiste in n uni: $11111\ldots111$. Per esempio, $R_5 = 11111$.
   (a) Dimostrare che se R_n è primo, allora anche n è primo.
   (b) Sia $n > 3$ primo. Dimostrare che ogni divisore primo di R_n è congruo a $1 \pmod n$.

3. 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 distinti di n.
   (c) Determinare H per $n = 91$.

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.

5. 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 $\mathbf{Z}_p^*$?

6. 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 $a/\mathrm{mcd}(a,k)$.

7. (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 $\frac{1}{n}$ (Suggerimento: si veda http://www.mat.uniroma2.it/∼eal/decimali.pdf).
   (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.

PER I SEGUENTI ESERCIZI È UTILE UN COMPUTER.

7. (Pollard ρ) Sia p un numero primo e $f : \mathbf{Z}_p \longrightarrow \mathbf{Z}_p$ la funzione data da $\overline{x} \mapsto \overline{x^2+1}$. Per $p = 41$ e 61 disegnare il seguente grafo diretto: i vertici sono le classi $\overline{x} \in \mathbf{Z}_p$. Esiste una freccia da $\overline{x}$ verso $\overline{y}$ se e soltanto se $f(\overline{x}) = \overline{y}$.

9. Implementare l'algoritmo ρ di Pollard e usarlo per
   (a) fattorizzare i numeri di Mersenne M_n per $1 \leq n \leq 60$;
   (b) fattorizzare i numeri di Fermat F_n, per $1 \leq n \leq 8$.

10. (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?