Notazione: Indichiamo con $\log n$ il logaritmo di n in base 2 e con $\ln n$ il logaritmo naturale di n , in base e . Alcuni esercizi richiedono PARI/GP.

Attenzione: i links ai file vanno ribattuti completamente (col copia-incolla non funzionano).

1. Siano dati i numeri

$$\begin{aligned} n1 &= \text{nextprime}(10^5) * \text{nextprime}(10^{10}), & n2 &= \text{nextprime}(10^6) * \text{nextprime}(10^{10}), \\ n3 &= \text{nextprime}(10^7) * \text{nextprime}(10^{10}), & n3 &= \text{nextprime}(10^8) * \text{nextprime}(10^{10}), \\ n5 &= \text{nextprime}(10^{10}) * \text{nextprime}(10^{50}), & n6 &= \text{nextprime}(10^{10}) * \text{nextprime}(10^{100}), \\ n7 &= \text{nextprime}(10^{10}) * \text{nextprime}(10^{200}), & n8 &= \text{nextprime}(10^{10}) * \text{nextprime}(10^{400}). \end{aligned}$$

- (a) Fattorizzarli col metodo ρ di Pollard.
 - (b) Quante iterate dobbiamo aspettarci di fare nei singoli casi?
 - (c) Come varia il numero di operazioni necessarie a fattorizzare $n5, n6, n7, n8$?
2. 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 $1 \leq n \leq 8$.
 3. Sia n un numero intero composto di 200 cifre. Dopo 10000 iterazioni l'algoritmo di Pollard ρ non ha trovato nessun fattore. Cosa possiamo concludere?
 4. Sia n un numero intero composto di 200 cifre, e sia $B = 10000$. Dopo quante iterazioni dell'algoritmo di Pollard ρ possiamo verosimilmente che escludere che n sia B -smooth (cioè che si decomponga in fattori primi minori o uguali a B , elevati ad opportuni esponenti)?
 5. Sia n un intero da fattorizzare. Stimare il numero di operazioni necessarie a fattorizzare un intero n col metodo ρ di Pollard ogni volta che n diventa dieci volte più grande: osservare la differenza fra il caso in cui il fattore più piccolo p ha una cifra decimale in più e il caso in cui il quoziente $\frac{n}{p}$ ha una cifra decimale in più (mentre p resta fisso).
 Esempio1: <http://www.mat.uniroma2.it/~geo2/pollard-exper1.txt>
 N.B.: Nel caso del metodo ρ di Pollard la stima è probabilistica: se ripetiamo il calcolo con gli stessi dati, impieghiamo sempre lo stesso tempo?
 6. Sia n un intero da fattorizzare. Stimare la complessità (probabilistica) del metodo di fattorizzazione che consiste nel calcolare il massimo comun divisore fra n e un numero a caso $1 \leq m \leq n$.
 7. Dimostreremo che se p è un numero primo ed $f \in \mathbb{Z}_p[X]$ è un polinomio di grado n a coefficienti in $\mathbb{Z}_p$ (ossia $f(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$, con $a_i \in \mathbb{Z}_p$ e $a_n \neq 0$), allora f ha al più n zeri in $\mathbb{Z}_p$.
 - (a) Sia $p > 2$ un primo. Determinare tutti gli zeri di $f(\bar{x}) = \bar{x}^2 - \bar{1} \in \mathbb{Z}_p[X]$.
 - (b) Sia $p = 11$. Determinare tutti gli zeri di $f(\bar{x}) = \bar{x}^2 - \bar{1} \in \mathbb{Z}_p[X]$. Determinare tutti gli zeri di $f(\bar{x}) = \bar{x}^2 - \bar{2} \in \mathbb{Z}_p[X]$.
 8. Enunciare e verificare il Lemma di Gauss (il Lemma 1 della nota sulla radice primitiva) per $n = 60$.
 9. Verificare che $p = 61$ è primo. Quali sono gli ordini possibili per gli elementi $\bar{x} \in \mathbb{Z}_p^*$? Quanti ce ne sono per ogni ordine? (vedi: Osservazione sulla formula di Gauss, nella nota sulla radice primitiva). Che ordine deve avere un generatore di $\mathbb{Z}_{61}^*$?
 10. Sia $p = 13$. Quali sono gli ordini possibili per gli elementi $\bar{x} \in \mathbb{Z}_p^*$? Quanti ce ne sono per ogni ordine?(vedi: Osservazione sulla formula di Gauss, nella nota sulla radice primitiva). Determinarli (vedi Lemma 2 della nota sulla radice primitiva).