TEN 2018. Esercizi1.

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.

1. Creare due interi di 600 cifre $N_1 = p*q$ ed $N_2 = p*r$, dove p, q, r sono primi di circa 300 cifre. Verificare che il comando $\gcd(N_1, N_2)$ calcola il fattore comune, anche se i numeri non sarebbero fattorizzabili con gli algoritmi a disposizione.

2. Creare un kit di chiavi RSA $N,\ E,\ D$, con $N = pq$ prodotto di primi di circa 300 cifre. Verificare che a partire da $N,\ E,\ D$ si possono ottenere i fattori p e q. Vedi:
   `http://www.mat.uniroma2.it/~geo2/TEN/RSAattack.txt`.

3. Verificare che i numeri di Carmichael

   $$321197185, \quad 9746347772161, \quad 8767496993623482137760 1, \quad 3280942684035956499117717275424 1$$

   passano il test del Piccolo Teorema di Fermat, ma non il test di Miller-Rabin. Vedi:
   `http://www.mat.uniroma2.it/~geo2/TEN/MRsteps.txt`.

4. Sia $F\colon \mathbb{Z}_{15} \to \mathbb{Z}_3 \times \mathbb{Z}_5, \quad \bar{x} \mapsto (\bar{x} \bmod 3, \bar{x} \bmod 5)$.
   (a) Determinare esplicitamente $F(\bar{x})$, per ogni $\bar{x} \in \mathbb{Z}_{15}$.
   (b) Verificare che $F(\mathbb{Z}_{15}^*) = \mathbb{Z}_3^* \times \mathbb{Z}_5^*$.

5. Sia n un intero composto, *senza fattori quadratici* (i.e. nella decomposizione di n in fattori primi, i primi appaiono con esponente 1), con la seguente proprietà

   $$\textit{se } p \textit{ divide } n, \textit{ allora } p-1 \textit{ divide } n-1.$$

   Verficare che n passa il Test del Piccolo Teorema di Fermat per ogni a con $\gcd(a, n) = 1$.