TEN 2019. Esercizi2.

**Notazione:** Indichiamo con $\log n$ il logaritmo di $n$ in base 2 e con $\ln n$ il logaritmo naturale di $n$, in base $e$.

1. Determinare le soluzioni dell'equazione $\bar{x}^2 = \bar{1}$ in $\mathbb{Z}_{11}$ e in $\mathbb{Z}_{21}$.

2. 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 $\gcd(a, n) = 1$.

3. Siano $E_1$ ed $E_2$ due interi tali che $\gcd(E_1, E_2) = 1$ e sia $N$ un intero positivo. Supponiamo di conoscere $m^{E_1} \bmod N$ e $m^{E_2} \bmod N$. Mostrare che da questi dati e' possibile ricavare $m$.

**Esercizi che richiedono PARI/GP:**

4. Verificare che $p = 2017$ è primo. Enunciare il Piccolo Teorema di Fermat per $p = 2017$. Verificarlo per qualche intero $x$ a caso che soddisfa $\gcd(x, 2017) = 1$.
5. Applicare il Piccolo Teorema di Fermat agli interi 67867, 7777853 e 8768767. Cosa se ne può dedurre?
6. Verificare che $n = 8911$ è 3-pseudoprimo, ma **non** è 2-pseudoprimo e **non** è 5-pseudoprimo.

7. Verificare che i numeri di Carmichael

$$321197185, \quad 9746347772161, \quad 87674969936234821377601, \quad 328094268403595649911771727542 41$$

   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`.

8. 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`.