TEN 2016. Esercizi 2.

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. Siano E_1 ed E_2 numeri naturali con $gcd(E_1, E_2) = 1$. Determinare m, conoscendo
$$m^{E_1} \mod N \qquad \text{ed} \qquad m^{E_2} \mod N.$$

2. Costruire un KIT di chiavi $\{N = p \cdot q,\ E, D\}$ per un utente del sistema crittografico RSA, con p, q primi dell'ordine di grandezza di 10^{250} (usare PARI-GP). Spedire all'utente il messaggio
$$m = 10000$$
dopo averlo criptato. Provate poi a decriptarlo con la chiave segreta.
Qual è la complessità totale di tutta l'operazione? E scegliendo p, q dell'ordine di grandezza di 10^{400}?

3. Calcolare $\varphi(2016)$ e $\varphi(9659869876987)$.

4. Vedi la Nota sulla funzione φ di Eulero per altri esercizi su φ.

5. Verificare che $p = 347$ è primo. Enunciare il Piccolo Teorema di Fermat per $p = 347$. Verificarlo per qualche classe a caso $\bar{x} \in \mathbb{Z}_p^*$.

6. Sia n un intero. Supponiamo che per ogni divisore primo p di n valga $p - 1 \,|\, n - 1$. Allora per ogni a con $\gcd(a, n) = 1$, vale
$$a^{n-1} \equiv 1 \mod n.$$

7. Verificare che i numeri di Carmichael
$$561,\ 1729,\ 2465,\ 2821,\ 6601,\ 41041,\ 825265,\ 321197185,\ 9746347772161$$
soddisfano le condizioni dell'esercizio precedente (fattorizzarli con PARI-GP e controllare). Verificare che superano il test di primalità basato sul Piccolo Teorema di Fermat, ma non il test di Miller-Rabin (possibilmente ripetuto per basi diverse). Per Test di Miller-Rabin potete usare
`http://www.mat.uniroma2.it/~geo2/TEN/MRsteps.txt`.

8. Sia $n = pq$, con p e q primi. Sia $\bar{x}_0 \neq \pm\bar{1}$ un elemento di $\mathbb{Z}_{pq}^*$ che soddisfa $\bar{x}_0^2 = \bar{1}$.
   (a) Verificare che n non è $\bar{x}_0$-pseudoprimo.
   (b) Determinare x_0 come sopra per $n = 21$.

9. Sperimentare col comando `nextprime( )` in Pari/GP.
   (a) Sia $n = 10^{10} + 47865876$ un numero di 10 cifre. Di quante cifre differisce approssimativamente da n il numero primo successivo?
   (b) Sia $n = 10^{100} + 47547645$ un numero di 100 cifre. Di quante cifre differisce approssimativamente da n il numero primo successivo?
   (c) Sia $n = 10^{500} + 6546546457657$ un numero di 500 cifre. Di quante cifre differisce approssimativamente da n il numero primo successivo?

10. Stimare il numero di primi
$$10^{40}-500 \le p \le 10^{40}+500, \qquad 10^{100}-1000 \le p \le 10^{100}+1000, \qquad 10^{100}-3000 \le p \le 10^{100}+3000.$$
Vai su `http://www.mat.uniroma2.it/~geo2/TEN/Primes.txt` e confronta...

11. Stimare la probabilità che un numero intero a caso dell'ordine di grandezza di 10^{200} sia primo. Quanti numeri primi possiamo aspettarci all'incirca nell'intervallo $[N - A, N + A]$, con $N = 10^{200}$ ed $A = 1500$? Quante cifre in comune avranno approssimativamente tali primi? Confrontare il risultato costruendo la lista effettiva dei primi nell'intervallo dato e sperimentando col comando *nextprime* in PARI-GP.
Ripetere con $N = 10^{350}$ ed $N = 10^{350} + 7657965$ ed $A = 1500$.