TEN 2017. 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:

? presenta la lista dei comandi divisi per argomento
?4 presenta la lista dei comandi utili in Teoria ei Numeri "NUMBER THEORETICAL functions"
?comando spiega l'uso del comando.

Esempi:
gcd(986987987,69797987)
43
bezout(986987987,69797987)
[-216252, 3057941, 43]

gcd(7538415671,3674509)
1
bezout(7538415671,3674509)
[609569, -1250557422, 1]

Mod(3674509, 7538415671)$^{-}$1
Mod(6287858249, 7538415671)

Mod(-1250557422,7538415671)
Mod(6287858249, 7538415671)

isprime(76876876)
0

factor(76876876)
[ 2 2]
[19219219 1]

1. Sia $n = 5956986598$. Decidere se le classi di congruenza modulo $n$ dei seguenti numeri appartengono o meno a $\mathbb{Z}_n^*$: $56893415,\ 3674509,\ 92367458$.
2. A partire dalla relazione $2804991 \cdot 657657 - 260518 \cdot 7080977 = 1$, calcolare:

$$\gcd(657657, 7080977), \quad \gcd(2804991, 260518); \quad \overline{260518}^{-1} \in \mathbb{Z}_{2804991}^*.$$

   Quali altri inversi possiamo ottenere dalla stessa relazione?
3. Sia $n = 2017$. Esibire qualche elemento di $\mathbb{Z}_{2017}^*$. Calcolare $2^{-1}$ in $\mathbb{Z}_{2017}^*$.
4. Calcolare $\varphi(15^3 \cdot 33 \cdot 2^4 \cdot 27)$.
5. Sia $n$ un intero positivo e sia $p$ un divisore primo di $n$. Verificare che:
   (a) $\varphi(p) \mid \varphi(n)$;
   (b) se $p^2 \nmid n$, allora $\varphi(n) = \varphi(p)\varphi(\frac{n}{p})$
   (c) se $p \mid \frac{n}{p}$, allora $\varphi(\frac{n}{p}) = \frac{n}{p}\prod_d(1 - \frac{1}{d})$, dove $d$ varia fra i divisori primi di $n$.
6. Siano dati due primi $p, q$ primi dell'ordine di grandezza di $10^{250}$. Costruire un KIT di chiavi $\{N = p \cdot q,\ E, D\}$ per un utente del sistema crittografico RSA. Spedire all'utente il messaggio

$$m = 11111$$

   dopo averlo criptato. Provare 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 $10^{400}$?

7. Siano $E_1$ ed $E_2$ numeri naturali con $gcd(E_1, E_2) = 1$. Determinare $m$, conoscendo

$$m^{E_1} \mod N \qquad \text{ed} \qquad m^{E_2} \mod N.$$

8. Verificare che $p = 2017$ è primo. Enunciare il Piccolo Teorema di Fermat per $p = 2017$. Verificarlo per qualche intero $x$ a caso che soddisfa $\gcd(x, 2017) = 1$.
9. Usare il Piccolo Teorema di Fermat per determinare (possibilmente...) se gli interi 67867, 7777853 e 8768767 sono o meno composti.
10. Determinare le soluzioni dell'equazione $\bar{x}^2 = \bar{1}$ in $\mathbb{Z}_{11}$ e in $\mathbb{Z}_{15}$.