TEN 2013-2014. Esercizi sugli argomenti delle prime 2 settimane di corso.

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. Sia $n = 7538415671$. Decidere se le classi di congruenza modulo n dei seguenti numeri stanno in $\mathbb{Z}_n^*$ o meno: 56893415, 3674509, 92367458.
2. A partire dalla relazione $62 \cdot 61728 - 97 \cdot 39455 = 1$, calcolare:
$$\gcd(62, 97), \quad \gcd(62, 39455), \quad \gcd(61728, 97), \quad \gcd(61728, 39455), \quad \overline{62}^{-1} \in \mathbb{Z}_{97}.$$
Quali altri inversi possiamo ottenere?
3. Fattorizzare $n = 1925$. Esibire qualche elemento di $\mathbb{Z}_{1925}^*$.
4. Verificare che $p = 347$ è primo. Enunciare il Piccolo Teorema di Fermat per $p = 347$. Verificarlo per qualche classe a caso $\bar{x} \in \mathbb{Z}_p^*$.
5. Sia n un intero privo di fattori quadratici (nella decomposizione di n in fattori primi non ci sono fattori al quadrato). Supponiamo che per ogni divisore primo p di n valga $p - 1 \mid n - 1$. Allora per ogni a con $\gcd(a, n) = 1$, vale
$$a^{n-1} \equiv 1 \mod n.$$
6. Verificare che i numeri di Carmichael
$$561,\ 1729,\ 2465,\ 2821,\ 6601,\ 41041,\ 825265,\ 321197185,\ 9746347772161$$
soddisfano le condizioni dell'esercizio precedente (fattorizzarlo 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/MRsteps.txt`.
7. 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}?
8. Siano E_1 ed E_2 numeri naturali con $gcd(E_1, E_2) = 1$. Conoscendo
$$m^{E_1} \mod N \qquad \text{ed} \qquad m^{E_2} \mod N,$$
determinare m.