Teoria Elementare dei Numeri Appello 4 13 luglio 2018, ore 16-18.

COGNOME ..... *NOME* .....

Inserire le risposte negli spazi predisposti, accompagnandole con *spiegazioni chiare e sintetiche*.
NON SI ACCETTANO RISPOSTE SCRITTE SU ALTRI FOGLI. Ogni esercizio vale 6 punti.

1. Sia φ la funzione di Eulero.
   (a) Dimostrare che se $n \in \mathbf{N}$ è dispari, allora $\varphi(n) = \varphi(2n)$.
   (b) Dimostrare che se $n \in \mathbf{N}$ è pari, allora $\varphi(n) \neq \varphi(2n)$.

2. (a) Descrivere brevemente il criptosistema a chiave pubblica RSA.
   (b) Supponiamo di voler costruire un kit di chiavi $\{N = pq, E, D\}$, con p, q primi di 300 cifre.
   (c) Come si costruisce uno pseudoprimo di 300 cifre? Qual è la complessità dei calcoli necessari?

3. Sia E la curva di equazione $Y^2 = X^3 - 2X$.
   (a) Verificare che E è una curva ellittica su $\mathbf{Z}_7$.
   (b) Determinare tutti i punti di $E(\mathbf{Z}_7)$.
   (c) Determinare la struttura del gruppo $E(\mathbf{Z}_7)$.
   (d) Esibire un punto di ordine massimo possibile in $E(\mathbf{Z}_7)$.

4. Sia dato il primo $p = 37$.
   (a) Determinare la più piccola radice primitiva di $\mathbf{Z}_{37}^*$.
   (b) Quante radici primitive ci sono in $\mathbf{Z}_{37}^*$?
   (c) Calcolare il logaritmo discreto di $\bar{7}$ e di $\bar{5}$ rispetto alla radice primitiva trovata al punto (a).

5. Sia E la curva ellittica di equazione $Y^2 = X^3 + 3X + 4$ su $\mathbf{Z}_{59}$ e sia P il punto $(0, 2)$ su $E(\mathbf{Z}_{59})$.
   (a) Verificare che $2P = (19, 28)$.
   (b) Sapendo che $3P$ ha ordine 9, determinare la cardinalità del gruppo $E(\mathbf{Z}_{59})$.