Teoria Elementare dei Numeri | Appello 2 | 28 febbraio 2013, ore 10-12.

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 $p = 7$ e sia data la curva $E: \quad Y^2 = X^3 + X$.
   (a) Verificare che E definisce una curva ellittica su $\mathbf{Z}_7$.
   (b) Determinare tutti i punti di $E(\mathbf{Z}_7)$.
   (c) Determinare se il gruppo $E(\mathbf{Z}_7)$ è o meno ciclico, motivando bene la risposta.

2. Determinare tre punti P, Q, R (diversi dal punto all'infinito...) sulla curva ellittica dell'esercizio 1, tali che
$$P + Q + R = \infty.$$

3. Sia $p = 61$. Fissiamo g una radice primitiva in $\mathbf{Z}_{61}$; per $\log a$ intendiamo il logaritmo discreto di $a \in \mathbf{Z}_p^*$ rispetto a g.
   (a) Dimostrare che $6 \log 2 = \log 3$.
   (b) Dimostrare che $2 \log 2 + \log 3 + \log 5 = 30$.
   (c) Dedurre che $\log 5 = 30 - 8 \log 2$.

4. Siano $N = 10^{1000}$ ed $A = 10^{100}$. Determinare quanti numeri primi ci sono approssimativamente nell'intervallo $[N - A, N + A]$.

5. Sia p un numero primo. Sia $\bar{a}$ una radice primitiva in $\mathbf{Z}_p^*$. Descrivere il metodo Baby-Step-Giant-Step per la risoluzione del logaritmo discreto in $\mathbf{Z}_p^*$.