Teoria Elementare dei Numeri | Appello 1 | 8 febbraio 2012, ore 14-16.

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) Calcolare $\varphi(2448)$, spiegando quali proprietà della funzione φ vengono usate.
   (b) Enunciare il Teorema di Lagrange per il gruppo $\mathbf{Z}_{2448}^*$.
   (c) Esibire una classe $\bar{x} \in \mathbf{Z}_{2448}$ per cui non vale l'enunciato del punto (b).

2. Sia E la curva di equazione $Y^2 = X^3 - 2X$ su $\mathbf{Z}_{11}$.
   (a) Verificare che E è una curva ellittica su $\mathbf{Z}_{11}$.
   (b) Verificare che i punti $P = (2, 2)$ e $Q = (-1, 1)$ appartengono a $E(\mathbf{Z}_{11})$.
   (c) Determinare un punto $R \in E(\mathbf{Z}_{11})$, tale che $P + Q + R = \infty$.
   (d) Determinare se in $E(\mathbf{Z}_{11})$ ci sono punti di ordine due.

3.(a) Verificare che $\bar{g} = \bar{5}$ è una radice primitiva in $\mathbf{Z}_{47}^*$.

(b) Calcolare $\log(17)$ in $\mathbf{Z}_{47}^*$ rispetto alla radice primitiva $\bar{g} = \bar{5}$.
Volendo, avete a disposizione le seguenti relazioni modulo 47

$$-2 \equiv 45 \equiv 3^2 \cdot 5, \quad 1 \equiv 48 \equiv 2^4 \cdot 3, \quad 4 \equiv 51 \equiv 3 \cdot 17.$$

4. A partire dalle relazioni $62^2 \equiv 2 \cdot 3^4 \cdot 5 \mod 1517$, $71^2 \equiv 2 \cdot 5 \cdot 7^2 \mod 1517$, determinare un fattore non banale di 1517 (almeno delineare il metodo).

5. Sia n un numero intero composto di 200 cifre e sia $B = 10000$. Dopo quante iterazioni (a vuoto) dell'algoritmo ρ di Pollard possiamo verosimilmente concludere che n non è B-smooth? (giustificare la risposta).