Teoria Elementare dei Numeri — Appello 2 — 22 febbraio 2011, 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 7,5 punti.

---

1. Sia E la curva di equazione $Y^2 = X^3 + X + 3$.
   (a) Verificare che E è una curva ellittica su $\mathbf{Z}_{11}$.
   (b) Determinare tutti i punti di $E(\mathbf{Z}_{11})$.
   (c) Sia $P = (7, 1)$. Calcolare $2P$ e $4P$.
   (d) Decomporre $E(\mathbf{Z}_{11})$ come prodotto di gruppi ciclici.

2. Determinare se 2 è o meno un quadrato modulo il numero primo $p = 67$.

3. Sia $m = 3 \cdot 5 \cdot 7 = 105$. Quante soluzioni ha l'equazione $x^2 \equiv 1$ in $\mathbf{Z}_{105}^*$? Determinarne 3 distinte.

4. Siano dati il numero primo $p = 227$ e la radice primitiva $g = 2$ in $\mathbf{Z}_{227}^*$. Conosciamo le seguenti congruenze:

$$2^{20} \equiv 3^2 \cdot 7, \qquad 2^{57} \equiv 3 \cdot 5, \qquad 2^{128} \equiv 3 \cdot 7^2, \qquad \text{mod } 227.$$

Usare queste informazioni per ottenere i logaritmi $\log 3$, $\log 5$, $\log 7$ in base $g = 2$. (Può essere utile sapere che l'inverso di 3 modulo 226 è 151.)