Teoria Elementare dei Numeri | Appello 2 | 28 febbraio 2012, ore 11-13.

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. Determinare tutte le soluzioni dell'equazione $\bar{x}^2 = \bar{4}$ in $\mathbf{Z}_{21}^*$ (almeno delineare bene il metodo).

2. Sia E la curva di equazione $Y^2 = X^3 + 1$ su $\mathbf{Z}_5$.
   (a) Verificare che si tratta di una curva ellittica.
   (b) Determinare l'ordine del punto $(2, 2)$ nel gruppo $E(\mathbf{Z}_5)$.
   (c) Determinare la struttura del gruppo $E(\mathbf{Z}_5)$.

3. Il signor Rossi e il signor Bianchi desiderano condividere un codice segreto e lo fanno adottando il sistema Diffie-Hellman-Merkle. Si accordano pubblicamente sul numero primo $p = 37$ e sulla radice primitiva $\bar{g} = \bar{2}$.
   (a) Verificare che $\bar{g} = \bar{2}$ è effettivamente una radice primitiva in $\mathbf{Z}_{37}^*$.
   (b) Una spia intercetta i numeri $\overline{n} = \overline{17}$ e $\overline{m} = \overline{13}$ che vengono scambiati fra Bianchi e Rossi. Cosa deve fare per ricostruire il codice segreto di Bianchi e Rossi?
   (c) La spia ricostruisce il codice segreto. Qual è questo codice?

4. Sia p un primo, $p \equiv 3 \mod 4$. Sia $a \in \mathbf{Z}_p^*$ un quadrato. Verificare che $a^{\frac{p+1}{4}}$ è una radice quadrata di a in $\mathbf{Z}_p^*$.

5. Stiamo cercando di fattorizzare l'intero n usando il metodo delle curve ellittiche, con smoothness bound B fissato. Dopo 1000 iterazioni troviamo il fattore primo p usando la curva ellittica E. Quale proprietà verosimilmente ha $E(\mathbf{Z}_p)$, che le precedenti 999 curve ellittiche su $\mathbf{Z}_p$ non avevano?