Teoria Elementare dei Numeri Appello 1 8 febbraio 2010, 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 data la seguente informazione $446 \cdot 101 - 45 \cdot 1001 = 1$.
   (a) Calcolare $\gcd(101, 1001)$.
   (b) Calcolare $\overline{101}^{-1}$ in $\mathbf{Z}_{1001}^*$ e $\overline{1001}^{-1}$ in $\mathbf{Z}_{101}^*$.

(a) Se vale $446 \cdot 101 - 45 \cdot 1001 = 1$, allora $\gcd(101, 1001)$ necessariamente divide 1. Di conseguenza è uguale a 1.

(b) La stessa equazione ci dice che $101 \cdot 446 \equiv 1 \mod 1001$: dunque $\overline{101}^{-1} = \overline{446}$ in $\mathbf{Z}_{1001}^*$. Similmente possiamo dedurre che $1001 \cdot (-45) \equiv 1 \mod 101$. Dunque $\overline{-45} = \overline{56} = \overline{1001}^{-1}$ in $\mathbf{Z}_{101}^*$.

2. Sia E la curva di equazione $Y^2 = X^3 + 3$.
   (a) Verificare che E è una curva ellittica su $\mathbf{Z}_7$.
   (b) Determinare tutti i punti di $E(\mathbf{Z}_7)$.
   (c) Scegliere un punto su $E(\mathbf{Z}_7)$. Che ordine ha?

(a) Il discriminante di E è dato da $27 \cdot 3^2 \equiv 5 \not\equiv 0 \mod 7$. Quindi E è una curva ellittica su $\mathbf{Z}_7$.

(b) I quadrati in $\mathbf{Z}_7$ sono $Q = \{\bar{0}, \bar{1}, \bar{2}, \bar{4}\}$ e le rispettive radici quadrate sono date da :

$$\{\bar{0}\}, \quad \{\bar{1}, \bar{6}\}, \quad \{\bar{3}, \bar{4}\}, \quad \{\bar{2}, \bar{5}\}.$$

Dalla seguente tabella segue che punti di $E(\mathbf{Z}_7)$ sono 13: il punto all'infinito e i seguenti punti al finito

X	$X^3 + 3 = Y^2$	Y	Punti
0	3	$\emptyset$	$\emptyset$
1	4	2, 5	(1,2), (1,5)
2	4	2, 5	(2,2), (2,5)
3	2	3, 4	(3,3), (3,4)
4	4	2, 5	(4,2), (4,5)
5	2	3, 4	(5,3), (5,4)
6	2	3, 4	(6,3), (6,4)

(c) Poiché il gruppo $E(\mathbf{Z}_7)$ ha ordine 13 (primo), è necessariamente ciclico. Poiché l'ordine di un elemento divide l'ordine del gruppo, tutti i punti di $E(\mathbf{Z}_7)$ hanno ordine 13.

3. Sia E la curva ellittica di equazione $Y^2 = X^3 + X + 1$ e sia $E(\mathbf{Z}_{11})$ il gruppo dei punti della curva su $\mathbf{Z}_{11}$.
   (a) Verificare che i punti $P = (1, 5)$ e $Q = (0, 1)$ appartengono ad $E(\mathbf{Z}_{11})$.
   (b) Calcolare $P + Q$, $-P$, $2Q$.

(a) Basta verificare che le coordinate di P e Q soddisfano l'equazione della curva (modulo 11):

$$25 \equiv 1 + 1^2 + 1 \equiv 3 \mod 11, \qquad 4 \equiv 3^3 + 3^2 + 1 \equiv 37 \mod 11.$$

(b) Dalle formule di addizione e di duplicazione troviamo

$$P + Q = (4, 5), \quad 2Q = (3, 3),$$

mentre $-P = (1, -5) = (1, 6)$.

4. Sia $p = 19$.
   (a) Verificare che $\bar{2}$ è una radice primitiva in $\mathbf{Z}_{19}^*$.
   (b) Calcolare $\log(5)$ rispetto alla radice primitiva $\bar{2}$.

(a) Abbiamo che $p - 1 = 18 = 2 \cdot 3^2$. Poiché $\bar{2}^9 \equiv \overline{-1} \not\equiv \bar{1} \mod 19$ e $\bar{2}^6 \equiv \bar{7} \not\equiv \bar{1} \mod 19$, si ha che effettivamente $\bar{2}$ è una radice primitiva in $\mathbf{Z}_{19}^*$.

(b)