Teoria Elementare dei Numeri — Appello 3 — 28 maggio 2009, ore 18–20.

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 $Y^2 = X^3 - 2X + 1$ su $\mathbf{Z}_{13}$.
   (a) Verificare che E è una curva ellittica su $\mathbf{Z}_{13}$.
   (b) Verificare che $P = (11, 6)$ e $Q = (9, 7)$ appartengono a $E(\mathbf{Z}_{13})$ e calcolare $P + Q$.
   (c) Determinare tutti i punti di $E(\mathbf{Z}_{13})$.

(a) Il discriminante della curva è $\Delta = 27 \cdot 1^2 + 4(-2)^3 \equiv 8 \not\equiv 0 \mod 13$. Quindi E definisce una curva ellittica su $\mathbf{Z}_{13}$.

(b) Sostituendo le coordinate di P e Q nell'equazione della curva si verifica che P e Q sono punti di $E(\mathbf{Z}_{13})$. Calcoliamo $P + Q$:
$m = y_2 - y_1)(x_2 - x_1)^{-1} \equiv 1 \cdot (-2)^{-1} \equiv 11^{-1} \equiv 6 \mod 13$
$x_3 = m^2 - x_1 - x_2 \equiv 3 \mod 13 \qquad y_3 = -(m(x_3 - x_1) + y_1) \equiv 3 \mod 13$
in totale $P + Q = (3, 3)$.

(c) I quadrati in $\mathbf{Z}_{13}$ sono $\{0, 1, 3, 4, 9, 10, 12\}$ e le rispettive radici quadrate sono:
$\sqrt{0} = 0, \ \sqrt{1} = 1, 12, \ \sqrt{3} = 4, 9, \ \sqrt{4} = 2, 11, \ \sqrt{9} = 3, 10, \ \sqrt{10} = 6, 7 \ \sqrt{12} = 5, 8 \mod 13.$
Per determinare tutti i punti "al finito" di $E(\mathbf{Z}_{13})$, calcoliamo $x^3 - 2x + 1$ al variare $x \in \mathbf{Z}_{13}$: ogni volta che $x^3 - 2x + 1$ è un quadrato modulo 13, si trovano due punti di $E(\mathbf{Z}_{13})$, possibilmente coincidenti, di coordinate rispettivamente $(x, \sqrt{x^3 - 2x + 1})$ e $(x, -\sqrt{x^3 - 2x + 1}) \mod 13$.
In questo caso i punti di $E(\mathbf{Z}_{13})$ risultano:

$$(0,1), \ (0,12), \ (1,0), \ (3,3), \ (3,10), \ (5,5), \ (5,8), \ (6,6), \ (6,7), \ (8,4), \ (8,9), \ (9,6), \ (9,7), \ (11,6), \ (11,7)$$

$$(\infty, \infty).$$

N.B. Le ultime due coppie di punti potevano essere determinate a partire dalla parte (b) dell'esercizio e dalle considerazioni precedenti.

2. Sia n un intero positivo.
   (a) Scrivere la formula generale per la funzione di Eulero $\varphi(n)$;
   (b) Calcolare $\varphi(616)$;
   (c) Scrivere $\mathbf{Z}_{616}^*$ come prodotto di gruppi ciclici.

(a) La funzione di Eulero è data da

$$\varphi(n) = n \prod_{p|n} (1 - \frac{1}{p}),$$

al variare di p fra i divisori primi distinti di n.

(b) Dal fatto che $616 = 2^3 \cdot 7 \cdot 11$, segue che $\varphi(616) = \varphi(2^3)\varphi(7)\varphi(11) = 4 \cdot 6 \cdot 10 = 240$.

(c) Per definizione $\varphi(616)$ è la cardinalità del gruppo $\mathbf{Z}_{616}^*$. Poiché $2, 7, 11$ hanno a due a due massimo comun divisore uguale a 1, si ha che $\mathbf{Z}_{616}^* \cong \mathbf{Z}_8^* \times \mathbf{Z}_7^* \times \mathbf{Z}_{11}^*$. Per il Teorema della Radice Primitiva, $\mathbf{Z}_7^*$ e $\mathbf{Z}_{11}^*$ sono gruppi ciclici di ordine rispettivamente 6 e 10. Dunque isomorfi rispettivamente a $\mathbf{Z}_6$ e $\mathbf{Z}_{10}$. Resta da esaminare $\mathbf{Z}_8^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$. Si verifica immediatamente che $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \mod 8$. Dunque tutti gli elementi di $\mathbf{Z}_8^*$ (diversi dall'identità) hanno ordine due. Ne segue che $\mathbf{Z}_8^* \cong \mathbf{Z}_2 \times \mathbf{Z}_2$ e

$$\mathbf{Z}_{616}^* \cong \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_6 \times \mathbf{Z}_{10}.$$

3. Sia $p = 61$.
   (a) Verificare che $\bar{2}$ è una radice primitiva di $\mathbf{Z}_{61}^*$.

(b) Determinare se $\bar{3}$ è una radice primitiva di $\mathbf{Z}_{61}^*$.
(c) Calcolare $\log(\bar{7})$ rispetto alla radice primitiva $\bar{2}$.

(a) Si ha che $\bar{2}$ è una radice primitiva di $\mathbf{Z}_{61}^*$ se e solo se $\bar{2}^{(p-1)/d} \not\equiv 1$, al variare di d fra $2, 3, 5$ che sono i divisori primi distinti di $p - 1 = 60$.
Infatti $\bar{2}^{12},\ \bar{2}^{20},\ \bar{2}^{30}\ \not\equiv 1 \mod 61$.

(b) Poiché $\bar{3}^{30}\ \equiv 1 \mod 61$, invece $\bar{3}$ non è una radice primitiva di $\mathbf{Z}_{61}^*$.

(c) Usiamo il calcolo dell'indice:

$$64 \equiv 3 \equiv 2^6 \mod 61, \qquad 63 \equiv 2 \equiv 3^2 \cdot 7 \mod 61.$$

Estraendo il logaritmo in base $\bar{2}$ e tenendo conto che $\log \bar{2} = 1$ troviamo

$$\log \bar{3} = 6 \log \bar{2} = 6 \qquad 2 \log \bar{3} + \log \bar{7} = \log \bar{2} = 1 \mod 60,$$

da cui

$$\log \bar{7} = 1 - 2 \log \bar{3} = 1 - 12 = 49 \mod 60.$$

4.(a) Richiamare la definizione di gruppo ciclico.
(b) Dare un esempio di gruppo ciclico di cardinalità maggiore o uguale a 6 (con le dovute spiegazioni).
(c) Determinare $\mathbf{Z}_{16}^*$ e verificare se è o meno un gruppo ciclico.

(a) Un gruppo $(G, \cdot)$ si dice ciclico se esiste un elemento $g_0 \in G$ con la propietà che ogni elemento di G è una opportuna potenza di g_0. In tal caso g_0 è un generatore di G.

(b) Per ogni $n \in \mathbf{Z}$, il gruppo $(\mathbf{Z}_n, +)$ è ciclico di ordine n, con generatore $\bar{1}$. Per ogni p primo, il gruppo $\mathbf{Z}_p^*$ è ciclico di ordine $p - 1$.
Sia ad esempio $p = 7$: $\mathbf{Z}_7^* = \{\bar{1},\ \bar{2},\ \bar{3},\ \bar{4},\ \bar{5},\ \bar{6}\}$. Si ha che $\bar{3}$ è un generatore di $\mathbf{Z}_7^*$. Infatti le potenze di $\bar{3}$ sono date da

$$\bar{3}^1 = \bar{3},\ \bar{3}^2 = \bar{2},\ \bar{3}^3 = \bar{6},\ \bar{3}^4 = \bar{4},\ \bar{3}^5 = \bar{5},\ \bar{3}^6 = \bar{1}$$

ed esauriscono tutto $\mathbf{Z}_7^*$.

(c) Il gruppo $\mathbf{Z}_{16}^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}, \bar{9}, \overline{11}, \overline{13}, \overline{15}\}$ ha cardinalità 8, quindi l'ordine dei suoi elementi può essere 2,4,8. Si verifica che ogni classe elevata alla quarta dà $\bar{1}$, per cui $\mathbf{Z}_{16}^*$ non è ciclico (un eventuale generatore dovrebbe avere ordine 8).