Teoria Elementare dei Numeri Appello 2 17 febbraio 2009, ore 9:30–11:30.

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. *Determinare tutte le soluzioni dell'equazione* $\bar{x}^2 \equiv \bar{4}$ *in* $\mathbf{Z}_{21}^*$. *A partire da esse determinare tutte le soluzioni intere della congruenza* $x^2 \equiv 4 \pmod{21}$ *e determinare quelle comprese nell'intervallo* $[-5, 20]$.

Sol. (a) Abbiamo

$$\bar{x}^2 \equiv \bar{4} \bmod 21 \quad \Leftrightarrow \quad \begin{cases} (\bar{x}+\bar{2})(\bar{x}-\bar{2}) \equiv \bar{0} \bmod 3 \\ (\bar{x}+\bar{2})(\bar{x}-\bar{2}) \equiv \bar{0} \bmod 7 \end{cases} \quad \Leftrightarrow$$

$$\begin{cases} \bar{x} \equiv \bar{2} \bmod 3 \\ \bar{x} \equiv \bar{2} \bmod 7 \end{cases} \bigcup \begin{cases} \bar{x} \equiv \bar{2} \bmod 3 \\ \bar{x} \equiv -\bar{2} \bmod 7 \end{cases} \bigcup \begin{cases} \bar{x} \equiv -\bar{2} \bmod 3 \\ \bar{x} \equiv \bar{2} \bmod 7 \end{cases} \bigcup \begin{cases} \bar{x} \equiv -\bar{2} \bmod 3 \\ \bar{x} \equiv -\bar{2} \bmod 7 \end{cases}.$$

Risolvendo i quattro sistemi troviamo le quattro soluzioni dell'equazione $\bar{x}^2 \equiv \bar{4}$ in $\mathbf{Z}_{21}^*$:

$$\bar{2}, \quad \overline{-2} \equiv \overline{19}, \quad \bar{5}, \quad \overline{-5} \equiv \overline{16}.$$

(b) Tutte le soluzioni intere dell'equazione si trovano a partire da una di esse aggiungendo un opportuno multiplo di 21:

$$2 + 21K, \quad 19 + 21M, \quad 5 + 21P, \quad 16 + 21Q, \qquad K, M, P, Q \in \mathbf{Z}.$$

(c) Le soluzioni comprese nell'i tervallo $[-5, 20]$ sono date da: $\{-5, -2, 2, 5, 16, 19\}$.

2. *Sia* $E(\mathbf{Z}_7)$ *la curva di equazione* $Y^2 = X^3 - 5X + 1$.
   (a) Verificare che $E(\mathbf{Z}_7)$ *è una curva ellittica e determinare tutti i punti di* $E(\mathbf{Z}_7)$.
   (b) Determinare se $E(\mathbf{Z}_7)$ *contiene punti di ordine 2.*
   (c) Sia $P = (0, 1) \in E(\mathbf{Z}_7)$. *Calcolare i multipli di* P *e determinare l'ordine di* P.

Sol. Il discriminante della curva è dato da $\Delta = 27 \cdot 1^2 + 4 \cdot 2^3 \equiv 3 \not\equiv 0 \bmod 7$. Dunque $E(\mathbf{Z}_{13})$ è una curva ellittica. Per determinare i punti di $E(\mathbf{Z}_7)$ osserviamo che i quadrati in $\mathbf{Z}_7$ sono:

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

Facendo variare $\bar{x} \in \mathbf{Z}_7$, calcoliamo $\bar{x}^3 - 5\bar{x} + \bar{1}$: a seconda se è o meno un quadrato modulo 7 determiniamo il punto o i punti di ascissa $\bar{x}$ etc...
Troviamo:

$$\bar{x} = \bar{0}, \quad \bar{x}^3 - 5\bar{x} + \bar{1} \equiv 1, \quad P_1 = (\bar{0}, \bar{1}), \ P_2 = (\bar{0}, \bar{6})$$

$$\bar{x} = \bar{1}, \quad \bar{x}^3 - 5\bar{x} + \bar{1} \equiv 4, \quad P_3 = (\bar{1}, \bar{2}), \ P_4 = (\bar{1}, \bar{5})$$

In tutti gli altri casi $\bar{x}^3 - 5\bar{x} + \bar{1}$ non è un quadrato.
Conclusione: la curva ellittica $E(\mathbf{Z}_7)$ ha i 4 punti qui sopra più il punto all'infinito. In particolare il gruppo ha ordine 5 ed è ciclico.
(b) La curva $E(\mathbf{Z}_7)$ non contiene punti di ordine 2: l'ordine di un elemento deve dividere l'ordine del gruppo...impossibile. Si può anche osservare che non ci sono punti con ordinata uguale a zero.
(c) A priori possiamo già dire che l'ordine di P è 5: ad ogni modo $P = (0, 1)$, $2P = (1, 5)$, $3P = (1, 2)$, $4P = (0, 6)$, $5P = (\infty, \infty)$.

3. *Sia* $p = 47$.
   (a) Determinare una radice primitiva $\bar{g}$ *in* $\mathbf{Z}_{47}^*$.
   (b) Calcolare log(2) *rispetto alla radice* $\bar{g}$.

Sol. (a) Abbiamo $p-1 = 46 = 2 \cdot 23$. Poiché $5^{23} \not\equiv 1 \bmod 47$ e $5^2 \not\equiv 1 \bmod 47$, abbiamo che 5 è una radice primitiva di $\mathbf{Z}_{47}^*$. (Non lo sono invece 2, 3, e 7).

(b) Usiamo il calcolo dell'indice:

$2.5^2 \equiv 3 \bmod 47$
$5.3^2 \equiv -2 \bmod 47$
da cui
$(2.5^2)^2.5 \equiv 3^2.5 \equiv -2 \bmod 47$
e quindi
$2 \equiv -5^{-5} \equiv 5^{18}$ (ricordiamo che $\log(-1) = (p-1)/2 = 23$).

In conclusione:

$$\log(2) = 18.$$

4. *Sia $p > 2$ un numero primo. Supponiamo che $a \in \mathbf{Z}$ sia un quadrato diverso da zero modulo p. Far vedere che:*
   (a) vale $a^{(p-1)/2} \equiv 1 \pmod{p}$;
   (b) Sia $p \equiv 3 \pmod 4$. Il numero $a^{(p+1)/4}$ è radice quadrata di a modulo p.

Sol. (a) Sia $a = g^2$. Allora, per il Piccolo Teorema di Fermat, vale

$$a^{(p-1)/2} = (g^2)^{(p-1)/2} = g^{p-1} \equiv 1 \bmod p.$$

(b) Se $p \equiv 3 \pmod 4$, allora $(p+1)/4$ è un intero e quindi $a^{(p+1)/4}$ è un elemento ben definito in $\mathbf{Z}_p^*$. Dobbiamo verificare che $(a^{(p+1)/4})^2 = a$. Infatti

$$(a^{(p+1)/4})^2 = a^{(p+1)/2} \equiv a^{(p-1)/2} \cdot a \equiv a.$$