Teoria Elementare dei Numeri 2016 Appello 2 24 febbraio 2017, 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 6 punti.

---

1. *(a) Spiegare se esiste o meno un elemento di ordine 8 in* $\mathbf{Z}_{55}^*$. *Se esiste esibirne uno.*
   (b) Spiegare se esiste o meno un elemento di ordine 10 in $\mathbf{Z}_{55}^*$. *Se esiste esibirne uno.*

Sol.: (a) $55 = 5 \cdot 11$ e per il teorema cinese del resto

$$\mathbf{Z}_{55} \cong \mathbf{Z}_5 \times \mathbf{Z}_{11} \quad \text{ed anche} \quad \mathbf{Z}_5^* \times \mathbf{Z}_{11}^*.$$

Quest'ultimo è il prodotto di un gruppo ciclico di ordine 4 e un gruppo ciclico di ordine 10 e l'ordine di un elemento $(\bar{x}, \bar{y}) \in \mathbf{Z}_5^* \times \mathbf{Z}_{11}^*$ è uguale a $mcm(ord(\bar{x}), ord(\bar{y}))$. In particolare è il *mcm* fra un divisore di 4 e un divisore di 10, ed è quindi un divisore di 20. Poiché 8 non è un divisore di 20, non esiste un elemento di ordine 8 in $\mathbf{Z}_{55}^*$.
(b) Se $\bar{a}$ è un generatore di $\mathbf{Z}_{11}^*$, ha ordine 10 in $\mathbf{Z}_{11}^*$ e l'elemento $(\bar{1}, \bar{a})$ ha ordine 10 in $\mathbf{Z}_5^* \times \mathbf{Z}_{11}^*$.

2. *Sia data la curva* $E: \quad Y^2 = X^3 + X + 1$.
   (a) Verificare che E *definisce una curva ellittica su* $\mathbf{Z}_5$.
   (b) Determinare tutti i punti di $E(\mathbf{Z}_5)$.
   (c) Sia $P = [3, 4] \in E(\mathbf{Z}_5)$. *Calcolare* $2P$ *e* $-P$.
   (d) Determinare la struttura del gruppo $(E(\mathbf{Z}_5), +)$.

Sol.: (a) Il discriminante della curva è $\Delta = 4A^3 + 27B^2 = 31 \equiv 1 \not\equiv 0 \mod 5$, per cui E definisce una curva ellittica su $\mathbf{Z}_5$.
(b) I quadrati in $\mathbf{Z}_5$ sono dati da $Q_5 = \{\bar{0}, \bar{1}, \bar{4}\}$, con radici quadrate $\sqrt{\bar{0}} = \bar{0}$, $\sqrt{\bar{1}} = \bar{1}, \bar{4}$, $\sqrt{\bar{4}} = \bar{2}, \bar{3}$.
I valori del polinomio $X^3 + X + 1$ su $\mathbf{Z}_5 = \{\bar{0}, \ldots, \bar{4}\}$ sono dati rispettivamente da $\bar{1},\ \bar{3},\ \bar{1},\ \bar{1},\ \bar{4}$.
Ne segue che i punti di $E(\mathbf{Z}_5)$ sono dati da

$$(\bar{0}, \bar{1}),\ (\bar{0}, \bar{4}),\ (\bar{2}, \bar{1}),\ (\bar{2}, \bar{4}),\ (\bar{3}, \bar{1}), (\bar{3}, \bar{4}),\ (\bar{4}, \bar{2}),\ (\bar{4}, \bar{3}),\ \infty.$$

(c) Sia $P = [3, 4]$. Troviamo $2P = [0, 4]$ e $-P = [3, 1]$. In particolare $2P \neq -P$.
(d) Il gruppo abeliano $(E(\mathbf{Z}_5), +)$ ha 9 elementi, quindi ci sono due possibilità:
è ciclico di ordine 9 isomorfo a $\mathbf{Z}_9$ (esiste almeno un elemento di ordine 9), oppure è isomorfo a $\mathbf{Z}_3 \times \mathbf{Z}_3$ (l'ordine di ogni elemento $\neq \infty$ è uguale a 3).
Il secondo caso è escluso, poiché $2P \neq -P$ che equivale a $3P \neq \infty$. Dunque l'ordine di P è maggiore di 3 e necessariamente uguale a 9 (deve essere un divisore di 9). Conclusione: siamo nel primo caso e $E(\mathbf{Z}_5) \cong \mathbf{Z}_9$.

3. *Sia* $p = 41$.
   (a) Verificare che $\overline{7}$ *è una radice primitiva di* $\mathbf{Z}_{41}$. *Quante ce ne sono?*
   (b) Calcolare $\log_{\overline{7}} \overline{33}$.

Sol.: (a) Abbiamo $p - 1 = 40 = 2^3 \cdot 5$, e $\overline{7}$ è una radice primitiva perché

$$\begin{cases} \overline{7}^8 \equiv 37 \not\equiv 1 \\ \overline{7}^{20} \equiv 40 \not\equiv 1 \end{cases} \mod 41.$$

In $\mathbf{Z}_{41}^*$, gruppo ciclico di ordine 40, ci sono $\varphi(40) = \varphi(2^3)\varphi(5) = (2^3 - 2^2)4 = 16$ radici primitive.
(b) Osserviamo intanto che $\log_{\overline{7}} \overline{33} = \log_{\overline{7}} \overline{3} + \log_{\overline{7}} \overline{11}$. Dalle relazioni modulo 41

$$3 \equiv 44 = 2^2 \cdot 11, \quad 2^2 \equiv 45 = 3^2 \cdot 5, \quad -1 \equiv 40 = 2^3 \cdot 5, \quad 1 \equiv 42 = 2 \cdot 3 \cdot 7,$$

otteniamo le relazioni fra i rispettivi logaritmi in base $\bar{7}$, modulo 40

$$\log 2+\log 3 \equiv -1, \quad 3\log 2+\log 5 \equiv 20, \quad -2\log 2+2\log 3+\log 5 \equiv 0, \quad 2\log 2-\log 3+\log 11 \equiv 0.$$

Tenendo conto che in base $\bar{7}$

$$\log 7 = 1, \quad \log(-1) = 20, \quad \log 1 = 0 \mod 40,$$

ricaviamo

$$\log 3 = 25, \quad \log 2 = 14, \quad \log 11 = 37 \mod 40,$$

da cui $\log_{\bar{7}} = 22$.

4. *Sia N un intero di circa 300 cifre. Quante iterate dell'algoritmo ρ di Pollard dobbiamo verosimilmente effettuare per escludere che N abbia fattori dell'ordine di 10^{10}?*

Sol.: Per il paradosso del compleanno un fattore dell'ordine di 10^{10} è individuato con alta probabilità dopo circa $\sqrt{10^{10}} = 10^5$ iterazioni dell'algoritmo ρ di Pollard.

5. *Sia $n = 52907$ e siano date le seguenti relazioni modulo n*

$$399^2 \equiv 2^5 \cdot 3 \cdot 5, \quad 763^2 \equiv 2^6 \cdot 3, \quad 773^2 \equiv 2^6 \cdot 3^5, \quad 976 \equiv 2 \cdot 5^3.$$

Quali sono possibili fattori non banali di n?

Sol.: Moltilicando fra loro la prima, la terza e la quarta equazione, otteniamo la relazione quadratica modulo n

$$\begin{aligned} & 399^2 \cdot 773^2 \cdot 976^2 \equiv (2^5 \cdot 3 \cdot 5) \cdot (2^6 \cdot 3^5) \cdot (2 \cdot 5^3) \\ \Leftrightarrow \quad & (399 \cdot 773 \cdot 976)^2 \equiv (2^6 \cdot 3^3 \cdot 5^2)^2 \\ \Leftrightarrow \quad & 36829^2 \equiv 43200^2. \end{aligned}$$

Poniamo $a = 36829$ e $b = 43200$. Allora $a + b \equiv 27122$ e $a - b \equiv 46536$ sono potenziali fattori non banali di n. Infatti

$$gcd(27122, 52907) = 191, \quad gcd(46536, 52907) = 277$$

e vale $52907 = 191 \cdot 277$.