Teoria Elementare dei Numeri Appello 1 30 giugno 2014, ore 15-17.

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. *Sia data la curva E di equazione $Y^2 = X^3 - X + 1$. Determinare un primo $p > 2$ tale che $E(\mathbf{Z}_p)$ sia una curva ellittica che contenga almeno un punto di ordine due.*

Sol.: Sia $E(\mathbf{Z}_p)$ una curva ellittica su $\mathbf{Z}_p$ (per p primo) con equazione di Weierstrass $Y^2 = X^3 + AX + B$. Un punto P (diverso da ∞) su $E(\mathbf{Z}_p)$ ha ordine due se $P + P = \infty$; equivalentemente, se $P = -P$. Poiché $-P$ ha ordinata opposta e quella di P, si ha che $P = (x, y)$ ha ordine due se e solo se $y = 0$ e x è una radice del polinomio di terzo grado $X^3 + AX + B$.

La curva $E: \quad Y^2 = X^3 - X + 1$ ha discriminante $\Delta = 4(-1)^3 + 27(1)^2 = 23$.
Per $p = 3$, $\Delta \equiv -1 \not\equiv 0$ modulo 3. Dunque $E(\mathbf{Z}_3)$ è una curva ellittica su $\mathbf{Z}_3$. Poiché il polinomio $X^3 - X + 1$ non ha zeri in $\mathbf{Z}_3$, la curva non ha punti di ordine due.
Per $p = 5$, $\Delta \equiv -2 \not\equiv 0$ modulo 5. Dunque $E(\mathbf{Z}_5)$ è una curva ellittica su $\mathbf{Z}_5$. Il punto $(3, 0) \in E(\mathbf{Z}_5)$ ed ha ordine due: 3 è uno zero del polinomio $X^3 + AX + B$. Volendo, si può verificare che $(3, 0) + (3, 0) = \infty \in E(\mathbf{Z}_5)$.

2. *Sia E la curva di equazione $Y^2 = X^3 - 4X - 1$ su $\mathbf{Z}_7$.*
   (a) Controllare che si tratta di una curva ellittica.
   (b) Determinare i punti di $E(\mathbf{Z}_7)$.
   (c) Determinare se $E(\mathbf{Z}_7)$ è o meno un gruppo ciclico, spiegando la risposta.

Sol.: (a) Il discriminante della curva è $\Delta = 4(-4)^3 + 27(-1)^2 \equiv -5 \not\equiv 0 \mod 7$. Quindi $E(\mathbf{Z}_7)$ è una curva ellittica.
(b)& (c) I quadrati in $\mathbf{Z}_7$ sono $Q = \{\bar{0}, \bar{1}, \bar{2}, \bar{4}\}$ e le rispettive radici quadrate sono

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

Calcolando i valori del polinomio $X^3 - 4X - 1$ al variare di $X \in \mathbf{Z}_7$ etc....troviamo

$$E(\mathbf{Z}_7) = \{(\bar{3}, \bar{0}),\ (\bar{6}, \bar{3}),\ (\bar{6}, \bar{4})\} \cup \infty.$$

Dunque $E(\mathbf{Z}_7)$ è un gruppo abeliano con quattro elementi, di cui uno solo $(\bar{3}, \bar{0})$ ha ordine. Ne segue che $E(\mathbf{Z}_7)$ è isomorfo al gruppo ciclico $\mathbf{Z}_4$.
($E(\mathbf{Z}_7)$ non è isomorfo a $\mathbf{Z}_2 \times \mathbf{Z}_2$ che ha ben tre elementi di ordine due).

3. *Sia $p = 41$.*
   (a) Verificare che $\bar{a} = \bar{7}$ è una radice primitiva di $\mathbf{Z}_p^*$.
   (b) Determinare il logaritmo discreto di $\overline{10}$ in base $\bar{a}$.

Sol.: (a) Abbiamo $p - 1 = 40 = 2^3 \cdot 5$ e

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

Dunque $\bar{7}$ è una radice primitiva di $\mathbf{Z}_{41}^*$.
(b) Dalle relazioni modulo 41

$-1 \equiv 40 \equiv 2^3 \cdot 5$
$2^3 \equiv 49 \equiv 7^2$

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

$3 \log 2 + \log 5 = \log(-1) = 20$

$3\log 2 = 2\log 7 = 2$.

Poiché $\gcd(3, 40) = 0$, esiste $\bar{3}^{-1} \in \mathbf{Z}_{40}^*$ ed è uguale a $\bar{3}^{-1} = \overline{27}$. Quindi possiamo ricavare

$$\log(2) = 2 \cdot 27 \equiv 14, \quad \log(5) = 20 - 3\log(2) \equiv 18, \quad \log(10) = \log(2) + \log(5) = 32 \mod 40.$$

Alternativamente, uno poteva usare Baby-Step-Giant-Step.

4. *Sia $n \sim 10^{80}$ e sia $B \sim 10^7$. Quanti interi B-smooth ci sono approssimativamente nell'intervallo $[n - M, n + M]$, dove $M \sim 10^{15}$?*

Sol.: Ossrivamo innanzitutto che $n >> M$. Quindi, all'interno dell'intervallo $[n - M, n + M]$, la probabilità che un intero sia B-smooth si può stimare con w^{-w}, dove $w = \log(n)/\log(B)$ (usando la funzione di Dickman). Nel nostro caso, abbiamo

$$w \sim 11.4285714, \qquad w^{-w} \sim 8.1033.$$

Pertanto, il numero di interi B-smooth nell'intervallo $[n - M, n + M]$, di lunghezza $2M$, si può stimare con

$$\sim 1620.$$

5. *Sia $n = 3599$. Supponiamo di conoscere le seguenti congruenze modulo n*

$$325^2 \equiv 2 \cdot 3 \cdot 11 \cdot 19, \quad 318^2 \equiv 2^5 \cdot 11, \quad 690^2 \equiv 2^3 \cdot 3 \cdot 43$$

$$208^2 \equiv 2^2 \cdot 19, \quad 639^2 \equiv 2 \cdot 19 \cdot 43, \quad 461^2 \equiv 2^2 \cdot 3^2 \cdot 5, \quad 765^2 \equiv 3^7$$

Quali interi sono potenziali fattori non banali di n? Spiegare la risposta.

Sol.: Moltiplicando fra loro un opportuno sottoinsieme delle relazioni date, cerchiamo di ottenere una relazione quadratica modulo n, della forma

$$a^2 \equiv b^2 \mod \text{n}.$$

Dopodiché potenziali fattori non banali di n sono

$$\gcd(a + b, n), \quad \gcd(a - b, n).$$

Moltiplicando ad esempio

$$325^2 \equiv 2 \cdot 3 \cdot 11 \cdot 19, \quad 208^2 \equiv 2^2 \cdot 19, \quad 318^2 \equiv 2^5 \cdot 11, \quad 765^2 \equiv 3^7$$

ricaviamo

$$(325 \cdot 208 \cdot 318 \cdot 765)^2 \equiv (2^4 \cdot 3^4 \cdot 11 \cdot 19)^2 \mod \text{n}.$$

Da cui

$$a \equiv 939 \quad b \equiv 939, \qquad a - b = 0, \quad a + b = 1878.$$

Sfortunatamente $\gcd(a + b, n) = 1$ e $\gcd(0, n) = n$ sono fattori banali di n...