Teoria Elementare dei Numeri Appello 4 24 settembre 2014, 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. *Sia E la curva di equazione* $E: \quad Y^2 = X^3 - 1$.
   (i) Verificare che E definisce una curva ellittica $E(\mathbf{Z}_{11})$ su $\mathbf{Z}_{11}$.
   (ii) Verificare che i punti $P = (\bar{1}, \bar{0})$ e $Q = (\bar{5}, \bar{5})$ appartengono a $E(\mathbf{Z}_{11})$.
   (iii) Determinare un punto $R = (\bar{x}, \bar{y}) \in E(\mathbf{Z}_{11})$ tale che $P + Q + R = \infty$, dove ∞ indica il punto all'infinito su $E(\mathbf{Z}_{11})$.
   (iv) Determinare i punti di ordine 2 su $E(\mathbf{Z}_{11})$.

Sol. (i) Il discriminante della curva è $\Delta = 27(-1)^2 = 27 \not\equiv 0 \mod 11$. Dunque E definisce una curva ellittica $E(\mathbf{Z}_{11})$ su $\mathbf{Z}_{11}$.

(ii) Abbiamo $0 \equiv 1^2 - 1$ e $5^3 \equiv 3 \equiv 125 - 1 = 124 \equiv 3 \mod 11$, per cui Pe Q stanno sulla curva $E(\mathbf{Z}_{11})$.

(iii) Vale $P+Q+R = \infty$ se e solo se $R = -(P+Q)$, ossia R è l'inverso di $P+Q$ rispetto all'operazione di somma definita sulla curva ellittica. Risulta $P + Q = (10, 8)$, per cui $R = (10, -8) \equiv (10, 3)$.

(iv) I punti di ordine due su $E(\mathbf{Z}_{11})$ sono i punti della curva con ordinata uguale a zero. Ce ne sono al massimo tre, visto che il polinomio $X^3 - 1 \in \mathbf{Z}_{11}[X]$ può avere al massimo tre zeri in $\mathbf{Z}_{11}$. Un punto di ordine due su $E(\mathbf{Z}_{11})$ è ad esempio $P(1, 0)$. Per vedere se ce ne sono altri, scriviamo $X^3 - 1 = (X - 1)(X^2 + X + 1)$ e controlliamo se $(X^2 + X + 1)$ si annulla per qualche $\alpha \in \mathbf{Z}_{11}$. Si ottiene che $P = (1, 0)$ è l'unico punto di ordine due.

P.S. La curva $E(\mathbf{Z}_{11})$ ha 12 punti:

$$(1,0),\ (3,2),\ (3,9),\ (5,5),\ (5,6),\ (7,1),\ (7,10),\ (8,4),\ (8,7),\ (10,3),\ (10,8),\ \infty.$$

2. *Sia n un intero di circa 150 cifre. Quanti primi ci sono ci sono approssimativamente nell'intervallo $[n - M, n + M]$, dove $M \sim 10^{15}$? (spiegare bene la risposta).*

Sol. Poiché $M << n$, la probabilità che un intero dell'intervallo $[n-M, n+M]$ sia primo è stimabile con $\frac{1}{\ln n} \sim= \frac{1}{150 \ln 10} \sim 0.00289$, ossia 3 su 1000. Dunque nell'intervallo $[n - M, n + M]$ ci sono approssimativamente $2 * M * \frac{1}{\ln n} \sim 2 * 10^{15} * 3 * 10^{-3} \sim 6 * 10^{12}$ primi.

3. *Sia p un numero primo.*
   (i) Dimostrare che un intero a è un quadrato modulo p se e solo se $a^{\frac{p-1}{2}} \equiv 1 \mod$ p.
   (ii) Determinare se 2 è un quadrato modulo 19.
   (iii) Sia a un intero. Quante radici ha l'equazione $\bar{x}^2 \equiv \bar{a}$ in $\mathbf{Z}_{19}$? (discutere i vari casi e dare un esempio di ogni situazione).

Sol. (i) & (iii) Vedi Esercizio 1 degli Esercizi7 (svolti).

(ii) Risulta $2^{(19-1)/2} \not\equiv 1 \mod 19$, per cui 2 non è un quadrato modulo 19. Questo vuol dire che non esiste alcun intero il cui quadrato è uguale a 2 modulo 19. In particolare l'equazione $\bar{x}^2 \equiv \bar{2}$ non ha soluzioni in $\mathbf{Z}_{19}$. L'equazione $\bar{x}^2 \equiv \bar{0}$ ha come unica soluzione $\bar{0} \in \mathbf{Z}_{19}$; Poiché 4 è un quadrato modulo 19, l'equazione $\bar{x}^2 \equiv \bar{4}$ ha esattamente due soluzioni $\bar{2}$ e $\overline{-2} \equiv \overline{17}$ in $\mathbf{Z}_{19}$. Poiché un polinomio di grado n a coefficienti in $\mathbf{Z}_p$, con p primo, ha al più n soluzioni, non ci sono altre possibilità.

4. *Sia $p = 37$.*
   (i) Determinare la più piccola radice primitiva $\bar{a}$ di $\mathbf{Z}_{37}^*$.
   (ii) Calcolare il logaritmo discreto $\log_{\bar{a}} \overline{15}$ di $\overline{15}$ in base $\bar{a}$.

Sol. (i) Abbiamo $p-1 = 36 = 2^2 * 3^2$. Poiché $2^{36/2} \equiv 36 \mod 37$ e $2^{36/3} \equiv 26 \mod 37$, la più piccola radice primitiva di $\mathbf{Z}_{37}^*$ è $\bar{a} = \bar{2}$.

(ii) Possiamo procedere con Baby-Step-Giant-Step, oppure col calcolo dell'indice. Dalle relazioni modulo 37

$$3 \equiv 40 \equiv 2^3 \cdot 5 \qquad -5 \equiv 32 \equiv 2^5,$$

otteniamo le relazioni modulo 36 fra i rispettivi logaritmi in base $\bar{2}$:

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

ossia

$$\log 3 - \log 5 = 3, \qquad \log 5 = 5 - 18 = -13,$$

da cui

$$\log(15) = \log 3 + \log 5 = -10 - 13 \equiv 13 \mod 36.$$

5. *Descrivere e spiegare il metodo $p-1$ di Pollard per fattorizzare i numeri interi.*

Sol. vedi Nota.