Teoria Elementare dei Numeri Appello 3 30 giugno 2015, 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. Richiamare la definizione di gruppo ciclico. Dimostrare che $\mathbf{Z}_2^*$ e $\mathbf{Z}_4^*$ sono gruppi ciclici, mentre $\mathbf{Z}_8^*$ non è un gruppo ciclico.

Sol.: Il gruppo $\mathbf{Z}_2^* = \{\bar{1}\}$ è banalmente ciclico; il gruppo $\mathbf{Z}_4^* = \{\bar{1}, \bar{3} = \overline{-1}\}$ è ciclico con generatore $\overline{-1}$ di ordine due. Il gruppo $\mathbf{Z}_8^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7} = \overline{-1}\}$ non è ciclico perchè non contiene nessun elemento di ordine 8: infatti $\bar{3}^2 = \bar{5}^3 = \bar{7}^2 = \bar{1}$ modulo 8.

2. Sia $E: \quad Y^2 = X^3 + 3X + 4$ e sia $p = 59$.
   (a) Verificare che E definisce una curva ellittica su $\mathbf{Z}_{59}$ e determinare l'intervallo di Hasse di $E(\mathbf{Z}_{59})$.
   (b) Verificare che $P = (0, 2)$ appartiene a $E(\mathbf{Z}_{59})$ e che $2P = (19, 28)$.
   (c) Sapendo che $3P$ ha ordine 9, determinare l'ordine di P.
   (d) Sfruttando le informazioni ottenute da (a),(b),(c), determinare l'ordine della curva $|E(\mathbf{Z}_{59})|$.

Sol.: (a) Il discriminante della curva $\Delta = 4 \cdot 3^3 + 27 \cdot 4^2 \equiv 9 \not\equiv 0 \mod 59$, quindi $E(\mathbf{Z}_{59})$ è una curva ellittica. L'intervallo di Hasse della curva è dato da

$$[59 + 1 - 2\sqrt{59}, 59 + 1 - 2\sqrt{59}] \sim [44.63, 75.36].$$

(b) $P = (0, 2)$ appartiene a $E(\mathbf{Z}_{59})$: basta sostituire le coordinate del punto nell'equazione;
$2P = (19, 28)$: usare le formule.

(c) Poiché $2P = (19, 28) \neq \infty, -P$ abbiamo che P ha ordine $\neq 2, 3$ (anche $\neq 1$, perché $P \neq \infty$). Poiché $3P$ ha ordine 9, abbiamo che $9 \cdot 3P = 27P = \infty$. Dunque **l'ordine di P divide** 27. Abbiamo appena osservato che è $\neq 3$. È anche $\neq 9$: altrimenti si avrebbe $9P = 3 \cdot 3P = \infty$, mentre per ipotesi 9 è il più piccolo multiplo di $3P$ che è uguale a ∞. Conclusione l'ordine di P è uguale a 27.

(d) Poiché l'ordine di P divide l'ordine del gruppo $|E(\mathbf{Z}_{59})|$ e $|E(\mathbf{Z}_{59})|$ è un intero dell'intervallo di Hasse, necessariamente $|E(\mathbf{Z}_{59})| = 54$.

3. Sia dato il primo $p = 61$.
   (a) Quante radici primitive ci sono in $\mathbf{Z}_{61}^*$? Determinare $\bar{a}$, la più piccola radice primitiva di $\mathbf{Z}_p^*$.
   (b) Nella base $\bar{a}$ trovata, calcolare i seguenti logaritmi: $\log_{\bar{a}} 60$, $\log_{\bar{a}} 15$, $\log_{\bar{a}} 11$.

Sol.: (a) Il gruppo $\mathbf{Z}_{61}^*$ è ciclico di ordine 60 e contiene $\varphi(60) = \varphi(2^2)\varphi(3)\varphi(5) = 2 \cdot 2 \cdot 4 = 16$ elementi di ordine 60 (qui φ indica la funzione di Eulero).
La più piccola radice primitiva di $\mathbf{Z}_{61}^*$ è $\bar{2}$: infatti abbiamo

$$2^{12} \equiv 9 \not\equiv 1, \quad 2^{20} \equiv 47 \not\equiv 1, \quad 2^{30} \equiv 60 \not\equiv 1 \qquad \mod 61.$$

(b) Abbiamo innanzitutto $\log_{\bar{2}} \overline{60} = \log_{\bar{2}} \overline{-1} \equiv 30$, $\log_{\bar{2}} \bar{2} \equiv 1$, $\log_{\bar{2}} \bar{1} \equiv 1$ modulo 60. A partire dalle relazioni

$$-1 \equiv 60 = 2^2 \cdot 3 \cdot 5, \quad 3 \equiv 64 = 2^6, \quad 5 \equiv 66 = 2 \cdot 3 \cdot 11 \qquad \mod 61,$$

otteniamo le seguenti relazioni fra i rispettivi logaritmi

$$30 \equiv 2\log_{\bar{2}} \bar{2} + \log_{\bar{2}} \bar{3} + \log_{\bar{2}} \bar{5}, \quad \log_{\bar{2}} \bar{3} \equiv 6\log_{\bar{2}} \bar{2}, \quad \log_{\bar{2}} \bar{5} \equiv \log_{\bar{2}} \bar{2} + \log_{\bar{2}} \bar{3} + \log_{\bar{2}} \overline{11} \qquad \mod 60,$$

da cui

$$\log_{\bar{2}} \bar{3} \equiv 6, \quad \log_{\bar{2}} \bar{5} \equiv 22, \quad \log_{\bar{2}} \overline{11} = 15 \qquad \mod 60.$$

Conclusione:

$$\log_{\bar{2}} \overline{60} \equiv 30, \quad \log_{\bar{2}} \overline{15} \equiv 28, \quad \log_{\bar{2}} \overline{11} = 15 \qquad \mod 60.$$

4. Sia N un intero di circa 200 cifre.
   (a) Quanti numeri primi ci sono approssimativamente nell'intervallo $[N-a, N+a]$, dove a è dell'ordine di grandezza di 10^{15}?
   (b) Quanti numeri B-smooth ci sono approssimativamente nello stesso intervallo, se B è dell'ordine di grandezza di 10^{50}?
   (spiegare bene le risposte).

Sol.: (a) La probabilità che N sia primo è circa $\frac{1}{\ln(N)} \sim \frac{1}{2*10^2*\ln(10)} \sim 0.002171472409516.....$ Poiché $a << N$, il numero dei primi nell'intervallo $[N-a, N+a]$ si può stimare con

$$\frac{1}{\ln(N)} * 2 * 10^{15} \sim \frac{1}{\ln(10)} * 10^{13} \sim 4342944819032,5....$$

(b) Sia $w = \ln(N)/\ln(B) = 4$. La probabilità che N sia B-smooth è stimabile con $w^{-w} = \frac{1}{256} \sim 0.00390625$. Poiché $a << N$, il numero dei primi nell'intervallo $[N-a, N+a]$ si può stimare con

$$w^{-w} * 2 * 10^{15} \sim \frac{1}{256} * 2 * 10^{15} \sim 7,8125 * 10^{12} \sim 7812500000000.00.$$

5. Sia p un numero primo e sia a un intero.
   (a) Quante radici ha l'equazione $\bar{x}^2 \equiv \bar{a}$ in $\mathbf{Z}_p$? (descrivere le varie possibilità).
   (b) Sia $p = 17$. Dare un esempio di ogni situazione, scegliendo opportunamente $\bar{a}$.

Sol.: (a) L'equazione $\bar{x}^2 \equiv \bar{0}$ ha come unica soluzione $\bar{0} \in \mathbf{Z}_p$; se $\bar{a}$ è un quadrato modulo p, l'equazione $\bar{x}^2 \equiv \bar{a}$ ha esattamente due soluzioni in $\mathbf{Z}_p$; se $\bar{a}$ non è un quadrato modulo p, l'equazione $\bar{x}^2 \equiv \bar{a}$ non ha nessuna soluzione in $\mathbf{Z}_p$. 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.

(b) Abbiamo che $\bar{4} = \bar{2}^2$ è un quadrato modulo 17. Quindi l'equazione $\bar{x}^2 \equiv \bar{4}$ ha esattamente due soluzioni $\bar{2}$ e $\overline{-2} \equiv \overline{15}$ in $\mathbf{Z}_{17}$. Invece $\bar{3}$ non è un quadrato modulo 17: infatti $\bar{3}^{(17-1)/2} \equiv \overline{16} \neq \bar{1}$. Dunque l'equazione $\bar{x}^2 = \bar{3}$ non ha soluzioni in $\mathbf{Z}_{17}$.