Teoria Elementare dei Numeri Appello 4 13 luglio 2018, ore 16-18.

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 φ la funzione di Eulero.*
   (a) Dimostrare che se $n \in \mathbf{N}$ è dispari, allora $\varphi(n) = \varphi(2n)$.
   (b) Dimostrare che se $n \in \mathbf{N}$ è pari, allora $\varphi(n) \neq \varphi(2n)$.

Sol. (a) n dispari equivale $\gcd(2, n) = 1$, da cui segue $\varphi(2n) = \varphi(2)\varphi(n) = \varphi(n)$.
(b) n pari si può scrivere come $n = 2^k m$, con $k \geq 1$ ed m dispari, e $2n = 2^{k+1}m$. Abbiamo $\varphi(n) = \varphi(2^k)\varphi(m)$ e $\varphi(2n) = \varphi(2^{k+1})\varphi(m)$. Poiché $\varphi(2^k) \neq \varphi(2^{k+1})$, ne segue che $\varphi(n) \neq \varphi(2n)$.

2. *(a) Descrivere brevemente il criptosistema a chiave pubblica RSA.*
   (b) Supponiamo di voler costruire un kit di chiavi $\{N = pq, E, D\}$, con p, q primi di 300 cifre. Quanti ce ne sono approssimativamente?
   (c) Come si costruisce uno pseudoprimo di 300 cifre? Qual è la complessità dei calcoli necessari?

Sol. (a) Vedi logo sulla pagina web :-)
(b) Ce ne sono approssimativamente

$$\pi(10^{300}) - \pi(10^{299}) \sim \frac{10^{300}}{300 \ln 10} - \frac{10^{299}}{299 \ln 10} \sim \frac{10^{299} \cdot 9}{300 \ln 10}.$$

(c) Si prende un numero a caso di 300 cifre e gli si applica il test di primalità di Miller-Rabin. Se il numero non passa il test, se ne prende un altro, si gli applica il test. E cosí via fino a che si trova uno pesudoprimo. Il teorema dei numeri primi ci premette di concludere che dopo $\ln 10^{300}$ tentativi presumibilmente avremo successo. Poiché anche il test di Miller-Rabin ha complessità polinomiale in $\ln 10^{300}$, la complessità dei calcoli necessari a produrre uno pseudoprimo di 300 cifre è polinomiale in $\ln 10^{300}$.

3. *Sia E la curva di equazione $Y^2 = X^3 - 2X$.*
   (a) Verificare che E è una curva ellittica su $\mathbf{Z}_7$.
   (b) Determinare tutti i punti di $E(\mathbf{Z}_7)$.
   (c) Determinare la struttura del gruppo $E(\mathbf{Z}_7)$.
   (d) Esibire un punto di ordine massimo possibile in $E(\mathbf{Z}_7)$.

Sol. (a) Il discriminante della curva è $\Delta = -32 \not\equiv 0 \mod 7$. Quindi E definisce una curva ellittica su $\mathbf{Z}_7$.
(b) ... col solito metodo si trova che i punti di $E(\mathbf{Z}_7)$ sono

$$(0,0),\ (2,2),\ (2,5),\ (3,0),\ (4,0),\ (6,1),\ (6,6),\ \infty.$$

Dunque $\#E(\mathbf{Z}_7) = 8$.
(c) Per la struttura di un gruppo abeliano di cardinalità 8, a priori ci sono tre possibilità

$$\mathbf{Z}_8, \quad \mathbf{Z}_2 \times \mathbf{Z}_4, \quad \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2.$$

Poiché $E(\mathbf{Z}_7)$ contiene tre elementi di ordine 2 (quelli con l'ordinata nulla), è necessariamente isomorfo a $\mathbf{Z}_2 \times \mathbf{Z}_4$.
(d) Gli elementi $(2,2),\ (2,5),\ (6,1),\ (6,6)$ hanno tutti ordine 4 (il loro ordine è $\neq 1, 2$ e divide 4).

4. *Sia dato il primo $p = 37$.*
   (a) Determinare la più piccola radice primitiva di $\mathbf{Z}_{37}^*$.

(b) *Quante radici primitive ci sono in* $\mathbf{Z}_{37}^*$*?*
(c) *Calcolare il logaritmo discreto di* $\bar{7}$ *e di* $\bar{5}$ *rispetto alla radice primitiva trovata al punto (a).*

Sol. (a) La più piccola radice primitiva di $\mathbf{Z}_{37}^*$ è $\bar{2}$: infatti $2^{36/2} \equiv 36 \not\equiv 1 \mod 37$ e $2^{36/3} \equiv 26 \not\equiv 1 \mod 37$.
(b) Dalle relazioni

$$-2 \equiv 35 = 5 \cdot 7, \quad 3 \equiv 40 = 2^3 \cdot 5, \quad 5 \equiv 42 = 2 \cdot 3 \cdot 7 \mod 37$$

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

$$\log \bar{5} + \log \bar{7} \equiv 18 + 1 = 19, \quad \log \bar{3} - \log \bar{5} \equiv 3, \quad \log \bar{3} - \log \bar{5} + \log \bar{7} \equiv -1 \mod 36.$$

Ricaviamo

$$\log \bar{7} \equiv 32, \quad \log \bar{5} = 23, \quad \log \bar{3} = 26.$$

5. *Sia* E *la curva ellittica di equazione* $Y^2 = X^3 + 3X + 4$ *su* $\mathbf{Z}_{59}$ *e sia* P *il punto* $(0, 2)$ *su* $E(\mathbf{Z}_{59})$.
   (a) *Verificare che* $2P = (19, 28)$.
   (b) *Sapendo che* $3P$ *ha ordine 9, determinare la cardinalità del gruppo* $E(\mathbf{Z}_{59})$.

Sol. (a) usare le formule...
(b) La cardinalità del gruppo $E(\mathbf{Z}_{59})$ è un intero dell'intervallo di Hasse
$[59 + 1 - 2\sqrt{59}, 59 + 1 + 2\sqrt{59}] = [44.63\,,\, 75.36]$.
Se $3P$ ha ordine 9, allora $27P = \infty$. Ne segue che l'ordine di P divide 27, e può essere solo 1, 3, 9, 27. Dal punto (a) vediamo che $P \neq \infty, -P, -2P$, da cui segue che l'ordine di P è diverso da 1,2,3. L'ordine di P è anche $\neq 9$, perchè altrimenti sarebbe $9P = 3(3P) = \infty$. Contro l'ipotesi che $3P$ ha ordine 9. Conclusione, l'ordine di P è 27 e l'ordine della curva è 54, ossia l'unico multiplo intero di 27 nell'intervallo $[44.63\,,\, 75.36]$.