Teoria Elementare dei Numeri — Appello 1 — 4 febbraio 2015, 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 ellittica su $\mathbf{Z}_5$ di equazione $Y^2 = X^3 + 2$.*
   (a) Determinare tutti i punti di $E(\mathbf{Z}_5)$.
   (b) Determinare l'ordine di ognuno di essi.

Sol.: (a) I punti della curva sono 6, precisamente

$$E(\mathbf{Z}_5) = \{(2,0),\ (3,2),\ (3,3),\ (4,1),\ (4,4)\} \cup \infty,$$

e il gruppo $E(\mathbf{Z}_5)$ è necessariamente un gruppo ciclico isomorfo a $\mathbf{Z}_6$ (ricordiamo che $\mathbf{Z}_2 \times \mathbf{Z}_3 \cong \mathbf{Z}_6$). Come in ogni gruppo ciclico, abbiamo un elemento di ordine 1 (il punto all'infinito, che è l'elemento neutro del gruppo), $\varphi(2) = 1$ elementi di ordine 2 (il punto $(2,0)$ con ordinata nulla), $\varphi(3) = 2$ elementi di ordine tre e $\varphi(6) = 2$ elementi di ordine 6. Prendiamo un punto $P \in E(\mathbf{Z}_5)$ a caso (diverso da ∞ e da $(2,0)$) e calcoliamo $2P = P + P$: se $2P = -P$, allora $3P = \infty$ e P ha necessariamente ordine 3. Lo stesso vale per il suo inverso. Se invece $2P \neq -P$, allora $3P \neq \infty$ e l'ordine di P è necessariamente 6. Lo stesso vale per il suo inverso. Calcolando ad esempio $(3,2) + (3,2) = (3,3)$, si vede che $2 \cdot (3,2) = (3,3) = -(3,2)$, da cui $3 \cdot (3,2) = \infty$. Dunque $(3,2)$ & $-(3,2) = (3,3)$ sono i due elementi di ordine 3. I rimanenti $(4,1)$ & $-(4,1) = (4,4)$ sono necessariamente di ordine 6.

2. *Siano Rossi e Bianchi due utenti che vogliono condividere una chiave mediante il Diffie-Hellman-Merkle key-exchange. Si accordano sul primo $p = 19$ e la radice primitiva $g = \overline{2}$. Una spia intercetta le stringhe $\overline{5}$ e $\overline{11}$ che i due utenti si scambiano. Qual è la chiave segreta di Rossi e Bianchi?*

Sol.: Siano m_R ed m_B gli esponenti segreti di Rossi e Bianchi. La spia vede passare le stringhe $5 \equiv 2^{m_R}$ e $11 \equiv 2^{m_R}$ modulo 19. Sarà in grado di conoscere la chiave segreta di Rossi e Bianchi $2^{m_R \cdot m_B} \equiv 2^{m_B \cdot m_R}$ modulo 19, una volta che ha calcolato

$$m_R = \log_{\overline{2}} \overline{5} \quad \text{e} \quad m_B = \log_{\overline{2}} \overline{11}.$$

Dalle relazioni

$$1 \equiv 20 = 2 \cdot 5, \quad 2 \equiv 21 = 3 \cdot 7, \quad 3 \equiv 22 = 2 \cdot 11 \qquad \text{mod } 19,$$

ricaviamo

$$m_R \equiv \log_{\overline{2}} \overline{5} \equiv 16, \quad \log_{\overline{2}} \overline{3} \equiv 13, \quad m_B \equiv \log_{\overline{2}} \overline{11} \equiv 12, \qquad \text{mod } 18.$$

La chiave cercata è

$$2^{m_R \cdot m_B} \equiv \overline{5^{12}} \equiv \overline{11^{16}} \qquad \text{mod } 19.$$

3. *Sia n un intero di 100 cifre e sia $B = 10^{15}$.*
   (a) Qual è la probabilità che n sia B-smooth?
   (b) Quante iterazioni a vuoto dell'algoritmo ρ di Pollard sono (all'incirca) necessarie a concludere che n presumibilmente non è B-smooth?

Sol.: (a) Sia $u = \log n / \log B \sim 100 \log 10 / 15 \log 10 \sim 6.666.....$ La probabilità che n sia B-smooth si può stimare con

$$u^{-u} \sim 3.215696554941889546854074709345303007 7 \text{ E-6}$$

(cf. Teorema di Dickman). Dunque è assai bassa.

(b) Se n ha un fattore $\leq B$, è probabile che venga individuato da $\sqrt{B}$ iterazioni dell'algoritmo ρ di Pollard. Per questo, se $\sqrt{B}$ iterazioni dell'algoritmo ρ di Pollard non producono nessun fattore di n, presumibilmente n non ha fattori $\leq B$, e a maggior ragione non è B-smooth.

4. *Sia $p \equiv 3 \mod 4$ un numero primo. Supponiamo che $a \in \mathbf{Z}$ sia un quadrato diverso da zero modulo p. Far vedere che:*
   (a) vale $a^{\frac{(p-1)}{2}} \equiv 1 \mod p$;
   (b) il numero $a^{\frac{(p+1)}{4}}$ è radice quadrata di a modulo p.

Sol.: (a) Vedi es.1(a) su Esercizi-risolti7 (crivello quadratico).

(b) Se $p \equiv 3 \mod 4$, l'esponente $\frac{(p+1)}{4}$ è un intero. Inoltre

$$(a^{\frac{(p+1)}{4}})^2 = a^{\frac{(p+1)}{2}} = a^{\frac{(p+1)}{2}} a^{-1} a = a^{\frac{(p-1)}{2}} a \equiv a \mod p,$$

cioè $a^{\frac{(p+1)}{4}}$ è radice quadrata di a modulo p (abbiamo usato il fatto che p è primo e che ogni $\bar{a} \neq \bar{0}$ è invertibile in $\mathbf{Z}_p$).

5. *Sia $p > 2$ un numero primo e sia E la curva su $\mathbf{Z}_p$ di equazione $Y^2 = X^3 - X$.*
   (a) Verificare che si tratta di una curva ellittica, per ogni primo $p > 2$.
   (b) Determinare i punti di ordine 2 di $E(\mathbf{Z}_p)$.
   (c) Sia $E[2]$ l'insieme dei punti di $E(\mathbf{Z}_p)$ di ordine ≤ 2. Verificare che $E[2]$ è un gruppo di ordine 4 isomorfo a $\mathbf{Z}_2 \times \mathbf{Z}_2$.

Sol.: (a) Il discriminante della curva è $4(-1)^3 \equiv -4 \not\equiv 0 \mod p$ (il primo p è dispari). Dunque E definisce una curva ellittica su $\mathbf{Z}_p$, per ogni primo $p > 2$.

(b) I punti di ordine due di $E(\mathbf{Z}_p)$ sono quelli con ordinata nulla ed ascissa una radice del polinomio $X^3 - X = X(X^2 - 1)$ in $\mathbf{Z}_p$:

$$(0,0),\ (1,0),\ (-1,0).$$

(c) Poiché il punto all'infinito ∞ ha ordine uno,

$$E[2] = \{(0,0),\ (1,0),\ (-1,0),\ \infty\}.$$

$E[2]$ è un sottogruppo di $E(\mathbf{Z}_p)$ (e quindi un gruppo) perché somma e inverso di elementi di ordine ≤ 2, hanno ordine ≤ 2:

$$(P+Q)+(P+Q) = 2P+2Q = \infty + \infty = \infty, \qquad (-P)+(-P) = 2(-P) = \infty.$$

Come gruppo $E[2]$ potrebbe essere isomorfo a $\mathbf{Z}_4$ oppure a $\mathbf{Z}_2 \times \mathbf{Z}_2$, ma avendo solo elementi di ordine ≤ 2, è necessariamente isomorfo a $\mathbf{Z}_2 \times \mathbf{Z}_2$.