Teoria Elementare dei Numeri 2016 Appello 1 6 febbraio 2017, 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 B un intero di 13 cifre. Supponiamo di avere $M \sim 10^{26}$ interi di 200 cifre. Quanti di essi sono probabilmente B-smooth?*

Sol. La probabilità che un intero di 200 cifre sia B-smooth con $B \sim 10^{13}$ si può stimare con

$$w^{-w} \sim 5.45919...10^{-19}, \qquad w = \frac{\log 10^{200}}{\log 10^1 3} = 15.38.$$

Ne segue che fra $M \sim 10^{26}$ interi di 200 cifre, probabilmente 54591944 di essi sono B-smooth.
Questo è la stima che si può fare nel caso del crivello quadratico, per controllare se un dato array verosimilmente contiene un numero sufficiente di interi B-smooth. Nel caso qui sopra no: infatti $54591944 << B$.

2. *Sia dato l'intero n, che si fattorizza come prodotto dei primi $p_1 = 7561$, $p_2 = 7591$ e $p_3 = 7577$, che soddisfano*

$$p_1 - 1 = 2^3 \cdot 3^3 \cdot 5 \cdot 7, \qquad p_2 - 1 = 2 \cdot 3 \cdot 5 \cdot 11 \cdot 23, \qquad p_3 - 1 = 2^3 \cdot 977.$$

Se applichiamo ad n l'algoritmo $p-1$ di Pollard con smoothness bound $B = 10$, quale fattore riusciamo verosimilmente ad individuare? E con smoothness bound $B = 30$?

Sol. Se applichiamo ad n l'algoritmo $p-1$ di Pollard con smoothness bound B, verosimilmente troviamo il prodotto di tutti i fattori primi p di n con la proprietà che $p-1$ è B-smooth. Con smoothness bound $B = 10$, riusciamo verosimilmente ad individuare p_1; con smoothness bound $B = 30$, riusciamo verosimilmente ad individuare $p_1 \cdot p_2$.

3. *Rossi e Bianchi sono due utenti che vogliono condividere una chiave mediante il Diffie-Hellman-Merkle key exchange. Si accordano sul primo $p = 31$ e la radice primitiva $g = \overline{3}$. Una spia intercetta le stringhe $\overline{10}$ e $\overline{15}$ che i due utenti si scambiano. Qual è la chiave segreta di Rossi e Bianchi?*

Sol. Risolvendo il logaritmo discreto determiniamo le chiavi personali di Rossi e Bianchi

$$E_R = \log_{\overline{3}} \overline{10} \quad \text{e} \qquad E_B = \log_{\overline{3}} \overline{15}.$$

Dopodiché la chiave segreta condivisa da Rossi e Bianchi sarà

$$\overline{3}^{E_R \cdot E_B} \mod 31.$$

Per le proprietà del logaritmo

$$\log_{\overline{3}} \overline{10} = \log_{\overline{3}} \overline{2} + \log_{\overline{3}} \overline{5}, \qquad \log_{\overline{3}} \overline{15} = \log_{\overline{3}} \overline{3} + \log_{\overline{3}} \overline{5} = \log_{\overline{3}} \overline{5} + 1.$$

Dalla relazione $\mod 31$

$$-1 \equiv 30 = 2 \cdot 3 \cdot 5$$

ricaviamo la relazione $\mod 30$ fra i rispettivi logaritmi

$$\log_{\overline{3}}(-1) \equiv \log_{\overline{3}} 2 + \log_{\overline{3}} 3 + \log_{\overline{3}} 5 \quad \Leftrightarrow \quad \log_{\overline{3}} 10 = 15 - 1 = 14.$$

Ci resta da determinare $\log_{\overline{3}} \overline{5}$. Usiamo Baby-Step-Giant-Step.

Fissiamo $m = 6 \sim \sqrt{31}$ e calcoliamo i baby steps:
$\bar{3}^0 = \bar{1}$
$\bar{3}^1 = \bar{3}$
$\bar{3}^2 = \bar{9}$
$\bar{3}^3 = \overline{27}$
$\bar{3}^4 = \overline{19}$
$\bar{3}^5 = \overline{26}$
$\bar{3}^6 = \overline{16}$
$\bar{3}^{-6} = \bar{2}$
e adesso i giant steps $\bar{5} \cdot \bar{3}^0 = \bar{5}$
$\bar{5} \cdot \bar{3}^{-6} = \overline{10}$
$\bar{5} \cdot \bar{3}^{-12} = \overline{20}$
$\bar{5} \cdot \bar{3}^{-18} = \bar{9}$

Abbiamo trovato una coincidenza nelle due liste:

$$\bar{3}^2 = \bar{9} = \bar{5} \cdot \bar{3}^{-18}$$

da cui

$$\bar{5} = \bar{3}^{20}, \quad \log_{\bar{3}} \bar{5} = 20, \quad \log_{\bar{3}} \overline{15} = 21.$$

La chiave segreta condivisa sarà dunque

$$\bar{3}^{21 \cdot 14} = \bar{2} \in \mathbf{Z}_{31}$$

4. *Sia data la curva* $E: \quad Y^2 = X^3 + 1$.
   (a) Verificare che E *definisce un curva ellittica su* $\mathbf{Z}_p$*, per ogni primo* $p > 3$.
   (b) Verificare che l'ordine della curva $\#E(\mathbf{Z}_p)$ *è pari per ogni primo* $p > 3$.

Sol.: (a) Il discriminante di E è dato da $\Delta = 27 \not\equiv 0$ per ogni primo $p > 3$.
(b) Sia $p > 3$ un primo. L'ordine della curva $\#E(\mathbf{Z}_p)$ è pari se e solo se l'insieme dei punti di $E(\mathbf{Z}_p)$ al finito è dispari. Questo avviene se e solo se esiste almeno un punto di ordine due (i punti di ordine due possono essere uno o tre), se e solo se il polinomio $X^3 + 1$ ha uno zero in $\mathbf{Z}_p$. È evidente che $\overline{-1}$ è uno zero di $X^3 + 1$, per ogni p.

5. *Sia data la curva* $E: \quad Y^2 = X^3 + 1$ *su* $\mathbf{Z}_7$.
   (a) Determinare tutti i punti di $E(\mathbf{Z}_7)$.
   (b) Scegliere due punti P *e* Q *su* $E(\mathbf{Z}_7)$*, con* $P \neq \pm Q$*, e determinare* $R \in E(\mathbf{Z}_7)$ *tale che* $P + Q + R = \infty$.
   (c) Determinare la struttura del gruppo $(E(\mathbf{Z}_7), +)$.

Sol.: (a) I quadrati modulo 7 sono dati da $Q_7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{4}\}$ con radici quadrate date da $\sqrt{\bar{0}} = \bar{0}$, $\sqrt{\bar{1}} = \bar{1}, \bar{6}$, $\sqrt{\bar{2}} = \bar{3}, \bar{4}$, $\sqrt{\bar{4}} = \bar{2}, \bar{5}$. I valori del polinomio $X^3 + 1$ su $\mathbf{Z}_7 = \{\bar{0}, \ldots, \bar{6}\}$ sono dati rispettivamente da $\bar{1}$, $\bar{2}$, $\bar{2}$, $\bar{0}$, $\bar{2}$, $\bar{0}$, $\bar{0}$. Ne segue che i punti di $E(\mathbf{Z}_7)$ sono dati da

$$(\bar{0}, \bar{1}),\ (\bar{0}, \overline{-1}),\ (\bar{1}, \bar{3}),\ (\bar{1}, \bar{4}),\ (\bar{2}, \bar{3}), (\bar{2}, \bar{4}),\ (\bar{3}, \bar{0}),\ (\bar{4}, \bar{3}),\ (\bar{4}, \bar{4}),\ (\bar{5}, \bar{0}),\ (\bar{6}, \bar{0}),\ \infty.$$

(b) Dati P e Q su $E(\mathbf{Z}_7)$, con $P \neq \pm Q$, il punto R cercato è $-(P + Q)$, etc...
(c) Il gruppo abeliano $(E(\mathbf{Z}_7), +)$ ha 12 elementi, di cui tre elementi di ordine due. Ci sono tre modelli possibili per un gruppo abeliano di 12 elementi:
- $\mathbf{Z}_{12} \cong \mathbf{Z}_4 \times \mathbf{Z}_3$ ciclico;
- $\mathbf{Z}_2 \times \mathbf{Z}_6 \cong \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_3$.

Il primo caso è escluso per la presenza di tre elementi di ordine due (in un gruppo ciclico ci sono esattamente $\varphi(2) = 1$ elementi di ordine due). Quindi siamo nel secondo caso.