Teoria Elementare dei Numeri 2017 Appello 1 1 febbraio 2018, ore 9:30–11:30.

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. *(a) Sia p un primo di 300 cifre. Di quante cifre differisce approssimativamente da p il primo successivo?*
   (b) Sia $B = 10^5$ e sia n un intero B-smooth di 300 cifre. Di quante cifre differisce approssimativamente da n l'intero B-smooth successivo?

Sol.: (a) La probabilità che un intero n di 300 cifre sia primo è circa $1/\ln n = 1/300\ln(10) \sim 0,00144\ldots \sim 1/10^3$. Dunque il primo successivo differisce da n di circa 3 cifre.
(b) La probabilità che un intero n di 300 cifre sia B-smooth con $B = 10^5$ è circa u^{-u}, dove $u = \log(n)/\log(B) \sim 60$. Poiché

$$u^{-u} \sim 2.04609... * E - 107 \sim e^{-245660673...} = 10^{-106.808988...},$$

l'intero B-smooth successivo differisce da n di circa 100 cifre.

2. *Sia $p > 2$ un primo e sia q un divisore primo di $2^p - 1$.*
   (a) Dimostrare che $q \equiv 1 \mod p$;
   (b) Dimostrare che $q \equiv 1 \mod 2p$.
   (c) Fattorizzare 2047.

Sol.: (a) Se q è un primo che divide $2^p - 1$, allora $2^p \equiv 1 \mod q$ e l'ordine di $2 \in \mathbf{Z}_q^*$ è uguale a p (deve dividere p, che è primo). Di conseguenza p divide $q - 1 = \#\mathbf{Z}_q^*$. Questo dimostra che $q \equiv 1 \mod p$.
(b) Poiché q è dispari (perché divide $2^p - 1$, che è dispari) si ha che $q \equiv 1 \mod 2$. Quindi per il Teorema cinese del resto vale anche $q \equiv 1 \mod 2p$.
(c) $2047 = 2^{11} - 1$. Quindi $p = 11$ e $2p = 22$. Il primo $q = 23$ è congruo a 1 modulo 22 e divide 2047: infatti 2047=23*49.

3. *Rossi e Bianchi sono due utenti che vogliono condividere una chiave segreta mediante il Diffie-Hellman-Merkle key exchange. Si accordano sul primo $p = 47$ e la radice primitiva $g = \bar{5}$. 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.: Siano m_R ed m_B le chiavi segrete di Rossi e di Bianchi. Assumiamo ad esempio $m_R = \log_5(15)$. Allora $m_B = \log_5(10)$ e la chiave cercata è $10^{m_R} = 10^{\log_5(15)} \mod 47$. Dunque dobbiamo calcolare

$$m_R = \log_5(15) = \log_5(3) + \log_5(5) = \log_5(3) + 1.$$

Cerchiamo $\log_5(3)$ col calcolo dell'indice. Dalle relazioni

$$1 \equiv 48 = 2^4 \cdot 3 \quad -2 \equiv 45 = 3^2 \cdot 5 \qquad \mod 47,$$

tenendo conto che $\log(1) = 0$, $\log(5) = 1$, $\log(-1) = 22$, troviamo le relazioni fra i logaritmi in base 5

$$4\log(2) + \log(3), \quad \log(-1) + 2\log(3) = 23 - 1 = 22 \qquad \mod 46.$$

Risolvendo si trova

$$\log(2) = 18, \qquad \log(3) = 20,$$

da cui si ricava $m_R = 21$ e la chiave segreta $K = 10^{\log_5(15)} = 10^{21} = 39 \mod 47$.

4. *Sia E la curva di equazione $Y^2 = X^3 - X$ su Z_5.*

(a) *Verificare che si tratta di una curva ellittica.*
(b) *Determinare la struttura del gruppo $E(Z_5)$.*

Sol.: Si verifica che il discriminante di E non si annulla modulo 5 e si tratta quindi di una curva ellittica. La curva E ha otto punti con coordinate in $\mathbf{Z}_5$ (incluso il punto allinfinito). I punti di ordine 2 sono tre (vale a dire i punti $(0,0)$ e $(\pm 1,0)$). Lunico gruppo abeliano di ordine 8 con tre elementi di ordine 2 è $\mathbf{Z}_4 \times \mathbf{Z}_2$. Abbiamo quindi che $E(\mathbf{Z}_5)$ è isomorfo a $\mathbf{Z}_4 \times \mathbf{Z}_2$.

5. *Sia n un intero di 100 cifre. Dopo quante iterazioni dell'algoritmo ρ di Pollard possiamo dedurre che n non ha fattori con meno di 10 cifre?*

Sol.: Se n ha un fattore $\leq k$, questo viene probabimente individuato dopo $\sqrt{k}$ iterazioni dell'algoritmo ρ di Pollard. Nel nostro caso $\sqrt{k}$ è 10^5.