Teoria Elementare dei Numeri. Esercizi 1. Complessità.

Convenzione: Su questo foglio $\log n$ indica sempre il logaritmo in base 2 di n.

1. Quante cifre binarie ha all'incirca un numero intero n ?

2. Quante cifre decimali ha un numero n di $\log n$ cifre binarie?

3. Fra i numeri interi compresi fra 0 e 1000000, quanti hanno almeno 6 cifre?

4. Siano n ed m due numeri interi rispettivamente di $\log n$ ed $\log m$ cifre binarie. Quante cifre binarie hanno $n+m$, $-n$, $n-m$, $n \cdot m$, n^a, con $a \in \mathbb{N}$?

5. Sia n un intero di 100 cifre decimali. Quante cifre hanno all'incirca $\sqrt{n}$, n^3, $n+\sqrt{n}$? Di quante cifre differiscono all'incirca n, $n+\sqrt{n}$ e $n-\sqrt{n}$?

6. *(complessità delle operazioni aritmetiche sugli interi)* Siano n ed m interi rispettivamente di $\log n$ e $\log m$ cifre binarie.
   (a) Verificare che $n+m$ richiede $\mathcal{O}(\log n + \log m)$ operazioni.
   (b) Verificare che $n-m$ richiede $\mathcal{O}(\log n + \log m)$ operazioni.
   (c) Verificare che $n \cdot m$ richiede $\mathcal{O}(\log n \cdot \log m)$ operazioni.
   (d) Verificare che n^a richiede $\mathcal{O}(\log^2 n \cdot 2^{\log a})$ operazioni.
   (e) Verificare che $m : n$ richiede $\mathcal{O}(\log m \log n)$ operazioni.

7. Sia $b \in N$ un intero positivo fissato. Sia x un intero. Determinare la complessità del calcolo dell'espressione di x in base b
$$x = (a_n a_{n-1} \dots a_1 a_0)_b.$$

8. *(complessità dell'algoritmo di Euclide)* Siano m ed n interi rispettivamente di $\log m$ e $\log n$ cifre binarie. Verificare che l'algoritmo di Euclide per determinare $\gcd(m,n)$, il massimo comun divisore fra m ed n, ha una complessità dell'ordine di $\mathcal{O}(\log m \cdot \log^2 n)$.

9. Siano $n > m > 0$ interi e sia $d = \gcd(n,m)$. L'algoritmo di Euclide esteso produce interi x, y che soddisfano l'equazione diofantea $nx + my = d$. Mostrare che $|x| \leq m/d$ e $|y| \leq n/d$.

10. Sia $n \in N$ un intero positivo fissato. Sia x un intero. Determinare la complessità del calcolo di $\bar{x} \in \mathbb{Z}_n$, ossia della classe resto di x modulo n.

11. *(complessità delle operazioni aritmetiche in $\mathbb{Z}_n$)* Siano dati $\bar{x}$ ed $\bar{y}$ in $\mathbb{Z}_n$.
   (a) Verificare che $\bar{x} + \bar{y}$ richiede $\mathcal{O}(\log n)$ operazioni.
   (b) Verificare che $\bar{x} - \bar{y}$ richiede $\mathcal{O}(\log n)$ operazioni.
   (c) Verificare che $\bar{x} \cdot \bar{y}$ richiede $\mathcal{O}(\log^2 n)$ operazioni.
   (d) Verificare che $\bar{x}^a$ richiede $\mathcal{O}(\log^2 n \cdot \log a)$ operazioni.
   (e) Verificare che $\bar{x}^{-1}$ richiede $\mathcal{O}(\log^3 n)$ operazioni.

12. Determinare la complessità del test di primalità di Miller-Rabin usando 3 basi.

13. Sia n un intero di 100 cifre decimali. Supponiamo che il test di Miller-Rabin su n usando 3 basi richieda un tempo T. Quanto tempo richiede lo stesso test su un numero m di 200 cifre decimali? E su un numero N di 1000 cifre decimali?