CR1 – Crittografia 1

Alfonso Pesiri

Tutorato 1 – 6 Marzo 2008

Esercizio 1. Se $n \in \mathbb{N}$, sia $\varphi(n)$ la funzione di Eulero.

1. Descrivere un algoritmo per calcolare $\varphi(n)$ e stimarne la complessità.

2. Supponiamo che sia nota la fattorizzazione (unica) di $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$. Dimostrare che è possibile calcolare $\varphi(n)$ con un numero polinomiale di operazioni bit.

Esercizio 2. Dato il numero binario $n = (111001011101)_2$, calcolare $[\sqrt{n}]$ usando l'algoritmo delle approssimazioni successive.
(*Non passare a base 10 e non usare la calcolatrice!*)

Esercizio 3. Si stimi la complessità di un qualsiasi algoritmo per calcolare un fattore primo di un intero n.

Esercizio 4. Sia $m = p \cdot q$ la fattorizzazione in primi di m. Supponiamo di non conoscere p e q: calcolare la complessità per fattorizzare m essendo noto $\varphi(m)$.
Se invece p e q sono noti, quale sarà la complessità $\mathfrak{T}(\varphi(m))$?

Esercizio 5. Se $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, sia $\sigma(n)$ la somma dei divisori di n:

$$\sigma(n) := \sum_{d|n} d.$$

Stimare $\mathfrak{T}(\sigma(n))$ utilizzando il fatto che σ è una funzione moltiplicativa.