Università degli studi di Roma Tre
Corso di Laurea in Matematica, a.a. 1999/2000
Matematica Applicata 2
Secondo Test

I. Si calcoli la parte intera del numero binario

$$\sqrt{101011101}$$

utilizzando l'algoritmo delle approssimazioni successive.

II. Si fattorizzi completamente $5^{24} - 1$.
(*Suggerimento:* Utilizzare la calcolatrice solo dopo aver utilizzato il cervello – Potete utilizzare senza dimostrarlo il fatto che 39001 è un numero primo.)

III. Supponiamo che $p = 31$ e $q = 53$. Poniamo anche $e = 7$. Supponiamo che Bernardo scelga $(p \times q, e)$ come chiave pubblica RSA.

a. Se Alice vuole spedire a Bernardo il messaggio 30 utilizzando la precedente chiave. Come deve codificare (crittografare) il messaggio?
b. Calcolare il coefficiente di decodifica d che deve utilizzare Bernardo per decodificare il messaggio.

IV. Sia n un numero (binario). Si descriva un algoritmo per calcolare la parte intera della radice r–esima di n e si stimi il relativo tempo di esecuzione (utilizzando la notazione "O")
a. nel caso in cui r è fissato;
b. nel caso in cui r non è fissato.