26 Luglio 1999 - ORE 15:30
ESAME DI MATEMATICA APPLICATA 2
Alberto Berretti e Francesco Pappalardi

1. Si dia una stima per il numero di operazioni bit necessarie al calcolo della parte intera della norma di un vettore di $\mathbf{R}^{\mathbf{n}}$ assumendo che tutte le coordinate sono minori di 1000000.

2. Calcolare la parte intera di $\sqrt{10110101011}$ utilizzando l'algoritmo delle approssimazioni successive. (si tratta di un numero binario.)

3. Dimostrare che $n^7 - n$ è sempre divisibile per 42.

4. Sia $q = 37$ e $p = 41$.
   (a) Utilizzare $n = pq$ per spedire il messaggio "MAI" utilizzando RSA. Fare le cose in modo che sia necessario spedire il numero minimo di trasmissioni. (Scegliere a caso il valore di e)
   (b) decodificare il messaggio "NO" utilizzando le notazioni precedenti e sapendo che il messaggio è stato ottenuto utilizzando una sola trasmissione.

5. Si costruisca un polinomio di grado 3 irriducibile su $\mathbf{F_7}$.
   (a) Si illustri il metodo per calcolare tutti i polinomi di grado tre irriducibili su $\mathbf{F_7}$.
   (b) Si dica quanti sono i polinomi primitivi su $\mathbf{F_7}$ spiegando la ragione della risposta.
   (c) Quanti elementi può avere il campo di spezzamento di un generico polinomio di grado 3 su $\mathbf{F_7}$?

N.B. È consentito l'uso di una calcolatrice non scientifica. Tempo concesso 120 minuti.