30 Settembre 1999 – ORE 14:00
ESAME DI MATEMATICA APPLICATA 2
Alberto Berretti e Francesco Pappalardi

1. **(20 punti)** Si dia una stima per il numero di operazioni bit necessarie per calcolare l'inversa di una matrice 4×4 in cui tutte le componenti sono $\leq N$.

2. **(20 punti)** Si calcoli

$$62400^{5461} \pmod{61345}$$

utilizzando il metodo dei quadrati successivi.

3. **(30 punti)** Supponiamo si voglia implementare RSA per spedire il messaggio $FINEMA$ utilizzando una sola trasmissione.
   (a) Quale è il valore minimo del modulo RSA n che è necessario scegliere?
   (b) Dare un esempio di una possibile scelta di n.
   (c) Implementare RSA utilizzando come esponente di codifica $e = 33$ (Questo implica che n dovrà essere scelto in modo opportuno).
   (d) Calcolare l'esponente di decodifica d.

4. **(30 punti)** Si fattorizzi il polinomio

$$f(x) = x^9 + x^3 + x$$

su $\mathbb{F}_2$.
   (a) Quanti elementi ha il campo di spezzamento $\mathbb{K}$ di $f(x)$.
   (b) Determinare un polinomio irriducibile $g(x) \in \mathbb{F}_2[x]$ tale che il suo campo di spezzamento sia $\mathbb{K}$.
   (c) Sia α una radice di $g(x)$. Calcolare se esiste il logaritmo discreto in base α di $\alpha + 1$.

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