1 Settembre 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 del determinante di una matrice 3×3 a coefficienti interi in cui gli elementi della prima colonna sono in valore assoluto minori di M, quelli della seconda colonna sono in valore assoluto minori di N e quelli della terza sono in valore assoluto minori di L.

2. Calcolare la parte intera di $\sqrt{1101010001101}$ utilizzando l'algoritmo delle approssimazioni successive. (si tratta di un numero binario.)

3. **(10 punti)** Si determini un numero intero y nell' intervallo $[-80, 0]$ tale che
$$\begin{cases} y \equiv 2 \pmod 3 \\ y \equiv 2 \pmod 7 \\ y \equiv 4 \pmod{11} \end{cases}$$

4. Supponiamo si voler utilizzare RSA per spedire il messaggio $PERA$ utilizzando un alfabeto di 22 lettere (compreso lo spazio).
   (a) Scegliere due numeri primi p e q in modo che sia possibile spedire il messaggio utilizzando un'unica trasmissione.
   (b) Dopo aver calcolato $n = p \cdot q$ e $\varphi(n)$, si scelga come esponente di codifica $e = 2$ e si codifichi il messaggio.
   (c) Si scriva il messaggio crittografato in termini dell' alfabeto.

5. Si costruisca un polinomio f di grado 4 irriducibile su $\mathbf{F_2}$. Si indichi con α una radice di f e con $\mathbf{F_2}[\alpha]$ il campo di spezzamento di f.
   (a) Si calcolino tutte le radici primitive di $\mathbf{F_2}[\alpha]$.
   (b) Si calcoli il logaritmo discreto di $\alpha^3 + \alpha$ in base $\alpha^2 + 1$.
   (c) Quanti elementi può avere il campo di spezzamento di un generico polinomio di grado 4 su $\mathbf{F_2}$?

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