

9 Luglio 1999 - ORE 15:00
ESAME DI MATEMATICA APPLICATA 2
Alberto Berretti e Francesco Pappalardi

1. Sia $f(x) = \sin(x)$.
 - (a) Si stimi il tempo necessario per calcolare il valore del polinomio di Taylor di grado 3 intorno a 0 in un valore intero $x = n$.
 - (b) Si stimi il tempo necessario per calcolare il valore del polinomio di Taylor di grado k intorno a 0 in un valore intero $x = n$.
2. Si determini un numero intero positivo x nell' intervallo $[60, 120]$ tale che

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 4 \pmod{5} \\ x \equiv 2 \pmod{4} \end{cases}$$

3. (SIMULAZIONE DI RSA). Sia $p = 29$, $q = 31$, $n = pq$. Assumiamo che la chiave (pubblica) di codifica sia $e = 13$.
 - (a) Calcolare la chiave (segreta) di decodifica d .
 - (b) Crittografare la parola "ciao". (Usare 4 messaggi).
 - (c) Dire se è possibile scegliere $e = 5$ come chiave pubblica
4. Sia \mathbf{F}_3 il campo finito con 3 elementi.
 - (a) Determinare tutti i polinomi irriducibili di grado 3 su \mathbf{F}_3 .
 - (b) Determinare tutti i polinomi primitivi di grado 3 su \mathbf{F}_3
 - (c) Si scelga un polinomio irriducibile $f(x)$ non primitivo del punto (a) e sia α una sua radice primitiva. Determinare tutte le radici primitive di $\mathbf{F}_3(\alpha)$.

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