Feb. 2008 — Advanced Algorithms — Max: 1 Hour
Calculators are **not** permitted
Proper justification to your answers is **absolutely** necessary.

Name and Roll No.: ______________________________

1. Find a basis of Eigen vectors for the map defined from $\mathcal{C}^3 \longrightarrow \mathcal{C}^3$ by the matrix $\begin{bmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix}$ $\boxed{3}$

2. Find all Eigen values of the above matrix. Express your answer in terms of a_0, a_1, a_2 and a_3 $\boxed{3}$

3. Find the cordinates of the vector $(1, 0, 0)$ in : $\mathcal{R}^3$ with respect to tbe basis $(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0)^T$, $(\frac{-1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0)^T$, $(0, 0, 1)^T$. $\boxed{3}$

4. How many elements in Z^*_{pq} have square roots if p and q are primes? (Justify your answer) $\boxed{3}$

5. Does -1 have a square root in Z^*_{209}? Find all roots (if any). (Note: $209 = 11 \times 19$). $\boxed{3}$

6. Show that a number n of the form p^2q, p, q primes is not a Carmichael number. You may assume that $Z^*_{p^2}$ is cyclic as well as the CRT. Don't assume any theorem proved about Carmichael numbers. $\boxed{4}$

7. Let $g(x) \in Z_p[X]$ be irreducible of degree n. Let $\beta(x) \in Z_p[X]/\langle g(x)\rangle$. Show that there exists $a_0, a_1, ..., a_n$ in Z_p, *not all zero* such that $a_0 + a_1\beta(x) + a_2\beta^2(x)... + a_n\beta^n(x) = 0 \mod g(x)$ $\boxed{4}$