EXERCISE 7- DUE BY 27/01/05

1) **Factoring**

Consider the algorithm which reduces factoring to order finding: for N odd, composite integer, choose at random $1 \leq x < N$, with $gcd(x, N) = 1$ and find the order r of x modulo N. If r is even and $x^{r/2} \neq \pm 1 (mod\, N)$, then compute $gcd(x^{r/2} \pm 1, N)$ to find a non-trivial factor of N. Use Euclid's algorithm to compute the gcd. Apply this procedure to factor $N = 221$.

2) **Quantum State Entropy**

Consider the quantum state corresponding to the density operator

$$\rho = p|\psi\rangle\langle\psi| + (1-p)|\phi\rangle\langle\phi|, \tag{1}$$

where $p \in (0,1)$; $|\psi\rangle = \frac{1}{\sqrt{3}}|0\rangle + i\sqrt{\frac{2}{3}}|1\rangle$ and $|\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Compute the von Neumann entropy $S(\rho)$ and the Shannon entropy $H(p)$ of this state.

3) **Schmidt decompositions**

Consider the two-party quantum state $|\Psi\rangle_{AB}$ defined on the Hilbert space $H_A \otimes H_B$, of dimension 2×3, given by

$$|\Psi\rangle = \frac{1}{2} e_1 \otimes f_1 - \frac{i}{\sqrt{6}} e_1 \otimes f_3 + \frac{1}{2} e_2 \otimes f_2 + \frac{i}{\sqrt{3}} e_2 \otimes f_3,$$

where $\{e_i, f_j, i = 1, 2,\ j = 1, 2, 3\}$ are canonical bases in H_A, H_B respectively. Find the Schmidt decomposition of $|\Psi\rangle$.