Problems to Hand In:

Problem 1. Using the extended Euclidean Algorithm, find the first 5 best rational approximations, i.e., $v_1/u_1, \ldots, v_5/u_5$, to each of the following:

(a) $\log 3 / \log 2$.
(b) $83711/27720$
(c) $\sqrt{2}$
(d) $\ln 2$

Problem 2.

(a) How many solutions does the equation $x^2 = 1$ have in the ring of integers mod $2^n$?
(b) How many solutions does the equation $x^2 = 1$ have in the ring of $2 \times 2$ matrices over $GF(p)$?

Problem 3. Two elements $a$ and $b$ of $GF(2^m)$ are said to be conjugate if they have the same minimal polynomials. Prove that $a$ and $a^2$ are conjugate in $GF(2^m)$. 