Math 55: Discrete Mathematics, Fall 2008
Reading and Homework Assignment 4

Reading:

Lectures 11 & 12: 3.7 from Pseudoprimes to end
Lecture 13: Supplementary notes on Factoring Algorithms

Homework (due Monday, 9/29):

Odd-numbered self-checking exercises:

3.7: 31, 33, 45, 47, 59

Problems to hand in:

3.7: 32, 46, 60

(A) In Exercise 46, also find the decryption exponent d and check that the first block of your encrypted message decrypts to the right thing using this exponent.

(B) Apply Miller's test to the base 2 (as discussed in 3.7 Exercise 30 and the lecture) to determine that one of the two numbers 1601, 1729 is composite. What can you say about whether the other one is prime?

(C) Use Pollard's algorithm, with $f(x) = x^2 + 2$, and starting value $y_0 = z_0 = 6$, to factor 17741.

(D) (i) Prove that $2^n + 1$ is a pseudo-prime to the base 2 if and only if n is a power of 2, and deduce that if $2^n + 1$ is prime, then n must be a power of 2.
(ii) Verify that $2^1 + 1$, $2^2 + 1$, $2^4 + 1$, $2^8 + 1$, and $2^{16} + 1$ are prime, but that 641 is a factor of $2^{32} + 1$.

Reminder: The first midterm exam is Friday, Oct. 3. The exam will cover the material on homework assignments 1 through 4.