(Math 170) Homework 4:

Due October 11, 2007

All exercises are from "The Heart of Mathematics" text book.

Exercise 1: Chapter 2.5 Exercise 4

Exercise 2: Chapter 2.5 Exercise 16

Exercise 3: Chapter 2.5 Exercise 19

Exercise 4: Chapter 2.5 Exercise 21

Exercise 5: Find $gcd(42, 99)$ and then find x, y such that $42x + 99y = gcd(42, 99)$

Exercise 6: Find $gcd(2000, 101)$ and then find x, y such that $2000x+101y = gcd(2000, 101)$

Exercise 7: Find $gcd(2001, 102)$ and then find x, y such that $2001x+102y = gcd(2001, 102)$

Exercise 8: What is $\phi(24)$? What is 7^{65} mod 24 ?

Exercise 9: What is $\phi(11 * 25^2)$? How many numbers less than or equal to 400 have a common factor with 400?

Exercise 10: Suppose Jon wants to send Alice a message. Alice chooses for the modular number $p \times q = 11 \times 13 = 143$ and for the encryption number $e = 7$.

(a) What is $\phi(pq)$?

(b) What is the decryption number d? (i.e a number such that $e \times d = 1 + \phi(pq) \times y$ for some y). Use the extended Euclidean Algorithm.

(c) Jon takes his message MES and encodes it by taking MES^e mod pq. If the result is 24, what is the original message?

(Hint: the following website might help with your calculations

http://www.acme.com/software/bigint/

where modinv(X, Y) returns a number A such that $X \times A = 1$ mod Y and modpow(X, Y, Z) returns X^Y mod Z).