**Cryptography and Coding Homework 5**

**Vedasagar Karthykeyan (vkarthy1)**

**Problem 1:**

function [ x ] = crt( n, b )

k = length(n);

m = n(1,1);

c = b(1,1);

for i=2:k

    [gcd, X, Y] = extendedEuclideanAlgo(m, n(1,i));

    x = c\*Y\*n(1,i) + b(1,i)\*X\*m;

    m = n(1,i)\*m;

    c = x;

end

x = mod(x, m);

Diary:

crt([2 3 5 7 11], [1 2 3 4 5])

ans =

1523

crt([3 4 7 11 13], [2 3 4 5 6])

ans =

5219

crt([3 5 7 11 13], [2 3 4 5 6])

ans =

14228

crt([5 7 9 11 13], [1 2 3 4 5])

ans =

22521

crt([2 3 5 7 9 11 13 17 19], [2 3 4 5 6 7 8 9 10])

ans =

17347846

**Problem 2:**

a)

function [ p ] = rel\_prime( M, N )

clc;

n = 0;

for i=1:N

    r\_1 = randi([1 M],1,1);

    r\_2 = randi([1 M],1,1);

    d = gcd(r\_1, r\_2);

    if d == 1

        n = n+1;

    end

end

p = n/N;

b)

rel\_prime (10000000, 10000000)

ans =

0.6080

e)

p = 1;

for i=primes(10000)

    p = p \* (1-(1/(i^2)));

end

p

prime\_prob

p =

0.6079

**Problem 3:**

a)

sum = 0;

for i=1:10000000

    sum = sum + (1/(i^2));

end

sum

rzf

sum =

1.6449

c)

1/sum

ans =

0.6079