For Problem 1

crt.m:

```
function output = crt(n,b)
%takes input vectors n and b, returns x
%which is congruent to each respective entry of b modulo
%the respective entry of n
%x is nonnegative and less than the product of entries
%of n
ln = length(n);
lb = length(b);
%check if two vectors are of different length
if ln ~= lb
   output='two vectors do not have equal length!';
   return
end
%check if input vectors have length less than 5
if ln < 5
   output='vector length is shorter than 5!';
   return
end
smalln = 1;
%check if entries in n are nonzero and pairwise relatively prime
%in the same time compute their product
for i=1:ln
   if n(i) == 0
      output='entry in n cannot be 0!';
      return
   end
   for j=1:i-1
      temp = extendedeuclid(n(j),n(i));
      if temp(1) ~= 1
         output='entries in n are not pairwise relatively prime!';
         return
      end
   end
   smalln = smalln * n(i);
end
x = 0;
%computes x
for k=1:ln
   bign = smalln/n(k);
   bigninv = inverse(bign,n(k));
   x = x + b(k) * bign * bigninv;
end
```

For Problem 1

```
output = mod(x,smalln);
```

Helper methods:

inverse.m:

```
function output = inverse(a,n)
%We assume the input a and n are relatively prime
%Since xa = qn + 1, we find xa - qn = 1
%we use extended euclid algorithm as subroutine
%we don't care what q is since we only need x
%if a<n, extendedeuclid will give us temp(3) as x
temp = extendedeuclid(a,n);
output=mod(temp(2),n);
if a<n
    output=mod(temp(3),n);
end

if temp(1) == a || temp(1) == n
   output=0;
end

if a == 0 || n == 0
   output=0;
end
end
```

extendedeuclid.m:

```
function output = extendedeuclid(a,b)
%we assume input a > b, if a < b, we swap them in the beginning
areal=a;
breal=b;
if a < b
    temp=a;
    areal=b;
    breal=temp;
end;
%initializing our matrix
output=[];
A=[];
Q=[];
X=[];
Y=[];
A(1)=areal;
```

For Problem 1

```
A(2)=breal;
Q(1)=0;
X(1)=1;
X(2)=0;
Y(1)=0;
Y(2)=1;
i=2;
%do euclid algorithm until A(i) is 0
while A(i) > 0
   Q(i)=floor(A(i-1)/A(i));
   A(i+1)=A(i-1)-Q(i)*A(i);
   X(i+1)=X(i-1)+Q(i)*X(i);
   Y(i+1)=Y(i-1)+Q(i)*Y(i);
   i=i+1;
end
%since in the end, i is 1 greater than the last i recorded in the matrix,
%and in matlab index 1 is actually index 0, these effects cancal out when
%we are deciding the signs of X and Y in the end
%the first column of output is gcd(a,b), second column is x, and third is y
output=[output;A(i-1)];
output=[output;(-1)^(i)*X(i-1)];
output=[output;(-1)^(i+1)*Y(i-1)];
end
```

For Problem 1

<u>problem1_diary.txt</u>

```
n = [0,1,2,3,4]

n =

    0    1    2    3    4

b = [1,2,3,4,5]

b =

    1    2    3    4    5

crt(n, b)

ans =

entry in n cannot be 0!

n = [1,3,5,7,9]

n =

    1    3    5    7    9

b = [1,2,3,4,5]

b =

    1    2    3    4    5

crt(n, b)

ans =

entries in n are not pairwise relatively prime!

n = [11,19,37,35,31]

n =

   11   19   37   35   31
```

For Problem 1

```
b = [2,3,4,5,6]

b =

    2     3     4     5     6

crt(n, b)

ans =

     754360

mod(754360-2,11)

ans =

    0

mod(754360-3,19)

ans =

    0

mod(754360-4,37)

ans =

    0

mod(754360-5,35)

ans =

    0

mod(754360-6,31)

ans =

    0
```

For Problem 1

```
n = [1,3,5,7,11]

n =

    1     3     5     7    11

b = [1,3,7,5,9]

b =

    1     3     7     5     9

crt(n, b)

ans =

  537

mod(537-1,1)

ans =

    0

mod(537-3,3)

ans =

    0

mod(537-7,5)

ans =

    0

mod(537-5,7)

ans =

    0

mod(537-9,11)
```

For Problem 1

```
ans =

    0

n = [1,2,3,5,7,11,19,23]

n =

    1     2     3     5     7    11    19    23

b = [1,1,1,1,1,1,1,1]

b =

    1     1     1     1     1     1     1     1

crt(n, b)

ans =

    1

b = [1,2,3,4,5,6,7,8]

b =

    1     2     3     4     5     6     7     8

crt(n, b)

ans =

     883944


mod(883944-1,1)

ans =

    0

mod(883944-2,2)
```

For Problem 1

```
ans =

    0

mod(883944-3,3)

ans =

    0

mod(883944-5,4)

ans =

    3

mod(883944-4,5)

ans =

    0

mod(883944-5,7)

ans =

    0

mod(883944-6,11)

ans =

    0

mod(883944-7,19)

ans =

    0

mod(883944-8,23)

ans =
```

For Problem 1

```
    0

n = [1,2,3,5,7,11,13,17]

n =

    1     2     3     5     7    11    13    17

b = [3,3,3,3,3,3,3,3]

b =

    3     3     3     3     3     3     3     3

crt(n, b)

ans =

    3

n = [1,2,3,5,7,11,13,17]

n =

    1     2     3     5     7    11    13    17

b = [3,3,4,3,3,3,3,3]

b =

    3     3     4     3     3     3     3     3

crt(n, b)

ans =

     170173

mod(170173-3,1)

ans =

    0
```

For Problem 1

```
mod(170173-3,2)

ans =

    0

mod(170173-4,3)

ans =

    0

mod(170173-3,5)

ans =

    0

mod(170173-3,7)

ans =

    0

mod(170173-3,11)

ans =

    0

mod(170173-3,13)

ans =

    0

mod(170173-3,17)

ans =

    0

diary off
```

For Problem 2

probability.m:

```
function output = probability(M,N)
%do this N times: randomly selects 2 integers 1-M
%and test if it is relatively prime to each other
%outputs probability of them being relatively prime
n = 0;
for i=1:N
   first = round(rand(1)*M);
   second = round(rand(1)*M);
   temp = extendedeuclid(first,second);
   %increment n count when two integers are relatively prime
   if temp(1) == 1
      n = n+1;
   end
end
output = double(n/N);
end
```

rho.m:

```
function output = rho(N)
%inputs a range 1...N
%outputs the product of (1-1/p^2) over all primes<N
x = 1;
for i = primes(N)
   x = double(x*(1 - double(1/i^2)));
end
output = double(x);
end
```

For Problem 2

problem2_diary.txt:

```
>> probability(100,100)

ans =

   0.6000

>> probability(1000,1000)

ans =

   0.6360

>> probability(1000,10000)

ans =

   0.6087

>> probability(10000000,10000000)

ans =

   0.6078

>> rho(100)

ans =

   0.6090

>> rho(10000)

ans =

   0.6079

diary off
```

For Problem 3

rz.m:

```
function output = rz(N)
%takes input of N
%returns the summation of 1/n^2 of n from 1 to N
x = 0;
for i = 1:N
   x =(x+(1/i^2));
end
output = double(x);
end
```

problem3_diary.txt:

```
rz(10000000)

ans =

   1.6449

diary off
```