Math 351
Workshop #2
September 12, 2007

The first two problems concern the best known "public key cryptosystem". This is due to R. Rivest, A. Shamir and L. Adleman (1977) and, in consequence, is known as RSA encryption. ``Public key" means that the encoding algorithm (which depends on two integers n and e called the ``keys") can be made public, so that anyone can encode a message. Although the process for decoding messages is known, it requires knowing the prime factorization of n. For large n, obtaining this factorization is such lengthy process that it is effectively impossible).}

We start with a preliminary result.

#1 Let a,r,s be integers with (r,s) = 1. If r divides a and s divides a, then (rs) divides a. Consequently, if p and q are distinct primes such that p divides a and q divides a, then (pq) divides a.

Now we can describe the RSA encryption method.

#2 Let p and q be distinct primes, n = pq, k = (p-1)(q-1), and let d be an integer with (d,k) = 1.

(a) Last week we saw that if p is prime and a is an integer then $p|(a^p-a)$ (Fermat's Little Theorem). Use this to conclude that if p does not divide a, then $p|(a^{p-1} - 1)$.

(b) Let p,q,k be as above. Show that for any integer a such that p∤a, $p|(a^k - 1)$.

(c) Let p,q,n,k,d be as above. Since (d,k) = 1, there are integers e and t such that de + kt = 1. Show that for any integer a, $n|(a^{de} - a)$.

In the RSA system, n and e are made public. A message is represented by a sequence of "blocks", each of which is an integer modulo n, say $a_1a_2...a_r$. The message is encrypted by replacing each block a_i by a_i^e. Thus the encrypted message is $a_1^e a_2^e ... a_r^e$. It is decrypted by taking the d-th power (modulo n) of each block.}

The next problem investigates how many solutions the equation [a]x = [b] can have in $\mathbf{Z}_n$. The first part of the problem asks you to work out some examples which will show that there may be no solution, there may be exactly one solution, or there may be more than one solution. The other parts of the problem ask you to describe how to find the number of solutions in all cases.

#3 (a) How many solutions does the equation [4]x = [6] have in $\mathbf{Z}_7$, in $\mathbf{Z}_{10}$, in $\mathbf{Z}_8$?

(b) Let d = (a,n). Show that if d does not divide b then [a]x = [b] has no solution in $\mathbf{Z}_n$.

(c) Let d = (a,n). Show that if d divides b then [a]x = [b] has at least one solution in $\mathbf{Z}_n$. (You might want to recall that d = ra + sn for some integers r and s and use this to write a solution.)

(d) Let d = (a,n) and assume d divides b. Show that the number of solutions of [a]x = [b] in $\mathbf{Z}_n$ is the same as the number of solutions of [a]x = [0]. (Hint: Suppose that [c_1] and [c_2] are solutions of [a]x = [b]. What can you say about [c_1 - c_2]?

(e) Let d = (a,n). How many solutions does [a]x = [0] have in $\mathbf{Z}_n$?

(f) Combine your results from (a) - (e) into a theorem of the form "The equation [a]x = [b] has a solution in $\mathbf{Z}_n$ if and only if ... If there is a solution, the number of solutions is ??"