CSE 321: Discrete Structures
Assignment #4
January 28, 2009
Due: Wednesday, February 4, in class

Reading Assignment: Sections 3.4 – 3.7 and 4.1 – 4.2.

Problems:

1. Let a, b and c be integers. Prove that if a does not divide bc, then a does not divide c.

2. Prove that any prime number bigger than 3 is congruent to 1 or 5 modulo 6.

3. Compute the greatest common divisor for each of the following pairs of numbers.

   (a) gcd($2^2 3^3 5^5,\ 2^5 3^3 5^4$)

   (b) gcd(20!, 127)

4. Use Euclids algorithm to compute the following, showing the values of x and y for each iteration of the algorithm.

   (a) gcd(1020, 1173)

   (b) gcd(1019, 1173)

5. Using only your brain, pencil, and paper (*e.g.*, no calculator), compute 23^{25} mod 31. Show your intermediate steps (as proof that you used your brain instead of a calculator). (Hint: If you use the method demonstrated in lecture, you should never need to compute any product greater than $15 \cdot 15$.)

6. In this problem, you will use the RSA cryptosystem to do some encryption and decryption. Please use the version presented in lecture. Your primes are $p = 23$ and $q = 41$, and you will encrypt and decrypt two-letter messages at a time.

   You will need either a calculator or computer program. If you're fast, it can be done in about 15 minutes using a checkbook calculator; if you do this, it pays to figure out how to use one memory location to compute integer remainders efficiently. Alternatively, it's fine if you decide to write a simple program to do the modular exponentiation, as long as you do it by the "repeated squaring and reduction" method used in lecture, and print out the intermediate results as described below.

   (a) What are the values of the public key n and the secret key s that correspond to the choices of p and q above?

   (b) You want to encrypt the two-letter message HA. You translate this into the integer 0801, since H is 8th letter and A is the first letter. Compute the encrypted message $C = E(801)$, showing the intermediate results after each reduction mod n.

(c) For the value of C that you obtained in the part (b), compute D(C), showing the intermediate results after each reduction mod n.

(d) There is an easy check if you got the right answer in part (c). Which one?

(e) Why are these choices of p and q insufficient for encrypting and decrypting all possible 2-letter messages using the method of parts (b) and (c)? Can you suggest a simple fix that would allow you to stick with these choices of p and q?

7. **Extra credit**: Prove that if a, b, and m are integers such that $m \geq 2$, and $a \equiv b$ (**mod** m) then gcd(a, m) = gcd(b, m).