CS 261 HW5

Prof. Jared Saia, University of New Mexico

Due Friday, March 12th

This homework covers material from Chapter 3.6 up to and including Chapter 3.7 in the textbook.

1. Let $c = gcd(29, 27)$. Write c as $s29 + t27$ for some integers s and t.

2. Find the following inverses using the technique described on pages 234-235 in the book (and in class). Show how you are using Euclid's algorithm to find the inverse.

   - The inverse of 4 mod 7
   - The inverse of 17 mod 141

3. Find the following solutions using the technique described on pages 234-235 in the book (and in class). Again, show how you are using Euclid's algorithm to find the solutions.

   - Solutions to the congruence $2x \equiv 2 \pmod 5$
   - Solutions to the congruence $3x \equiv 1 \pmod{17}$

4. Your friend is thinking of a number x that is between 0 and 14. She tells you that this number has a remainder of 1 when divided by 3 and a remainder of 0 when divided by 5. Use the Chinese Remainder Theorem to solve for this number.

5. Your friend is thinking of a number x between 1 and 100. For any y and z both less than 15, you can ask her the value of x mod y and the value of x mod z. Give values y and z that will allow you to determine x based on her responses. Justify your answer. Hint: There are many pairs that will work (and many that will not!).

6. Exercise 3.7.48

7. Consider an RSA key set with $p = 11$, $q = 29$, $n = 319$ and $e = 3$. What value of d should be used for the secret key? What is the encryption of the message $M = 100$?

8. In this problem you'll use RSA to encrypt and decrypt a message when $n = 43 * 59 = 2,537$ and $e = 13$.

   - Consider the message "HELP". Translate each letter into integers and group together pairs of integers as on pages 243-244 of the book. Now use RSA to encrypt these integers into an encrypted message.
   - Now use RSA decryption to decrypt the encrypted message from the previous step and verify that you do get back the original message.

9. Imagine that you are trying to secretly communicate with a friend via radio broadcast; that an enemy is listening in on every message sent between you and your friend; but that this enemy is unable to factor numbers. Assume you're using RSA and that you've chosen $p = 43$, $q = 59$ and $e = 13$ as above. Describe exactly what number(s) you will send to your friend so that your friend can communicate a message to you secretly. Next, assume that your friend wants to send the message "HELP" to you secretly after receiving your broadcast. Describe how she does this and why you can read the message but the adversary can not. Note: You need to say both what you send to your friend **and** what your friend sends to you.