CS 261 HW5

Prof. Jared Saia, University of New Mexico

Due Thursday, April 4th

This homework covers material from Chapter 4.4 up to and including Chapter 4.6 in the textbook.

1. Let $c = gcd(29, 27)$. Write c as $s29 + t27$ for some integers s and t.
2. Prove that the product of any 4 consecutive integers is divisible by 12.
3. Find the following inverses using the technique described in Chapter 4.4 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
4. Find the following solutions using the technique described in Chapter 4.4 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 $3x \equiv 1 \pmod{17}$
5. 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.
6. Your friend is thinking of a number x between 1 and 100. For any positive integers 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!).

7. Exercise 4.4.30: "Complete the proof of the Chinese Remainder Theorem..."

8. Decrypt the following message that was encrypted with a Caesar cypher: "Cpklv nhtlz ybpulk tf spml. Nvvk aopun P ohcl adv tvyl!". Hint: One approach is to read the section on decryption of Caesar cyphers at the end of section 4.6.

9. Use Fermat's Little Theorem to find find 7^{212} modulo 11. Show your work.

10. Exercise 4.4.67: "Describe a brute force algorithm for solving the discrete logarithm problem..."

11. In this problem you'll use RSA to encrypt and decrypt a message when $p = 43$, $q = 59$ and $e = 13$.

    - Consider the message "HELP". Translate each letter into integers and group together pairs of integers into blocks. Next 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. What value do you use for d?

12. 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.