Math 1111 Fall 2015 – Problem Set 5

1. Find the decimal representation of each of the following binary numbers. (Spaces added for readability.)
    a. 1 011
    b. 100 000
    c. 101 101 101
    d. 111 000 000 001

2. Find the binary representation of each of the following decimal numbers.
    a. 78
    b. 128
    c. 300
    d. 513

3. Suppose you're given the following cipher: 15-17-22-11-1-22-24-31. You find a clue that leads you to believe these numbers are given in some base other than the usual base 10. Find the plaintext for this cipher.[1]

4. Suppose *x* is a two-digit positive integer when represented in decimal form. How many digits could *x* have…
    a. When represented in binary form?
    b. When represented in base-3?
    c. When represented in hexadecimal (base-16)?

5. In class, we considered how to encrypt the plaintext "HELLO" using the key 541. First, we converted "HELLO" to ASCII, then to binary. Then, we converted the key, 541, to binary. Then, we wrote out the plaintext in binary alongside the key, repeated as many times as necessary. Then, we added corresponding digits using mod-2 arithmetic, as shown:

Plaintext	1001000	1000101	1001100	1001100	1001111
Key	1000011	1011000	0111011	0000111	0110000
Ciphertext	0001011	0011101	1110111	1001011	1111111

    a. What do you get when you "add" the *ciphertext* to the key—adding corresponding digits using mod-2 arithmetic?

[1] This problem was adapted from *The Beekeeper's Apprentice* by Laurie R. King. In this novel, Sherlock Holmes takes on a 15-year-old girl as his apprentice in his retirement years.

b. Decrypt the following ciphertext, using the same encryption method and key (541) as above. (You'll need to find an ASCII table online to finish your decryption.)

`0000111 0010001 1111101 1000001 1111001 0110011`

6. Consider the integers 4025 and 1242.
   a. Use the Euclidean Algorithm to find the greatest common divisor of 4025 and 1242.
   b. Use your work from part (a) to find integers s and t such that $4025s + 1242t = \gcd(4025, 1242)$.

7. Suppose Bob is sending a message to Alice using the RSA encryption process detailed in the "From Bob to Alice" handout. Let $p = 7$, $q = 11$, and $e = 49$. Find a value for d as described in Step 4 using the Euclidean algorithm.

8. Consider the set of integers $S = \{1, 2, \ldots, n\text{-}1\}$, where n is a positive integer. Define the operation $\square$ on this set as follows: If a and b are integers in the set S, then $a \square b = (ab) \text{ MOD } n$.

   Note that this operation is **closed** (that is, if a and b are in S, then $a \square b$ is also in S), **associative** (that is, $a \square (b \square c) = (a \square b) \square c$, for any a, b, and c in S), and has an **identity** (1). If we can show that every element in S has an **inverse** under this operation, then S (along with this operation) satisfies the conditions to be a **group**.

   Argue that if n is prime, then S is a group.

   (Hint: Use one of the theorems from our discussion of the RSA algorithm.)