

## Math 1111 – Problem Set 5

1. On a certain multiple-choice exam, there are five questions, each with four choices. Bubba has not studied for the exam at all and decides to guess answers at random. What is the probability that...
  - a. The first question he gets right is the 5th question?
  - b. He gets all questions right?
  - c. He gets at least one question right?
  - d. He gets exactly three questions right?
  - e. He gets at least three questions right?
2. After becoming suspicious that the Twitter account @everycolorbot is using least significant bit steganography to hide messages in its tweets, you pull up the eight most recent RGB colors posted by the account:  
  
`#6afe87 #d5fd0f #aafa1e #57f43c #aee879 #5ed0f2 #bea1e5 #7f43ca`  
  
If your hunch is correct, and if @everycolorbot is using the red channel to encode its secret messages, what letter is encoded in these eight colors?
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.<sup>1</sup>
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? (Provide both the minimum and maximum digits possible.)
  - b. When represented in base-3? (min and max)
  - c. When represented in hexadecimal (base-16)? (min and max)
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:

---

<sup>1</sup> 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.

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

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

- Consider the integers 4025 and 1242.
  - Use the Euclidean Algorithm to find the greatest common divisor of 4025 and 1242.
  - Use your work from part (a) to find integers  $s$  and  $t$  such that  $4025s + 1242t = \gcd(4025, 1242)$ .
- 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.
- Consider the set of integers  $S = \{1, 2, \dots, n-1\}$ , 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. And make use of the fact that  $(a \text{ MOD } n) (b \text{ MOD } n) \text{ MOD } n = (ab) \text{ MOD } n$ .

- Consider the affine cipher  $y = (mx + b) \text{ MOD } 26$ , where  $x$  is an integer between 0 and 25 corresponding to a letter in the plaintext,  $y$  is an integer between 0 and 25 representing the corresponding letter in the ciphertext, and  $m$  and  $b$  are constants, each integers between 0 and 25. Suppose that the plaintext “ca” corresponds to the ciphertext “RF” under this cipher. To

what does the plaintext "vi" correspond?