CSCI2824 Assignment 5

Due date: Monday March 7 in class
Submission Format: both, hard hard copy in class and online on moodle

Your answers should be clear and well-organized, and written in full sentences in proper English when asked to provide explanations. Please type your answers, or write VERY neatly. Also, be advised that **late submissions will not be accepted**.
Do not forget to staple your hard-copy sheets if you have multiple pages.

Problems

1. In class, we discussed the Chinese remainder theorem, and we showed an algorithm for "decoding" the remainders of two distinct primes. For example, suppose we want to know which number between 0 and 34 has remainder 1 when divided by 5 and 2 when divided by 7. We begin by finding the Bezout theorem parameters that would allow multiples of 5 and 7 to add up to 1:

   5*3 + 7*(-2) = 1

   Then, we multiply our two desired remainders (here, 1 and 2) by the two terms in our Bezout expression. The first remainder is multiplied into the second term, and the second remainder is multiplied into the first term:

   5*3*2 + 7*(-2)*1 = 30-14 = 16

   And now we can conclude (and check) that 16 has remainder 1 when divided by 5 and remainder 2 when divided by 7.

   Your job is to extend this technique to 3 distinct primes. (We could continue on to more than 3 primes, but this problem provides the general idea of how to continue.) Suppose we choose 3 primes (let's say, 3, 5, and 7). Now, we want to find a number that has a remainder of 0 when divided by 3, 4 when divided by 5, and 5 when divided by 7. In other words, our desired number n should have the properties:

   n mod 3 = 0
   n mod 5 = 4
   n mod 7 = 5

   And we'll assume that n is in the range between 1 and 104 (since we are interested in numbers that are less than 3*5*7 = 105).
   Show that you can extend the technique from class to find the desired number.
   Hint: you want to use the very same technique that you used for two primes, but now use that technique sequentially. First, find a number that has remainder 0, mod 3 and remainder 4, mod 5; this will give you a number j with

the right remainder mod 15. Now find a number between 1 and 104 that has remainder j, mod 15 and remainder 5, mod 7. This will be your desired number.

2. A carrier has delivered a letter to Julius Caesar from one of his commanders. The commander was supposed to report number of soldiers in enemy troop, But the letter happens to be encrypted to avoid revealing information to anyone other than Caesar. The letter shows the following text:

> Smxxuo fdunq tme dagstxk mdagzp 1000 eaxpuqde, ngf U'y zaf dqmxxk egdq ar ftq qjmof zgynqd. U emi ftqud bmdmpq mzp tqdq ue itmf tmbbqzqp. itqz ftqk iqdq xuzuzs gb uz daie ar 11, U oagzfqp ftmf ftq ruzmx "dqymuzpqd" dai tme 9 eaxpuqde. Itqz ftqk iqdq xuzuzs gb uz daie ar 13, U rusgdqp ftmf ftq ruzmx "dqymuzpqd" dai tme 1 eaxpuqd mzp itqz ftqk xuzqp gb uz daie ar 17, ftqdq iqdq 14 eaxpuqde uz ftq ruzmx "dqymuzpqd" dai.

   Suppose you are trusted consultant of Caesar and you have to tell him the exact number of enemy soldiers from this letter.

   a. Decipher this letter. (show your **frequency analysis** result and the **key** you found. You can write a program to do this or use online tools to do the frequency analysis and word shift. But if you do so mention what source you used in your sheet)

   b. What is the exact number of soldiers?

3. **Divisors and totient function**
   a. Suppose we have a given positive natural number m that is greater than the nth prime but less than the n+1th prime. (For example, 12 is greater than 11, the 5th prime, but less than 13, the 6th prime.) Now we express our number m in the form:

$$m = 2^{e_1} \times 3^{e_2} \times 5^{e_3} \times 7^{e_4} \times \ldots \times {p_n}^{e_n}$$

   where the exponents can include 0. Write an expression, in terms of the exponents $e_1, \ldots, e_n$, that denotes the number of distinct divisors of our number including 1 and m itself. (For example, 12 has 6 divisors: 1, 2, 3, 4, 6, and 12.) you can write it down for a couple of numbers and then for a given "n" try to find a function between **number of devisors of n** and **set of exponents $e_1, \ldots, e_n$**

   b. Suppose a number m is the product of two distinct primes, p and q. prove that the Euler totient of m is equal to (p-1)(q-1). For instance, the Euler totient of 35 (which is 5 * 7) is equal to 4*6, or 24. But remember that when you prove a theory you need to write it in terms of variables rather

than numbers. (hint: you might want to check additive or multiplicative properties of totient function)

4. **Set Theory**
   At Boulder High School in the freshman class, 37 students use variety of forms of transportation to get to school every day.
   20 of them sometimes arrive to school by car,
   12 students bike to school at least occasionally,
   16 students take the bus some days.
   If 4 students use all three of these options,
   2 either bike or take the bus,
   6 come by car or bike,
   and 5 arrive by car when they do not come on the bus,
   how many students always use some other type of transportation?

5. The following problem will take you step by step through a proof that for all sets A, B, we have $|A \setminus B| = |A| - |A \cap B|$. Give very short and succinct arguments for each part below to complete the reasoning. Please do not use Venn diagrams.
   a. Prove that $A = (A \setminus B) \cup (A \cap B)$.
      (Hint: You should prove that $(A \setminus B) \cup (A \cap B) \subseteq A$ and vice-versa)
   b. Prove that $(A \setminus B) \cap (A \cap B) = \{\}$
      (Hint: Try a proof by contradiction for this statement.).