CRYPTOGRAPHY MISSION 05 DOSSIER

Deadline: Thursday, 5 October 2017 at 10:50am
This mission covers Sections 3.1, 3.2, 3.3, 3.4, 3.6.

Check one:

☐ I received help from the following classmate(s) on this assignment:

____.

☐ I did not receive any help on this assignment.

1. Graded Problems

1. Let $F_1 = 1, F_2 = 1, F_{n+1} = F_n + F_{n-1}$ define the Fibonacci numbers $1, 1, 2, 3, 5, \cdots$.
   a. List the first 15 Fibonacci numbers.

   b. Compute the greatest common divisor for the following pairs: F_{10} and F_7, F_6 and F_9, F_6 and F_{12}, F_{10} and F_{13}.

c. Look at your previous examples. It turns out that $\gcd(F_m, F_n) = F_{\gcd(m,n)}$. Write out **two** specific and detailed examples to verify that you believe this is true.

d. Play with some examples, and make a conjecture about $\gcd(F_n, F_{n-1})$ for $n \geq 1$. Are there any patterns? Describe them here.

2. a. Use the Euclidean algorithm to compute $\gcd(8207, 4811)$.

b. Factor 8207 and 4811 by using CoCal's `factor(a,b)`. In a sentence or two, explain why the Euclidean algorithm is the faster method of computing the gcd (rather than factoring and using the definition of gcd).

3. You can also compute a gcd using CoCalc's `gcd(a,b)`. For this problem, determine the solution for the following gcd computations.

   a. $\gcd(234, 6013)$

   b. $\gcd(74951, 26269)$

   c. $\gcd(5223389, 188434513)$

4. (Fermat's Little Theorem and Euler's Theorem) Recall that $(a^b)^c = a^{bc}$. Compute each of the following without a calculator or computer (you can double-check with code).

   a. $\varphi(35)$

   b. $514^{372} \mod 13$

   c. $2^{49} \mod 15$

5. (Honors) This problem is going to walk you through another way of thinking about the proof of Fermat's Little Theorem but using combinatorics. Recall that we have $a^{p-1} \equiv 1 \bmod p$ for a number a and a prime p in which $\gcd(a, p) = 1$. This can be rewritten as $a^p \equiv a \bmod p$ or that $a^p - a$ is divisible by p.

   a. Suppose $p = 5$. Consider all the possible strings of $p = 5$ symbols, using an alphabet with $a = 2$ different symbols. For example, if your letters are A and B, then a possible string is $ABAAA$. How many different strings are there? List them.

   b. Think of each letter in the string as a bead, and tie them into a "necklace." If you rotate one necklace corresponding to a string and get another string, they are considered the same. For example: $ABAAA$ and $AABAA$ form the same necklace. Group your necklaces together. How many unique necklaces are there?

   c. Notice that 2 of the strings only have one letter of the alphabet. All of the other necklaces have 5 strings. So this shows that $2^5 - 2$ is divisible by 5. Use this reasoning and a sentence or two to explain how this proves Fermat's Little Theorem in general.

2. Recommended Exercises

These will not be graded but are recommended if you need more practice.

- Section 3.13: # 1, 3, 5, 7, 9, 15
- Section 3.14: # 1, 5, 7