# CRYPTOGRAPHY MISSION 04 SOLUTIONS

**Deadline: Thursday, 22 September 2016 at 3:05pm**
This mission covers Sections 3.1 and 3.3.

## 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.

$F_1 = 1, F_2 = 1, F_3, = 2, F_4 = 3, F_5 = 5, F_6 = 8, F_7 = 13, F_8 = 21, F_9 = 34, F_{10} = 55, F_{11} = 89, F_{12} = 144, F_{13} = 233, F_{14} = 377, F_{15} = 610$

   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 $F_{13}$.

$$\gcd(F_{10}, F_7) = \gcd(55, 13) = 1$$
$$\gcd(F_6, F_9) = \gcd(8, 34) = 2$$
$$\gcd(F_6, F_{12}) = \gcd(8, 144) = 8$$
$$\gcd(F_{10}, F_{13}) = \gcd(55, 233) = 1$$

   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.

Note that $\gcd(F_3, F_4) = \gcd(2, 3) = 1$, $\gcd(3, 4) = 1$, and $F_1 = 1$.

Note that $\gcd(F_3, F_9) = \gcd(2, 34) = 2$, $\gcd(3, 9) = 3$, and $F_3 = 2$.

   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.

Some examples:

$$\gcd(F_3, F_4) = \gcd(2, 3) = 1$$
$$\gcd(F_5, F_6) = \gcd(5, 8) = 1$$
$$\gcd(F_7, F_8) = \gcd(13, 21) = 1$$

Conjecture: $\gcd(F_n, F_{n-1}) = 1$ since we always seem to be getting 1 so far.

2. You can compute a gcd using SageMath's `gcd(a,b)`. Determine the solution for the following gcd computations.

   a. $\gcd(234, 6013)$

   | |
   |---|
   | 1 |

   b. $\gcd(74951, 26269)$

   | |
   |---|
   | 241 |

   c. $\gcd(5223389, 188434513)$

   | |
   |---|
   | 30193 |

3. In class, we started practicing writing proofs or formal mathematical arguments. In this problem, we're going to walk through the proof of a theorem.

   a. The Theorem you want to prove is: Let $a, b, c, d$, and $n$ be integers with $n > 0$. If $a \equiv b \bmod n$ and $c \equiv d \bmod n$, then $ac \equiv bd \mod n$. First, come up with an example (with specific numbers) to convince yourself this is true.

   Suppose we have the following numbers:

   $$\begin{aligned} a &= 1 \\ b &= 6 \\ c &= 11 \\ d &= 16 \\ n &= 5 \end{aligned}$$

   Note that $1 \equiv 6 \bmod 5$ and $11 \equiv 16 \bmod 5$. If we multiply, we get $ac = 1 \cdot 11 = 11 \bmod 5 \equiv 1 \bmod 5$ as well as $bd = 6 \cdot 16 = 96 \bmod 5 \equiv 1 \bmod 5$.

   b. Which part of the theorem is the hypothesis? This is what you assume.

   Let $a, b, c, d$, and $n$ be integers with $n > 0$. If $a \equiv b \bmod n$ and $c \equiv d \bmod n$...

   c. Which part of the theorem is the conclusion? This will be what you show is true based on the hypothesis.

   ... then $ac \equiv bd \mod n$.

   d. Write out the definition of $a \equiv b \bmod n$.

   This means $n \mid (a - b)$ or $(a - b) = nk$ for some integer $k$.

   e. Now write the proof. Start by assuming the hypothesis. Use the necessary definitions and work your way towards the conclusion.

*Proof.* Let $a, b, c, d$, and $n$ be integers with $n > 0$. If $a \equiv b \bmod n$ and $c \equiv d \bmod n$, then by definition, we have $n \mid (a-b)$ and $n \mid (c-d)$. This implies $(a-b) = nk$ for some integer $k$, and $(c-d) = nl$ for some integer $l$. Rewrite these two equations to get:

$$a = nk + b$$
$$c = nl + d.$$

Consider

$$\begin{aligned} ac &= (nk+b)(nl+d) \\ &= n^2kl + nkd + bnl + bd \\ ac - bd &= n(nkl + kd + bl.) \end{aligned}$$

Since $nkl + kd + bl$ is just another integer, this means $n \mid (ac - bd)$ or that

$$ac \equiv bd \bmod n.$$

$\square$