The University of Sydney
School of Mathematics and Statistics

Tutorial 3 (Week 4)

MATH2068/2988: Number Theory and Cryptography — Semester 2, 2017

Web Page: http://www.maths.usyd.edu.au/u/UG/IM/MATH2068/
Lecturer: Dzmitry Badziahin

More difficult questions are marked with either * or **. Those marked * are at the level which MATH2068 students will have to solve in order to be sure of getting a Credit, or to have a chance of a Distinction or High Distinction. Those marked ** are mainly intended for MATH2988 students.

This tutorial is all about the famous *Fibonacci numbers* F_n, $n \in \mathbb{N}$. These are defined by

$$F_0 = 0, \quad F_1 = 1, \quad F_n = F_{n-1} + F_{n-2} \text{ for all } n \geq 2.$$

Thus, each Fibonacci number is the sum of the two preceding Fibonacci numbers. The Fibonacci sequence begins

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181, 6765, \ldots$$

Tutorial Exercises:

1. For any integer $m \geq 2$, we can consider the "Fibonacci sequence modulo m", i.e. the sequence of residues of the Fibonacci numbers modulo m. This is the sequence starting $0, 1, 1, \ldots$ where each term is the residue mod m of the sum of the two preceding terms.

(a) Write out the Fibonacci sequence modulo 2 until the pattern is clear. For which n is F_n even?

(b) Write out the Fibonacci sequence modulo 3 until the pattern is clear. For which n is F_n a multiple of 3?

(c) Find the residues of F_{2016} modulo 5 and modulo 7.

2. Prove by induction that the following matrix-power formula holds for all positive integers n:

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}^n = \begin{bmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{bmatrix}.$$

3. Work out the value of $F_{n-1}F_{n+1} - F_n^2$ for $n = 1, 2, 3, 4, 5$. You should see a pattern; prove that this pattern always holds. (Hint: the previous question helps.)

4. The *Lucas numbers* L_n, $n \in \mathbb{N}$, are defined by the same recurrence as the Fibonacci numbers, but with different initial conditions:

$$L_0 = 2, \quad L_1 = 1, \quad L_n = L_{n-1} + L_{n-2} \text{ for all } n \geq 2.$$

Work out the value of $L_n - F_{n-1}$ for $n = 1, 2, 3, 4, 5, 6$. You should see a pattern; prove that this pattern always holds.

*5. Let d be a positive integer.

(a) Prove by induction (on n) that for all nonnegative integers n,

$$F_{d+n} \equiv F_{d+1}F_n \pmod{F_d}.$$

(Hint: prove both the $n = 0$ and $n = 1$ cases as base cases for the induction.)

(b) Using the previous part, prove by induction (on m) that for all positive integers m, $F_{dm} \equiv 0 \pmod{F_d}$. In other words, if $d \mid e$, then $F_d \mid F_e$.

Extra Exercises:

6. Work out the value of $F_{n-1}^2 + F_n^2$ for $n = 1, 2, 3, 4, 5, 6$. You should see a pattern; prove that this pattern always holds.

*7. Find closed formulas for the Fibonacci numbers F_n and the Lucas numbers L_n, either by using general methods of solving recurrences or by diagonalizing the matrix on the left-hand side in Q2 to compute its powers.

**8. Let p be a prime number, and let $t_1 = 1$. Now define t_i recursively, for $i > 1$, as follows: if $t_i \neq 0$, choose a number s_i such that $s_i t_i \equiv 1 \pmod{p}$ and let t_{i+1} be the residue of $1 + s_i$ modulo p; if $t_i = 0$, the sequence stops. Note that we always have $0 \leq t_i < p$.

(a) Show that the sequence $(t_1, t_2, \ldots)$ has no repeated terms; in particular, it can't go on forever, so it must have the form $(t_1, t_2, \ldots, t_\ell)$ where $t_\ell = 0$. (Hint: suppose there were repeated terms, and consider the first of them.)

(b) Prove by induction that $F_i t_i \equiv F_{i+1} \pmod{p}$ for all $i \in \{1, \cdots, \ell\}$.

(c) Hence show that at least one of the Fibonacci numbers $F_2, F_3, \ldots, F_{p+1}$ is a multiple of p.

Selected numerical answers:

1(c). 2, 0. **3.** -1, 1, -1, 1, -1. **4.** 1, 2, 3, 5, 8, 13.