CSL202: Discrete Mathematical Structures
Tutorial/Homework: 05

1. Consider the following algorithm that takes as input an integer array A and its size n.

```
FunnyAlgo(A, n)
  - if (n < 2^20)
     - for i = 1 to n − 1
        - for j = 1 to i
           - A[j + 1] ← A[j] + 1
  - else
     - for i = 2 to n
        - A[i] ← A[i] + A[i − 1]
```

   (a) State true or false: The running time is $O(n^2)$?
   (b) State true or false: The running time is $\Omega(n)$?
   (c) State true or false: The running time is $\Omega(n^2)$?
   (d) Write the running time of the algorithm in Θ notation. That is give a tight bound on the worst-case running time of the above algorithm.

2. Show that if a and b are both positive integers, then $(2^a - 1)\ (mod\ (2^b - 1)) = 2^{a\ (mod\ b)} - 1$.

3. (a) Show that the positive integers less than 11, except 1 and 10, can be split into pairs of integers such that each pair consists of integers that are inverses of each other modulo 11.
   (b) Use part (a) to show that $10! \equiv -1\ (mod\ 11)$.

4. Prove that an integer $(a_{n-1}, ..., a_0)$ is divisible by 11 if and only if $a_0 + a_2 + a_4 + ... \equiv a_1 + a_3 + ...\ (mod\ 11)$.

5. Recall the Euclid-GCD(a, b) algorithm discussed in the lectures for finding the gcd of two integers a and b. Prove the following theorem:

   Theorem 1.0.1 (Lame's theorem) *For any integer $k \geq 1$, if $a > b \geq 1$ and $b < F_{k+1}$, then the call Euclid-GCD(a, b) makes fewer than k recursive calls.*

   Here F_k denotes the k^{th} number in the Fibonacci sequence $(0, 1, 1, 2, 3, 5, 8, 13, ...)$

6. Design an algorithm that takes as input positive integers a, b, m and outputs $a^b\ (mod\ m)$ (input/output is in binary). Discuss the worst-case time complexity of your algorithm.

7. Show that if p is prime, the only solutions of $x^2 \equiv 1 \ (mod\ p)$ are integers x such that $x \equiv 1 \ (mod\ p)$ or $x \equiv -1 \ (mod\ p)$.