AMERICAN UNIVERSITY OF BEIRUT

MATH 211 Fall 2017 TEST II

NAME: SECTION:

(1) In the following, Circle T for true or F for False. No justification is needed for this part. (1 point each)

T F $\log n^n$ is $\Theta(\log(n!))$ but n^n is not $\Theta(n!)$.

T F $\log_d c$ is a rational number if and only if $\log_c d$ is a rational number, where c and d are two positive integers not equal to 1.

T F For any integer n, $gcd(0, n) = 1$.

T F The inverse of $n(\mod n+1)$ always exists, for all integers $n \geq 1$

T F If $a \equiv 3(\mod 12)$ and $b \equiv 10(\mod 12)$ then $(a-b)(a+b) \equiv 1(\mod 6)$

T F The binary expansion of $(AA1F)_{16}$ is $(1010, 1010, 1, 1111)_2$

T F If $a \equiv b(\mod m)$ then $a \equiv b(\mod 2m)$

T F If C and k are witnesses to the big Oh notation: $f(x)$ is $O(g(x))$ then C and $k+1$ are also witnesses.

T F If $p_1, \cdots, p_n$ are n prime numbers, then the integer $Q = p_1 p_2 \cdots p_n + 1$ must have a prime divisor, other than itself, which is not in the set $\{p_1, \cdots, p_n\}$

T F In general, the complexity of the linear search algorithm is $O(\log n)$ while the complexity of the worst case scenario is $\Theta(n)$, when the problem size is n

(2) Given is the following algorithm

```
procedure proc(a_1,...,a_n: integers)
for(i:=1 to n)
   bi:=0
   for(j:=1 to i)
      if aj>0 then bi:=bi+aj
return (b1,...,bn)
```

(a) (2 pt.) what does this algorithm return when the input is the sequence $(-5, -3, 2, -1, 3, 7)$?

(b) (3 pt.) count the number of comparisons as a function of the input size n

- (3 pt.) The three consecutive odd integers 3, 5 and 7 are all prime. Prove that these are the only three consecutive odd integers that are all prime.

- (3 pt.) Suppose that an integer n is represented in base 3 as $(a_{k-1}a_{k-2}\cdots a_1a_0)_3$. Develop a divisibility test to check whether n is even or odd without converting n to decimal.

- (4 pt.) Showing your steps, solve the following system of congruence equations for the unknown x, using the method of substitution. Note: you need to apply the extended Euclidean Algorithm to find inverses when needed.

$$\begin{cases} 15x \equiv 3 \pmod{58} \\ 21x \equiv 10 \pmod{85} \end{cases}$$

- (a) (2 pt.) Convert the integer 41 into binary representation

(b) (2 pt.) Use the modular exponentiation algorithm to calculate $4^{41}(\mod 13)$, showing all steps and intermediate values in the execution of the algorithm

(c) (2 pt.) Verify you answer to the previous question using Fermat's Little Theorem

- (a) (3 pt.) Show carefully that $x^2 - x$ is $O(8x^2)$

(b) (3 pt.) Show carefully that $8x^2$ is $O(x^2 - x)$

- (3 pt.) Show that if $gcd(a, m) = 1$ and if b is any integer, then there exists an integer c such that $ac \equiv b(\mod m)$