

NAME:

SECTION:

(1) True/False Questions: (1 point each).

T F $f(x)$ is $O(1)$ means that $f(x)$ is a constant function.

T F If $f(x)$ is $\Omega(g(x))$ then there exist unique constants C and k such that $|g(x)| < C|f(x)|$ for all $x > k$.

T F For any positive integers A, b and m , $(a \bmod m) + (b \bmod m) = (a + b \bmod m)$

T F It is not possible to find functions $f(x)$ and $g(x)$ such that $f(x)$ is $O(g(x))$ and $g(x)$ is $O(f(x))$.

T F If $f_1(x)$ is $O(g_1(x))$ and $f_2(x)$ is $O(g_2(x))$ then the function $f_1(x)f_2(x)$ is $O(\max(g_1(x), g_2(x)))$.

T F If $a \neq 0$ and $ab \equiv ac \pmod{m}$ then $b \equiv c \pmod{m}$.

T F Given that $\text{lcm}(a, b) = 14$ and $a \times b = 42$ then necessarily $\text{gcd}(a, b) = 3$.

T F Consider the following two linear congruential generators, both of the form $x_{n+1} = ax_n + b \pmod{m}$.

(I) $a = 7, b = 4, x_0 = 3$ and $m = 9$

(II) $a = 7, b = 3, x_0 = 3$ and $m = 9$

The first generator is better.

T F The integer 111222333444 is divisible by 3 and 6 but not divisible by 9.

T F The complexity of the linear search algorithm is $O(n)$.

- (2) (3 pts.) Show by using mathematical induction that for every nonnegative integer n , the integer $n^5 - n$ is divisible by 5.

- (3) (3 pts.) Write the bubble sort algorithm and show the steps needed to sort the sequence 5, 7, 2.

- (4) (3 pts.) Given is the following procedure written in pseudo-code:

```

procedure lst(input: a1,...,an: integers)
  L:=1
  M:=a1
  for i=2 to n
    if (ai > m) then
      begin
        m:=ai
        L:=i
      end
    else
      if (ai = m) then
        L:=i
  {output: M and L}

```

Provide the output of this function when the input sequence 4, 4, 2, 3, 2, 4, 3, 1 is entered, and state what the code does in general.

- (5) (3 pts.) Use the Euclidean Algorithm to find $\gcd(50, 14)$ and then represent it in the form $as + bt$.

- (6) Given is the following procedure written in pseudo-code:

```
procedure locc(input:  $a_1, \dots, a_n$ : integers)
  m:=  $a_1$ 
  for i=2 to n
    if ( $a_i < m$ ) then m:= $a_i$ 
  l:=0
  for i=2 to n
    if ( $a_i = m$ ) then l:=i
  {output: l}
```

- (a) (2 pts.) Provide the output of this function when the input sequence 4, 4, 2, 3, 2, 4 is entered, and state what the code does in general.

- (b) (2 pts.) Calculate the number of comparisons if the above code as a function of the the input size n .

- (7) (3 pts.) Show that a composite integer n must have a prime divisor less than or equal to \sqrt{n} .

(8) (3 pts.) Solve the congruence equation $15x \equiv 7 \pmod{11}$

(9) (4 pts.) Find a function $g(n)$ so that $4n^2 - 5$ is $\Theta(g(n))$. Make sure you include the necessary witnesses.