TEST 2

Davis
CS222

Name:
Pledge:

Show all work; unjustified answers may receive less than full credit.

(15pts.) **1.** Show that the relation on the integers defined by aRb if $7|(a-b)$ is an equivalence relation. List the equivalence classes $[0]$, $[3]$, and $[10]$.

Reflexive: $7|(a-a)$ for every a, so aRa. Symmetric: if $7|(a-b)$, then $(a-b)=7m$ for some m, so $(b-a)=7(-m)$, which implies that bRa. Transitive: if aRb and bRc, then there is an m so that $(a-b)=7m$ and there is an n so that $(b-c)=7n$. This implies that $(a-c)=(a-b)+(b-c)=7m+7n=7(m+n)$, which means that aRc.

The equivalence class $[0]=\{0,\pm 7,\pm 14,\pm 21,\ldots\}$. The equivalence classes $[3]$ and $[10]$ are the same, and they are both $\{3,10,17,24,31,\ldots,-4,-11,-18,\ldots\}$.

(15pts.) **2.** Is the relation $\{(0,1),(1,2),\ldots,(9,10),(10,10)\}$ a function on the set $\{0,1,2,\ldots,10\}$? If it is a function, is it 1-1? onto?

The relation mentioned above is a function since for every element of the domain there is exactly one element of the range (this is the vertical line test stated formally). This function is not 1-1 since both 9 and 10 go to 10 in the range. This function is not onto since nothing goes to 0.

(15pts.) **3.** Write pseudo code for an algorithm that outputs the largest and second largest elements in the sequence $s_1,\ldots,s_n$.

```
Procedure biggest_two(s,n)
   input the sequence and the number of elements in the sequence.
If s_1 < s_2
swap(s_1, s_2)
Big:=s_1
Second_Big:=s_2
For i=3,n
begin
If s_i > Big
begin
Second_Big:=Big
Big:=s_i
end
If Second_Big < s_i < Big
Second_Big:=s_i
end
return[Big,Second_Big]
```

(15pts.) **4.** Suppose that the pair $a,b,a>b$, requires $n\geq 1$ modulus operations when input into the Euclidean algorithm. Show that $a\geq f_{n+1}$ and $b\geq f_n$, where $\{f_n\}$ denotes the Fibonacci sequence.

See notes in class (this is induction on the number of mod operations required. If (a,b) requires $n+1$ operations, then do one operation and use the inductive hypothesis on b and the remainder r. The Fibonacci sequence finishes this off).

(15pts.) **5.** Write a pseudo code for a recursive algorithm to calculate the number of ways a basketball team can score n points for $n \geq 2$ (assume that the only ways to score points are 2 and 3 point baskets).

1. procedure bball_points(n)

2. If n=2 or n=3

3. return(1)

4. count:=bball_points(n-2) + bball_points(n-3)

5. return(count)

(15pts.) **6.** Is the following true or false: If $f(n) = O(g(n))$, then $g(n) = O(f(n))$. If true, give a proof; if false, give a counterexample.

False, using $f(n) = n$ and $g(n) = n^2$.

(10pts.) **7.** Suppose $p = 5, q = 7$, and $e = 11$ are chosen for the RSA cryptosystem. Verify that $d = 11$ is the decryption exponent that will work for this system. Encode the message $M = 2$.

$ed = 11(11) = 121 = 1$ mod 24. To encode $M = 2$, we raise it to the 11 power and reduce it mod 35, yielding 18 as the encrypted message.