MA/CSSE 473 Exam #1 Fall, 2014 (Day 16) Name_____ Section: 01(9:55) __ 02(10:50)__

Resources allowed: Calculator, one 8.5 x 11 sheet of paper (one-sided, hand-written).
Resources not allowed: Anything that can communicate or has headphones/earphones.

It is possible to get so caught up in getting all of the points for one problem and spend so much time on it that you do not get to the other problems. Don't do that! I will be generous with partial credit if you have the main ideas. You should first do the problems you are confident about, and then do the rest. Time is likely to be a factor on this exam.

For Instructor use:

Problem	Possible	Earned
1	20	
2	10	
3	10	
4	15	
5	10	
6	5	
7	5	
8	5	
Total	80	

Consider the recurrence
$T(n) = aT(n/b) + f(n)$, $T(1)=c$,
where $f(n) = \Theta(n^k)$ and $k \geq 0$,
The solution is

- $\Theta(n^k)$ if $a < b^k$
- $\Theta(n^k \log n)$ if $a = b^k$
- $\Theta(n^{\log_b a})$ if $a > b^k$

1.(20) This problem deals with primality testing *via* the Fermat and Miller-Rabin tests. 153 is a composite number. The chart below shows all of the computations for the Miller-Rabin tests. For each number **a**, I first show **a**, then the sequence of numbers that the Miller-Rabin algorithm computes for that **a** (smallest number first).

(a) Using the notation that we used in class, what are the u and t for N=153? u = t =

(b) How many of the numbers shown are Fermat liars? _____

(c) For how many of those Fermat liars does the Miller Rabin test demonstrate that 153 is in fact composite? _____

```
1 [1, 1, 1, 1]
2 [110, 13, 16, 103]
3 [27, 117, 72, 135]
4 [13, 16, 103, 52]
5 [23, 70, 4, 16]
6 [63, 144, 81, 135]
7 [88, 94, 115, 67]
8 [53, 55, 118, 1]
9 [117, 72, 135, 18]
10 [82, 145, 64, 118]
11 [56, 76, 115, 67]
12 [45, 36, 72, 135]
13 [4, 16, 103, 52]
14 [41, 151, 4, 16]
15 [9, 81, 135, 18]
16 [16, 103, 52, 103]
17 [17, 136, 136, 136]
18 [18, 18, 18, 18]
19 [127, 64, 118, 1]
20 [146, 49, 106, 67]
21 [81, 135, 18, 18]
22 [40, 70, 4, 16]
23 [131, 25, 13, 16]
24 [54, 9, 81, 135]
25 [70, 4, 16, 103]
26 [134, 55, 118, 1]
27 [99, 9, 81, 135]
28 [73, 127, 64, 118]
29 [11, 121, 106, 67]
30 [72, 135, 18, 18]
31 [58, 151, 4, 16]
32 [77, 115, 67, 52]
33 [135, 18, 18, 18]
34 [34, 85, 34, 85]
35 [35, 1, 1, 1]
36 [144, 81, 135, 18]
37 [10, 100, 55, 118]
38 [47, 67, 52, 103]
39 [108, 36, 72, 135]
40 [148, 25, 13, 16]
41 [122, 43, 13, 16]
42 [36, 72, 135, 18]
43 [151, 4, 16, 103]
44 [116, 145, 64, 118]
45 [90, 144, 81, 135]
46 [28, 19, 55, 118]
47 [38, 67, 52, 103]
48 [126, 117, 72, 135]
49 [94, 115, 67, 52]
50 [50, 52, 103, 52]
51 [0, 0, 0, 0]
52 [52, 103, 52, 103]
53 [8, 64, 118, 1]
54 [27, 117, 72, 135]
55 [64, 118, 1, 1]
56 [74, 121, 106, 67]
57 [63, 144, 81, 135]
58 [139, 43, 13, 16]
59 [104, 106, 67, 52]
60 [117, 72, 135, 18]
61 [133, 94, 115, 67]
62 [107, 127, 64, 118]
63 [45, 36, 72, 135]
64 [55, 118, 1, 1]
65 [92, 49, 106, 67]
66 [9, 81, 135, 18]
67 [67, 52, 103, 52]
68 [68, 34, 85, 34]
69 [18, 18, 18, 18]
70 [25, 13, 16, 103]
71 [44, 100, 55, 118]
72 [81, 135, 18, 18]
73 [91, 19, 55, 118]
74 [29, 76, 115, 67]
75 [54, 9, 81, 135]
76 [121, 106, 67, 52]
77 [32, 106, 67, 52]
78 [99, 9, 81, 135]
79 [124, 76, 115, 67]
80 [62, 19, 55, 118]
81 [72, 135, 18, 18]
82 [109, 100, 55, 118]
83 [128, 13, 16, 103]
84 [135, 18, 18, 18]
85 [85, 34, 85, 34]
86 [86, 52, 103, 52]
87 [144, 81, 135, 18]
88 [61, 49, 106, 67]
89 [98, 118, 1, 1]
90 [108, 36, 72, 135]
91 [46, 127, 64, 118]
92 [20, 94, 115, 67]
93 [36, 72, 135, 18]
94 [49, 106, 67, 52]
95 [14, 43, 13, 16]
96 [90, 144, 81, 135]
97 [79, 121, 106, 67]
98 [89, 118, 1, 1]
99 [126, 117, 72, 135]
100 [145, 64, 118, 1]
101 [101, 103, 52, 103]
102 [0, 0, 0, 0]
103 [103, 52, 103, 52]
104 [59, 115, 67, 52]
105 [27, 117, 72, 135]
106 [115, 67, 52, 103]
107 [125, 19, 55, 118]
108 [63, 144, 81, 135]
109 [37, 145, 64, 118]
110 [2, 4, 16, 103]
111 [117, 72, 135, 18]
112 [31, 43, 13, 16]
113 [5, 25, 13, 16]
114 [45, 36, 72, 135]
115 [106, 67, 52, 103]
116 [143, 100, 55, 118]
117 [9, 81, 135, 18]
118 [118, 1, 1, 1]
119 [119, 85, 34, 85]
120 [18, 18, 18, 18]
121 [76, 115, 67, 52]
122 [95, 151, 4, 16]
123 [81, 135, 18, 18]
124 [142, 121, 106, 67]
125 [80, 127, 64, 118]
126 [54, 9, 81, 135]
127 [19, 55, 118, 1]
128 [83, 4, 16, 103]
129 [99, 9, 81, 135]
130 [22, 25, 13, 16]
131 [113, 70, 4, 16]
132 [72, 135, 18, 18]
133 [7, 49, 106, 67]
134 [26, 64, 118, 1]
135 [135, 18, 18, 18]
136 [136, 136, 136, 136]
137 [137, 103, 52, 103]
138 [144, 81, 135, 18]
139 [112, 151, 4, 16]
140 [149, 16, 103, 52]
141 [108, 36, 72, 135]
142 [97, 76, 115, 67]
143 [71, 145, 64, 118]
144 [36, 72, 135, 18]
145 [100, 55, 118, 1]
146 [65, 94, 115, 67]
147 [90, 144, 81, 135]
148 [130, 70, 4, 16]
149 [140, 16, 103, 52]
150 [126, 117, 72, 135]
151 [43, 13, 16, 103]
152 [152, 1, 1, 1]
```

(d) State Fermat's Little Theorem. Give the basic outline (in a small number of sentences) of the proof that we did in class.

2. (10 points) In class we did (in great detail) a proof of:
Lemma: If there is an s which is neither 1 or -1 (mod N), but $s^2 \equiv 1 \pmod N$, then N is not prime.
(a) (2)We actually proved the contrapositive of the lemma. State the contrapositive.

(b) (8) Consider the following steps in the proof. The questions below will ask about the reasons why the steps are valid.

1. Hypothesis: N is prime, and $s^2 \equiv 1 \pmod N$
2. $(s - 1)(s + 1) \equiv 0 \pmod N$
3. N divides $(s - 1)(s + 1)$
4. Either N divides s-1 or N divides s + 1
5. The conclusion of the contrapositive (which I am not stating here because I don't want to tell you the answer to (a).

For each of the above steps, give a very brief justification of why that step is valid:

Step 2:

Step 3:

Step 4:

Step 5:

I chose small numbers for the next two problems, so that the arithmetic can be done with the assistance of a simple calculator. Because the possible answers come from a very small set, you *could* get the answers by trial and error. But I insist that you show me how you get your answers, in a way that demonstrates that you understand the algorithms.

3. (10) Show how to use the extended Euclid's algorithm to find the inverse of 5 (mod 48). Your answer should be a number in the range 1 … 47.

   Answer: _____

   Show how to get your answer using extended Euclid:

4. (15) Bob has advertised his RSA public key as (N=65, e=29). Eve intercepts an encoded message m' that someone sends to Bob using Bob's public key, and that encoded message is: 2

   What was the original message m before it was encoded? _____
   Briefly show how you got your answer; you do not have to write a lot, but convince me that you understand RSA.

5. (10) Use the "ratio of limits" technique to show that if $1 < a < b$, a^n is $O(b^n)$ but b^n is not $O(a^n)$.

6. (5) In lexicographic order, the permutation that follows 46358721 is _____

7. (5) In the Johnson-Trotter permutation generation algorithm for N=6, the state at one point is ← → ← → → →
[2, 4, 1, 3, 5, 6]
Show the permutations and direction arrows for the next two permutations.

8. (5) If we use brute force integer multiplication and addition, and brute-force matrix multiplication, what is the big-theta running time (in terms of *n*) for the number of bit multiplications needed to multiply *n* *n*-by-*n* matrices whose entries are *n*-bit integers? Circle one of the choices below. Briefly show how you get your answer

$\Theta(n^2)$ $\Theta(n^3)$ $\Theta(n^4)$ $\Theta(n^5)$ $\Theta(n^6)$ $\Theta(n^7)$ $\Theta(n^8)$ $\Theta(n^9)$ $\Theta(n^{10})$ $\Theta(n^{11})$ $\Theta(n^{12})$