CECS 528, Learning Outcome Assessment 1, Pink, Fall 2023, Dr. Ebert

NO NOTES, BOOKS, ELECTRONIC DEVICES, OR INTERPERSONAL COMMUNICATION ALLOWED. Submit each solution on a separate sheet of paper.

Problem

LO1. Complete the following problems.

(a) Show each of the subproblem instances that must be solved when using the recursive division algorithm for finding the quotient and remainder of x/y. Do this for $x = 136$ and $y = 18$. Make sure to provide the solution to each subproblem instance. Hint: there are nine subproblem instances, including the original problem instance.

(b) For the Strassen-Solovay primality test with $n = 21$, determine whether or not $a = 2$ is a witness to n not being prime. Do this by evaluating *both* sides of the test congruence, mod 21.

Solutions

LO1. Complete the following problems.

(a) Show each of the subproblem instances that must be solved when using the recursive division algorithm for finding the quotient and remainder of x/y. Do this for $x = 136$ and $y = 18$. Make sure to provide the solution to each subproblem instance. Hint: there are nine subproblem instances, including the original problem instance.

Solution.

x	y	q	r
136	18	7	10
68	18	3	14
34	18	1	16
17	18	0	17
8	18	0	8
4	18	0	4
2	18	0	2
1	18	0	1
0	18	0	0

(b) For the Strassen-Solovay primality test with $n = 21$, determine whether or not $a = 2$ is a witness to n not being prime. Do this by evaluating *both* sides of the test congruence, mod 21.

Solution.

We must evaluate both $2^{\frac{21-1}{2}} = 2^{10} \bmod 21$, and $\left(\frac{2}{21}\right)$.

We have,

$$2^5 \equiv 11 \bmod 21 \Rightarrow 2^{10} \equiv 121 \equiv -5 \bmod 21.$$

Also,

$$\left(\frac{2}{21}\right) = -1$$

since $21 \equiv -3 \bmod 8$. Therefore, $a = 2$ is a witness, since $-5 \not\equiv -1 \bmod 21$.