CECS 528, Learning Outcome Assessment 1, Yellow, 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) Demonstrate each step (line) of Euclid's algorithm on inputs $a = 54$ and $b = 14$. Then work backwards to provide a linear combination of 54 and 14 that sums to $(54, 14)$.

(b) For the Strassen-Solovay primality test with $n = 23$, verify that $a = 2$ satisfies the test congruence. Do this by evaluating *both* sides of the test congruence, mod 23.

Solution

LO1. Complete the following problems.

(a) Demonstrate each step (line) of Euclid's algorithm on inputs $a = 54$ and $b = 14$. Then work backwards to provide a linear combination of 54 and 14 that sums to $(54, 14)$.
Solution.

a	$(b)(q)$	r
54	(14)(3)	12
14	(12)(1)	2
12	(2)(6)	0

So $(54, 14) = 2$ and

$$14 + 12(-1) = 2 \Leftrightarrow$$

$$14 + (54 + 14(-3))(-1) = 54(-1) + 14(4) = 2.$$

(b) For the Strassen-Solovay primality test with $n = 23$, verify that $a = 2$ satisfies the test congruence. Do this by evaluating *both* sides of the test congruence, mod 23.
Solution.
We must evaluate both $2^{\frac{23-1}{2}} = 2^{11}$ mod 23, and $\left(\frac{2}{23}\right)$.
We have,

$$2^5 \equiv 9 \bmod 23.$$

and

$$2^6 \equiv -5 \bmod 23 \Rightarrow 2^{11} \equiv 2^5 \cdot 2^6 \equiv (9)(-5) \equiv 1 \bmod 23.$$

Also,

$$\left(\frac{2}{23}\right) = 1$$

since $23 \equiv -1 \bmod 8$. Therefore, $a = 2$ satisfies the test congruence, since $1 \equiv 1 \bmod 23$.