CECS 528, Learning Outcome Assessment 1, Spring 2024, 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 all the steps needed to compute $\left(\frac{15}{43}\right)$.

(b) For the Strassen-Solovay primality test verify that $a = 2$ is an accomplice when $n = 13$, but is a witness when $n = 15$.

a) $\left(\frac{15}{43}\right) = \left(\frac{3}{43}\right)\left(\frac{5}{43}\right) = -\left(\frac{43}{3}\right)\left(\frac{43}{5}\right) = -\left(\frac{1}{3}\right)\left(\frac{3}{5}\right)$

$-\left(\frac{5}{3}\right) = -\left(\frac{2}{3}\right) = 1$ since $3 \equiv 3 \bmod 8$.

b) $n=13$: $2^{\frac{13-1}{2}} \equiv 2^6 \equiv 2^2 \cdot 2^4 \equiv 4 \cdot 3 \equiv -1 \bmod 13$

Also, $\left(\frac{2}{13}\right) = -1$ since $13 \equiv -3 \bmod 8$. ✓ $\therefore$ 2 is an accomplice in support of 13 being prime.

For $n=15$,

$2^{\frac{15-1}{2}} \equiv 2^7 \equiv 2^3 \cdot 2^4 \equiv 8 \bmod 15$

$\left(\frac{2}{15}\right) = 1$ since $15 \equiv -1 \bmod 8$. But $8 \not\equiv 1 \bmod 15$.

Therefore, 2 is a witness to 15 not being prime.