MATH 233: ASSIGNMENT 1

DUE: FRIDAY, FEBRUARY 2, 11:59PM ON GRADESCOPE
UNIVERSITY OF ROCHESTER, SPRING 2024

Problem 1. Let a and b be positive integers and k be an integer. Prove that

$$\gcd(a, b) = \gcd(a + kb, b)$$

using the definition of the greatest common divisors, and use this to show that the last remainder in the Euclidean algorithm is indeed the greatest common divisor of a and b.

Problem 2. (3.13.1) Show your work. Do not use a calculator.

(a) Find integers x and y such that $17x + 101y = 1$.

(b) Find 17^{-1} (the multiplicative inverse of 17) mod 101.

Problem 3. (3.13.6) Find all solutions (mod 50) of each modular equation.

(a) $4x \equiv 20 \pmod{50}$

(b) $4x \equiv 21 \pmod{50}$

Problem 4. (3.13.11) Let

$$F_1 = 1, \quad F_2 = 1, \quad F_{n+1} = F_n + F_{n-1}$$

define the Fibonacci numbers $1, 1, 2, 3, 5, 8, \ldots$.

(a) Use the Euclidean algorithm to compute $\gcd(F_n, F_{n-1})$ for all $n \geq 2$.

(b) Find $\gcd(11111111, 11111)$.

(c) Let $a = 111 \cdots 11$ be formed with F_n repeated 1's and let $b = 111 \cdots 11$ be formed with F_{n-1} repeated 1's. Find $\gcd(a, b)$. (Hint: Compare your computations in parts (a) and (b).)

Problem 5. (2.8.1) Caesar wants to arrange a secret meeting with Marc Antony, either at the Tiber (the river) or at the Coliseum (the arena). He sends the ciphertext $EVIRE$ (using a shift cipher). However, Antony does not know the key, so he tries all possibilities. Where will he meet Caesar? What is the key? (Hint: This is a trick question.)

Problem 6. (2.8.7) A child has learned about affine ciphers. The parent says $NONONO$. The child responds with *hahaha*, and quickly claims that this is a decryption of the parent's message. The parent asks for the encryption function. What answer should the child give?