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.

Solution. Let $d = \gcd(a, b)$. Since d divides both a and b, it follows that d divides $a + kb$ as well. If there exists a positive integer d' greater than d dividing both $a + kb$ and b, then d' should also divide $a = (a + kb) - kb$, which contradicts the fact that d is the greatest positive integer dividing both a and b. Therefore, there is no such d', which implies $\gcd(a + kb, b) = d$.

Now consider the following Euclidean algorithm.

$$\begin{array}{cc}
a = q_1 b + r_1 & \qquad b \\[1em]
b = q_2 r_1 + r_2 & \qquad r_1 \\[1em]
\vdots & \qquad \vdots \\[1em]
r_{k-2} = q_k r_{k-1} + r_k & \qquad r_{k-1} \\[1em]
r_{k-1} = q_{k+1} r_k & \qquad r_k
\end{array}$$

From the first statement we have

$$\gcd(a, b) = \gcd(q_1 b + r_1, b) = \gcd(r_1, b) = \gcd(b, r_1).$$

Similarly,

$$\gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{k-2}, r_{k-1}) = \gcd(r_{k-1}, r_k).$$

Since r_k divides r_{k-1}, we have

$$\gcd(r_{k-1}, r_k) = r_k.$$

Therefore,

$$\gcd(a, b) = r_k.$$

$\square$

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.

Solution. (a) We first execute the Euclidean algorithm:

$$\begin{aligned} 101 &= 5 \cdot 17 + 16 & \quad 17 \\ 17 &= 1 \cdot 16 + 1 & \quad 16 \\ 16 &= 16 \cdot 1 & \quad 1 \end{aligned}$$

Now we have

$$\begin{aligned} 1 &= 17 - 1 \cdot 16 \\ &= 17 - (101 - 5 \cdot 17) \\ &= 6 \cdot 17 - 101. \end{aligned}$$

Therefore, $(x, y) = (6, -1)$ satisfies the given equation. (Note that there are *infinitely many* pairs satisfying the given equation.)

(b) From part (a), we know that

$$17 \cdot 6 \equiv 1 \pmod{101}.$$

Therefore, the multiplicative inverse of 17 is

$$17^{-1} \equiv 6 \pmod{101}.$$

□

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

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

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

Solution. (a) Since $\gcd(4, 50) = 2$ divides 20, we divide the entire equation by 2 to get a new equation

$$2x \equiv 10 \pmod{25}.$$

Now $\gcd(2, 25) = 1$ and $2^{-1} \equiv 13 \pmod{25}$, so

$$x \equiv 10 \cdot 13 \equiv 130 \equiv 5 \pmod{25}$$

is the solution of the new equation. Therefore,

$$x \equiv 5, 30 \pmod{50}$$

are solutions of the original equation.

(b) Since $\gcd(4, 50) = 2$ does not divide 21, there is no solution.

□

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 $a = 111\cdots11$ be formed with F_n repeated 1's and let $b = 111\cdots11$ be formed with F_{n-1} repeated 1's. Find $\gcd(a, b)$. (Hint: Compare your computations in parts (a) and (b).)

Solution. (a) We directly check that

$$\gcd(F_2, F_1) = \gcd(F_3, F_2) = 1.$$

Now assume that $n \geq 4$. Then we observe that

$$2F_{n-1} > F_n = F_{n-1} + F_{n-2} > F_{n-1}$$

for all $n \geq 4$. Therefore, the first step of the Euclidean algorithm should be

$$F_n = 1 \cdot F_{n-1} + F_{n-2},$$

so the next pair in the Euclidean algorithm is (F_{n-1}, F_{n-2}). Repeating this process, we can conclude that

$$\gcd(F_n, F_{n-1}) = \gcd(F_{n-1}, F_{n-2}) = \cdots = \gcd(F_3, F_2) = 1.$$

(b) $\gcd(11111111, 11111) = 1$ by the following Euclidean algorithm.

$$\begin{array}{cc}
11111111 = 10^3 \cdot 11111 + 111 & 11111 \\
11111 = 10^2 \cdot 111 + 11 & 111 \\
111 = 10 \cdot 11 + 1 & 11 \\
11 = 11 \cdot 1 & 1 = \gcd(11111111, 11111)
\end{array}$$

(c) Denote $111\cdots11$ formed with F_n repeated 1's by M_n, so that $a = M_n$ and $b = M_{n-1}$. Then

$$\begin{array}{rr} M_n = & 111\cdots11111\cdots11 \\ -10^{F_{n-2}}M_{n-1} = & 111\cdots11000\cdots00 \\ \hline M_{n-2} = & 111\cdots11 \end{array}$$

shows that

$$a = 10^{F_{n-2}}b + M_{n-2}.$$

Therefore, the Euclidean algorithm proceeds as follows.

$$\begin{aligned} M_n &= 10^{F_{n-2}}M_{n-1} + M_{n-2} & \qquad M_{n-1} \\ M_{n-1} &= 10^{F_{n-3}} \cdot M_{n-2} + M_{n-3} & \qquad M_{n-2} \\ &\vdots & \vdots \end{aligned}$$

This algorithm eventually ends with pairs $(111, 11)$ and $(11, 1)$ as in part (b), so we can conclude that

$$\gcd(a, b) = \gcd(M_n, M_{n-1}) = 1.$$

□

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.)

Solution. A decryption $x \mapsto x - 4 \pmod{26}$ yields a plaintext `arena` and another decryption $x \mapsto x + 13 \pmod{26}$ yields a plaintext `river`. Therefore, Antony cannot determine where to meet Caesar. □

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?

Solution. Let $x \mapsto \alpha x + \beta \pmod{26}$ be the encryption function. Since it should send $h = 7$ to $N = 13$ and $a = 0$ to $O = 14$, we have

$$7\alpha + \beta \equiv 13 \pmod{26} \quad \text{and} \quad \beta \equiv 14 \pmod{26}.$$

From two equations, it follows that

$$7\alpha \equiv 25 \pmod{26} \quad \Rightarrow \quad \alpha \equiv 7^{-1} \cdot 25 \equiv 11 \pmod{26}.$$

Therefore, the encryption function is

$$x \mapsto 11x + 14 \pmod{26}.$$

□