Homework 1

Matthew Pipes

January 29, 2026

Problem 1: Reductions Modulo m

(a) $(130 \cdot 142)\%3$

Since $130 = 3(43) + 1$, we have $130 \equiv 1 \pmod 3$.
Since $142 = 3(47) + 1$, we have $142 \equiv 1 \pmod 3$.
Thus, $130 \cdot 142 \equiv 1 \cdot 1 \equiv 1 \pmod 3$.
Since $0 \leq 1 < 3$, it follows that $(130 \cdot 142)\%3 = 1$.

(b) $(-2000)\%91$

Since $-2000 = 91(-22) + 2$, we have $-2000 \equiv 2 \pmod{91}$.
Since $0 \leq 2 < 91$, it follows that $(-2000)\%91 = 2$.

(c) $(3^{76})\%13$

We first break the exponent down: $3^{76} = (3^3)^{25} \cdot 3$.
Since $3^3 = 27 = 13(2) + 1$, we have $27 \equiv 1 \pmod{13}$.
Then $3^{76} = (27)^{25} \cdot 3 \equiv 1^{25} \cdot 3 \equiv 3 \pmod{13}$.
Since $0 \leq 3 < 13$, it follows that $(3^{76})\%13 = 3$.

Problem 2: Relationship Between Moduli

(a) $N\%24 = 2 \implies N\%6$

Proof. Let N be an integer such that $N\%24 = 2$. By the division algorithm, there exists an integer k such that:

$$N = 24k + 2$$

We can rewrite this expression to find the reduction modulo 6:

$$N = 6(4k) + 2$$

Let $q = 4k$. Since k is an integer, q is also an integer. Thus, we have $N = 6q + 2$. Since $0 \leq 2 < 6$, by the uniqueness of the division algorithm, the remainder of N divided by 6 is 2. Therefore, $N\%6 = 2$. □

(b) Possible values of $N\%24$ given $N\%6 = 2$

If $N\%6 = 2$, then by the division algorithm $N = 6k + 2$ for some integer k. To find the possible values of $N\%24$, we consider the possible remainders of k when divided by 4 (since $24 = 6 \cdot 4$). Let $k = 4q + r$, where $r \in \{0, 1, 2, 3\}$.

- If $k = 4q$, then $N = 6(4q) + 2 = 24q + 2$. Here, $N\%24 = 2$.
- If $k = 4q + 1$, then $N = 6(4q + 1) + 2 = 24q + 8$. Here, $N\%24 = 8$.
- If $k = 4q + 2$, then $N = 6(4q + 2) + 2 = 24q + 14$. Here, $N\%24 = 14$.
- If $k = 4q + 3$, then $N = 6(4q + 3) + 2 = 24q + 20$. Here, $N\%24 = 20$.

Thus, the possible values for $N\%24$ are $\{2, 8, 14, 20\}$.

Problem 3: Shift Cipher Cryptanalysis

To decrypt the message, we first map the alphabet to integers 0 through 25, where $A = 0, B = 1, \ldots, Z = 25$.

Step 1: Finding the Key (k)

We are given that the plaintext "snow" has been encoded to the ciphertext "JEFN". We compare the first letters to determine the shift k:

- Plaintext $s = 18$
- Ciphertext $J = 9$

The shift k is calculated as $k \equiv (C - P) \pmod{26}$:

$$k \equiv (9 - 18) \equiv -9 \equiv 17 \pmod{26}$$

Step 2: Decrypting "NZEKVI"

Using the decryption function $P \equiv (C - 17) \pmod{26}$ on the intercepted ciphertext "NZEKVI":

- $N = 13 \implies 13 - 17 = -4 \equiv 22 \pmod{26} \to \mathbf{W}$
- $Z = 25 \implies 25 - 17 = 8 \pmod{26} \to \mathbf{I}$
- $E = 4 \implies 4 - 17 = -13 \equiv 13 \pmod{26} \to \mathbf{N}$
- $K = 10 \implies 10 - 17 = -7 \equiv 19 \pmod{26} \to \mathbf{T}$
- $V = 21 \implies 21 - 17 = 4 \pmod{26} \to \mathbf{E}$
- $I = 8 \implies 8 - 17 = -9 \equiv 17 \pmod{26} \to \mathbf{R}$

The decrypted message is **"WINTER"**. The type of attack performed is a Known Plaintext Attack.

Problem 4: Divisibility Proof

Proof. Let a, b, and c be integers such that $a|b$ and $a|c$. We will show that for any integers u and v, a divides $ub + vc$.

By the definition of divisibility, there exist integers m and n such that:

$$b = am \quad \text{and} \quad c = an$$

Multiplying these expressions by u and v respectively yields:

$$ub = u(am) \quad \text{and} \quad vc = v(an)$$

Using the associative property of multiplication, we can rewrite these as:

$$ub = a(um) \quad \text{and} \quad vc = a(vn)$$

Adding these two expressions together, we get:

$$ub + vc = a(um) + a(vn)$$

Factoring out the common factor of a yields:

$$ub + vc = a(um + vn)$$

Since u, v, m, and n are all integers, the sum of their products $x = um + vn$ is also an integer by the closure properties of integers. Thus, we have:

$$ub + vc = ax$$

Finally, by the definition of divisibility, it follows that $a|(ub + vc)$, as desired. □

Problem 5: Peer Review Problem

Problem: Let m be any positive integer. Prove that if r is the reduction of N modulo m with $r \neq 0$, then $m - r$ is the reduction of $-N$ modulo m.

Proof. By the definition of the reduction modulo m, we know there exists an integer q such that:

$$N = mq + r, \quad \text{where } 0 < r < m$$

The condition $r \neq 0$ is given, ensuring r is strictly positive. To find the reduction of $-N$ modulo m, we multiply the entire equation by -1:

$$-N = -mq - r$$

To express this in the standard form of the Division Algorithm, where the remainder must be non-negative, we strategically add 0 in the form of $-m + m$:

$$-N = -mq - m + m - r$$

Factoring out m from the first two terms yields:

$$-N = m(-q - 1) + (m - r)$$

Let $Q = -(q + 1)$. Since q is an integer, Q is also an integer. This gives us the form:

$$-N = mQ + (m - r)$$

To confirm that $m - r$ is the valid reduction of $-N$ modulo m, we must verify that it satisfies the required bounds $0 \leq m - r < m$:

1. Since $r < m$, it follows that $m - r > 0$.

2. Since $r > 0$, it follows that $m - r < m$.

Thus, we have $0 < m - r < m$. Because $m - r$ is within the required range $[0, m)$, it is indeed the unique reduction of $-N$ modulo m. □