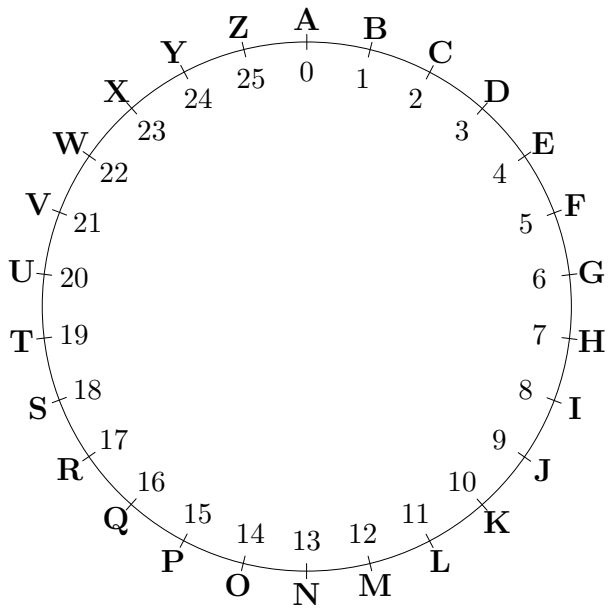
Math 5248: Homework 2

Matthew Pipes
February 5, 2026

Goal Utilization

In this assignment, I completed the following goals:

- **Problem 2:** Performed a known-plaintext attack on the affine cipher.
- **Problem 2:** Clearly communicated computational solutions with enough explanation for another student to follow.
- **Problem 3:** Used the formal definition of a unit in a mathematical proof.
- **Problem 4:** Used the Euclidean algorithm to find an inverse of one number modulo some integer.
- **Problem 5:** Utilized the formal definition of divisibility within a mathematical proof.



Problem 1: Affine Cipher Encryption and Decryption

Part (a): Encrypt the word "Cryptology" using the key (5, 4):

We work through the word **"CRYPTOLOGY"** character by character, using the encryption algorithm for an affine cipher:

$$E(x) = ax + b \pmod{26}$$

1. **c** ($x = 2$): $5(2) + 4 = 14 \equiv 14 \pmod{26} \longrightarrow$ **O**
2. **r** ($x = 17$): $5(17) + 4 = 89 \equiv 11 \pmod{26} \longrightarrow$ **L**
3. **y** ($x = 24$): $5(24) + 4 = 124 \equiv 20 \pmod{26} \longrightarrow$ **U**
4. **p** ($x = 15$): $5(15) + 4 = 79 \equiv 1 \pmod{26} \longrightarrow$ **B**
5. **t** ($x = 19$): $5(19) + 4 = 99 \equiv 21 \pmod{26} \longrightarrow$ **V**
6. **o** ($x = 14$): $5(14) + 4 = 74 \equiv 22 \pmod{26} \longrightarrow$ **W**
7. **l** ($x = 11$): $5(11) + 4 = 59 \equiv 7 \pmod{26} \longrightarrow$ **H**
8. **o** ($x = 14$): $5(14) + 4 = 74 \equiv 22 \pmod{26} \longrightarrow$ **W**
9. **g** ($x = 6$): $5(6) + 4 = 34 \equiv 8 \pmod{26} \longrightarrow$ **I**
10. **y** ($x = 24$): $5(24) + 4 = 124 \equiv 20 \pmod{26} \longrightarrow$ **U**

The final cipher-text is: **"OLUBVWHWIU"**

Part (b): Decrypt the ciphertext "NS" using this cipher.

To decrypt, we first need to find the multiplicative inverse of a, a^{-1}. That is,

$$a \cdot a^{-1} \equiv 1 \pmod{26}$$

Note that $5(21) = 105$, and $105 = 4(26) + 1$. Thus, $a^{-1} = 21$. We can now use the decryption algorithm:

$$D(y) = a^{-1}(y - b) \pmod{26}$$

1. **n** ($y = 13$): $21(13 - 4) = 21(9) \equiv 7 \pmod{26} \longrightarrow \mathbf{H}$
2. **s** ($y = 18$): $21(18 - 4) = 21(14) \equiv 8 \pmod{26} \longrightarrow \mathbf{I}$

Thus, the decrypted text reads **"HI"**.

Problem 2: Finding a and b from a message encrypted with an affine cipher

Given **"HELLO"** $\longrightarrow$ **"FKHHC"**:

1. **"HELLO"** $\equiv (7, 4, 11, 11, 14) \pmod{26}$
2. **"FKHHC"** $\equiv (5, 10, 7, 7, 2) \pmod{26}$

We choose the following system, representing the mapping "$H \to F$" and "$E \to K$" in the form $ax + b \equiv y \pmod{26}$

$$7a + b \equiv 5 \pmod{26} \ (1)$$
$$4a + b \equiv 10 \pmod{26} \ (2)$$

Then, we work through the following steps to solve for a:

$(7a + b) - (4a + b) \equiv (5 - 10) \pmod{26}$	Subtract equation (2) from (1)
$3a \equiv -5 \pmod{26}$	Simplify coefficients
$3a \equiv 21 \pmod{26}$	Find the positive remainder: $-5 + 26 = 21$
$9 \cdot 3a \equiv 9 \cdot 21 \pmod{26}$	Multiply by $3^{-1} \equiv 9 \pmod{26}$
$27a \equiv 189 \pmod{26}$	Multiply across
$a \equiv 7 \pmod{26}$	Reduce modulo 26: $189 = (7 \times 26) + 7$

Thus, $a = 7$, and we substitute a into one of the equations, say $4a + b \equiv 10 \pmod{26}$, and then solve for b:

$4(7) + b \equiv 10 \pmod{26}$	Substitute $a = 7$ into equation (2)
$28 + b \equiv 10 \pmod{26}$	Multiply coefficients
$2 + b \equiv 10 \pmod{26}$	Reduce $28 \pmod{26}$ since $28 = (1 \times 26) + 2$
$b \equiv 8 \pmod{26}$	Subtract 2 from both sides

Thus, $a = 7$ and $b = 8$, and the final key is $(7, 8)$.

Problem 3: Prove that n is a unit $\pmod{4n-1}$

Proof. Let n be a positive integer. We say that n is a **unit** modulo $4n-1$ if there exists an integer x such that

$$nx \equiv 1 \pmod{4n-1}$$

Let $x = 4$. Consider the algebraic identity:

$$4n = 4n$$

We can rewrite the right hand side of the equation by subtracting and adding one, exposing the modulus $4n-1$:

$$4n = (4n-1) + 1$$

We know that:

$$4n - 1 \equiv 0 \pmod{4n-1}$$

Then, adding 1 to both sides yields:

$$4n \equiv 1 \pmod{4n-1}$$

Because we have found an integer $x = 4$ such that $n \cdot 4 \equiv 1 \pmod{4n-1}$, the integer 4 serves as the multiplicative inverse of n. Therefore, by the definition of a unit, n is a unit modulo $4n-1$. $\square$

Problem 4: Euclidean Algorithm To Find Multiplicative Inverse

To find the multiplicative inverse of 206 modulo 5427, we first apply the Euclidean algorithm to find the greatest common divisor and then use the Extended Euclidean Algorithm to solve for the inverse.

Forward Phase: Euclidean Algorithm

$$\begin{aligned} 5427 &= 26(206) + 71 \\ 206 &= 2(71) + 64 \\ 71 &= 1(64) + 7 \\ 64 &= 9(7) + 1 \end{aligned}$$

Backward Phase: Extended Euclidean Algorithm

Starting with the final remainder of 1, we substitute back through our equations:

$$\begin{aligned} 1 &= 64 - 9(7) \\ 1 &= 64 - 9(71 - 64) \\ 1 &= 10(64) - 9(71) \\ 1 &= 10(206 - 2 \cdot 71) - 9(71) \\ 1 &= 10(206) - 29(71) \\ 1 &= 10(206) - 29(5427 - 26 \cdot 206) \\ 1 &= 764(206) - 29(5427) \end{aligned}$$

Because $764(206) \equiv 1 \pmod{5427}$, the multiplicative inverse of 206 modulo 5427 is 764.

Problem 5: Peer Review Problem

Problem: Suppose a, b, q and r be any integers such that $a = bq + r$. Using only the definition of the greatest common divisor as the largest common divisor of x and y, prove that $\gcd(a, b) = \gcd(b, r)$.

Proof:

- Let S_1 be the set of common divisors of a and b: $S_1 = \{d \in \mathbb{Z} : d \mid a \text{ and } d \mid b\}$
- Let S_2 be the set of common divisors of b and r: $S_2 = \{d \in \mathbb{Z} : d \mid b \text{ and } d \mid r\}$

To show that $\gcd(a, b) = \gcd(b, r)$, we will show that $S_1 = S_2$ by double inclusion.

Forward Case ($S_1 \subseteq S_2$): Let $d \in S_1$. Thus, $d \mid a$ and $d \mid b$ with $a = dm$, $b = dn$ for some integers m and n. We solve $a = bq + r$ for r and substitute:

$$r = a - bq = dm - dnq = d(m - nq) = dQ$$

Thus, $d \mid r$. Since we assumed $d \mid b$ and we have shown $d \mid r$, we know $d \in S_2$ and $S_1 \subseteq S_2$.

Backward Case ($S_2 \subseteq S_1$): Let $d \in S_2$. Thus, $d \mid b$ and $d \mid r$ with $b = dj$, and $r = dk$ for some integers j and k. We substitute into $a = bq + r$:

$$a = bq + r = djq + dk = d(qj + k) = dQ$$

Thus, $d \mid a$. Since we assumed $d \mid b$ and we have shown $d \mid a$, we know that $d \in S_1$ and $S_2 \subseteq S_1$.

Conclusion Since we have shown that $S_1 \subseteq S_2$ and $S_2 \subseteq S_1$, we have $S_1 = S_2$. Since our sets are identical, we have:

$$\max(S_1) = \max(S_2)$$
$$\gcd(a, b) = \gcd(b, r)$$

□