Example 4 — Affine Cipher Warm-Up

Goal. Determine which letter replaces `K` when the encryption function

$$f(p) = (7p + 3) \bmod 26$$

is used.

Big idea (the why):

The affine cipher multiplies the plaintext value by a "stretch" factor and then shifts it. It combines multiplication and addition inside modular arithmetic.

Encryption: $E(p) = (ap + b) \bmod 26$ Decryption: $D(c) = a^{-1}(c - b) \bmod 26$.

The constants a and b are keys. a must be coprime to 26 so that a^{-1} exists.

Step 1 — Convert letter K to a number

$$K \to 10$$

Step 2 — Apply the function $f(p) = (7p + 3) \bmod 26$

$$f(10) = (7 \cdot 10 + 3) \bmod 26 = 73 \bmod 26 = 21.$$

Step 3 — Convert number 21 back to a letter

$$21 \to V$$

Result: K is encrypted as V.

Why it works:

Multiplying by 7 mixes up the order of letters more effectively than a simple shift, yet because 7 and 26 are coprime, every letter still maps to exactly one output.

Practice (your turn!)

Problem A (easier). Using $f(p) = (3p + 1) \bmod 26$, find what letter replaces `C`. *Hint:* $C = 2$.

Problem B (similar). Using $f(p) = (5p + 7) \bmod 26$, find what letter replaces `H`. *Hint:* compute carefully, mod 26.

Problem C (harder). Encrypt the word `DOG` using $f(p) = (11p + 8) \bmod 26$. Write each step clearly: letter $\to$ number $\to$ formula $\to$ result $\to$ letter.

Reflection. Why must a be coprime with 26 for this cipher to be reversible?