ALGEBRA · MODULAR ARITHMETIC

Affine Cipher Lab Study Guide

How to encode a message, find the inverse of a in two ways, and decode, each with fully worked examples. Letters are numbered A = 0, B = 1, and so on up to Z = 25, and every remainder is between 0 and 25.

1. What is the affine cipher?

The affine cipher is a **substitution cipher**: every letter is always replaced by the same other letter. Each letter becomes a number (A = 0, B = 1, and so on up to Z = 25), a formula changes the number, and the result becomes a letter again. The two numbers a and b in the formula are the **key**.

ENCODE

$$E(x) = (ax + b) \bmod 26$$

Multiply by a, add b, then keep the remainder after dividing by 26.

DECODE

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

Subtract b, multiply by a^{-1}, then keep the remainder.

- **Caesar and Atbash.** The Caesar cipher is the special case $a = 1$, which shifts every letter b places along the alphabet. Julius Caesar is said to have shifted by 3, so $b = 3$. Atbash, which reverses the alphabet (A becomes Z, B becomes Y), is $a = 25$, $b = 25$.
- **Not every a works.** a must share no factor with 26, which is written $\gcd(a, 26) = 1$. Otherwise two letters encode to the same letter and the message can't be decoded. With $a = 2$, for example, A (0) and N (13) both become A. That leaves 12 usable values: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25.
- **Easy to break.** 12 choices for a and 26 for b give only 12 × 26 = 312 keys, so anyone can break the cipher by trying every key, or by counting how often each letter appears (frequency analysis, a method described by the 9th-century scholar al-Kindi). The affine cipher is for learning, not for keeping secrets.
- **Decoding needs an inverse.** a^{-1} is the inverse of a mod 26: the number that gives a remainder of 1 when you multiply it by a and divide by 26. For $a = 7$ it is 15, because 7 × 15 = 105 = 4 × 26 + 1.

2. Letters and their numbers

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Number	0	1	2	3	4	5	6	7	8	9	10	11	12

Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Number	13	14	15	16	17	18	19	20	21	22	23	24	25

3. Encoding step by step

To encode, use $E(x) = (ax + b) \bmod 26$ on every letter.

1. **Check the key.** $\gcd(a, 26)$ must be 1.
2. **Turn each letter into a number** (A = 0 … Z = 25).
3. **Encrypt each different letter once:** $x \rightarrow ax + b \rightarrow$ reduce mod 26 (subtract multiples of 26) → letter.
4. **Put the words together.** Spaces stay where they are.
5. **Write the final answer**, then check one letter by decoding it.

Worked example 1: MATH IS FUN with $a = 7$, $b = 11$

Step 1: gcd(7, 26) = 1, so the key works. Steps 2 and 3, one row for each different letter:

Letter	x	$7x + 11$	mod 26	Cipher
M	12	84 + 11 = 95	95 − 78 = 17	R
A	0	0 + 11 = 11	11	L
T	19	133 + 11 = 144	144 − 130 = 14	O
H	7	49 + 11 = 60	60 − 52 = 8	I
I	8	56 + 11 = 67	67 − 52 = 15	P
S	18	126 + 11 = 137	137 − 130 = 7	H
F	5	35 + 11 = 46	46 − 26 = 20	U
U	20	140 + 11 = 151	151 − 130 = 21	V
N	13	91 + 11 = 102	102 − 78 = 24	Y

Step 4, word by word:

Plaintext	Numbers	After $(7x + 11) \bmod 26$	Ciphertext
MATH	12, 0, 19, 7	17, 11, 14, 8	RLOI
IS	8, 18	15, 7	PH
FUN	5, 20, 13	20, 21, 24	UVY

Final answer: **MATH IS FUN → RLOI PH UVY**

To check by decoding (with $a^{-1} = 15$, found in sections 4 and 5): R = 17 → 15(17 − 11) = 90, and 90 − 78 = 12 = M. ✓

Worked example 2: MATH ROCKS with $a = 7$, $b = 17$

The same a with a different b gives a completely different message.

Letter	x	$7x + 17$	mod 26	Cipher
M	12	84 + 17 = 101	101 − 78 = 23	X
A	0	0 + 17 = 17	17	R
T	19	133 + 17 = 150	150 − 130 = 20	U
H	7	49 + 17 = 66	66 − 52 = 14	O
R	17	119 + 17 = 136	136 − 130 = 6	G
O	14	98 + 17 = 115	115 − 104 = 11	L
C	2	14 + 17 = 31	31 − 26 = 5	F
K	10	70 + 17 = 87	87 − 78 = 9	J
S	18	126 + 17 = 143	143 − 130 = 13	N

Plaintext	Numbers	After $(7x + 17) \bmod 26$	Ciphertext
MATH	12, 0, 19, 7	23, 17, 20, 14	XRUO
ROCKS	17, 14, 2, 10, 18	6, 11, 5, 9, 13	GLFJN

Final answer: **MATH ROCKS → XRUO GLFJN**

To check by decoding: X = 23 → 15(23 − 17) = 90, and 90 − 78 = 12 = M. ✓

4. Finding the inverse: the Extended Euclidean Algorithm

Goal: find a^{-1} so that $a \cdot a^{-1} \equiv 1 \pmod{m}$. Here $m = 26$.

Idea: write $1 = s \cdot m + t \cdot a$. The $s \cdot m$ term is 0 mod m, so $t \cdot a \equiv 1$ and t is the inverse.

1. **Divide repeatedly (forward pass).** Write dividend = quotient × divisor + remainder. The old divisor becomes the new dividend and the remainder becomes the new divisor. Stop when the remainder is 0.
2. **Check the gcd.** The last remainder that isn't 0 is gcd(a, m). If it is 1, the inverse exists. Otherwise there is no inverse, so stop.
3. **Rearrange** each equation (except the one ending in 0) as remainder = dividend − quotient × divisor.
4. **Substitute backwards.** Start with the equation for remainder 1. Replace the smaller remainders one at a time using the equations from step 3, working back up. Collect like terms. Keep the numbers as labels: don't multiply them out. Stop when only m and a remain.
5. **Read off t**, the number multiplying a.
6. **If t is negative**, add m until it is between 0 and $m - 1$.
7. **Check:** $a \times t \bmod m = 1$.

Example: the inverse of 11 mod 26

Forward pass

> 26 = 2 × 11 + 4
>
> 11 = 2 × 4 + 3
>
> 4 = 1 × 3 + 1
>
> 3 = 3 × 1 + 0

Rearranged

> (A) 4 = 26 − 2 × 11
>
> (B) 3 = 11 − 2 × 4
>
> (C) 1 = 4 − 1 × 3

The last remainder that isn't 0 is 1, so gcd(11, 26) = 1 and the inverse exists.

Back-substitution

> 1 = 4 − 1 × 3
>
> Start with (C).
>
> 1 = 4 − 1 × (11 − 2 × 4) = 4 − 11 + 2 × 4 = 3 × 4 − 1 × 11
>
> Replace the 3 using (B).
>
> 1 = 3 × (26 − 2 × 11) − 1 × 11 = 3 × 26 − 6 × 11 − 1 × 11 = 3 × 26 − 7 × 11
>
> Replace the 4 using (A).

So $t = -7$, and $-7 + 26 = 19$. Check: $11 \times 19 = 209 = 8 \times 26 + 1$. ✓

$11^{-1} \equiv 19 \pmod{26}$

Example: the inverse of 7 mod 26

Forward pass

$26 = 3 \times 7 + 5$

$7 = 1 \times 5 + 2$

$5 = 2 \times 2 + 1$

$2 = 2 \times 1 + 0$

Rearranged

(A) $5 = 26 - 3 \times 7$

(B) $2 = 7 - 1 \times 5$

(C) $1 = 5 - 2 \times 2$

The last remainder that isn't 0 is 1, so gcd(7, 26) = 1 and the inverse exists.

Back-substitution

$1 = 5 - 2 \times 2$

Start with (C).

$1 = 5 - 2 \times (7 - 1 \times 5) = 5 - 2 \times 7 + 2 \times 5 = 3 \times 5 - 2 \times 7$

Replace the 2 using (B).

$1 = 3 \times (26 - 3 \times 7) - 2 \times 7 = 3 \times 26 - 9 \times 7 - 2 \times 7 = 3 \times 26 - 11 \times 7$

Replace the 5 using (A).

So $t = -11$, and $-11 + 26 = 15$. Check: $7 \times 15 = 105 = 4 \times 26 + 1$. ✓

$7^{-1} \equiv 15 \pmod{26}$

Common mistakes

1. **Multiplying the numbers out during back-substitution.** Keep 26, 11, 4 … as labels and only combine the numbers in front of them.
2. **Sign errors when multiplying out a minus.** $-2 \times (11 - 2 \times 4) = -2 \times 11 + 4 \times 4$.
3. **Forgetting to make *t* positive** (step 6).
4. **Skipping the gcd check.** 13 has no inverse mod 26, because gcd(13, 26) = 13.

Quick reference: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23 and 25 have inverses mod 26.

5. Finding the inverse: Gauss' Method

Idea: write the inverse as the fraction $\frac{1}{a}$. Multiply the top and bottom by the same number, reduce both mod 26, and repeat until the bottom is 1 (or −1). The top is then the inverse. Multiplying the top and bottom by the same number doesn't change the fraction's value.

1. **Write the inverse as a fraction:** $a^{-1} \equiv \frac{1}{a} \pmod{26}$.
2. **Pick a multiplier k** so that k × bottom lands as close as possible to a multiple of 26 (just above or just below).
3. **Multiply** the top and bottom by k.
4. **Reduce the bottom mod 26.** A negative remainder is allowed when it is smaller in size ($21 \equiv -5$).
5. **Repeat** until the bottom is 1 or −1. If it is 1, the top is the inverse. If it is −1, change the sign of the top, adding 26 if needed.
6. **Check** that a × inverse mod 26 = 1.

Example: the inverse of 7 mod 26

Multiples of 7 near 26: 21 (5 below) and 28 (2 above). Take $k = 3$. ($k = 4$ is a dead end; see "Warning: dead ends".)

Round	Fraction	Multiply by	New fraction	Reduce mod 26
1	1/7	× 3	3/21	3/(−5)
2	3/(−5)	× 5	15/(−25)	15/1

The bottom is 1, so $7^{-1} \equiv 15$. Check: $7 \times 15 = 105 = 4 \times 26 + 1$. ✓

Example: the inverse of 11 mod 26

Multiples of 11 near 26: 22 gives −4 (even: a dead end); 33 gives 7 (odd: safe). Take $k = 3$.

Round	Fraction	Multiply by	New fraction	Reduce mod 26
1	1/11	× 3	3/33	3/7
2	3/7	× 3	9/21	9/(−5)
3	9/(−5)	× 5	45/(−25)	45/1

The bottom is 1, and 45 − 26 = 19, so $11^{-1} \equiv 19$. Check: $11 \times 19 = 209 = 8 \times 26 + 1$. ✓

> **Shortcut: aim for any multiple of 26, not just 26.** 11 × 2 = 22 (near 26, gives −4); 11 × 5 = 55 (near 52, gives +3); 11 × 7 = 77 (near 78, gives −1).
>
> So 1/11 = 7/77 ≡ 7/(−1). The bottom is −1, so change the sign of the top: −7 + 26 = 19. One round.

Warning: dead ends

Gauss' Method can stall when the modulus isn't prime (26 = 2 × 13). For example, 1/7 × 4 = 4/28 ≡ 4/2, a dead end: 2 shares a factor with 26, so no multiplier turns it into 1.

Rule for mod 26: after each step, make sure the new bottom is odd and not 13.

Quick check: add 26 to the top

Add 26 to the top of $1/a$ until a divides it. For a = 7: 1, 27, 53, 79, 105. 105 ÷ 7 = 15, so $7^{-1} \equiv 15$.

Rules to remember

- Do the same thing to the top and the bottom.
- Reduce only mod 26 (no ordinary cancelling).
- Negative bottoms are fine.
- Avoid even bottoms, and 13, mod 26.
- If you end with −1, change the sign of the top and add 26.

6. Decoding

To decode, use $D(y) = a^{-1}(y - b) \bmod 26$ on every cipher letter.

1. **Find a^{-1}** with the Extended Euclidean Algorithm or Gauss' Method.
2. **Turn each cipher letter into a number** y (A = 0 … Z = 25).
3. **Decrypt each different letter once:** $y \to y - b \to$ multiply by $a^{-1} \to$ reduce mod 26 $\to$ letter. To reduce a negative number, add multiples of 26 until it is between 0 and 25.
4. **Put the words together.** Spaces stay where they are.

Worked example: RLOI PH UVY with $a = 7, b = 11$

From sections 4 and 5, $a^{-1} = 15$, so $D(y) = 15(y - 11) \bmod 26$.

Cipher letter	y	$y - 11$	$15(y - 11)$	mod 26	Plain
R	17	6	90	90 − 78 = 12	M
L	11	0	0	0	A
O	14	3	45	45 − 26 = 19	T
I	8	−3	−45	−45 + 52 = 7	H
P	15	4	60	60 − 52 = 8	I
H	7	−4	−60	−60 + 78 = 18	S
U	20	9	135	135 − 130 = 5	F
V	21	10	150	150 − 130 = 20	U
Y	24	13	195	195 − 182 = 13	N

Ciphertext	Numbers	After $15(y - 11) \bmod 26$	Plaintext
RLOI	17, 11, 14, 8	12, 0, 19, 7	MATH
PH	15, 7	8, 18	IS
UVY	20, 21, 24	5, 20, 13	FUN

Final answer: **RLOI PH UVY → MATH IS FUN**

7. Inverses mod 26

All 12 usable values of a with their inverses. Each product $a \times a^{-1}$ is one more than a multiple of 26. The pairs swap: the inverse of 3 is 9 and the inverse of 9 is 3.

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25
$a \times a^{-1}$	1	27	105	105	27	209	105	391	209	105	391	625