# Number
# In-class Exercises

1. Prove **Theorem 4.1** (d).

For all $a, b, c \in \mathbf{Z}$

**d)** $a|b \Rightarrow a|bx$ for all $x \in \mathbf{Z}$.

2. Prove **Theorem 4.5** (a).

*Let $a_1, a_2, b_1, b_2$, and $n$ be integers with $n > 1$.*
*If $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$, then*

**(a)** $a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$, *and*

3. Compute $3^{21} \bmod 53$.

Hint: start from $3^2 \bmod 53$
then $3^4 \bmod 53$
$3^8 \bmod 53$
:

4. What are the solutions of the linear congruence

$$3x \equiv 4 \pmod 7?$$

5. Let $S = 42$. Finding $S^{-1}$, where $S^{-1} \times S \equiv 1 \pmod{101}$

# Number
# Suggested Exercises

**1.** If $n \in \mathbf{Z}^+$, and $n$ is odd, prove that $8|(n^2 - 1)$.

**2.** Let $a, b, c \in \mathbf{Z}^+$ with $\gcd(a, b) = 1$. If $a|c$ and $b|c$, prove that $ab|c$. Does the result hold if $\gcd(a, b) \neq 1$?

3. Use Euclid's Algorithm to calculate the Greatest Common Divisor of 140 and 1099.

# 4. **Morpheus cipher**.

The Cipher works as follows:

## Morpheus Cipher:

1) You will need a **plaintext**, along with two integers **a** and **b**

2) Convert your plaintext to a numeric vector **P**.

3) Divide **P** into pairs*. For each pair, $(P_1, P_2)$, create the cipher pair $(C_1, C_2)$ using

$$C_1 \equiv a P_1 + b P_2 \pmod{26}$$
$$C_2 \equiv b P_1 - a P_2 \pmod{26}$$

4) Recombine the cipher pairs to create the full cipher vector **C**.

5) Once all **C** entries have been found, convert your vector back to text.

* You and your friend agree to only send even length messages

## Example: a=2, b=5

B O A T — Plaintext to number codes vector P

1 14 0 19

(1,14)(0,19) — Pair up

Pair 1: $(P_1, P_2) = (1, 14)$
$C_1 = 2\times1 + 5\times14 \equiv 20 \pmod{26}$
$C_2 = 5\times1 - 2\times14 \equiv 3 \pmod{26}$

Pair 2: $(P_1, P_2) = (0, 19)$
$C_1 = 2\times0 + 5\times19 \equiv 17 \pmod{26}$
$C_2 = 5\times0 - 2\times19 \equiv 14 \pmod{26}$

Recombine: 20 3 17 14 — vector C

to word: U D R O — to ciphertext

Text & code is provided.

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

4. **Morpheus cipher**. (continued)

Assuming you have access to ciphertext, and both parameters $a$ and $b$, describe how you would go about inverting the Morpheus cipher in order to recover the plaintext.

From the example, suppose you received ciphertext "UDRO", how do you recover the original plaintext "BOAT"?