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 $x \in \mathbf{Z}$.

Proof : $a|b$ means $b = \mathrm{a} \cdot \mathrm{n}$ for some $\mathrm{n} \in \mathbf{Z}$.

Multiply both sides by any $x \in \mathbf{Z}$

$x \cdot b = a \cdot n \cdot x$, where $(\mathrm{n} \cdot x)$ is also an integer.

Thus, $a|bx$

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*

Proof : $a_1 \equiv a_2 (mod\ n)$ and $b_1 \equiv b_2 (mod\ n)$

Mean $n|(a_1 - a_2)$ and $n|(b_1 - b_2)$.

By Theorem 4.1 (e) we have

$$n|(a_1 - a_2) + (b_1 - b_2)$$

$$\Rightarrow \quad n|(a_1 + b_1) - (a_2 + b_2)$$

Thus, $a_1 + b_1 \equiv a_2 + b_2 (mod\ n)$

3. Compute 3^{21} mod 53.

Hint: start from 3^2 mod 53

then 3^4 mod 53

3^8 mod 53

$\vdots$

$$
\begin{aligned}
3^2 \pmod{53} &= 9 \\
3^4 \pmod{53} &= 9^2 \pmod{53} = 81 \pmod{53} = 28 \\
3^8 \pmod{53} &= 28^2 \pmod{53} = 784 \pmod{53} = 42 \\
3^{16} \pmod{53} &= 42^2 \pmod{53} = 1764 \pmod{53} = 15 \\
\Rightarrow 3^{21} \pmod{53} &= 3^{16+4+1} \pmod{53} = (15 \times 28 \times 3) \pmod{53} = 1260 \pmod{53} = 41
\end{aligned}
$$

4. What are the solutions of the linear congruence

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

$5 \times 3x \equiv 5 \times 4 \pmod{7}$

$5 \times 3 \equiv 15 \equiv 1 \pmod{7}$

$5 \times 4 \equiv 20 \equiv 6 \pmod{7}$

it follows that if x is a solution, then $x \equiv 6 \pmod{7}$.

So, solutions are, 6, 13, 20, …, and -1, -8, -15, …. etc.

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

$$
\begin{aligned}
101 \bmod 42 &= 17 &\implies&& 101 - 2 \times 42 &= 17 \\
42 \bmod 17 &= 8 &\implies&& 42 - 2 \times 17 &= 8 \\
17 \bmod 8 &= 1 &\implies&& 17 - 2 \times 8 &= 1
\end{aligned}
$$

$$
\begin{aligned}
42 - 2 \times 17 = 8 \quad &\implies \quad 42 - 2 \times (101 - 2 \times 42) = 8 \\
& \quad 5 \times 42 - 2 \times 101 = 8
\end{aligned}
$$

$$
\begin{aligned}
17 - 2 \times 8 = 1 \quad &\implies \quad (101 - 2 \times 42) - 2 \times (5 \times 42 - 2 \times 101) = 1 \\
& \quad 5 \times 101 - 12 \times 42 = 1
\end{aligned}
$$

$S^{-1} = -12$

Number
Suggested Exercises

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

Proof：

Let $n = 2k + 1, k \geq 0$ & $k \in \mathbf{Z}^+$

$$
\begin{aligned}
&n^2 - 1 \\
&= (2k+1)^2 - 1 \\
&= 4k^2 + 4k \\
&= 4k(k+1)
\end{aligned}
$$

Since one of k, $k+1$ must be even,say it is $2m$ for some $m \in \mathbf{Z}^+$

therefore, $n^2 - 1 = 4 \cdot 2m = 8m$. It follows 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 $\gcd(a, b) \neq 1$?

Proof :

$$gcd(a,b) = 1 \Rightarrow ax + by = 1 \quad for\ som\ x, y \in \mathbf{Z}.$$

Then $c = acx + bcy.$

$$a|c \Rightarrow c = ad,\ \ b|c \Rightarrow c = be,\ \ for\ som\ d, e \in \mathbf{Z}.$$

$$\begin{aligned} \text{so } c &= acx + bcy \\ &= \mathrm{a}(be)x + b(ad)y \\ &= \mathrm{ab}(ex + dy) \qquad \Longrightarrow ab|c \qquad \because (ex + dy) \in \mathbf{Z}. \end{aligned}$$

The result is false if $gcd(a,b) \neq 1.$

For example, let a=12, b=18, c=36.Then $a|c,\ b|c,\ but\ (ab) \nmid c.$

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

$1099 = 7 * 140 + 119$

$140 = 1 * 119 + 21$

$119 = 5 * 21 + 14$

$21 = 1 * 14 + \mathbf{7}$

$14 = 2 * 7 + 0$

$\gcd(140, 1099) = 7$

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

1 14 0 19 — number codes vector P

(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"?

$$C_1 \equiv aP_1 + bP_2 \pmod{26}$$

$$C_2 \equiv bP_1 - aP_2 \pmod{26}$$

$$aC_1 \equiv a^2P_1 + abP_2 \pmod{26} \quad \cdots\text{①}$$

$$aC_2 \equiv abP_1 - a^2P_2 \pmod{26} \quad \cdots\text{②}$$

$$bC_1 \equiv abP_1 + b^2P_2 \pmod{26} \quad \cdots\text{③}$$

$$bC_2 = b^2P_1 - abP_2 \pmod{26} \quad \cdots\text{④}$$

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

Note that we have a, b, and C_1, C_2 and would like to find P_1 and P_2

① + ④ $\quad aC_1 + bC_2 \equiv (a^2+b^2)P_1 \pmod{26} \cdots$ ⑤

③ − ② $\quad bC_1 - aC_2 \equiv (a^2+b^2)P_2 \pmod{26} \cdots$ ⑥

Notice that P_1 and P_2 can be recovered uniquely if $\gcd((a^2+b^2), 26) = 1$.

Let $k = (a^2+b^2)$, find its inverse k^{-1} modulo 26.

Table of inverses for mode 26

1^{-1}	3^{-1}	5^{-1}	7^{-1}	9^{-1}	11^{-1}	15^{-1}	17^{-1}	19^{-1}	21^{-1}	23^{-1}	25^{-1}
1	9	21	15	3	19	7	23	11	5	17	25

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

Now suppose we have obtained k^{-1}.

$$k k^{-1} \equiv 1 \pmod{26}$$

$$(a^2+b^2)\, k^{-1} \equiv 1 \pmod{26}$$

from ⑤ $$(ac_1+bc_2)\cdot k^{-1} \equiv (a^2+b^2)\cdot k^{-1}\cdot P_1 \pmod{26}$$

$$(ac_1+bc_2)\cdot k^{-1} \equiv P_1 \pmod{26}$$

$$P_1 \equiv k^{-1}\cdot(ac_1+bc_2) \pmod{26}$$

from ⑥ $$(bc_1-ac_2)\cdot k^{-1} \equiv (a^2+b^2)\cdot k^{-1}\cdot P_2 \pmod{26}$$

$$P_2 \equiv k^{-1}\cdot(bc_1-ac_2) \pmod{26}$$