Problem 8.1

(a) $(\mathbb{Z}, \cdot)$ → no inverse

(b) $(\mathbb{R}^n, +)$ → yes

$i \begin{pmatrix} k_1 \\ \vdots \\ k_n \end{pmatrix} \rightarrow \begin{pmatrix} -k_1 \\ \vdots \\ -k_n \end{pmatrix}$

(c) $(\mathbb{R}^n, \cdot)$ → no closure

+ "no inverse" for 0

$i \begin{pmatrix} k_1 \\ \vdots \\ k_n \end{pmatrix} \rightarrow \begin{pmatrix} 1/k_1 \\ \vdots \\ 1/k_n \end{pmatrix}$

(d) $\left[r e^{i\theta}\right]^n = r^n e^{in\theta} = 1$

$$r_1^n e^{in\theta_1} \cdot r_2^n e^{in\theta_2}$$

Closure Ok

$$= (r_1 r_2)^n e^{i(\theta_1 + \theta_2)n}$$

Associativity ok

Identity element ok

$$1^n e^{i0n} = 1$$

Inverse element $\boxed{\text{ok}}$

$r_1 = 1$

$$r_1^n e^{in\theta_1} = 1$$

$$r_2^n e^{in\theta_2} = 1$$

$$\underbrace{(r_1 \cdot r_2)}_{=1}{}^n e^{in(\theta_1+\theta_2)} = 1$$

$$1 \quad e^{in(\theta_1+\theta_2)} = 1$$

(e) Closure Ok

$$e^{i\theta} \cdot e^{i\theta} = e^{i2\theta}$$

$\boxed{\text{YES}}$

Asso. Ok

Id $e^{i0} = 1$
Ok

Inverse Ok

$$e^{i\theta} \cdot e^{-i\theta} = 1$$

(g) Closure Ok

$\boxed{\text{NO}}$

$$0 \wedge 1 \in \{0,1\}$$

Assoc. Ok
Id $\boxed{1}$ Ok
Inverse $\boxed{\text{no}}$ Ok

(g) $\{0, 1, 2, 3, 4\}$

Closure. Ok

Assoc. Ok

Id. $[1]_5$

Inverse. $\boxed{\text{NO}}$

(h) Closure Ok

Assoc. ok

Id. ok

Inverse ok.

i Closure. $\boxed{\text{no}}$

Assoc ok

Id $\boxed{\text{no}}$

2

$G, *$ identity is $[1]$

inversible is

$\mathbb{Z}/5\mathbb{Z}^* \times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$H, \otimes$ id is $[1]$

$z^4 = 1$	1	$e^{\frac{\pi i}{2}}$	$e^{\pi i}$	$e^{\frac{3\pi i}{2}}$
1	1	$e^{\frac{\pi i}{2}}$	$e^{\pi i}$	$e^{\frac{3\pi i}{2}}$
$e^{\frac{\pi i}{2}}$	$e^{\frac{\pi i}{2}}$	$e^{\pi i}$	$e^{\frac{3\pi i}{2}}$	1
$e^{\pi i}$	$e^{\pi i}$	$e^{\frac{3\pi i}{2}}$	1	$e^{\frac{\pi i}{2}}$
$e^{\frac{3\pi i}{2}}$	$e^{\frac{3\pi i}{2}}$	1	$e^{\frac{\pi i}{2}}$	$e^{\pi i}$

$e^{\frac{1}{2}k\pi i}$

$$\varphi(a * b) = \varphi(a) \otimes \varphi(b)$$

Match φ identity el :

G	H
$1 \to 1$	
$4 \to e^{\pi i}$	

$2^4 = 1$
$3^4 = 1$

2, 3 have the same order (4)
and $e^{\frac{\pi i}{2}}$ order 4

$e^{\frac{3\pi i}{2}}$ order 4

$\Rightarrow$ they can be matched

$2 \to e^{\frac{\pi i}{2}}$
$3 \to e^{\frac{3\pi i}{2}}$

OR

$2 \to e^{\frac{3\pi i}{2}}$
$3 \to e^{\frac{\pi i}{2}}$

(b) ~~they do not have the same cardinality~~

they do
you're dumb
bro

(c) order id is 00

$(\mathbb{Z}/2\mathbb{Z},+)\times(\mathbb{Z}/2\mathbb{Z},+)$	00	01	10	11
00 → 1	00	01	10	11
01 → 1	01	00	11	10
10 → 1	10	11	00	01
11 → 1	11	10	01	00

$0 \to 1 \quad 1 \to 3 \quad 2 \to 2 \quad 3 \to 4$

$\mathbb{Z}/4\mathbb{Z}, +$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

(d) They do not have the same cardinality

Problem 8.2

18	1
36	2
54	3
72	4
90	5
108	6
126	7
144	8
162	9

$18 = 2 \cdot 3^2$

(1)

tous les nb dont diviser 6

El	Order
1	1
5	6
7	3
11	6
13	3
17	2

$13 \cdot 13$
$= 130 + 39$
$= 169$
$= [7]_{18}$

$7 \cdot 13 = 91$
$= 91$

$17 \cdot 17$
$= 170 + 119$
$= \boxed{8} + \boxed{11}$
$= (19) = (1)$

$11 \cdot 11$
$= 121$

5 25 125

7 $(49)_{18} = [13]_{18}$
$13 \cdot 7 = 91$
$= 91$
$[91]_{18} = [1]_{18}$

$[13]_{18}$
$11 \cdot 13 = 110 + 33$
$= 143$

$[17]_{18}$
$17 \cdot 11 = 170 + 77$

2 orders have to be the same

orders needed

→ same cardinality (could be 6)

1
6
3
6
3
2

$0 \to 1$

$1 \to 6$

$2 \to 3$

$3 \to 2$

$4 \to 3$

$5 \to 6$

Problem 8.3

①

$$x\,[x]^{-1} = [1]_{17}$$

$$y\,[y]^{-1} = [1]_{121}$$

$$\Rightarrow \quad x[x]^{-1}\,y[y]^{-1} = [1]$$

② invertible elements in 17: $\{1, 2, \dots, 16\}$ $\rightarrow$ 16

invertible elements in 121: $\{1, 2, \dots, 121\} \setminus \{11, 22, 33, 44, 55, 66, 77, 88, 99, 110\}$ $\rightarrow$ $11 \cdot 11$

$$16 \cdot (120 - 10)$$
$$= 16 \cdot 110$$

③ 2 and 13 are coprime

↳ $\phi(13) = 12$

$$2^{12} \equiv 1 \, [13]$$

$\Rightarrow$ we try all the divisors of 12, do not work!

④ $\phi(19) = 18$

$$x^{18} \equiv 1 \, [19]$$
$$x^{19} \equiv x \, [19]$$

x can be $\{0, 1, \dots, 18\}$

Problem 2.4

(1) Yes, the key is independent of the message

(2) $c = r + k \mod m$ (otherwise if sum $> m$ we know that the key or the plaintext $> m$)

(3)