ZK BOOTCAMP

Homework 1

① $s = \{0, 1, 2, 3, 4, 5, 6\} = \mathbb{Z}_7$.

ⓐ $4+4$

$= 8 \bmod 7 = 1$

ⓑ 3×5

$= 15 \bmod 7 = 1$

ⓒ What is the inverse of 3?

According to fermat's little theorem

$a^{-1} = a^{p-2} (\bmod p)$

$3^{-1} = 3^{7-2} \bmod 7$

$= 3^5 \bmod 7$

$= 243 \bmod 7$

$= 5$

$$\begin{array}{r} 7 \,)\, 243 \,(\, 34 \\ 21 \\ \hline 33 \\ 28 \\ \hline 5 \end{array}$$

---

② operation → "+"

s → group

To consider 's' is a group, all 4 properties should be valid.

① . closure [Result of a+b is in group]

For example, $a=4$ $b=4$

$a+b = 8 \bmod 7 = 1$

Result "1" is in group, closure property is proved.

② Associativity. [$(a+b)+c = a+(b+c)$, all a,b,c is in group]

For example, $a=0, b=1, c=2$

$(0+1)+2 = 0+(1+2)$

$1 \bmod 7 + 2 = 0 + 3 \bmod 7$

$8+2 = 0+10$

$10 \bmod 7 = 10 \bmod 7$

$3 = 3$ hence proved.

③ Identity [exists element e in group, for every element a in group $e \cdot a = a \cdot e = a$]

For example, $e=1, a=4$

$1 \cdot 4 = 4 \cdot 1 = 4$ hence proved.

④ Inverse element [for each a in group, there exists b in group, $b = a^{-1}$ such that $a+b = b+a = e$
e → identity element]

For example,

$a = 2$

$b = 2^{-1} \Rightarrow 2^{7-2} \bmod 7$ [∵ According to Fermats little theorem]

$2^5 \bmod 7$

$32 \bmod 7$

5

$2+5 = 5+2 = 7$ is in the group

hence proved.

③ $-13 \bmod 5$

congruence

$a \equiv b \bmod m$.

ie $a = mr + b$

X

* When dealing with negative numbers in a modulus operation we add divisor untill the dividend is positive.

* $-13 + 5 = -8$

$-8 + 5 = -3$

$-3 + 5 = 2$

Ans: 2

---

④ By substituting method we get $x = 2$

Given: $x^3 - x^2 + 4 \cdot x \cdot 0 - 12$

$$\begin{array}{c|cccc} 2 & 1 & -1 & 4 & -12 \\ & 0 & 2 & 2 & 12 \\ \hline & 1 & 1 & 6 & \boxed{0} \end{array}$$

$\boxed{x^2 + x + 6}$

$x^3 - x^2 + 4x - 12 = (x-2)(x^2+x+6)$

$x^2 + 3x - 2x + 6$

$x(x+3) - 2(x+3)$

$\dfrac{-1 \pm \sqrt{-23}}{2}$

↓

2 Roots

$\boxed{\therefore \text{positive root} = 2}$

$\boxed{\therefore \text{Degree} = 3}$