KAIST 전산학과 최광무

4-1 수(number)

약수와 배수

$a, b \in \mathbb{Z}$(단 $a \neq 0$), 만일 ($\exists\, c \in \mathbb{Z}$: $b = ac$) 혹은 ($\frac{b}{a} \in \mathbb{Z}$)일 때 $a \mid b$라고 쓰고,

a는 b의 약수(約數; factor, divisor)이고,

b는 a의 배수(倍數; multiple)이다.

나머지와 몫

$a \in \mathbb{Z}$, $d \in \mathbb{Z}^+$, $\exists_1 q, r \in \mathbb{Z}$: $a = dq + r$(단 $0 \leq r < d$)일 때,

$q = a$ **div** d이고 $r = a$ **mod** d이다.

$a \div d = q \cdots r$ 또는 (q, r)이라 쓰고,

a를 d로 나눈(divides) 몫(quotient)은 q, 나머지(remainder)는 r이다.

몫 연산(Modulus Arithmetic)

div, **mod**: $\mathbb{Z} \times (\mathbb{Z} - \{0\}) \to \mathbb{Z}$로 정의된다.

$\div$: $\mathbb{Z} \times (\mathbb{Z} - \{0\}) \to \mathbb{Z} \times \mathbb{Z}$

$a \div d = (a$ **div** $d,\ a$ **mod** $d)$

$\forall\, m \in \mathbb{Z}^+$: $\mathbf{mod}_m$: $\mathbb{Z} \to \mathbb{Z}_m$ 단($\mathbb{Z}_m = \{0, 1, 2, \cdots, m-1\}$)

예) $5\ (\mathbf{mod}_3)$[1] $= 2$, $(-5)\ (\mathbf{mod}_3) = 1$.

예) $(5+3)\ (\mathbf{mod}_3) = 2$, $(5 \cdot 3)\ (\mathbf{mod}_3) = 0$.

$\forall\, m \in \mathbb{Z}^+$: $+_m$, $\cdot_m$: $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_m$.

$\forall\, a, b \in \mathbb{Z}$: $a +_m b \stackrel{\text{def}}{=} (a+b)\ (\mathbf{mod}_m)$ $\quad a \cdot_m b \stackrel{\text{def}}{=} (a \cdot b)\ (\mathbf{mod}_m)$

예) $5 +_3 3 = 2$, $(5 \cdot_3 3) = 0$.

치역뿐 아니라 정의역도 $\mathbb{Z}_m (\subseteq \mathbb{Z})$으로 줄여보자.

$\forall\, m \in \mathbb{Z}^+$: $\oplus_m$, $\odot_m$: $\mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m$.

$\forall\, a, b \in \mathbb{Z}_m$: $a \oplus_m b \stackrel{\text{def}}{=} (a+b)\ (\mathbf{mod}_m)$ $\quad a \odot_m b \stackrel{\text{def}}{=} (a \cdot b)\ (\mathbf{mod}_m)$

예) $2 \oplus_3 0 = 2$, $2 \odot_3 0 = 0$.

(Col) $\forall\, a, b \in \mathbb{Z}$: $(a\ (\mathbf{mod}_m)) \oplus_m (b\ (\mathbf{mod}_m)) = (a+b)\ (\mathbf{mod}_m)$[2]

$(a\ (\mathbf{mod}_m)) \odot_m (b\ (\mathbf{mod}_m)) = (a \cdot b)\ (\mathbf{mod}_m)$[3]

예) $(5\ \mathrm{mod}_3) \oplus_3 (3\ \mathrm{mod}_3) = 2 \oplus_3 0 = 2$,

$(5\ \mathrm{mod}_3) \odot_3 (3\ \mathrm{mod}_3) = 2 \odot_3 0 = 0$.

연산 $(\mathbb{Z}_m, \oplus_m)$와 $(\mathbb{Z}_m, \odot_m)$은 각각 연산 $(\mathbb{Z}, +)$와 $(\mathbb{Z}, \cdot)$의 homomorphic image[4] 라고 한다.

---

1) $\mathbf{mod}_m$은 일진 후순위(unary postfix) 연산자이다.

2) $\mathbf{mod}_m$을 일진 전순위(unary prefix) 함수 h로 바꾸면, $h(a) \oplus_m h(b) = h(a+b)$이다.

3) $\mathbf{mod}_m$을 일진 전순위(unary prefix) 함수 h로 바꾸면, $h(a) \odot_m h(b) = h(a \cdot b)$이다.

4) 교과서 12장 3절 참조