Modulos distributive

태그	
공개여부	☑
날짜	
작성일자	

$$(A+B)\ \%\ C = (A\%C + B\%C)\ \%\ C$$
$$(A-B)\ \%\ C = (A\%C - B\%C)\ \%\ C$$
$$(A\times B)\ \%\ C = (A\%C \times B\%C)\ \%\ C$$

위와 같이 모듈러 연산은 나머지를 구하는 연산자이며 다음의 분배법칙이 모두 성립한다. 왜 이런지 궁금해서 계속 찾아보다가 간신히 찾은게 칸 아카데미에서 증명한 내용이다. 더하기 부분만 증명을 하도록 해보자.

$$A=CQ_1+R_1\ \ (0\leq R_1<C,\ \ Q_1\in Z)$$
$$B=CQ_2+R_2\ \ (0\leq R_2<C,\ \ Q_2\in Z)$$

C로 나눴을 때 각각의 몫과 나머지를 갖기 때문에 다음과 같이 타나낼 수 있다.

또한 이걸 더하기했을 때 식의 좌변에 각각 대입하면 아래와 같이 된다.

$$(CQ_1+R_1+CQ_2+R_2)\ \%\ C$$
$$= (C\times(Q_1+Q_2)+R_1+R_2)\ \%\ C$$

이제 모듈러 연산의 특성에 따라 나머지만을 연산하기 때문에 나머지만 남게 된다. → C로 나눴을 때 몫은 Q1+Q2, 나머지는 R1+R2

*C의 배수끼리 더하면 결과도 C의 배수

$$(R_1+R_2)\ \%\ C$$

여기서 나머지 각각이 A,B에 대한 모듈러 연산이기 때문에

$$R_1+R_2 = A\%C + B\%C$$

모듈러 연산의 분배법칙이 증명된다.

뺄셈,곱셈은 이와 동일한 원리로 증명된다고 하지만 **나눗셈은 분배법칙이 성립하지 않는다.**

따라서 나눗셈에 대한 분배법칙을 계산할 때는 곱셈의 역원을 활용해야 한다.