5. 모듈로 연산

모듈로(modulo) 연산은 정수 연산으로 **나머지**를 구하는 연산이다. **mod**로 표기한다.

// 예제 1 : 모듈로 연산

0 mod 5 = 0 1 mod 5 = 1 7 mod 5 = 2 8 mod 5 = 3 9 mod 5 = 4	연산 결과가 **양수**이면, 추가로 처리할 것이 없다.
−1 mod 5 = −1 + **5** = 4 −7 mod 5 = −2 + **5** = 3 −8 mod 5 = −3 + **5** = 2 −9 mod 5 = −4 + **5** = 1	**// 연산 결과가 음수**이면, (mod m) 연산 결과에 **+m**을 한다. • −8 mod 5 = **−3** → 연산 결과가 음수 ↓연산 결과가 음수이면, **+5**를 한다. • −8 mod 5 = **−3 + 5** = **2**

// 모든 정수를 5로 나누었을 때, 나머지에 따라 분류하면 다음과 같다.(잉여류)

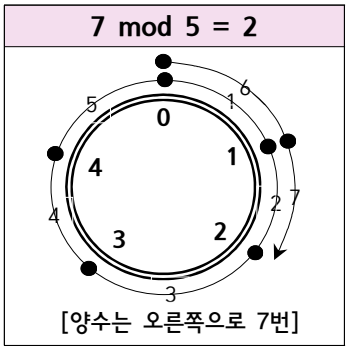
• 나머지가 **0**인 정수의 집합 = {…, −15, −10, −5, 0, 5, 10, 15, …}
• 나머지가 **1**인 정수의 집합 = {…, −14, −9, −4, 1, 6, 11, 16, …}
• 나머지가 **2**인 정수의 집합 = {…, −13, −8, −3, 2, 7, 12, 17, …}
• 나머지가 **3**인 정수의 집합 = {…, −12, −7, −2, 3, 8, 13, 18, …}
• 나머지가 **4**인 정수의 집합 = {…, −11, −6, −1, 4, 9, 14, 19, …}

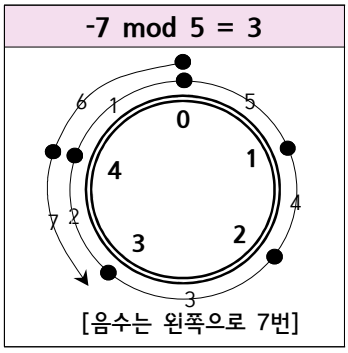
↓이를 **합동식**으로 나타내면 다음과 같다.

… ≡ −15 ≡ −10 ≡ −5 ≡ **0** ≡ 5 ≡ 10 ≡ 15 … (mod 5)
… ≡ −14 ≡ −9 ≡ −4 ≡ **1** ≡ 6 ≡ 11 ≡ 16 … (mod 5)
… ≡ −13 ≡ −8 ≡ −3 ≡ **2** ≡ 7 ≡ 12 ≡ 17 … (mod 5)
… ≡ −12 ≡ −7 ≡ −2 ≡ **3** ≡ 8 ≡ 13 ≡ 18 … (mod 5)
… ≡ −11 ≡ −6 ≡ −1 ≡ **4** ≡ 9 ≡ 14 ≡ 19 … (mod 5)

• **결론** : **법 5**에 대한 합동인 수는 양변에 **5**를 **더하거나 뺄** 수 있다. 결과는 같다.

// 시계를 이용한 모듈로 이해하기





// 예제 2 : 분수에 대한 모듈로 연산

• $5 \times 3^{-1} \bmod 11 = 5 \times \frac{1}{3} \bmod 11$

↓

↓ **분수** 형태의 나눗셈을 가진 모듈로 연산은 **역원**을 이용한다.

↓ 즉, 곱셈에 대한 **3**의 역원을 구한다.(모듈로 **11**에서 **3**의 역원은 **4**이다)

↓ **3** × **4** mod 11 = **12** mod 11 = **1**이므로, **3**의 역원은 **4**이다.

↓ 역원 **4**를 이용하면, **분수** 형태가 **제거**된다.(곱셈에서는 **1**을 곱하여도 그 결과는 같다)

↓

$= 5 \times \frac{1}{3} \times \underline{3 \times 4} \bmod 11 = 5 \times 4 \bmod 11 = 20 \bmod 11 = 9 \bmod 11$

↓

$\underline{3 \times 4 \bmod 11 = 1}$ 이다. 곱셈에서는 **1**을 곱하여도 그 결과는 같다.

// 보충 설명 : 모듈로 연산에서 분수의 분모에 대한 역원 구하기

$3^{-1} \bmod 11 = \frac{1}{3} \bmod 11$	3 × **4** mod **11** = 12 mod **11** = **1**이므로, **3**의 **역원**은 **4**이다.
$3^{-1} \bmod 13 = \frac{1}{3} \bmod 13$	3 × **9** mod **13** = 27 mod **13** = **1**이므로, **3**의 **역원**은 **9**이다.
$3^{-1} \bmod 17 = \frac{1}{3} \bmod 17$	3 × **6** mod **17** = 18 mod **17** = **1**이므로, **3**의 **역원**은 **6**이다.

• **모듈로 연산에서 역원은 모듈로** 값에 따라 다르다.

• $3^{-1} \times \underline{3 \times 4} \bmod 11 = 1 \times 4 \bmod 11 = 4 \bmod 11$

↓

$\underline{3 \times 4 \bmod 11 = 1}$ 이다. 곱셈에서는 **1**을 곱하여도 그 결과는 같다.

ㄴ, 이 부분은 개인에 따라 잘 이해되지 않을 수도 있다.**(그냥 암기하면 되는 부분)**

// **참고** : **분수** 형태의 나눗셈을 가진 모듈로 연산

• **분수** 형태의 모듈로 연산은 **타원곡선암호**에서 **기울기**를 계산할 때, 필요하다.

• **타원곡선암호**는 두 점을 더하는 계산이 필요하다.

• **타원곡선암호**는 두 점을 더하는 원리를 이용하여 **공개키**를 구한다.

// 예제 3 : 모듈로에서 지수 연산

모듈러 연산에서 지수연산은 **곱셈의 반복**으로 간단하게 계산할 수 있다.

- 2^{90} = 1,237,940,039,290,000,000,000,000,000
  ↳, 매우 큰 수 계산은 컴퓨터에서 **오버플로 오류**를 발생시킨다.
- 매우 큰 수 계산은 **분할과 정복**(divide and conquer)을 이용하면 해결할 수 있다.

- $2^{10} \bmod 13 = 1024 \bmod 13 =$ **10**
- $2^{20} \bmod 13 = (2^{10} \times 2^{10}) \bmod 13 = (10 \times 10) \bmod 13 = 100 \bmod 13 =$ **9**
- $2^{40} \bmod 13 = (2^{20} \times 2^{20}) \bmod 13 = (9 \times 9) \bmod 13 = 81 \bmod 13 =$ **3**
- $2^{50} \bmod 13 = (2^{10} \times 2^{40}) \bmod 13 = (10 \times 3) \bmod 13 = 30 \bmod 13 =$ **4**
- $2^{90} \bmod 13 = (2^{40} \times 2^{50}) \bmod 13 = (3 \times 4) \bmod 13 = 12 \bmod 13 =$ **12**

- $10^9 \bmod 13 = ?$

↓
↓ **곱셈 반복**
↓

- $10^2 \bmod 13 = (10 \times 10) \bmod 13 = 100 \bmod 13 =$ **9**
- $10^4 \bmod 13 = (10^2 \times 10^2) \bmod 13 = (9 \times 9) \bmod 13 = 81 \bmod 13 =$ **3**
- $10^8 \bmod 13 = (10^4 \times 10^4) \bmod 13 = (3 \times 3) \bmod 13 = 9 \bmod 13 =$ **9**
- $10^9 \bmod 13 = (10 \times 10^8) \bmod 13 = (10 \times 9) \bmod 13 = 90 \bmod 13 =$ **12**

- $2^{13} \bmod 77 = ?$

↓
↓ **곱셈 반복**
↓

- $2^3 \bmod 77 = 8 \bmod 77 =$ **8**
- $2^5 \bmod 77 = 32 \bmod 77 =$ **32**
- $2^{10} \bmod 77 = (2^5 \times 2^5) \bmod 77 = (32 \times 32) \bmod 77 = 1024 \bmod 77 =$ **23**
- $2^{13} \bmod 77 = (2^3 \times 2^{10}) \bmod 77 = (8 \times 23) \bmod 77 = 184 \bmod 77 =$ **30**

• 30^{37} mod 77 = ?

↓

↓ **곱셈 반복**

↓

• 30^{2} mod 77 = 900 mod 77 = **53**

• 30^{4} mod 77 = $(30^{2} \times 30^{2})$ mod 77 = (53×53) mod 77 = 2809 mod 77 = **37**

• 30^{6} mod 77 = $(30^{2} \times 30^{4})$ mod 77 = (53×37) mod 77 = 1961 mod 77 = **36**

• 30^{7} mod 77 = (30×30^{6}) mod 77 = (30×36) mod 77 = 1080 mod 77 = **2**

• 30^{8} mod 77 = $(30^{4} \times 30^{4})$ mod 77 = (37×37) mod 77 = 1369 mod 77 = **60**

• 30^{10} mod 77 = $(30^{2} \times 30^{8})$ mod 77 = (53×60) mod 77 = 3180 mod 77 = **23**

• 30^{20} mod 77 = $(30^{10} \times 30^{10})$ mod 77 = (23×23) mod 77 = 529 mod 77 = **67**

• 30^{30} mod 77 = $(30^{10} \times 30^{20})$ mod 77 = (23×67) mod 77 = 1541 mod 77 = **1**

• 30^{37} mod 77 = $(30^{7} \times 30^{30})$ mod 77 = (2×1) mod 77 = 2 mod 77 = **2**

// 몽고메리 알고리즘(Montgomery algorithm)

• 몽고메리 알고리즘은 모듈러 연산에서 **지수 연산을 빠르게 계산**할 수 있다.

• RSA 알고리즘은 모듈러 지수 연산에 기반하고 있다.(C = M^{e} mod n)

• RSA 알고리즘 구현에 몽고메리 알고리즘을 적용하면 지수 연산을 빠르게 계산할 수 있다.