● 오일러 파이 함수(Euler's phi function)

◈ **최대공약수와 최소공배수**

① 두 정수 12와 18의 공통된 약수는 다음과 같다.

• 12의 약수 = { −12, −6, −4, −3, −2, −1, 1, 2, 3, 4, 6, 12 }
18의 약수 = { −18, −6, −3, −2, −1, 1, 2, 3, 6, 18 }

• 12와 18의 공약수 = { −6, −3, −2, −1, 1, 2, 3, 6 }
• 최대공약수 **gcd(12, 18) = 6**이다. 가장 큰 공통된 약수이다.

---

② 두 정수 4와 6의 공통된 배수는 다음과 같다. [4, 6] = 12

{ …, −48, −36, −24, −12, 0, 12, 24, 36. 48, … }

• 두 정수 4와 6의 공통된 배수 중 가장 작은 양수는 12이다.
• 공배수 중에서 양수이면서 가장 작은 수 12를 **최소공배수**(lcm)라 한다.

---

gcd / lcm 표현 방법

• gcd(12, 18) = 6은 간단하게 (12, 18) = 6처럼 표현한다. → 소괄호 사용(중요함)
• lcm(4, 6) = 12는은 간단하게 [4, 6] = 12처럼 표현한다. → 대괄호 사용

[예제] 두 수 96과 60의 최대공약수와 최소공배수는?

2) 96, 60
2) 48, 30
3) 24, 15
8, 5 → 8과 5는 서로소가 된다.

• 최대공약수 gcd(96, 60) = 2 × 2 × 3 = **12**
• 최소공배수 lcm(96, 60) = 2 × 2 × 3 × 8 × 5 = 480

◈ **서로소(relatively prime / disjoint)**

① 최대공약수 gcd가 1인 두 정수를 서로소라 한다.
→ 다르게 정의하면, 서로소는 1과 −1 이외에는 공약수를 갖지 않는 두 정수이다.

② 두 정수의 쌍 (4, 9), (7, 13), (3, 4) 등은 각각 서로소 관계이다.

4의 약수 = { −4, −2, −1, 1, 2, 4 } 이고,
9의 약수 = { −9, −3, −1, 1, 3, 9 } 이다.

• 4와 9의 공약수는 1과 −1 뿐이다. 4와 9는 서로소이고, (4, 9) = 1이다.
• 정보보안을 공부하면서 "**(4, 9) = 1**"와 같은 표현을 많이 보게 될 것이다.

③ 서로소는 영어로 disjoint이다. 두 수가 별개라는 뜻이다.

◈ **오일러 파이 함수(Euler's phi function) − Φ, φ**

Φ(n)	• 오일러 Φ 함수는 **1**부터 **n**까지의 양의 정수 중에서 • 마지막 **n과 서로소 관계**에 있는 **수의 개수**를 나타내는 함수이다. • 그리스 대소문자 $\Phi(n)$ 또는 $\varphi(n)$으로 표기하고, 통상적으로 '**파이엔**'으로 읽는다.

예제 1

1, 2, 3, 4, 5에서 6과 서로소인 수는 몇 개인가?

[풀이] Φ(6) = ?

정수	공약수	설명
1	(1, 6) = 1	• 양의 정수에서 서로소는 1 이외에는 공약수를 갖지 않는 두 정수이다. • 6과 서로소 관계의 수는 1, 5이다. (2개) • 해서, $\Phi(n) = \Phi(6) = 2$
2	(2, 6) = 1, 2	
3	(3, 6) = 1, 3	
4	(4, 6) = 1, 2	
5	(5, 6) = 1	

예제 2

1, 2, 3, 4, 5, 6에서 7과 서로소인 수는 몇 개인가?

[풀이] Φ(7) = ?

정수	공약수	설명
1	(1, 7) = 1	• 양의 정수에서 서로소는 1 이외에는 공약수를 갖지 않는 두 정수이다. • 정수 1에서 6까지 모두 7과 서로소 관계이다. (6개) • 해서, $\Phi(n) = \Phi(7) = 6$
2	(2, 7) = 1	
3	(3, 7) = 1	
4	(4, 7) = 1	
5	(5, 7) = 1	
6	(6, 7) = 1	

• 양의 정수에서 서로소는 1 이외에는 공약수를 갖지 않는 두 정수이다.
• 따라서, 7과 서로소인 수는 1, 2, 3, 4, 5, 6이다. 즉, 6개이다.
• 소수 7은 자신인 7을 제외한 모든 수가 자신 7과 서로소인 관계에 있다.

예제 3

1, 2, 3, 4, 5, 6, 7, 8, 9, 10에서 11과 서로소인 수는 몇 개인가?

[풀이]----------

11의 약수 = {1, 11} → **11은 소수이다.**

∴ $\Phi(n) = \Phi(11) = 11 - 1 = 10$

• 소수인 경우, $\Phi(n)$ 값은 자신 n에서 1을 뺀 값이 된다.[$\Phi(n)$의 성질]

// 양의 정수 1부터 80까지의 오일러 파이 함수 값

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Φ(n)	**1**	**1**	**2**	**2**	**4**	**2**	**6**	**4**	**6**	**4**	**10**	**4**	**12**	**6**	**8**	**8**	**16**	**6**	**18**	**8**
n	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
Φ(n)	**12**	**10**	**22**	**8**	**20**	**12**	**18**	**12**	**28**	**8**	**30**	**16**	**20**	**16**	**24**	**12**	**36**	**18**	**24**	**16**
n	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
Φ(n)	**40**	**12**	**42**	**20**	**24**	**22**	**46**	**16**	**42**	**20**	**32**	**24**	**52**	**18**	**40**	**24**	**36**	**28**	**58**	**16**
n	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
Φ(n)	**60**	**30**	**36**	**32**	**48**	**20**	**66**	**32**	**44**	**24**	**70**	**24**	**72**	**36**	**40**	**36**	**60**	**24**	**78**	**32**

• 핵심 : n이 **소수**이면, $\Phi(n)$ 값은 자신에서 1을 뺀 값이다. 즉, **$\Phi(n) = n - 1$**

기출문제 분석

1. 오일러 함수 Φ( )를 이용해 정수 n=15에 대한 Φ(n)을 구한 값으로 옳은 것은? (단, 여기서 오일러 함수 Φ( )는 RSA 암호 알고리즘에 사용되는 함수이다) [2018년 서울 9급]

① 1
② 5
③ 8
④ 14

♤ **오일러 파이 함수(Euler's phi function) – Φ, φ**

• 오일러 Φ 함수는 1부터 n까지의 양의 정수 중에서
• 마지막 **n과 서로소 관계**에 있는 **수의 개수**를 나타내는 함수이다.
• 그리스 대소문자 $\Phi(n)$ 또는 $\varphi(n)$으로 표기하고, 통상적으로 '파이엔'으로 읽는다.

• 양의 정수에서 서로소는 1 이외에는 공약수를 갖지 않는 두 정수이다.

• 따라서, 15와 서로소인 수는 1, 2, 4, 7, 8, 11, 13, 14이다. 즉, 8개이다.

$\therefore \Phi(n) = \Phi(15) = 8$

정답 : ③