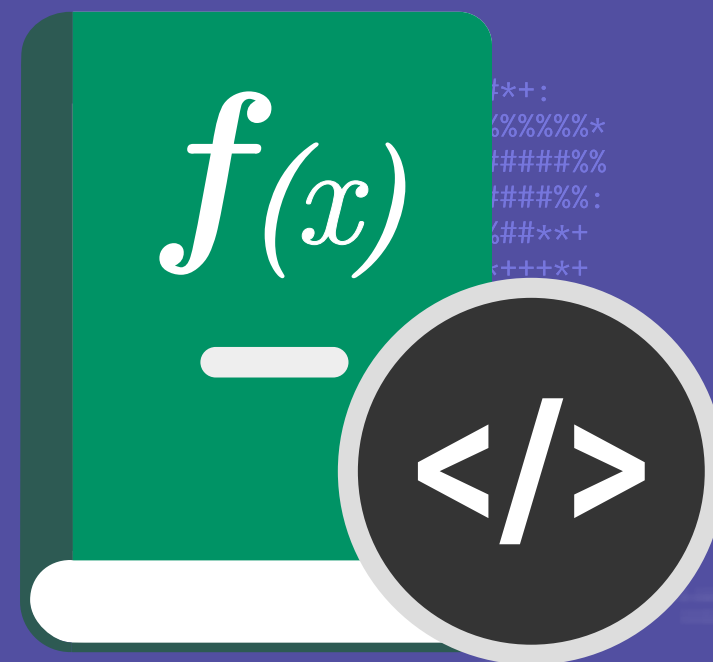


/\* elice \*/

# 수포자를 위한 프로그래밍 수학

컴퓨터 과학의 근간



조웅오 선생님

# 커리큘럼

1 ○

## 정수론: 소수 - 컴퓨터 과학의 근간


- 소수와 소인수분해의 특징을 이해
- 소인수 분해와 현대암호

2 ○

## 수열: 수학적 귀납법 - 알고리즘 기초 다지기

- 수열과 수학적 귀납법
- 분할 정복 알고리즘

# 커리큘럼

- 
- 3** 확률과 통계: 경우의 수와 확률 - 데이터 분석 첫걸음
- 확률과 통계의 기본 지식
  - 데이터 분석 기초
- 4** 선형대수: 벡터와 행렬 - 컴퓨터 비전의 세계로
- 벡터와 행렬의 연산
  - 컨볼루션 연산

# 수강 대상



프로그래밍을 이제 막 배워 **실제 문제에 적용**해 보고 싶은 분



프로그래밍과 관련된 **수학 지식**을 **기초**부터 배우고 싶은 분



**수학 지식**이 프로그래밍과 **어떤 관련**이 있는지 궁금한 분

# 수강 목표

프로그래밍에 담긴 수학 원리를 이해합니다.

컴퓨터 과학의 기본을 수학을 통해 익힙니다.

한층 고도의 프로그래밍 실력을 기릅니다.

# 목차

1. 모듈러 연산
2. 소수의 정의
3. 소수 판별법
4. 에라토스테네스의 체
5. 소수의 개수
6. 소인부 분해
7. 현대암호와 소인수 분해
8. 정리

# 개요

## 1장을 배우고 나면!

1. 소수의 특성을 알고 판별법을 알 수 있습니다.
2. 소인수분해의 방법과 특징에 대해 알 수 있습니다.
3. 소수 판별과 소인수분해를 컴퓨터 입장에서 구현할 수 있습니다.
4. 현대 암호에서 소인수 분해가 어떻게 쓰이는 지 이해합니다.

# 모듈러 연산

나눗셈의 나머지를 구하는 연산

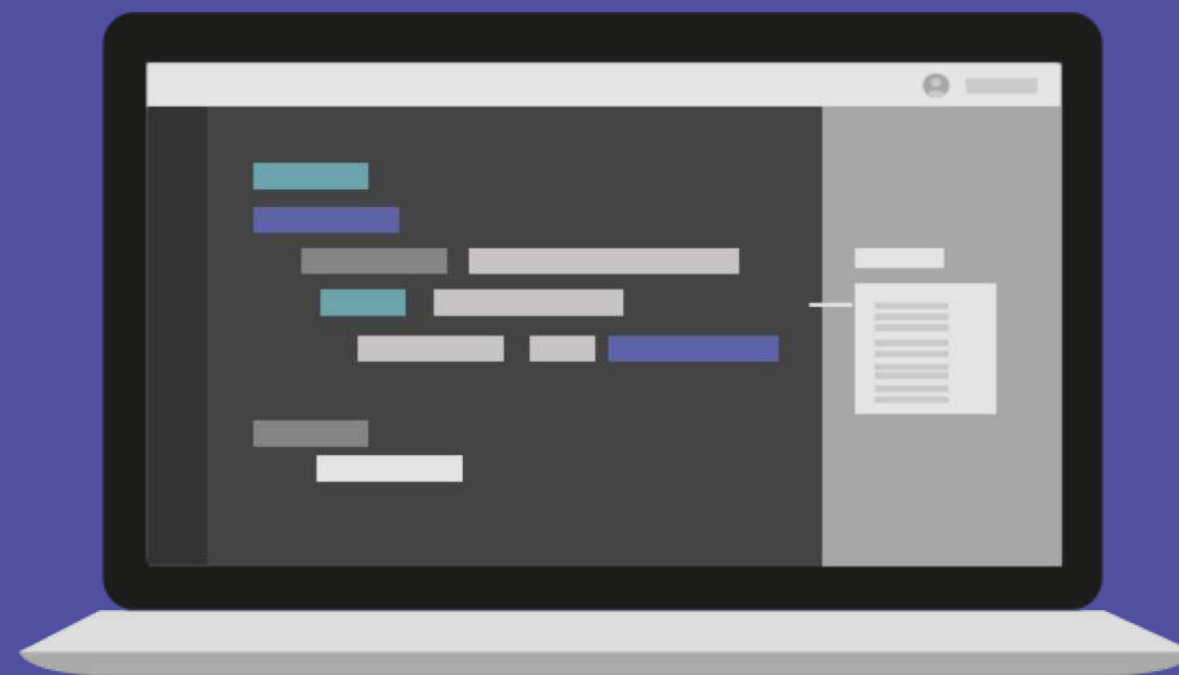
$A \bmod B = A$ 를  $B$ 로 나눈 나머지

코드로는?

**$A \% B$**



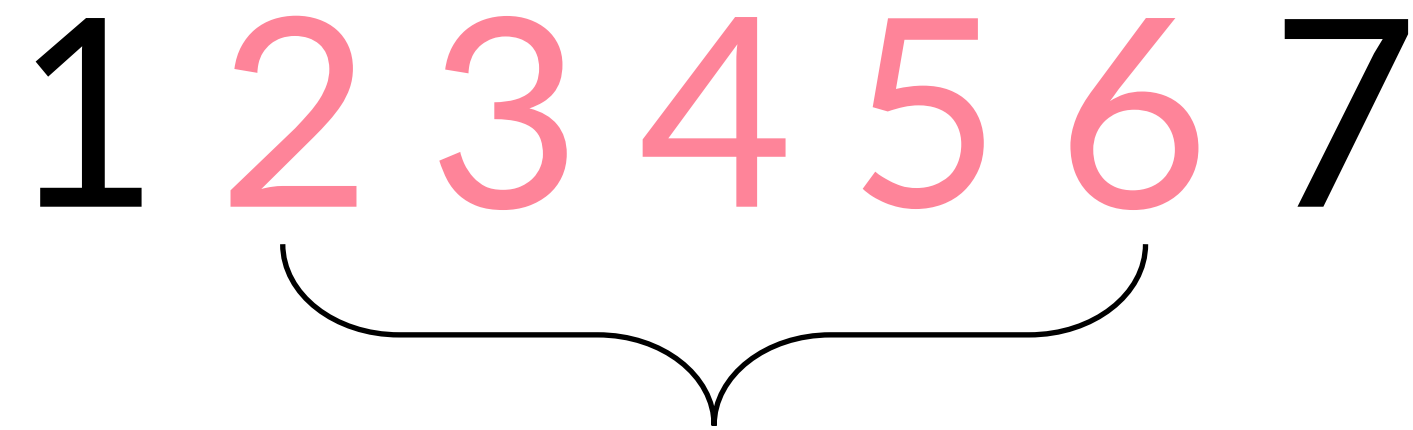
# [실습1] 나머지 값



# 소수의 정의

소수: 자신보다 작은 두개의 자연수를 곱하여  
만들 수 없는 1보다 큰 자연수

1 2 3 4 5 6 7



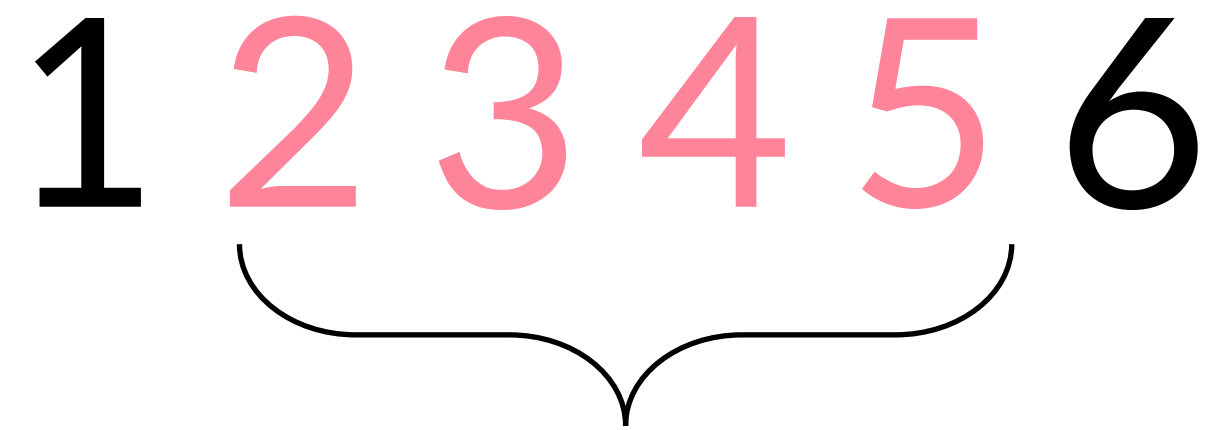
1과 7사이의 숫자를 곱해서 7을 만들 수 있을까?

=> NO! 따라서 7은 소수

# 소수의 정의

합성수: 1보다 큰 자연수 중 소수가 아닌 수

1 2 3 4 5 6



1과 6사이의 숫자를 곱해서 6을 만들 수 있을까?

=> YES! ( $2 \times 3 = 6$ ) 따라서 6은 합성수

# 소수의 정의

소수 : 2 3 5 7 11 13 17 ...

합성수 : 4 6 8 9 10 12 14 15 16 ...

★ 중요 ★ 1은 소수도 합성수도 아니다!

# 소수 판별법

## <사람의 경우>

나누어떨어질 것 같은 수부터 시도해본다.

Ex) “121? 11로 나누면 되겠는데?”

나누어떨어지는 수가 있으면 **합성수**

모든 수가 ‘안 됨’을 확인하면 **소수**로 인정

# 소수 판별법

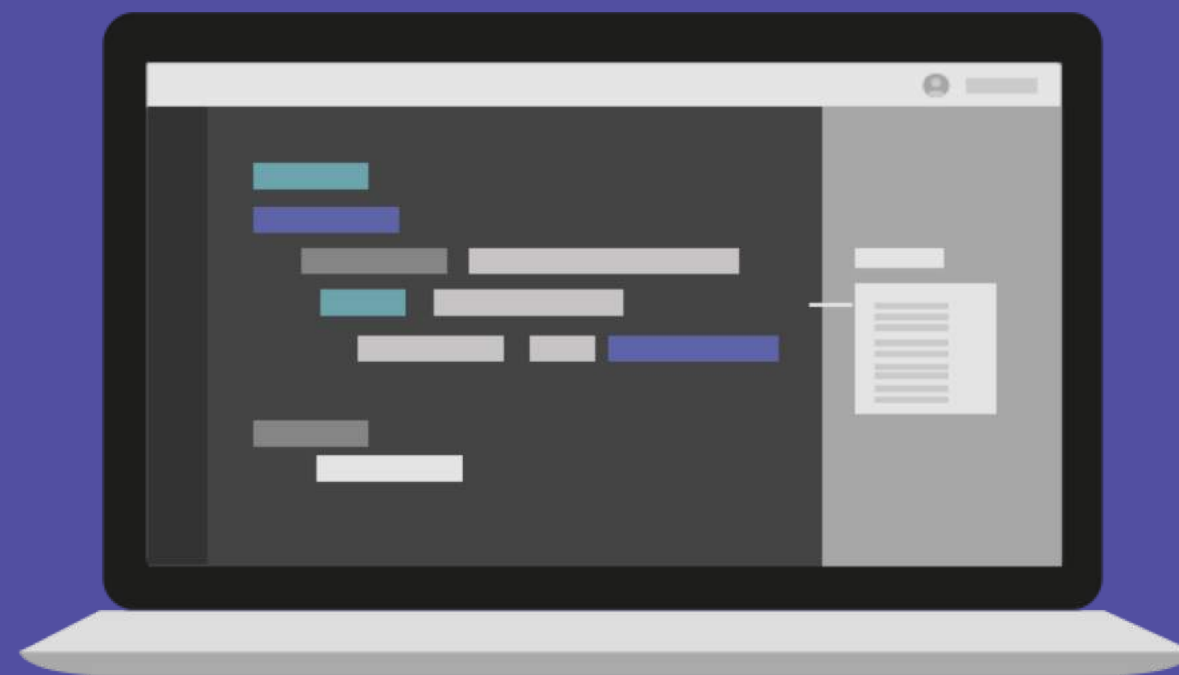
## <컴퓨터의 경우>

2부터  $n-1$ 까지 차근차근 시도해본다 (For Loop)

중간에 나누어 떨어지는 수가 있으면 **합성수**

$n-1$ 까지 통과했으면 **소수**

# [실습2] 소수 판별



# 에라토스테네스의 체

주어진 범위 내에 있는 소수를 찾는 빠른 방법





# 에라토스테네스의 체

범위 내의 숫자 리스트를 준비

	2	3	4	5	6	7	8	9	10	Prime numbers
11	12	13	14	15	16	17	18	19	20	
21	22	23	24	25	26	27	28	29	30	
31	32	33	34	35	36	37	38	39	40	
41	42	43	44	45	46	47	48	49	50	
51	52	53	54	55	56	57	58	59	60	
61	62	63	64	65	66	67	68	69	70	
71	72	73	74	75	76	77	78	79	80	
81	82	83	84	85	86	87	88	89	90	
91	92	93	94	95	96	97	98	99	100	
101	102	103	104	105	106	107	108	109	110	
111	112	113	114	115	116	117	118	119	120	

# 에라토스테네스의 체

## 2를 소수로 판정

	2	3	4	5	6	7	8	9	10	Prime numbers
11	12	13	14	15	16	17	18	19	20	2
21	22	23	24	25	26	27	28	29	30	
31	32	33	34	35	36	37	38	39	40	
41	42	43	44	45	46	47	48	49	50	
51	52	53	54	55	56	57	58	59	60	
61	62	63	64	65	66	67	68	69	70	
71	72	73	74	75	76	77	78	79	80	
81	82	83	84	85	86	87	88	89	90	
91	92	93	94	95	96	97	98	99	100	
101	102	103	104	105	106	107	108	109	110	
111	112	113	114	115	116	117	118	119	120	

# 에라토스테네스의 체

2의 배수를 모두 제거

	2	3	4	5	6	7	8	9	10	Prime numbers
11	12	13	14	15	16	17	18	19	20	2
21	22	23	24	25	26	27	28	29	30	
31	32	33	34	35	36	37	38	39	40	
41	42	43	44	45	46	47	48	49	50	
51	52	53	54	55	56	57	58	59	60	
61	62	63	64	65	66	67	68	69	70	
71	72	73	74	75	76	77	78	79	80	
81	82	83	84	85	86	87	88	89	90	
91	92	93	94	95	96	97	98	99	100	
101	102	103	104	105	106	107	108	109	110	
111	112	113	114	115	116	117	118	119	120	

# 에라토스테네스의 체

## 3을 소수로 판정

	2	3	4	5	6	7	8	9	10	Prime numbers
11	12	13	14	15	16	17	18	19	20	2 3
21	22	23	24	25	26	27	28	29	30	
31	32	33	34	35	36	37	38	39	40	
41	42	43	44	45	46	47	48	49	50	
51	52	53	54	55	56	57	58	59	60	
61	62	63	64	65	66	67	68	69	70	
71	72	73	74	75	76	77	78	79	80	
81	82	83	84	85	86	87	88	89	90	
91	92	93	94	95	96	97	98	99	100	
101	102	103	104	105	106	107	108	109	110	
111	112	113	114	115	116	117	118	119	120	



# 에라토스테네스의 체

3의 배수를 모두 제거

	2	3	4	5	6	7	8	9	10	Prime numbers
11	12	13	14	15	16	17	18	19	20	2 3
21	22	23	24	25	26	27	28	29	30	
31	32	33	34	35	36	37	38	39	40	
41	42	43	44	45	46	47	48	49	50	
51	52	53	54	55	56	57	58	59	60	
61	62	63	64	65	66	67	68	69	70	
71	72	73	74	75	76	77	78	79	80	
81	82	83	84	85	86	87	88	89	90	
91	92	93	94	95	96	97	98	99	100	
101	102	103	104	105	106	107	108	109	110	
111	112	113	114	115	116	117	118	119	120	

# 에라토스테네스의 체

5를 소수로 판정

	2	3	4	5	6	7	8	9	10	Prime numbers
11	12	13	14	15	16	17	18	19	20	2 3 5
21	22	23	24	25	26	27	28	29	30	
31	32	33	34	35	36	37	38	39	40	
41	42	43	44	45	46	47	48	49	50	
51	52	53	54	55	56	57	58	59	60	
61	62	63	64	65	66	67	68	69	70	
71	72	73	74	75	76	77	78	79	80	
81	82	83	84	85	86	87	88	89	90	
91	92	93	94	95	96	97	98	99	100	
101	102	103	104	105	106	107	108	109	110	
111	112	113	114	115	116	117	118	119	120	

# 에라토스테네스의 체

5의 배수를 모두 제거

	2	3	4	5	6	7	8	9	10	Prime numbers
11	12	13	14	15	16	17	18	19	20	2 3 5
21	22	23	24	25	26	27	28	29	30	
31	32	33	34	35	36	37	38	39	40	
41	42	43	44	45	46	47	48	49	50	
51	52	53	54	55	56	57	58	59	60	
61	62	63	64	65	66	67	68	69	70	
71	72	73	74	75	76	77	78	79	80	
81	82	83	84	85	86	87	88	89	90	
91	92	93	94	95	96	97	98	99	100	
101	102	103	104	105	106	107	108	109	110	
111	112	113	114	115	116	117	118	119	120	



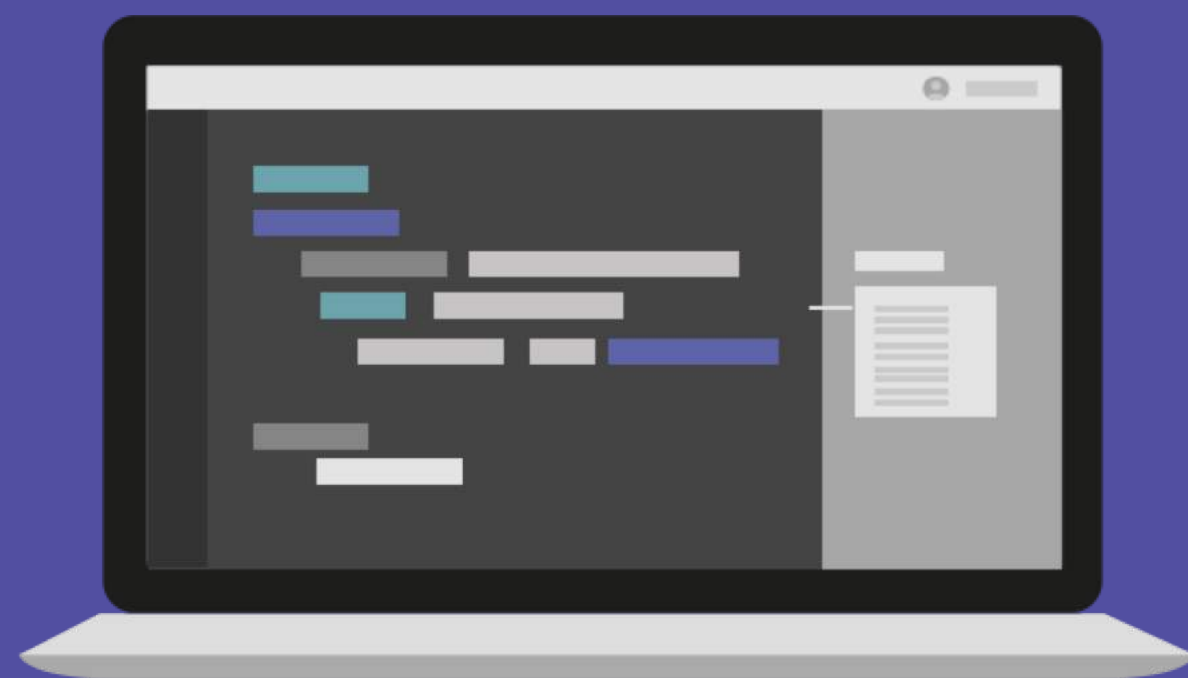
# 에라토스테네스의 체

위의 과정을 반복

	2	3	4	5	6	7	8	9	10	Prime numbers
11	12	13	14	15	16	17	18	19	20	2    3    5    7
21	22	23	24	25	26	27	28	29	30	11   13   17   19
31	32	33	34	35	36	37	38	39	40	23   29   31   37
41	42	43	44	45	46	47	48	49	50	41   43   47   53
51	52	53	54	55	56	57	58	59	60	59   61   67   71
61	62	63	64	65	66	67	68	69	70	73   79   83   89
71	72	73	74	75	76	77	78	79	80	97   101   103   107
81	82	83	84	85	86	87	88	89	90	109   113
91	92	93	94	95	96	97	98	99	100	
101	102	103	104	105	106	107	108	109	110	
111	112	113	114	115	116	117	118	119	120	

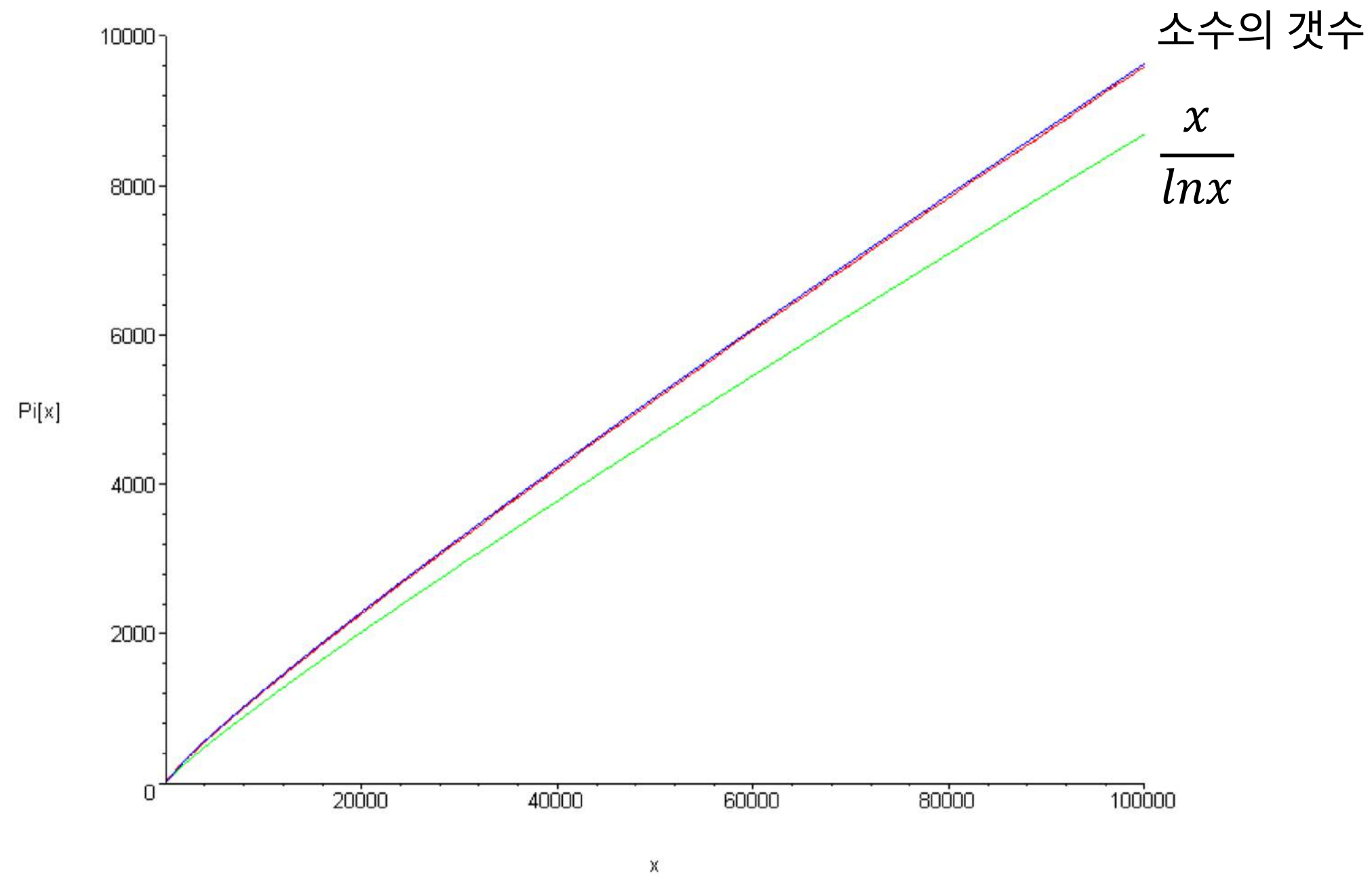


# [실습3] 에라토스테네스의 체

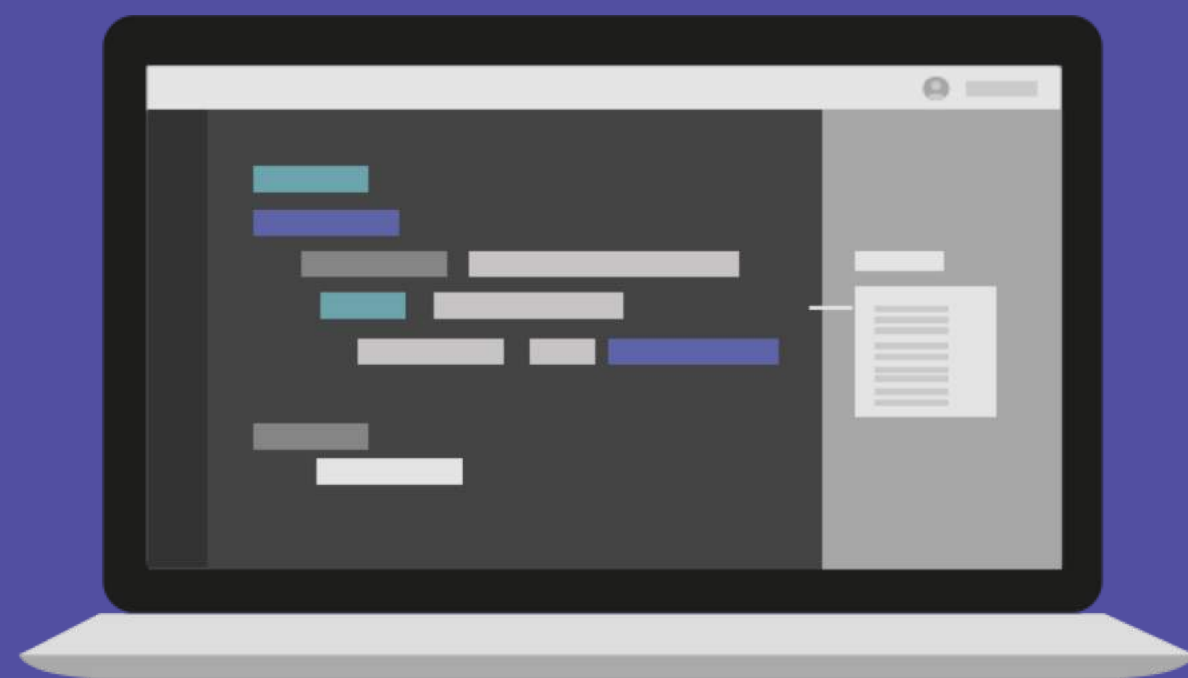


# 소수의 개수

소수의 개수는  $\frac{x}{\ln x}$  함수로 근사가 가능하다!



# [실습4] 소수의 개수



# 소인수 분해

## 소인수 분해란?

어떤 수를 소수들의 곱으로만 나타내는 것

# 소인수 분해

[예시]

$$9 = 3 \times 3$$

$$12 = 2 \times 2 \times 3$$

$$15 = 3 \times 5$$

$$60 = 2 \times 2 \times 3 \times 5$$

# 소인수 분해

소수는 **그 자체로** 이미 소인수 **분해** 완료된 수

$$2 = 2$$

$$3 = 3$$

$$7 = 7$$

$$11 = 11$$

# 소인수 분해

## <컴퓨터의 경우>

60을 소인수분해 해보자

# 소인수 분해

## <컴퓨터의 경우>

2로 나누어 본다.

$$60 = 2 \times 30$$

소인수 리스트

[ 2 ]



# 소인수 분해

## <컴퓨터의 경우>

다시 한 번 2로 나누어 본다.

$$30 = 2 \times 15$$

소인수 리스트

[ 2, 2 ]

# 소인수 분해

## <컴퓨터의 경우>

더 이상 2로 나뉘지 않으므로 3으로 나누어 본다.

$$15 = 3 \times 5$$

소인수 리스트

[ 2, 2, 3 ]

# 소인수 분해

## <컴퓨터의 경우>

남은 5가 소수이므로 소인수 분해 종료.

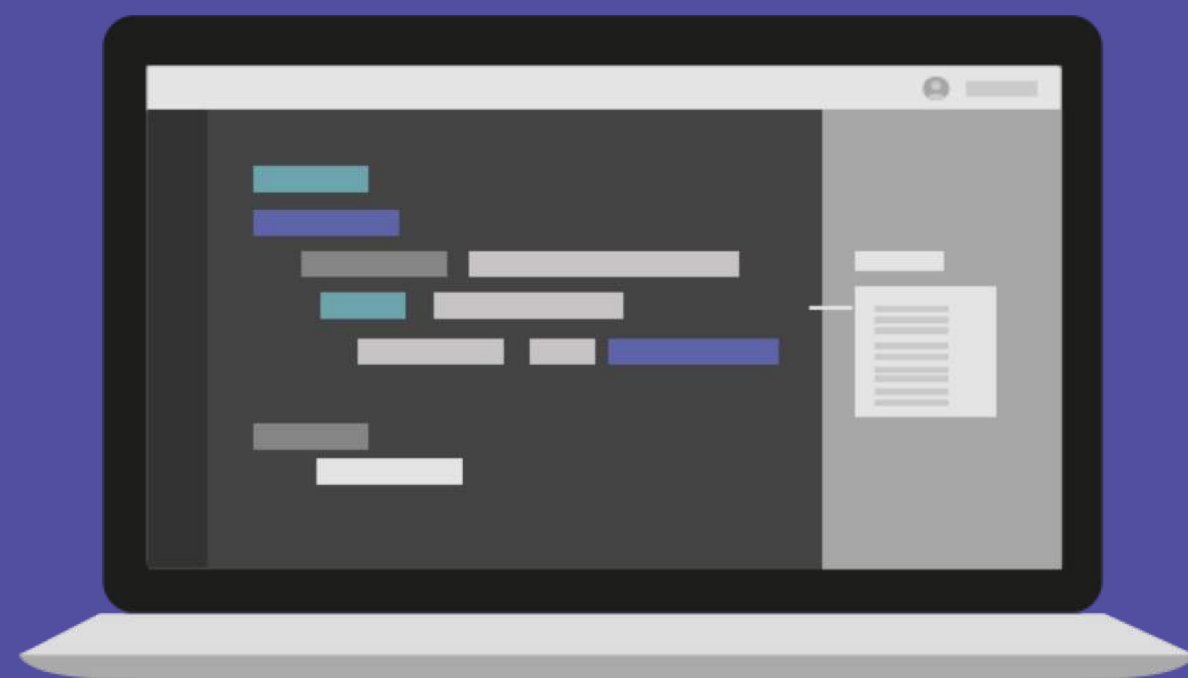
$$5 = \text{소수}$$

소인수 리스트

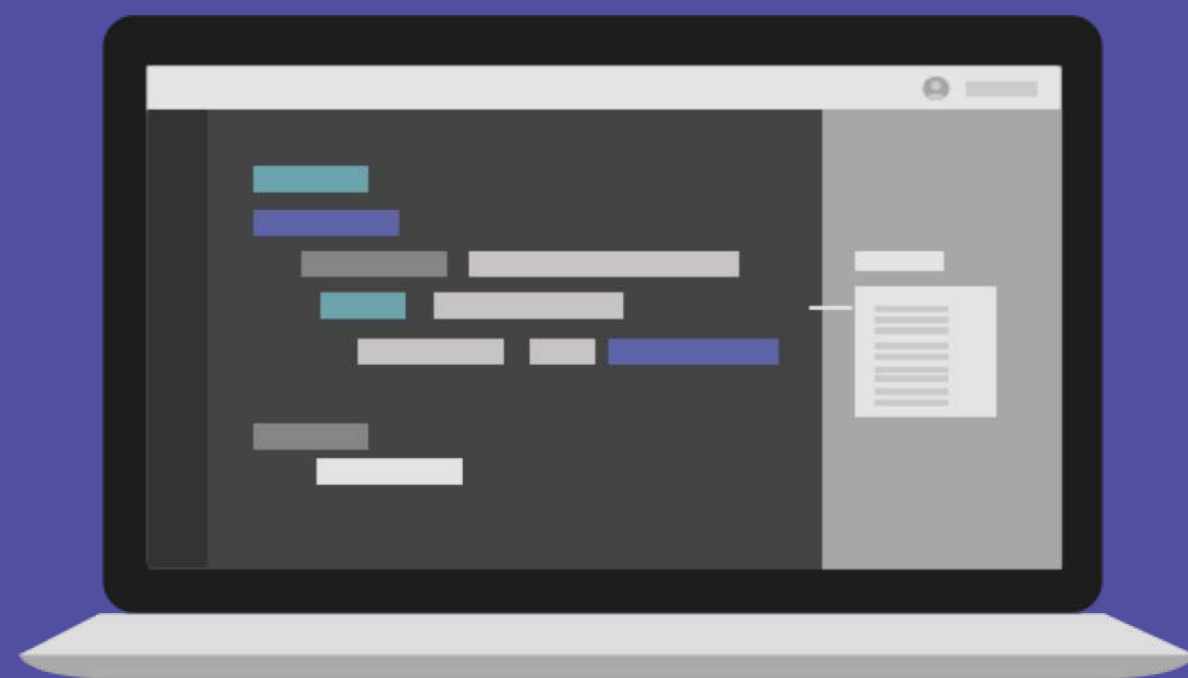
[ 2, 2, 3, 5 ]

$$\therefore 60 = 2 \times 2 \times 3 \times 5$$

# [실습5] 소인수



# [실습6] 소인수 분해



# 현대암호와 소인수 분해

소인수 분해는 어려운 문제!

Easy!



$$524287 \times 21474864 = 11258992021968$$



Very Hard...

# 비밀색 주고받기

도청중...

Eve

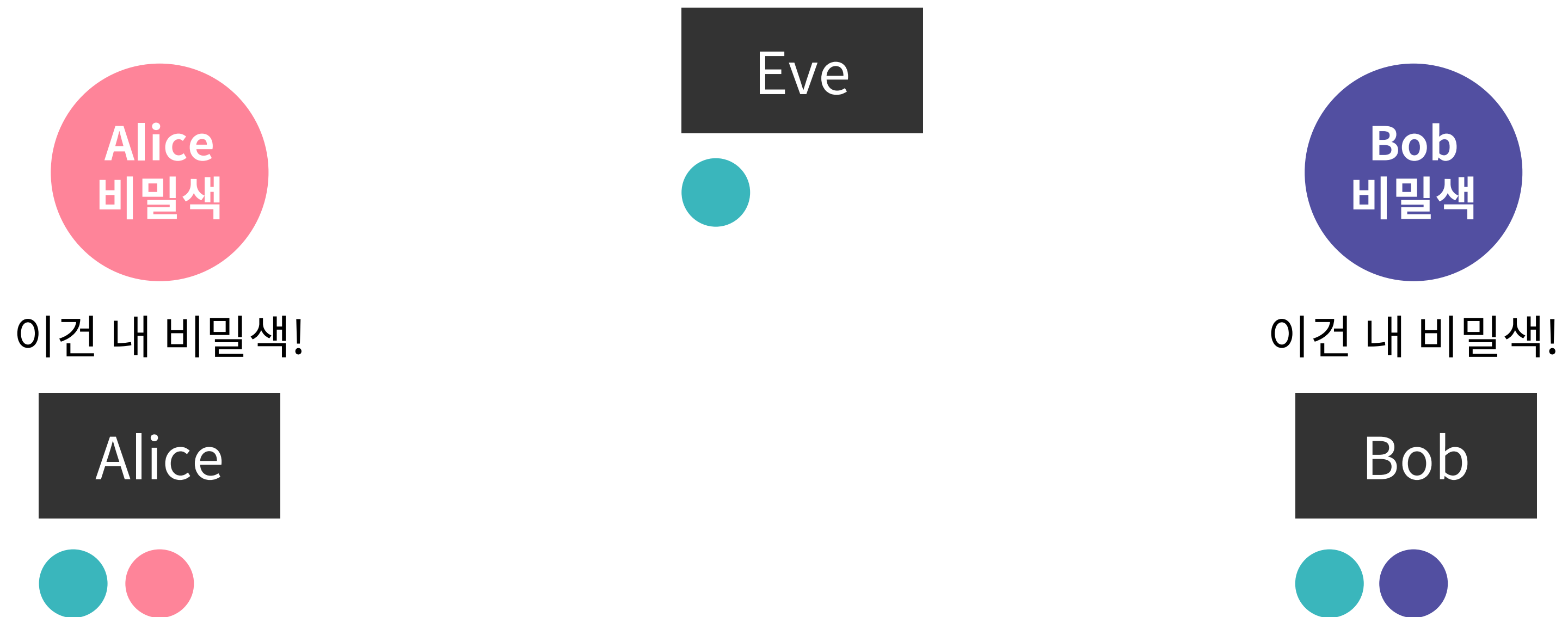
공개색

Alice

Bob

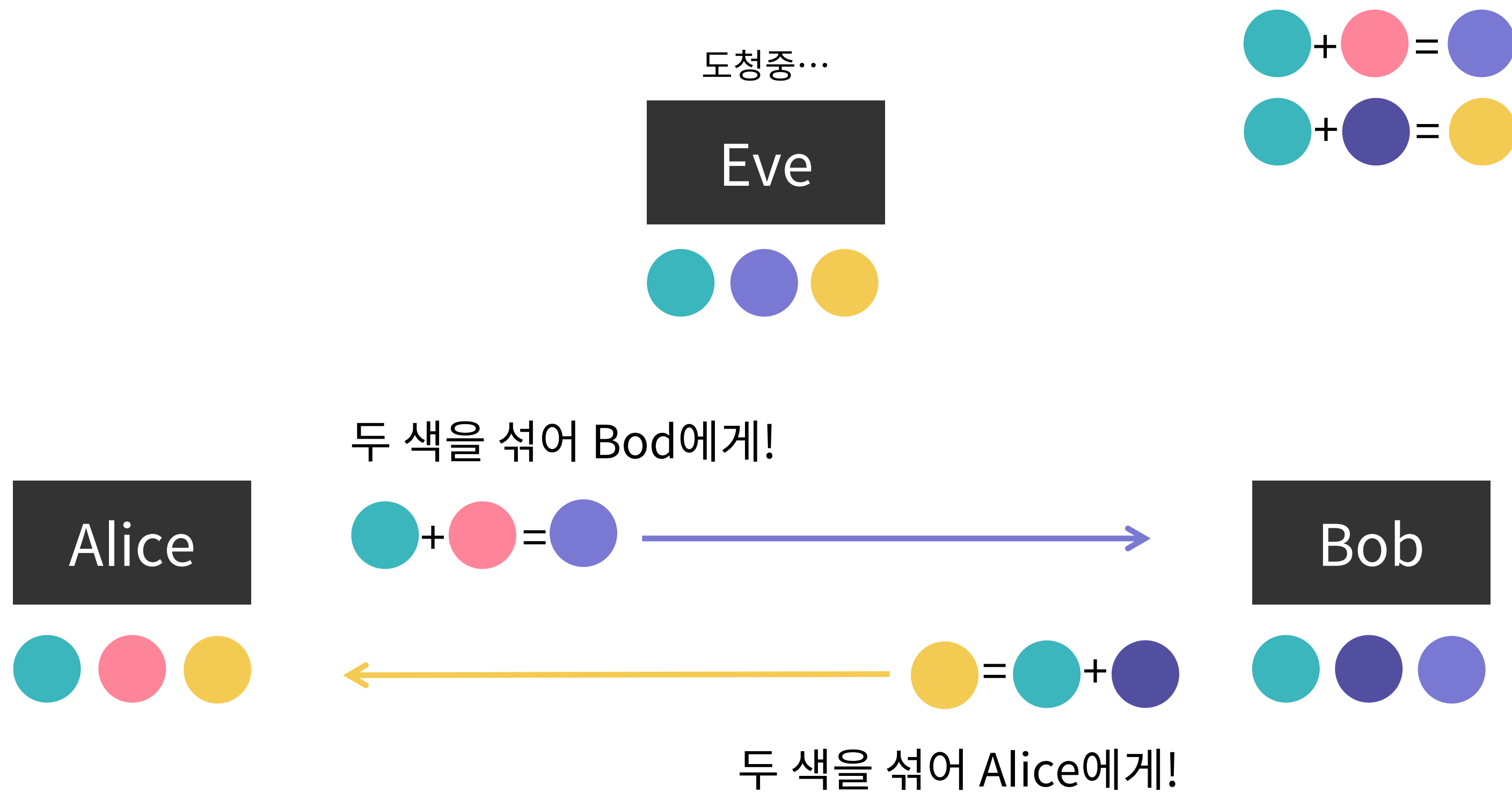
모두에게 공개합니다!

# 비밀색 주고받기





# 비밀색 주고받기

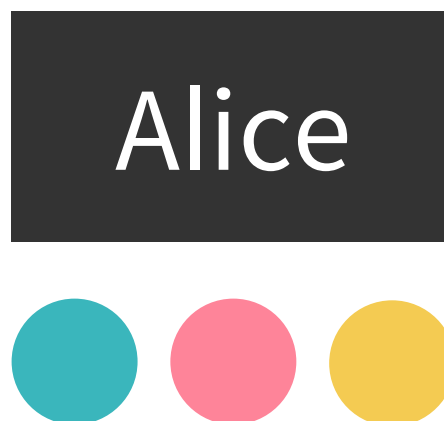


# 비밀색 주고받기

$$\begin{aligned} \text{Teal} + \text{Pink} &= \text{Purple} \\ \text{Teal} + \text{Purple} &= \text{Yellow} \end{aligned}$$

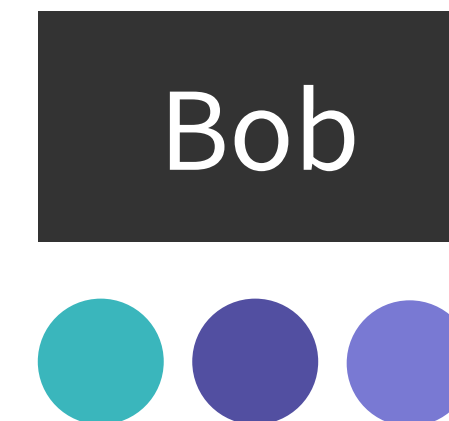


비밀색 완성!



$$\begin{aligned} \text{Pink} + \text{Yellow} &= \text{Pink} + (\text{Teal} + \text{Purple}) \\ &= (\text{Pink} + \text{Teal}) + \text{Purple} = \text{Purple} + \text{Purple} \end{aligned}$$

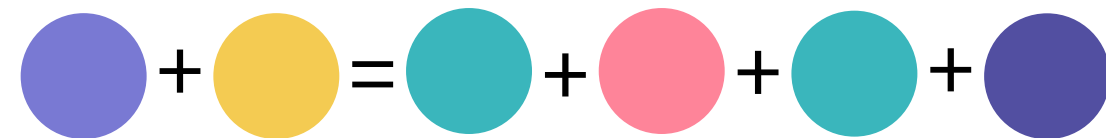
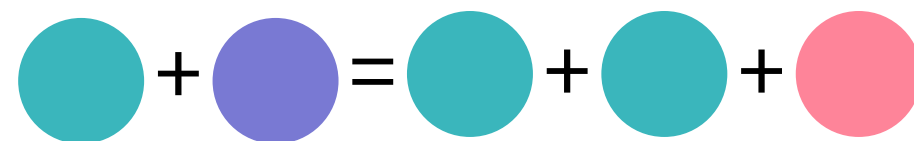
비밀색 완성!



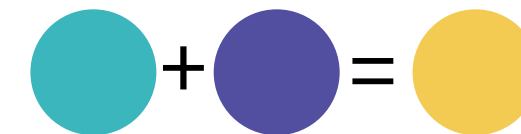
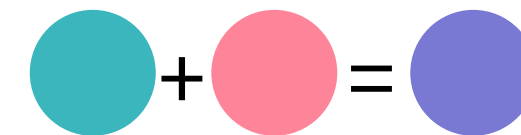
# 비밀색 주고받기

???

Eve



비밀색



# 이번 장에서는!

1. 모듈러 연산에 대해 배웁니다.
2. 소수의 특성과 판별법에 대해 배웁니다.
3. 소인수분해의 방법과 특징에 대해 배웁니다.
4. 특히 소인수분해는 현대 암호학에서  
매우 중요하다는 사실을 배웁니다.

/\* elice \*/

문의 및 연락처

[academy.elice.io](https://academy.elice.io)

[contact@elice.io](mailto:contact@elice.io)

[facebook.com/elice.io](https://facebook.com/elice.io)

[medium.com/elice](https://medium.com/elice)