

알고리즘 기초 세미나

02: 정수론

연세대학교 전우제^{kiwiyou}

2023.11.25.r2

합동식

- N 개의 정수 A_1, A_2, \dots, A_N 이 있을 때, $A_1 + A_2 + \dots + A_N$ 을 3으로 나눈 나머지를 구하자.
- A_i 가 최대 10^{18} 이고, N 이 최대 10^5
- 합이 너무 커요 $\pi\pi$
- A_i 를 직접 더하지 않고 나머지만을 구할 수 있을까?

합동식

- $(A + B) \bmod 3 = (A \bmod 3 + B \bmod 3) \bmod 3$
- 놀랍게도 이 성질은 +뿐만 아니라 $-$, \times 에도 적용되는데...
- 놀랍게도 이 성질은 3이 아닌 모든 양의 정수에도 적용되는데...
- 수식으로는 $A \bmod 3 = B \bmod 3 \Leftrightarrow A \equiv B \pmod{3}$
- 구현 시에는 모든 수, 모든 $+$, $-$, \times 시마다 나머지를 취하기
- $\bmod N$ 에서 모든 수의 범위는 0 이상 N 미만으로 줄어든다!

과제

- [9711 피보나치](#)
- [4375 1](#)
- [14928 큰 수 \(BIG\)](#)
- [27965 N결수](#)

소수 판정

- 1과 자기 자신만을 양의 약수로 가지는 2 이상의 정수
- 양의 정수 N 이 소수인지 판단하기
- 1부터 N 까지 전부 나누면 $\mathcal{O}(N)$
- 조금 더 빠르게 할 수 있을까?

소수 판정

- 42의 약수 1, 2, 3, 6, 7, 14, 21, 42
 - $1 \times 42 = 42$
 - $2 \times 21 = 42$
 - $3 \times 14 = 42$
 - $6 \times 7 = 42$
- **앞쪽** 절반만 본다면 $\mathcal{O}(\sqrt{N})$

소수 판정

```
1: function IS-PRIME( $N$ )  
2: if  $N = 1$  then  
3:     return false  
4: for  $i = 2$  upto floor (sqrt ( $N$ )) do  
5:     if  $N \equiv 0 \pmod{i}$  then  
6:         return false  
7: return true
```

- sqrt나 floor는 실수 오차를 동반하고, 느릴 수 있음

```
1: function IS-PRIME-2( $N$ )  
2: if  $N = 1$  then  
3:     return false  
4:  $i \leftarrow 2$   
5: while  $i^2 \leq N$  do  
6:     if  $N \equiv 0 \pmod{i}$  then  
7:         return false  
8:      $i \leftarrow i + 1$   
9: return true
```

- 정수 연산은 정확

소수 판정

- N 의 두 번째로 큰 소인수는 항상 \sqrt{N} 이하
- 작은 약수부터 찾아 나눌 때, 나누어지지 않을 때까지 나눠보기

```
1: function FACTORIZE( $N$ )  
2:  $i \leftarrow 2$   
3: while  $i \leq N$  do  
4:   while  $N \equiv 0 \pmod{i}$  do  
5:     print  $i$   
6:      $N \leftarrow N/i$   
7:    $i \leftarrow i + 1$   
8: if  $N \neq 1$  then  
9:   print  $N$ 
```


과제

- [24039 2021은 무엇이 특별할까?](#)
- [27065 2022년이 아름다웠던 이유](#)
- [28138 재밌는 나머지 연산](#)

에라토스테네스의 체

- N 이하의 소수를 모두 구해야 하는 경우 $\mathcal{O}(N\sqrt{N})$
- 중복 연산이 너무 많아요
- 약수를 세는 것보다 배수를 세는 것이 빠르다

에라토스테네스의 체

- 2 이상 N 이하의 각 정수가 소수인지를 배열에 저장
- 처음에는 모든 수가 소수라고 가정
- 가장 작은 소수를 하나 찾으면, 그 수의 배수는 소수가 아니라고 확정
- 시간복잡도는 $\mathcal{O}(N \log \log N)$

에라토스테네스의 체

```
1: function FIND-PRIMES( $N$ )
2: isPrime[2.. $N$ ]  $\leftarrow$  true
3: primeList  $\leftarrow$  {}
4: for  $i = 2$  upto  $N$  do
5:     if isPrime[ $i$ ] then
6:         add  $i$  to primeList
7:          $j \leftarrow 2 \times i$ 
8:         while  $j \leq N$  do
9:             isPrime[ $j$ ]  $\leftarrow$  false
10:             $j \leftarrow j + i$ 
11:return primeList
```

에라토스테네스의 체

- 체에 true, false 대신 그 수의 소인수를 넣는다면?

```
1: function FIND-PRIME-FACTORS( $N$ )
2: primeFactor[ $i$ ]  $\leftarrow i$ 
3: for  $i = 2$  upto  $N$  do
4:     if primeFactor[ $i$ ] =  $i$  then
5:          $j \leftarrow 2 \times i$ 
6:         while  $j \leq N$  do
7:             primeFactor[ $j$ ]  $\leftarrow i$ 
8:              $j \leftarrow j + i$ 
9: return primeFactor
```

과제

- [1929 소수 구하기](#)
- [2421 저금통](#)
- [16563 어려운 소인수분해](#)