

정수로 11장 소수의 성질

* 소수: 1과 자신만을 약수로 가지는 수

ex) 2, 3, 5, 7, 11, 13, ... (유한)
N-2번의 나눗셈.

(N) 이 소수이려면 $1, 2 \sim N-1$

$\Rightarrow 2 \sim \sqrt{N} < m \leq N-1$
 $m \mid N \Rightarrow N = k \cdot m$

$m > \sqrt{N} \Rightarrow m = N \Rightarrow k \mid N \quad k < \sqrt{N}$

$2 \leq a \leq \sqrt{N} \Rightarrow \sqrt{N-2}$

* 소수는 무한하다.

pt) 귀류법. 소수는 유한하다고 가정하자.

2, 3, 5, 7, 11, 13, ...

$p_1, p_2, p_3, \dots, p_k \Rightarrow p_k$ 는 마지막 소수

$A = p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_k + 1 > p_k$ 에라토스테네스의 체

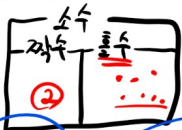
$A \equiv 1 \pmod{p_i} \Rightarrow A$ 도 소수
 $\exists q \mid A$ (q는 소수) $q \neq p_i$

$q \mid A$ (q는 소수) $q \neq p_i$

$q \mid p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$
 $(p_1 \cdot p_2 \cdot \dots \cdot p_k + 1) - (p_1 \cdot p_2 \cdot \dots \cdot p_k) = 1$
 $q \mid 1 \Rightarrow 1 \quad q = 1$

* 짝수인 소수?

2는 유일한 짝수인 소수



$1 \pmod{4}$: 5, 13, 17
 $3 \pmod{4}$: 3, 7, 11

* $3 \pmod{4}$ 인 소수는 무한하다.

pt) 유한하다. $\exists p_1, p_2, \dots, p_k, q_i$

$A = 4 \cdot p_1 \cdot p_2 \cdot \dots \cdot p_k + 3 > p_k$

A는 합성수.

$A = q_1 \cdot q_2 \cdot \dots \cdot q_s \quad 1/2 = \frac{1}{2} - \frac{1}{2} - \frac{1}{2}$

$q_1 \sim q_s \quad 1 \pmod{4}$
 $a \equiv 1 \pmod{4}, b \equiv 1 \pmod{4}$

$ab \equiv 1 \pmod{4}$

$\exists q_i \equiv 3 \pmod{4} \quad q_i \mid A$
 $p_1, p_2, p_3 \nmid A$

