정수론 11강 소수의 성질

* 소수 : 1과 자신만을 약수로 가지는 수

ex) 2, 3, 5, 7, 11, 13, ... ? (무한)

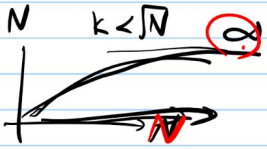
N이 소수이려면 1, 2 ~ N-1 (N-2번의 나눗셈.)

⇒ 2 ~ $\sqrt{N}$ < m ≤ N-1

$m \mid N \Rightarrow N = k \cdot m$

$m \geq \sqrt{N}$, $k \leq \sqrt{N}$ ⇒ $mk = N$ → $k \mid N$ $k < \sqrt{N}$

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



* 소수는 무한하다.

pf) 귀류법. 소수는 유한하다고 가정하자.

2, 3, 5, 7, 11, 13, ⋯

$p_1, p_2, p_3, \cdots, p_k$ → A ⇒ p_k는 마지막 소수

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

$A \equiv 1 \pmod{p_i}$ ⇒ A도 소수

$\sqrt{A}$ 2, ⋯ $\sqrt{A}$ 2|A

3 6 소수 합성수 ④|A

$\exists q \mid A$ (q는 소수) $q = p_i$

$q \mid p_1 \cdots p_k + 1$ $q \mid p_1 \cdots p_k$

$(p_1 \cdots p_k + 1) - (p_1 \cdots p_k) = 1$

$q \mid 1 \rightarrow 1$ $q = 1$

* 짝수인 소수?

2는 유일한 짝수인 소수

$1 \pmod 4$: 5, 13, 17

$3 \pmod 4$: 3, 7, 11

* $3 \pmod 4$인 소수는 무한하다.

pf) 유한하다. $3, p_1, p_2, \cdots, p_k$ q_i

$A = 4 \cdot p_1 \cdots p_k + 3 > p_k$

A는 합성수.

$A = q_1 q_2 \cdots q_s$ /2 = 2 = 2 = 3

$q_1 \sim q_s$ $1 \pmod 4$

$ab \equiv 1 \pmod 4$, $b \equiv 1 \pmod 4$

$ab \equiv 1 \pmod 4$

$\exists q_i \equiv 3 \pmod 4$ $q_n \mid A$

$p_1, p_2, p_3 \nmid A$