#09-1. 귀류법

나정휘
https://justiceHui.github.io/

귀류법

귀류법

- 명제의 결론이 부정이라고 가정했을 때 모순이 발생함을 보여 원래 명제가 참임을 증명

- 모든 n에 대해 P(n)이 참임을 증명
  - P(n)이 거짓이 되는 n이 있다고 가정
  - P(n)이 거짓이 되는 n이 있으면 모순이 일어나는 것을 보임
  - P(n)이 거짓이 되는 n이 없으므로 모든 n에 대해 P(n)은 참

귀류법

$n > 1$인 정수의 소인수분해가 유일함을 증명

- 소인수분해의 존재성은 강한 수학적 귀납법을 이용해 증명할 수 있음 (5차시)
- 유일하게 존재함을 증명해야 함

- (Euclid Lemma) $a \mid bc$ 이고 $\gcd(a, b) = 1$이면 $a \mid c$임

- n의 서로 다른 소인수분해 $n = p_1p_2 \ldots p_s = q_1q_2 \ldots q_t$가 존재한다고 가정하자.
  - 일반성을 잃지 않고 $s \geq t$인 경우만 생각
  - $q_1 \mid n = p_1p_2p_3 \ldots p_s$ 인데 p_1과 q_1은 모두 소수이므로 $q_1 \mid p_1$이거나 $q_1 \mid p_2p_3 \ldots p_s$
  - 동일한 논리로 $q_1 \mid p_1$ or $q_1 \mid p_2$ or $q_1 \mid p_3$ or … or $q_1 \mid p_s$
  - 따라서 $q_1 = p_i$인 i가 존재하고, $q_1 = p_1$이 되도록 p를 재배열하자.

  - 비슷하게 $q_2 = p_2$, $q_3 = p_3$, … 이 되도록 p를 재배열할 수 있음
  - 만약 $s > t$ 이면 $p_{t+1}p_{t+2} \ldots p_s \neq 1$이므로 $s = t$가 되어야 함
  - 모든 $1 \leq i \leq t$에 대해 $p_i = q_i$이므로 소인수분해는 유일하게 존재함

- 산술의 기본 정리(Fundamental Theorem of Arithmetic)
  - 1보다 큰 모든 정수는 순서가 바뀐 것을 제외하고 소수들의 곱으로 유일하게 표현할 수 있음

귀류법

√3이 유리수가 아님을 증명

- √3이 유리수라고 가정하자.
- √3은 $n,m > 0$이고 $\gcd(n, m) = 1$인 두 정수 n, m을 이용해 $\sqrt{3} = m/n$으로 나타낼 수 있음
- 양변을 제곱하고 이항하면 $3n^2 = m^2 > 1$

- $m > 1$이므로 m을 소수들의 곱 $m = p_1 p_2 \ldots p_k$으로 나타낼 수 있음
- $3 \mid m^2$ 이므로 $3 \mid p_1^2 p_2^2 \ldots p_k^2$, 유클리드 보조 정리에 의해 $3 = p_1$이 되도록 p를 재배열할 수 있음

- $3n^2 = 3^2 p_2^2 p_3^2 \ldots p_k^2$ 이므로 $n^2 = 3 p_2^2 p_3^2 \ldots p_k^2$
- $3 \mid n^2$ 이므로 유클리드 보조 정리에 의해 $3 \mid n$
- n과 m 모두 3의 배수이므로 $\gcd(n, m) \geq 3$

- $\gcd(n, m) = 1$이라고 가정했는데 $\gcd(n, m) \geq 3$ 이므로 모순 발생
- 따라서 √3은 유리수가 아님

귀류법

소수는 무한히 많음을 증명

- 소수가 유한하다고 가정하고, 그 소수를 $p_1 \le p_2 \le \cdots \le p_k$라고 하자.
- $n = p_1 p_2 \cdots p_k + 1 > 1$ 을 생각해 보자.
- FTA에 의해 $n = q_1 q_2 \ldots q_j$ 로 나타낼 수 있음 (모든 $1 \le i \le j$ 에 대해 $q_i \in \{p_1, p_2, \ldots, p_k\}$)

- n과 $p_1 p_2 \ldots p_k$ 모두 q_1의 약수이므로 $n - p_1 p_2 \ldots p_k$도 q_1의 약수임
- 따라서 $(n - p_1 p_2 \ldots p_k) / q_1 = 1 / q_1$이 정수

- $q_1 \neq 1$이므로 $1 / q_1$이 정수라는 것에 모순 발생

귀류법

4n+3 꼴의 소수는 무한히 많음을 증명

- Note: 4n+1 꼴의 정수들의 곱은 4n+1 꼴

- 4n+3 ($n \geq 1$) 꼴의 소수가 유한하다고 가정하고, 그 수들을 $7 = p_1 \leq p_2 \leq \ldots \leq p_k$라고 하자.
- $Q = p_1 p_2 \ldots p_k$, $M = 4Q+3$이라고 정의하면 $M > p_k$ 이므로 M은 소수가 아님

- FTA에 의해 M은 3 이상의 홀수 소수들의 곱 $q_1 q_2 \ldots q_s$ 로 나타낼 수 있음
- 4n+1 들의 곱은 항상 4n+1 꼴이므로 $q_i = 4n+3$ 꼴인 q_i가 존재하고, 따라서 $q_i = p_j$인 j가 존재함

- 정의에 의해 p_j가 M, Q를 나누므로 $p_j \mid 3 = M - Q$ 임을 알 수 있음
- 하지만 $p_j \geq 7$이므로 모순 발생

질문?