소수의 무한성과 분포

이상준 교수
(덕성여대 수학과)
2015년 2학기

교재 : 친절한 수론 길라잡이 (4판)
조셉 실버만 지음, 김병찬,김지영,이종규,박부성 옮김

강의 슬라이드: 이상준, 오연주(15학번)

무한 소수 정리

- **무한 소수 정리**: 소수는 무한히 많다.
- **증명: (귀류법)** 소수가 유한개 있다고 가정하고, 모든 소수가 $p_1, p_2, \cdots, p_n$ 이라고 하자.
  - $p = p_1 p_2 \cdots p_n + 1$ 이라고 하자.
  - $p \neq p_i$ $(i=1,2,\cdots,n)$이기 때문에 p는 소수가 아니다.
  - 산술의 기본정리 (소인수분해정리)에 의해
    p는 소수의 곱으로 표현되므로 어떤 소수 p_i 로 나누어진다.
  - $p = q \cdot p_i + 1$ 이므로 모순!!

존재성 vs 목록

- **중요:** 앞의 증명은 존재성을 알려줄 뿐만 아니라 실제로 “무한한 소수의 목록”을 준다.
  - 2
  - 2+1 = 3
  - 2·3+1 = 7
  - 2·3·7+1 = 43
  - 2·3·7·43+1 = 1807 = 13·139
  - 2·3·7·43·13+1 = 23479 = 53·443
    ⋮

새로운 질문

- **사실1:** 2를 제외한 모든 소수는 홀수이다.
- **따름정리:** 홀수인 소수는 무한히 많다.
- **사실2:** 홀수는 1 (mod 4) 이거나 3 (mod 4) 이다.
- **질문:** 1 (mod 4) 인 소수는 무한히 많은가?
  3 (mod 4) 인 소수는 무한히 많은가?

관찰

- **관찰:** 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, ...
- **추측:** 두 집합 모두 충분히 많은 소수가 있어 보이지만, 눈에 띄는 규칙은 없어보인다.
- 더 긴 소수의 목록을 보자.

$p \equiv 1 \pmod 4$	$5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109,$ $113, 137, 149, 157, 173, 181, 193, 197, \ldots$
$p \equiv 3 \pmod 4$	$3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, 103,$ $107, 127, 131, 139, 151, 163, 167, 179, \ldots$

출처: 조셉 실버만, 친절한 수론 길라잡이

- **정리 [3 (mod 4) 소수 정리]:** 3 (mod 4)꼴인 소수는 무한히 많다.
- **증명: (귀류법)**
  - 3 (mod 4)인 소수가 유한개만 있다고 가정하고, 3, p_1, p_2, …, p_r 라 하자.
  - $A = 4p_1p_2\cdots p_r + 3$이라 하자. (A를 만드는 곱에 3을 포함시키지 않았음에 주의하라!)
  - A는 3 (mod 4)이면서 3, p_1, p_2, …, p_r 가 아니므로 합성수이다.
  - 산술의 기본정리에 의해 A를 소수의 곱 $A = q_1q_2\cdots q_s$ 으로 나타낼 수 있다.
  - **주장:** q_i 중 적어도 하나는 3 (mod 4) 이다. (증명은 다음 페이지에)
  - q_i 는 3, p_1, p_2, …, p_r 중 하나이다.
    - q_i=3 이라면 $3 \nmid A$ 이다.
    - $q_i=p_j$ 라면 $A = 4p_1p_2\cdots p_r + 3$ 이므로 $q_i \nmid A$ 이다.
  - 다른 한편으로는 $A = q_1q_2\cdots q_s$ 이므로 $q_i \mid A$ 이다. **모순!**

- **주장:** q_i 중 적어도 하나는 3 (mod 4) 이다.
- **주장의 증명: (귀류법)**
  - 아니라고 가정하자. 즉, i=1,⋯,s에 대해, $q_i \equiv 1 \pmod 4$ 라 하자.
  - 1 (mod 4) 인 두 수를 곱하면 1(mod 4)이다.
    왜냐하면 (4k+1)(4m+1)=4(4km+k+m)+1 이기 때문이다.
  - 그러므로 $A \equiv 1 \pmod 4$ 이다. **모순!**

$1 \pmod 4$에 대한 질문

- **질문1:** “3 (mod 4)인 소수가 무한히 많이 있다”는 앞의 증명을
  “1 (mod 4)인 소수가 무한히 많이 있다”를 보이기 위해 사용할 수 있을까?
- **질문2:** 사용할 수 없다면 무엇 때문인가?

- **정리:** 1 (mod 4)인 소수가 무한히 많이 있다.
- **증명: 21장**에서!

mod 5 에 대해서

- 앞에서 소수의 분류를 mod 4에 대해서만 해야 할 이유는 없다.
- **질문**: mod 5에 대해서는 어떤 결과를 얻을 수 있는가?
- **사실**: 5 이외의 모든 소수는 법 5에 대해 1,2,3,4 중 하나와 합동이어야 한다.
- **관찰**: 각 집합에 대한 소수의 목록은 다음과 같다.

$p \equiv 1 \pmod 5$	$11, 31, 41, 61, 71, 101, 131, 151, 181, 191, 211, 241$
$p \equiv 2 \pmod 5$	$2, 7, 17, 37, 47, 67, 97, 107, 127, 137, 157, 167, 197$
$p \equiv 3 \pmod 5$	$3, 13, 23, 43, 53, 73, 83, 103, 113, 163, 173, 193, 223$
$p \equiv 4 \pmod 5$	$19, 29, 59, 79, 89, 109, 139, 149, 179, 199, 229, 239$

출처: 조셉 실버만, 친절한 수론 길라잡이

- **추측**: 모든 목록은 무한히 많은 소수를 포함할 것이다.

mod m 에 대해서

- **질문**: 법 m과 하나의 수 a를 고정했을 때, a (mod m)꼴인 소수가 무한히 많을 것인가?
- **답**: 그렇지 않다.
- **사실**: 만일 gcd(a,m)≠1이라면, a (mod m)꼴인 소수가 많아야 하나 존재한다.
- **증명**: 소수 p ≡ a (mod m) 라 하자.
  - p ≡ a+km = gcd(a,m)·n (k,n: 정수)
  - 그러므로 a (mod m)인 소수는 많아야 하나 존재한다.
    (gcd(a,m)이 소수이고 n=1 일 때)

디리클레의 등차수열 속 소수 정리

- **정리 (Dirichlet, 디리클레):** a와 m은 gcd(a,m)=1 인 자연수라고 하자.
  a (mod m)꼴인 소수는 무한히 많이 있다.
- **증명:** 어려우므로 생략! (복소수의 미적분이 필요)
- **주목:**
  1. 이미 3 (mod 4)인 경우의 디리클레 정리를 증명하였다.
  2. 5 (mod 6)인 경우는 연습문제 12.2를 통해 물어볼 것이다.
  3. 1 (mod 4)인 경우는 **21장**에서 다룰 예정이다.