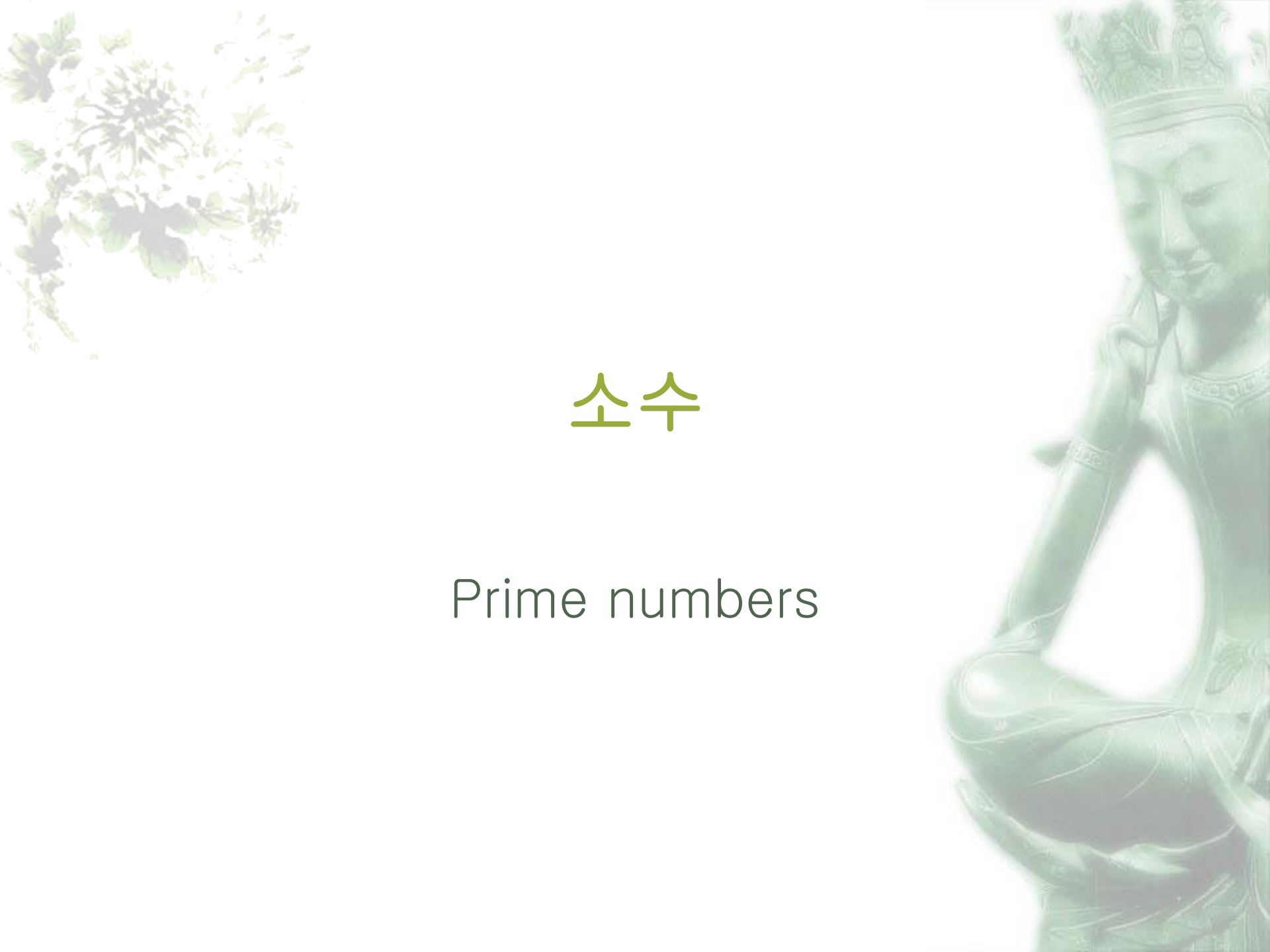


소수

Prime numbers

소수양식

- 소수 : 1과 자신 이외에는 약수가 없는 자연수
- $p \mid m \Leftrightarrow m = pk$ k는 자연수

- 소수양식1 : 소수 p가 곱 mn을 나누면 p는 두 수 m, n중 적어도 하나를 나눈다.
- 소수양식2 : 모든 자연수는 소수이거나 소수들의 곱으로 표현된다. 소수들의 곱의 순서를 무시하면 유일한 방법으로 표현 된다 (소인수분해 : 산술의 기본정리)

- 소수양식3 : 무한히 많은 소수가 존재한다.
- 유클리드의 증명법(귀류법): 어떤 명제를 증명할 때 그 부정의 명제의 모순을 보여주어, 결론을 긍정할 수밖에 없음을 보임 :
- 아리스토텔레스(당시)의 논리에서 배중율(진 아니면 위)을 이용함. 즉 소수가 유한개 뿐이면 그 소수를 모두 곱한 후 1을 더한 수가 소수이면 유한개+1 개가 되어 소수를 계속 만들 수 있으므로 모순이고 그 수가 합성수라도 모순이 된다.

소수의 무한성

간략한 증명

- $p_1, p_2, \cdots, p_n$ 이 소수의 수열일 때

  $P_n = (p_1 \times p_2 \cdots \times p_n) + 1$ 이라 하자.

  만약 P_n이 소수라면 n 보다 더 많은 소수가 존재.

  만약 P_n이 합성수라면 P_n은 $p_1, p_2, \cdots, p_n$과 다른(더 큰) 소수로 나누어 져야 한다.
  어느 경우든 n 보다 더 많은 소수가 존재한다.

소수의 밀도

$$P_n = (p_1 \times p_2 \cdots \times p_n) + 1$$

- $P_1 = 2 + 1 = 3$
- $P_2 = (2 \times 3) + 1 = 7$
- $P_3 = (2 \times 3 \times 5) + 1 = 31$
- $P_4 = (2 \times 3 \times 5 \times 7) + 1 = 211$
- $P_5 = (2 \times 3 \times 5 \times 7 \times 11) + 1 = 2,311$
- $P_6 = 59 \times 509$
- $P_7 = 19 \times 97 \times 227$
- $P_8 = 347 \times 27,953$

- 소수의 밀도 $\frac{\pi(N)}{N}$? 단순한 양식 없음. 무질서하지도 않음
  - 예) 1,000까지 소수밀도는 0.168
    1,000,000 까지 소수밀도0.078
    100,000,000 까지 소수밀도는 0.058

- 소수양식4 : (Chebyshef 1850년) :
  - 임의의 자연수와 그 2배 사이에 소수가 있음을 증명.

소수정리

- 소수양식5 : (J. Hadamard & C. Poussin 1896년) 소수정리 발견 :

  자연수 N에 비례하여 소수밀도 $\frac{\pi(N)}{N}$는 $\frac{1}{\ln N}$에 수렴한다. 단, $\ln N$은 자연로그를 나타낸다.

- 시계산술 (유한산술, 법 산술) modular arithmetic: Gauss(1777-1855) 의 수론 연구(1801년 출간)에 수록.
- $a \equiv b(\mathrm{mod}\ p) \Leftrightarrow a - b = kp,\ \ k$는 자연수
- $2+3 \equiv 5(\mathrm{mod}12),\ \ 7+6 \equiv 1(\mathrm{mod}12)$
  $7/5 \equiv 11(\mathrm{mod}12),\ \ 5/6 \equiv ?(\mathrm{mod}12)$
- 법 p가 소수인 경우에는 나눗셈이 가능 (수학적 구조가 체(field)인 경우)

소수양식6 : 페르마의 작은 정리

- Fermat (1601-1665) 프랑스의 지방의회 소속 변호사, 아마추어 수학자. 수학자에게 보낸 편지(1640)내용
- a가 임의의 자연수이고 p는 a를 나눌 수 없는 소수이면 p는 반드시 $a^{p-1}-1$를 나눈다.

  예) $a=8,\ p=5$이면 $8^{5-1}-1=4096-1=4095$는 5의 배수이다.
- 19는 $145^{18}-1$을 나눈다.

$$145^{18}-1=802830827198685151406498569488525390624$$

작은 정리

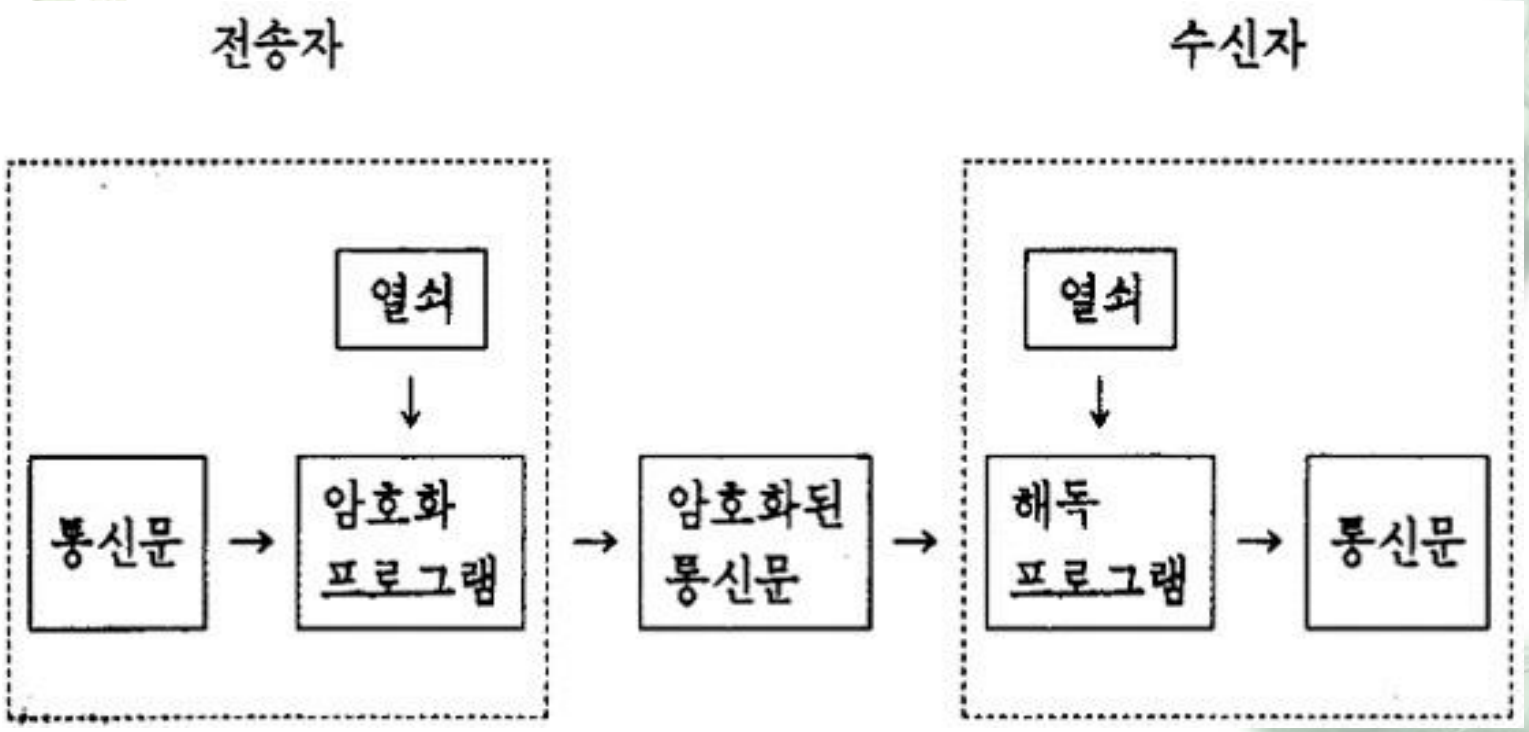
- p가 소수이고 $1 < a < p$이면 $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$이다 . 완벽한 증명은 1736년 스위스 수학자 오일러(L. Euler)가 함.
- 계 : p가 2보다 큰 소수이면 $2^{p-1} \equiv 1 (\mathrm{mod}\ p)$이다.
- (소수 판정에 이용)

- 작은 정리를 이용하여 주어진 p가 소수인지 아닌지 판정하기 위해서는 $2^{p-1}-1$이 p의 배수인지 확인하면 된다. 배수가 아니면 a는 소수가 아니다. 그러나 배수이면 p가 소수라고 단정하기 이르다. 이를테면 341은 11과 31의 곱이나, 위의 조건을 만족한다.
- 이 소수 판정의 불확실성 때문에 페르마의 작은 정리는 완벽한 소수 판정법은 아니다.

ARCL 소수 판정법

- 1986년 L.M. Adleman, R.S. Rumely, H. Cohen, H.W. Lenstra 는 불확실성을 제거하는 방법을 찾아냄(ARCL 판정법이라 불림). 이것이 통신문의 암호화에 이용된다. 그 이유는 소수 판정은 쉬워지나 소인수분해는 어렵기 때문이다. 공개열쇠(거대 소수의 곱)와 해독열쇠(두 개의 거대한 소수)를 이용한다. 암호화와 해독과정은 일반화 된 작은 정리와 관련 있다.

암호와 해독



- RSA 방식의 예
- 1) $p=11, q=3$을 선택하자
- 2) 공개열쇠 $n=pq=33, m=(p-1)(q-1)=20$ 여기서 20과 1외에는 공약수를 갖지 않는 정수 e를 임의로 택한다. e=3으로 하여 n=33과 e=3을 공개
- 3) 비밀열쇠 d를 q에 d를 곱한 값을 m으로 나누었을 때 나머지가 1이 되도록 d를 정한다. 즉 d=7로 두면 $3x7 \equiv 1 \pmod{20}$ 이다.
- 4) 암호문을 정한다. 사전에 [그 주식을 산다]란 문장을 5로 약속했다고 하자.

- 5) 암호문 $5^3=125\equiv 26 \pmod{33}$, 26을 암호로 보낸다.
- 6) 암호문 해독 $26^7 = 8031810176 \equiv 5 \mod(33)$.
- 7) 해독 후 실행: 그 주식을 산다.
- 같은 방법으로 전자 상거래 시 고객이 거짓말을 할 수 없도록 전자서명을 받을 때에도 이 같은 방법으로 본인임을 확인한다.

- 상품의 바코드에는 안전장치 체크숫자가 있다. 이
의 확인은 다음 방법을 사용함.

그림 1

$$8+8\times3+0+1\times3+0+3\times3+7+0\times3+0+2\times3+7+8\times3+2$$
$$= 8+24+0+3+0+9+7+0+0+6+7+24+2$$
$$= 90$$

바코드의 제일 끝에 있는 숫자 2가 체크 숫자다. 이것은 홀수번째 자리에 있는 숫자들은 그대로 더하고 짝수번째 자리에 있는 숫자들은 3배해서 더한 합이 10의 배수가 되도록 만든 것이다.

그림 2

$$8\times3+8+0\times3+0+9\times3+6+0\times3+5$$
$$=70$$

상품번호가 8개의 숫자로 이뤄진 경우에는 홀수번째에 있는 숫자들을 3배해서 더하고, 짝수번째 있는 숫자들은 그대로 더한 합이 10의 배수가 되도록 체크 숫자를 정한다.

그림 3

$$8\times10+9\times9+7\times8+2\times7+8\times6+2\times5+1\times4+0\times3+8\times2+X\times1$$
$$= 80+81+56+14+48+10+4+0+16+10$$
$$= 319 = 29\times11$$

10자리로 이뤄진 도서번호에서는 10개의 숫자에 10부터 1까지의 자연수를 차례로 곱해서 더한 합이 11의 배수가 되도록 체크숫자를 정한다.

Goldbach 의 추측

- 소수양식7 : Goldbach 의 추측 :
  (1742년 Euler에게 보낸 편지)

2 보다 큰 모든 짝수는 두 소수의 합이다.

T. Oliveirae Silva는 10^{18} 이하에서 참임을 확인(컴퓨터)

4 = 2+2　　6 = 3+3

8 = 3+5　　10 = 3+7 = 5+5

12 = 5+7　　14 = 3+11 = 7+7

16 = 3+13 = 5+11　　18 = 5+13 = 7+11

20 = 3+17 = 7+13　　22 = 3+19 = 5+17 = 11+11

쌍둥이 소수의 추측

- 소수양식8 : 쌍둥이 소수의 추측
  쌍둥이 소수의 쌍이 무한히 많이 존재하는가?
- 쌍둥이소수 3과 5, 5와 7, 11과 13, 17과 19, 1031과 1033,
  1,000,000,000,061 과 1,000,000,000,063

Mersenne 소수

- 소수양식9 : Mersenne의 소수

  1644년 Mersenne 의 [물리수학론]

- $M_n = 2^n - 1$은 n=2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257 에 대하여 소수이고 257 미만의 나머지 수에 대하여는 합성수라 주장.

- 1947년 오류발견 (M_{67}, M_{257}은 합성수, M_{61}, M_{89}, M_{107}은 소수). M_n이 소수이면 n도 소수이나 그 역은 성립하지 않는다.

- M_n이 소수이면 이 소수를 Mersenne 소수라 한다.
- M_{85943}는 33번째 Mersenne 소수로 1994년 Cray 슈퍼컴퓨터를 이용 발견. $M_{1257787}$과 $M_{1398267}$은 1996년, … , 38번째 Mersenne 소수는 $M_{6972593}$은 1999년에 발견되었다. 이와 같이 큰 소수를 찾는 이유는 통신문의 암호화의 문제뿐 아니라 슈퍼컴퓨터의 체계의 정확성을 시험하는 좋은 방법이기 때문이다. 39번째 $M_{13466917}$가 400만 자릿수 이상인 수로서 2001년 11월 14일 캐나다 사람인 Michael Cameron(당시 20세)에 의하여(800 MHz AMD PC이용) 발견되었음. 41번째 소수는 2004년 5월15일 Josh Findley가 2.4 GHz Pentium 4 컴퓨터를 이용 발견하였다. 49번째는 2016년 1월 발견된 22,338,618자리의 소수이다.

- 과제 : 가장 최근에 발견된 Mersenne 소수를 찾아보세요! 다른 소수판정법도 찾아보세요! WEB페이지 인쇄. 다음 주 강의시간까지 제출하세요

페르마의 마지막 정리

- 소수양식 10 : 페르마의 마지막 정리
- $z^n = x^n + y^n$이 2보다 큰 임의의 지수 n에 대하여 자연수해를 전혀 갖지 않는다. (미지수가 0인 자명한 해는 무시한다):
- 페르마가 읽었던 책 디오판투스의 산학 제 II권 문제 8(주어진 제곱수를 두 개의 다른 제곱수의 합으로 써라) 옆의 여백에 쓴 기록. 문제 8은 $3^2 + 4^2 = 5^2$과 같이 피타고라스의 정리와 연관된 문제임.

- 역사적 사건의 흐름
- n=3의 경우 1753 오일러 증명 (오류 있었음)
- n=5 인 경우 Dirichlet & Legendre 1825년 증명(오일러의 증명확장 오류제거)
- n=7인 경우 Lame 1839년 해결
- 1847년 독일 수학자 Kummer에 의하여 정규성이란 양식을 발견 100보다 작은 정규성을 가진 소수에 대하여 해결
- 1922년 모델(Mordell)의 추측-
  페르마의 마지막 정리가 곡면의 종수와 관계됨을 예측
- 1983 모델의 추측을 Faltings가 증명
- 1986 시무라-타니야미-베유의 추측증명
- 1993년 Andrew Wiles 마지막정리 해결

수학적 귀납법과 수치적 양식

- $p(n)$: 자연수에 관한 명제
- 전제: $p(1)$이 참
- 전제: $p(k)$가 참이면 $p(k+1)$도 참
- 결론: $p(n)$이 모든 자연수에 대하여 참

- 수학적 귀납법의 증명은 귀류법의 간접증명.
  직접증명법과 차이 !도미노!

일반 귀납법의 약점

- 귀납추리의 문제 : 유한 번 사건 확인으로 무한 번인 보편 사건을 이끌어 낼 수 없다고 보는 견해.
- 확증불가능의 문제 : 보편법칙을 경험으로 확증하는 것은 불가능하다는 견해.
- 예) 러셀의 칠면조 : 6시에 모이 먹는 칠면조가 언제나 6시에 모이를 먹는다는 정당성은 매일 확인될 수 있지만 어느 순간에 칠면조가 도살되면 보편 확증은 거짓으로 판명될 수 있다.
- %%% 가장 믿을 만하다는 자연과학체계도 이 정도인데 다른 신념체계는?

과제물, 정리, 예습

- 과제물
  - 최근에 발견된 메르센 소수를 찾아 관련 web페이지를 발견자를 포함하여 인쇄 제출.
  - 다음주 강의 시간에 들어오면서 제출
- 정리
  - 소수의 양식 10가지 정리하기
  - 삼단논법 이해하기
- 예습
  - 아리스토텔레스의 논리학에 대하여 알아오기
  - 비판적 사고에 대하여 책을 읽거나 자료를 조사해 오기