합동, 거듭제곱, 그리고 페르마의 소정리

이상준 교수
(덕성여대 수학과)
2015년 2학기

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

강의 슬라이드: 이상준, 오연주(15학번)

- **질문**: 정수 a를 선택하여 거듭제곱 a^2, a^3, a^4... (mod m)을 계산하면 어떤 규칙성이 있는가?
- **단순한 경우**: m=p 이 소수인 경우.
- **예**:

p=3

a	a^2	a^3	a^4
0	0	0	0
1	1	1	1
2	1	2	1

$a^k \pmod 3$

p=5

a	a^2	a^3	a^4	a^5	a^6
0	0	0	0	0	0
1	1	1	1	1	1
2	4	3	1	2	4
3	4	2	1	3	4
4	1	4	1	4	1

$a^k \pmod 5$

p=7

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8
0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
2	4	1	2	4	1	2	4
3	2	6	4	5	1	3	2
4	2	1	4	2	1	4	2
5	4	6	2	3	1	5	4
6	1	6	1	6	1	6	1

$a^k \pmod 7$

출처: 조셉 실버만, 친절한수론길라잡이

- **질문**: 패턴을 찾아라.

페르마의 소정리

- **관찰:** $a \neq 0$ 이면 $a^2 \equiv 1 \pmod 3$, $a^4 \equiv 1 \pmod 5$, $a^6 \equiv 1 \pmod 7$
- **추측:** 모든 정수 $1 \leq a < p$에 대해 $a^{p-1} \equiv 1 \pmod p$이다.
- **페르마의 소정리 (Fermat's little theorem):**

  p가 소수이고, a가 $a \neq 0 \pmod p$인 정수이면,

  $a^{p-1} \equiv 1 \pmod p$가 성립한다.
- **예:** $6^{22} \equiv 1 \pmod{23}$, $73^{100} \equiv 1 \pmod{101}$

- **예시** ① $2^{35} \pmod 7$을 계산하라
  - **답**: $2 \not\equiv 0 \pmod 7$이므로 페르마의 소정리에 의해 $2^6 \equiv 1 \pmod 7$.
    - $2^{35} = 2^{6\cdot 5+5} = (2^6)^5 2^5 \equiv 2^5 \equiv 32 \equiv 4 \pmod 7$
- **예시** ② $x^{103} \equiv 4 \pmod{11}$을 풀어라
  - **답**: $x \not\equiv 0 \pmod{11}$이므로, 페르마의 소정리에 의해 $x^{10} \equiv 1 \pmod{11}$.
    - 그러므로 $x^{103} \equiv x^{10\cdot 10+3} \equiv x^3 \pmod{11}$
      $x^3 \equiv 4 \pmod{11}$인 x를 찾기위해 조사하면

$x \pmod{11}$	0	1	2	3	4	5	6	7	8	9	10
$x^3 \pmod{11}$	0	1	8	5	9	4	7	2	6	3	10

- **연습문제:**
  - ① $11^{104} \pmod{17}$을 계산하라
  - ② $x^{39} \equiv 3 \pmod{13}$풀어라

페르마의 소정리 증명

- $a \not\equiv 0 \pmod p$이라 하자. 그리고 $a, 2a, 3a, \cdots, (p-1)a \pmod p$을 생각하자.
- **보조정리:** $\{a, 2a, \cdots, (p-1)a \pmod p\} = \{1, 2, 3, \cdots, p-1 \pmod p\}$
  - **주장1:** $1 \le k \le p-1$에 대해 $ka \not\equiv 0 \pmod p$
    - **증명:** $p \nmid k,\ p \nmid a \Rightarrow p \nmid ka$
  - **주장2:** $1 \le i < j \le p-1$에 대해 $ia \not\equiv ja \pmod p$
    - **증명:** $ia \equiv ja$라 가정하자. $(j-i)a \equiv 0 \pmod p$
      $p \nmid (j-i),\ p \nmid a$ 이므로, $p \nmid (j-i)a$. 모순!
- **주장1**과 **주장2**에 의해 $\{a, 2a, \cdots, (p-1)a \pmod p\} = \{1, 2, 3, \cdots, p-1 \pmod p\}$

$$a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod p$$

$$a^{p-1} \equiv 1 \pmod p$$

따름정리

- **페르마의 소정리 (Fermat's little theorem):**
  p가 소수이고, a가 $a \not\equiv 0 \pmod{p}$인 정수이면, $a^{p-1} \equiv 1 \pmod{p}$가 성립한다.
- **따름정리:** p가 소수이면 모든 정수 a에 대해 $a^p \equiv a \pmod{p}$가 성립한다.
- **따름정리 증명:**
  - **경우1:** $a \not\equiv 0 \pmod{p}$이면... 페르마 소정리 결과의 양변에 a를 곱해 성립.
  - **경우2:** $a \equiv 0 \pmod{p}$이면, 좌우변이 모두 $0 \pmod{p}$이므로 성립.

응용: 소수 판정

- **응용**: 페르마의 소정리는 주어진 수가 소수인지 아닌지를 판별하는데 도움을 준다.
- **질문**: 1234567 이 소수인가?
  - **답**: $2^{1234566} \equiv 899557 \pmod{1234567}$. 그러므로 1234567은 소수가 아니다!
- **질문**: $2^{1234566}$을 어떻게 계산할까?
  - **답: 거듭제곱 (16장)**을 이용!
- **질문**: 1234567 를 소인수분해는?
  - 답을 내기 위해서는 더 많은 계산량이 필요하다.
    컴퓨터로 계산가능: 1234567 = 127·9721.

응용: 소수 판정(계속)

- **질문:** $m=10^{100}+37$은 소수인가?
- **답:** 거듭제곱을 이용하면 $2^{m-1} \not\equiv 1 \pmod{m}$을 보일 수 있다.
  그러므로 m은 소수가 아니다.
- **질문:** $m=10^{100}+37$ 을 소인수분해하라.
- **답을 모른다**: m이 너무 큰 수이므로 컴퓨터로도 계산불가능!

소수 판정 (19장)

- **질문**: 주어진 자연수 n이 소수인가?
  - **경우1**: 어떤 자연수 a가 존재해서 $a^n \not\equiv a \pmod{n}$ 이다.
    - 이 때 a는 n이 소수가 아니라는 **증거(evidence)**이고, n은 소수가 아니다!
  - **경우2**: a<n인 모든 자연수 a에 대해 $a^n \equiv a \pmod{n}$ 이다.
    - n이 소수가 아니라는 증거가 없다.
    - n이 합성수가 아니라고도 단언할 수 없다.
    - n은 높은 확률로 소수이다.

Carmichael number

- **정의:** a<n인 모든 자연수 a에 대해 $a^n \equiv a \pmod n$ 이면
  n을 **Carmichael number (카마이클 수)**라 한다.
- Carmichael number (카마이클 수)가 소수라고 확정할 수는 없지만
  높은 확률로 소수라고 말할 수는 있다.