소수 (Prime Number)

IT융합공학부
권혁동

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB
https://crypto.modoo.at

Contents

CryptoCraft LAB

소수(Prime Number)란?

- **1** 또는 **자기 자신**으로 밖에 **나누어지지 않는 1이외의 정수**
  - 약수가 딱 2개만 존재하는 수
  - 여러 소수의 곱셈으로 이루어진 수는 합성수로 칭함
  - **1은 예외**로 지정되어 소수도 합성수도 아님
- 소수의 특별한 규칙은 과학에 큰 영향을 끼침

무한 소수 증명

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61 …

- 소수의 일부 예시
- **2는** 소수 중 **유일하게 짝수**
  - 2를 제외하고 모든 소수는 홀수

무한 소수 증명

소수는 무한하게 이어지는가?

- 유클리드의 증명
  - 만약 어떤 소수가 있고 그 소수보다 큰 수를 찾을 수 있다 가정
  - 상기의 과정을 계속 반복할 수 있다면 소수가 무한하다는 것이 증명

무한 소수 증명

- 유한개의 소수 목록 $p_1, p_2, \ldots, pr$를 가정
- 이 모든 **소수를 곱한 다음 1을 더한 것**을 A로 가정
  - $A = p_1 p_2 \ldots pr + 1$
- 만약 **A가 소수**라면?
  - 이전에 주어진 어떤 수보다 크기 때문에 **A는 새로운 소수**

무한 소수 증명

- 만약 **A는 소수가 아니라면?**
  - 소수가 아닌 수는 **소수의 곱으로 표현**할 수 있음
  - A는 적당한 소수로 나누어지며 그 중 가장 작은 것을 q라 가정
- q는 $p_1 p_2 \dots pr + 1$을 나눌 수 있다 가정
  - q가 p_i 중 하나라면 상기의 식을 나눌 수 있어야 함
  - 하지만 **1을 나눌 수가 없으므로 q는 목록의 소수가 아님**
  - q를 목록에 추가한다면 새로운 소수의 목록이 발생함
- 따라서 **소수의 수는 무한**

소수 판별

- **소수의 특징으로 인해 암호에도 많이 활용됨**
- 대표적인 경우로 RSA 알고리즘이 존재
- 매우 긴 소수를 사용
  - p, q는 약 140길이

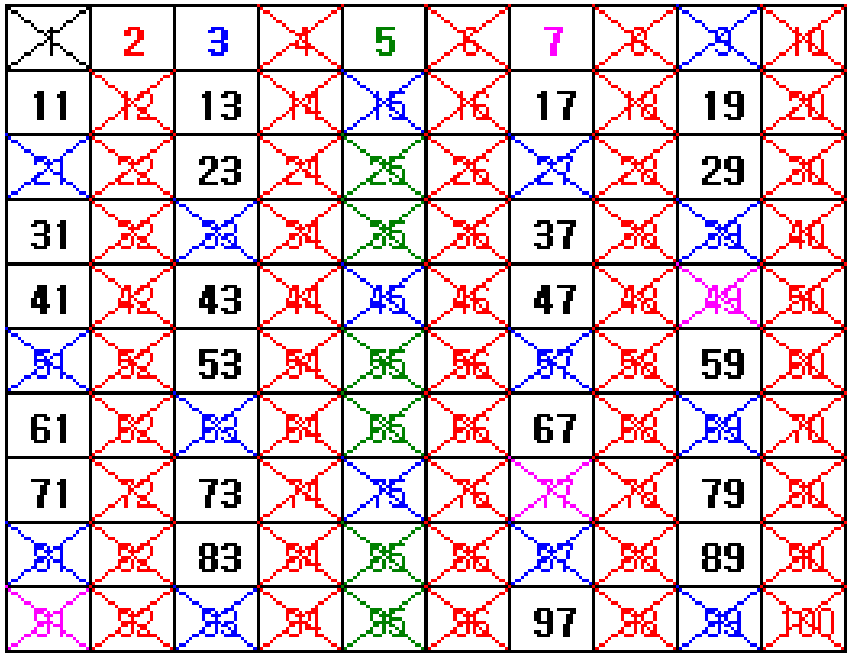
소수 판별

생성한 소수가 진짜 소수인지 판별 가능한가?

- 아직까지는 완벽한 방법은 존재하지 않음
  - 확실한 소수 판별
  - 소수일 것이라 추측

소수 판별

- **에라토스테네스의 체**
- 소수를 획득하고자 하는 범위 n을 설정
  - 2를 제외한 2의 배수를 지움
  - 3을 제외한 3의 배수를 지움
  - 5를 제외한 5의 배수를 지움 …
- 모든 **소수의 배수를 삭제**
  - $\sqrt{n}$이하의 배수만 삭제해도 동일



소수 판별

- 페르마의 소정리
  - 모든 정수 a에 대해 $a^p \equiv a \ (mod\ p)$이다
  - 상기 정리의 대우 명제를 활용
  - $2^m\ ! \equiv 2\ (\ mod\ m)$이라면 m은 소수가 아님
  - 즉 $a^p\ ! \equiv a\ (mod\ p)$일 때 p는 소수가 아니다
- 확실하게 소수를 판별하지는 못하나 **높은 확률로 소수 판독** 가능