소인수 분해 알고리즘 완전정복

07.

소인수 분해를 위한 쇼어의 양자 알고리즘

7. 소인수 분해를 위한 쇼어의 양자 알고리즘

- **소인수 분해, 다항 시간에는 불가능하다!**
  - **피터 쇼어: 응, 아니야! 양자 컴퓨터만 있으면 가능하다규.**
    - Shor, Peter W. "*Algorithms for quantum computation: discrete logarithms and factoring*." Proc. 35th ann. symp. on found. of comp. science. IEEE, 1994.

7. 소인수 분해를 위한 쇼어의 양자 알고리즘

- **두 개의 큰 소수로 구성된 합성수의 소인수 분해 문제**
  - $N = p \times q$ 일 때, 매우 큰 소수 p, q에 대해서 소인수 분해 가능?
  - 고전 컴퓨터로는 지수시간 복잡도를 극복할 수 없음
  - 두 소수의 합성수 N을 이용해서 p, q를 공개키, 비밀키로 사용: RSA 암호화
  - 다항시간에 소인수 분해 가능하면?: RSA 붕괴 $\rightarrow$ 지구 멸망

7. 소인수 분해를 위한 쇼어의 양자 알고리즘

- **쇼어의 소인수 분해 알고리즘**
  - **입력: 합성수** N $(N = p \times q$**이고** p**와** q**는 소수)**
  - **출력:** N**의 소인수** p, q
  - **입출력 사례:**
    - $N = 15$
    - $p = 3, q = 5$ **또는** $p = 5, q = 3$

7. 소인수 분해를 위한 쇼어의 양자 알고리즘

- **쇼어의 소인수 분해 알고리즘**
  1. 1보다 크고 N보다 작은 정수 a를 임의로 선택
  2. 만일, $\gcd(N, a) \neq 1$이면, p를 찾았다!
     - 따라서, $p = \gcd(N, a), q = N/\gcd(N, a)$
  3. 함수 $f(x) = a^x \pmod N$의 주기(period) r을 찾는다.
     - 여기서 찾은 주기 r이 짝수가 아니면, 1번 단계부터 다시 시작한다.
  4. 주기 r로부터 두 개의 최대공약수 gcd_1, gcd_2 를 찾는다.
     - $gcd_1 = \gcd(N, a^{r/2} + 1), gcd_2 = \gcd(N, a^{r/2} - 1)$
  5. gcd_1, gcd_2이 1과 N이라면, 1번 단계부터 다시 시작한다.
     - 아니면, 마침내 소인수들을 찾았으므로, $p = gcd_1, q = gcd_2$ 리턴

7. 소인수 분해를 위한 쇼어의 양자 알고리즘

- **뭔 말인지 알겠지? 모름.** *~~너 같으면 알겠냐?~~*

$$N = 15 = 3 \times 5$$

- **1보다 크고 N보다 작은 정수 a를 임의로 선택**

$a = \{3, 5, 6, 9, 10, 12\}$ $a = \{2, 4, 7, 8, 11, 13, 14\}$

$\gcd(N, a) = \{3, 5, 3, 3, 5, 3\}$ $\gcd(N, a) = \{1, 1, 1, 1, 1, 1\}$

7. 소인수 분해를 위한 쇼어의 양자 알고리즘

$$N = 15 = 3 \times 5$$

$$a = \{2, 4, 7, 8, 11, 13, 14\}$$

- 함수 $f(x) = a^x \pmod N$의 **주기(period) r을 찾는다.**
- **여기서 찾은 주기 r이 짝수가 아니면, 1번 단계부터 다시 시작한다.**

$a = 2$: $f(0), f(1), f(2), f(3), f(4), f(5), \ldots$

$1 \pmod{15}, 2 \pmod{15}, 4 \pmod{15}, 8 \pmod{15}, 16 \pmod{15}, 32 \pmod{15}, \ldots$

$1, 2, 4, 8, 1, 2, 4, 8, 1, \cdots$

7. 소인수 분해를 위한 쇼어의 양자 알고리즘

$$N = 15 = 3 \times 5$$

$a = 7$:

$$1 (\mathrm{mod}\, 15), 7 (\mathrm{mod}\, 15), 49 (\mathrm{mod}\, 15), 343 (\mathrm{mod}\, 15), 2401 (\mathrm{mod}\, 15), \cdots$$

$$1, 7, 4, 13, 1, 7, 4, 13, 1, 7, \cdots$$

$a = 4$:

$$1 (\mathrm{mod}\, 15), 4 (\mathrm{mod}\, 15), 16 (\mathrm{mod}\, 15), 64 (\mathrm{mod}\, 15), 256 (\mathrm{mod}\, 15), \cdots$$

$$1, 4, 1, 4, 1, 4, 1, 4, 1, 4, \cdots$$

7. 소인수 분해를 위한 쇼어의 양자 알고리즘

$$N = 15 = 3 \times 5$$

- **주기 r로부터 두 개의 최대공약수 gcd_1, gcd_2 를 찾는다.**

$$gcd_1 = \gcd(N, a^{r/2} + 1),\ gcd_2 = \gcd(N, a^{r/2} - 1)$$

$a = 7,\ r = 4$:

$$gcd_1 = \gcd(15, 50) = 5$$
$$gcd_2 = \gcd(15, 48) = 3$$

7. 소인수 분해를 위한 쇼어의 양자 알고리즘

- 왜 때문에?
  - "쇼어 알고리즘의 파이썬 구현"
    - written by 주니온.
  - 구글 드라이브에서 다운로드

주니온TV@Youtube

자세히 보면 유익한 코딩 채널

https://bit.ly/2JXXGqz

- 여러분의 구독과 좋아요는 강의제작에 큰 힘이 됩니다.
- 강의자료 및 소스코드: 구글 드라이브에서 다운로드
  (다운로드 주소는 영상 하단 설명란 참고)

  https://bit.ly/3baJZBx