알고리즘 중급 세미나

06: 고급 정수론

연세대학교 전우제|kiwiyou

2023.01.22.r1

분할 정복을 이용한 거듭제곱

- a^b를 계산하기
- $b = x_1 2^0 + x_2 2^1 + x_3 2^2 + x_4 2^3 + \cdots$
- $a^b = a^{x_1} \times a^{2x_2} \times a^{4x_3} \times a^{8x_4} \times \cdots$
- $\mathcal{O}(\log b)$번의 곱셈으로 충분
- 덧셈에도 응용 가능

분할 정복을 이용한 거듭제곱

- 비트 연산을 이용

```
1: function Power(a, b)
2:     r ← 1
3:     while b > 0 do
4:         if b bitand 1 = 1 then
5:             r ← r × a
6:         a ← a × a
7:         b ← rshift(b, 1)
8:     return r
```

분할 정복을 이용한 거듭제곱

- 행렬곱을 이용한 선형 점화식의 계산

$$a_{n+2} = 3a_{n+1} + 2a_n + 1$$

$$\begin{pmatrix} 3 & 2 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a_{n+1} \\ a_n \\ 1 \end{pmatrix} = \begin{pmatrix} a_{n+2} \\ a_{n+1} \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} 3 & 2 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}^n \begin{pmatrix} a_2 \\ a_1 \\ 1 \end{pmatrix} = \begin{pmatrix} a_{n+2} \\ a_{n+1} \\ 1 \end{pmatrix}$$

분할 정복을 이용한 거듭제곱

- 행렬곱에 $\mathcal{O}(k^3)$ 시간이 걸리므로 $\mathcal{O}(k^3 \log n)$
- 슈트라센 알고리즘: 행렬곱은 $\mathcal{O}(k^{2.8})$ 정도에 계산 가능
- 키타마사법: $\mathcal{O}(k \log k \log n)$

분할 정복을 이용한 거듭제곱

- Functional Graph: 진출차수가 1인 그래프
- 어떤 정점 v에서 그래프를 따라 k번 이동한 위치를 구하시오.
- $\mathcal{O}(N \log k)$

모듈러 곱셈 역원

- 연산 $\circ$의 항등원 e: $a \circ e = e \circ a = a$
- a의 역원 a^{-1}: $a \circ a^{-1} = a^{-1} \circ a = e$
- a의 법 N에 대한 곱셈 역원 a^{-1}: $a \times a^{-1} \equiv 1 \pmod{N}$
- $\exists x \in \mathbb{Z} : a \times a^{-1} + N \times x = 1$

모듈러 곱셈 역원

- 페르마의 소정리: $a^{p-1} \equiv a \pmod{p}$
- $a^{p-2} \times a = a^{p-1} \equiv 1 \pmod{p}$
- $a^{-1} \equiv a^{p-2} \pmod{p}$

모듈러 곱셈 역원

- 확장 유클리드 호제법
- $ax + by = \gcd(a, b)$를 만족하는 두 정수 x, y

$$
\begin{aligned}
a \times 1 + b \times 0 &= a \quad a \times 0 + b \times 1 = b \\
a \times 0 + b \times 1 &= b \quad a \times 1 + b \times (-q) = c \qquad \cdots (a = bq + c) \\
a \times 1 + b \times (-q) &= c \quad a \times (-1) + b \times (1 + q') = d \cdots (b = cq' + d) \\
&\vdots \\
ax + by &= \gcd(a, b) \quad ax' + by' = 0
\end{aligned}
$$

- 유클리드 호제법과 같은 $\mathcal{O}(\log \max(a, b))$