1. 문제 관찰

A^b mod c =

1. 예제를 통한 통찰

10 ^ 11 mod 12 =

이 문제의 경우 식을 바꿔서

10 ^ 11 mod 10으로 생각해보자.

이 수식은 이렇게 말로 설명할 수 있다.

10진수에서 10의 11승을 했을 때 1의 자리 수는 몇이 되는가?

본능적으로 10 % 10 = 0 이기 때문에 답은 0이라고 알 수 있다.

반대로 10 ^ 11 mod 12를 했을 때를 생각해보자.

12진수에서 10의 11승을 했을 때 1의 자리 수는 몇이 되는가? 로 생각할 수 있다.

재귀적인 풀이를 생각하자면, 이렇게도 생각할 수 있다.

숫자를 조금 바꿔서

8^7 mod 12를 푼다고 생각해보자.

8^1 mod 12 = 7 즉 12진수에서 7의 1의 자리 수는 8이다.

8^2 mod 12 = 1 즉 12진수에서 8 \* 8의 1의 자리 수는 4이다.

8^3 mod 12 = 1 즉 12진수에서 8 \* 8 \* 8 의 1의 자리 수는 8이다.

위에서 8 \* 8의 부분이 직전의 4의 값이 들어오고, 직전의 8의 값엔 처음의 mod값인 8이 들어오는 연쇄작용을 볼 수가 있다.

여기서 재귀함수를 생각해보면,

8 ^ 7 mod 12 = (8 ^ 6 mod 12) \* 8 % 12가 되는 것을 알 수가 있다.

여기서 지수법칙을 응용하면 재귀함수의 시간 복잡도를 더욱 낮출 수 있다.

(3 ^ 2) \* (3 ^2) = 3 ^ (2 + 2) = 3 ^ (2\*2) 가 되는 것을 응용하는 것인데,

위에 8 ^ 7 mod 12 = (8 ^ 6 mod 12) \* 8 % 12 이 수식에서 재귀로 들어가는 8 ^ 6 mod 12 이 부분에 주목하면

(8 ^ 3) \* (8 ^ 3) = 8 ^ 6이 되는 것을 알 수가 있다.

양 변에 mod를 추가해주면

{(8 ^ 3) \* (8 ^ 3)} mod 12 = (8 ^ 6) mod 12 가 성립한다. 또한,

((8 ^ 3) mod 12) )\* (( 8 ^ 3) mod 12) = (8 ^ 6) mod 12 도 성립하여, 직관적으로 재귀함수가 성립하는 것을 알 수가 있다.

1. 알고리즘