목차

ANSI

페르마의 소정리 (Fermat's Little Theorem)

- 정수 a와 소수 p에 대하여,

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

- 특히 a와 p가 서로소이면,

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

- $64^{70} \bmod 71$을 계산해볼까요?

Claim

$$\{x \,|x = k \times a \pmod p \text{ where } 1 \le k \le p-1\} = \{1, \ldots, p-1\}$$

Proof

- 귀류법을 이용하여 증명해 봅시다.
- $k_1 a \equiv k_2 a \pmod p$를 만족하는 $1 \le k_1 < k_2 \le p-1$이 존재한다고 가정합시다.
- 만약 $(k_2 - k_1)a \equiv 0 \pmod p$이라면 $p \mid a$ 혹은 $p \mid (k_2 - k_1)$를 만족해야 합니다.
- p보다 작은 모든 자연수에 대하여 $\gcd(p, *) = 1$이고, $\gcd(a, p) = 1$이므로 가정에 모순
- 따라서 위 두 집합은 합동입니다.

Claim

$$a^{p-1} \equiv 1 \pmod{p} \text{ where } \gcd(a,p) = 1$$

Proof

- 앞서 증명한 내용에 의해 $\prod_{i=1}^{p-1} ia \equiv \prod_{i=1}^{p-1} i \pmod{p}$

$$\therefore (p-1)! \times (a^{p-1} - 1) \equiv 0 \pmod{p}$$

- $p \nmid (p-1)!$ 이므로 $a^{p-1} = 1$ 입니다.

ANSi

결론

- $a^{p-1} \equiv 1 \equiv a \times a^{-1} \equiv a \times a^{p-2} \pmod p$

$$\therefore a^{p-2} \equiv a^{-1} \pmod p$$

- 이는 유리수 체계에서만 정의되던 곱셈의 역원을 정수 체계에서도 구할 수 있음을 의미합니다.
- 위 결과를 확장하여, 오일러 피 함수(Euler totient function) 또한 증명 가능합니다. 일반화하면,

$$a^{\phi(n)} \equiv 1 \pmod n \ (\text{where } \gcd(a, n) = 1)$$

BOJ 13172 – Σ

생냑

조합(Combination), 이항계수(Binomial Coefficient)

- $\binom{n}{k} = \dfrac{n!}{(n-k)! \times k!}$
- 소수 M에 대하여, $\binom{n}{k} \mod M$을 구해봅시다.

조합의 분자 계산

- $n! \mod M = (n-1)! \times n \mod M$
- Let $f(i) = i! \Rightarrow f(n) \mod M = f(n-1) \times n \mod M$

그렇다면 $\dfrac{1}{(n-k)!k!} \bmod M$ 는 어떻게 계산할 수 있을까요?

조합의 분모 계산

- $\dfrac{1}{n!} = \dfrac{1}{(n+1)!} \times (n+1) \bmod M$
- Let $g(i) = \dfrac{1}{i!} \Rightarrow g(n) \bmod M = g(n+1) \times (n+1) \bmod M$
- Recall FIT, $g(n) = f(n)^{p-2} \bmod M$

BOJ 11401 – 이항계수 3

생냑

예제가 매우 부실한 이유는 문제의 핵심이 될 리가 없기 때문입니다. (~~게으르기도하고요~~)

차례

- a^b 를 빠르게 구하는 방법 : 분할 정복
- Group에서 곱하기가 잘 정의된 연산이라면 a 가 정수일 필요가 있을까요?

행렬 제곱 (Matrix Power)

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}^b$$

- 곱셈 횟수 : $\mathcal{O}(\log b)$
- 곱셈 시간 : $\mathcal{O}(n^3)$
- 시간 복잡도 : $\mathcal{O}(n^3 \log b)$

ANSi

피보나치 수열

- 피보나치 수열의 n번째 항은 다이나믹 프로그래밍으로 구할 수 있습니다.
- 10^{10}째 항은 어떻게 구할 수 있을까요?
- 피보나치 수열 $f_n = f_{n-1} + f_{n-2}$을 빠르게 풀어 봅시다.
- $\begin{pmatrix} f_n \\ f_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} f_{n-1} \\ f_{n-2} \end{pmatrix}$

ANSI

피보나치 수열

- $\begin{pmatrix} f_n \\ f_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} f_{n-1} \\ f_{n-2} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^2 \begin{pmatrix} f_{n-2} \\ f_{n-3} \end{pmatrix} = \cdots = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{n-1} \begin{pmatrix} f_1 \\ f_0 \end{pmatrix}$
- 시간 복잡도 : $\mathcal{O}\left(2^3 \log n\right)$

선형 점화식 (Linear Recurrence)

- $a_n = c_{n-1}a_{n-1} + c_{n-2}a_{n-2} + \cdots + c_1 a_1$
- 위의 결과를 확장해 n 번째 항을 빠르게 구할 수 있을까요?

BOJ 2086 – 피보나치 수의 합

BOJ 2086 – 피보나치 수의 합

✓ $\star = \sum_{i=1}^{n} f_i$ 의 값을 잘 나타낼 수 있을까요?

$$f_1 + f_2 = f_3$$

$$f_2 + f_3 = f_4$$

$$\cdots$$

$$f_n + f_{n+1} = f_{n+2}$$

take sum : $\star + (\star + f_{n+1} - f_1) = \star + f_{n+1} + f_{n+2} - f_1 - f_2$

BOJ 13976 – 타일 채우기 2

ANSi

BOJ 13976 – 타일 채우기 2

- N 이 홀수라면 답이 없습니다.
- $N = 2$부터 차근 차근 해결하다보면,

$$dp_i = 3 \cdot dp_{i-2} + 2(dp_{i-4} + dp_{i-6} + \cdots + dp_2) + 2$$

- 조금 더 변형해보면,

$$\begin{pmatrix} dp_n \\ dp_{n-2} \end{pmatrix} = \begin{pmatrix} 4 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} dp_{n-2} \\ dp_{n-4} \end{pmatrix}$$

BOJ 25962 – 선우의 셋리스트

~~졸업해버린선우를기리며~~

- 이젠 쉽습니다.

BOJ 12728 – n제곱계산

BOJ 12728 – n제곱계산

- $x^2 - 6x + 4 = 0$ 이 떠오르지 않을 수 없습니다.
- $\alpha^n = 6\alpha^{n-1} - 4\alpha^{n-2}, \beta^n = 6\beta^{n-1} - 4\beta^{n-2}$
- 더하고 싶지 않을 수 없습니다.

$$\gamma_n = \alpha^n + \beta^n = 6\gamma_{n-1} - 4\gamma_{n-2}$$

- $\gamma^n \in \mathbb{N}$ 이고 $0 < \beta^n < 1$ 이므로, α^n 의 정수부는 $\gamma^n - 1$ 입니다.
- 따라서 $\gamma^n \pmod{1000}$ 을 구합시다.