Number Theoretic Algorithms

다항식의 가감승제, 평가 및 보간

September 17, 2019

1 $\mathbb{Z}_p$에서만 다항식 다루기

우리는 이미 주어진 소수 p에 대해서만 문제를 풀 수 있으면 임의 길이의 자연수에 대해 문제를 풀 수 있다는 사실을 알고 있습니다. 또, 지난 시간에 봤던 여러 좋은 성질들 덕에, 우리는 다항식을 $\mathbb{Z}_p$에서 다루는 게 훨씬 더 좋겠다는 사실을 추측해 볼 수 있습니다.

앞으로 나올 많은 내용은 유한 체이면 증명이 훨씬 쉬워지거나, 유한 체인 경우에**만** 성립하는 정리들입니다. 따라서 이후에 등장하는 모든 체는 유한 체로 가정합니다. 또, 결과가 유한 체에서만 성립하면 체를 *체*와 같이 기울인 글씨로, 그렇지 않은 경우 체와 같이 바로 선 글씨로 표기하겠습니다.

2 덧셈, 뺄셈 및 곱셈과 나눗셈의 차이

체 F에서 차수 n 이하인 두 다항식에 대해, 덧셈 및 뺄셈은 coefficientwise 정의되었으므로, 큰 수를 계산하는 알고리즘과 마찬가지로 $\mathcal{O}(n)$ 시간에 처리할 수 있습니다. 곱셈은 naïve하게 생각하면 $\mathcal{O}(n^2)$이고, 우리의 관심사는 여전히 subquadratic입니다. 사실 큰 수를 곱할 때 이미 다항식 두 개를 subquadratic에 곱해 돌아오는 방법을 사용했으므로, $\mathcal{O}(n \log n)$ 시간에 처리할 수 있는 방법을 압니다. 하지만 나눗셈은 큰 수의 나눗셈대로 잘 되지 않는데, 이유는 크게 두 가지입니다:

- 나눗셈이 곱셈의 **역연산이 아닙니다.** 우리가 예전에 정수 나눗셈을 계산하는데 실수에서만 성립하는 논증인 Newton's method를 자연스럽게 들고 나올 수 있었던 이유는, 정수의 자연스러운[1] 확장이 실수 체로 유일하기 때문이었습니다. 예를 들어 p-adic number에서의 나눗셈은 이러한 논증으로 풀 수 없습니다. 그런데 다항식 환은 수로 이루어진 체보다 훨씬 안 좋은 공간입니다!
- 곱셈에서 **받아올림**이 되지 않습니다. 받아올림은 본질적으로 "지수 k인 항을 몇 개 모으시면 지수를 $(k+1)$로 올려 드려요!"와 같은, 수학에서는 말도 안 되는 이벤트입니다. 만일 지수를 올릴 수 있었다면, 모든 계수를 올리는 지수에 맞추어 수로 변환하는 방법으로 Newton's method를 적용할 수 있었을 것입니다.

[1] 완비순서체의 유일성. 이 종이 안에는 정의하기가 너무 어렵습니다.

따라서 이 알고리즘이 subquadratic이 되기 위해서는 약간의 피와 땀과 눈물이 필요해 보입니다...

3 제곱미만 나눗셈

다항식에서는 오히려 "받아올림"이 일어나지 않고 계수가 독립적으로 계산된다는 사실에 주목합니다. 만일 다항식의 계수를 뒤집으면, 기존의 다항식 f를 g로 나누는 식 $f = gq + r$이 다음과 같은 식으로 변형됩니다.

$$\begin{aligned} x^n f\left(\frac{1}{x}\right) &= x^n g\left(\frac{1}{x}\right) q\left(\frac{1}{x}\right) + x^{n-k} r\left(\frac{1}{x}\right) \\ &= x^m g\left(\frac{1}{x}\right) \cdot x^{n-m} q\left(\frac{1}{x}\right) + x^{n-k} r\left(\frac{1}{x}\right) \end{aligned}$$

이때 $n := \deg f$, $m = \deg g$, $k = \deg r$로 두겠습니다. 따라서, 계수를 뒤집은 함수 $\hat{f}$, $\hat{g}$, $\hat{q}$에 대해, $\hat{q} = \hat{f}\hat{g}^{-1} \mod x^{n-m+1}$입니다.[2] 따라서 $\hat{g}^{-1} \mod x^{n-m+1}$을 빠른 시간 안에 구할 수 있다면 $\hat{q}$를 빠른 시간 안에 구할 수 있습니다!

3.1 Divide and Conquer

주어진 다항식 p에 대해 $p^{-1} \mod x^l =: a$가 주어져 있을 때, $p^{-1} \mod x^{2l}$을 빠르게 구하는 방법에 대해 생각해 봅시다. $p = p_0 + x^l p_1$이고, 정답은 $c = a + bx^l$ 꼴일 것이므로,

$$\begin{aligned} pc &= (p_0 + p_1 x^l)(a + bx^l) \\ &= p_0 a + (p_1 a + p_0 b)x^l \\ &= 1 + (p_1 a + p_0 b + u)x^l \mod x^{2l} \\ \therefore b &= -p_0^{-1}(u + p_1 a) \mod x^l \\ &= -a(u + p_1 a) \mod x^l \end{aligned}$$

(multiplication inverse가 어디에서의 inverse인지 주의해서 읽으시기 바랍니다.) 또한 $l = 0$인 경우 $a = 1$이 되게 할 수 있으므로, $\hat{g}^{-1} \mod x^{n-m+1}$을 $M(n)$ 시간에 구할 수 있습니다.

4 평가 및 보간

다항식의 경우에는 큰 수와 달리 수를 대입하여 계산하는 평가가 가능합니다. 사실 큰 수의 곱셈을 계산할 때도 다항식의 강점인 평가를 적극 활용했습니다.

다항식과 수 $a_1, \cdots, a_n$이 주어졌을 때 $\Phi(f)(a_1), \cdots, \Phi(f)(a_n)$을 계산하는 과정을 **평가**라고 하고, 수의 쌍 $(a_1, b_1), \cdots, (a_n, b_n)$이 주어졌을 때 $\Phi(f)(a_i) = b_i \ \forall i = 1, \cdots, n$인 $\deg f$가 최소인 다항식 f를 찾는 과정을 **보간**이라고 합니다.

[2] $k \le m - 1$로부터 $n - k \ge n - m + 1$을 얻을 수 있습니다.

4.1 Φ-identification과 평가

체 F 위에서 다항식 f와 수 $a_1, \cdots, a_n$이 주어져 있다고 합시다. 인접한 항을 묶어 곱셈 횟수를 줄여도, naïve 알고리즘은 $\mathcal{O}(n \deg f)$ 시간에 동작합니다. 이보다 시간을 더 줄일 마땅한 방법이 떠오르지 않으므로, **자릿수에 대한 분할 정복**을 사용하려고 시도해 봅시다.

그런데 다항식의 "자릿수"는 차수일 것 같은데, 이 상태로는 차수를 줄일 마땅한 방법이 떠오르지 않습니다... 다항식 곱셈을 정의할 때, 우리는 Φ-identification을 사용하지 않고[3] Ψ-identification을 사용했습니다. Φ-identification을 사용하면, 예를 들어 $\mathbb{Z}_2$에서 $f(x) := x^2$, $g(x) := x^2 + 1$로 둘 경우 이런 문제가 발생하기 때문인데,

$$\begin{aligned}
&\Phi(fg)(0) = \Phi(f)(0) \cdot \Phi(g)(0) = 0 \cdot 1 = 0 \\
&\Phi(fg)(1) = \Phi(f)(1) \cdot \Phi(g)(1) = 1 \cdot 0 = 0 \\
&\therefore (fg)(x) := 0, \quad x^2 + x, \quad x^5 + x^3 + x^2 + x, \quad \cdots
\end{aligned}$$

먼저 이 문제를 해결해 보도록 합시다.

간단하게 예측할 수 있는 결과는, 두 다항식 f와 g의 곱을 Φ-identification으로 정의한 함수 중 하나를 h라 하면,

- h는 **존재**합니다. $h := fg$로 놓으면 되고, Ψ-identification의 곱셈이 Φ-identification의 곱셈이 되도록 잘 정의했기 때문입니다.
- 차수가 가장 작은 h는 **유일**합니다. h에 관계없이 $(fg - h)$가 $(x^{|F|} - x)$로 나누어떨어져야 하기 때문에, $h = 0$이거나 $\deg h < |F|$인 h가 존재합니다. 따라서 다항식 나눗셈의 유일성으로부터 최소 차수 h의 유일성을 얻습니다.

그렇다면, 평가할 수가 $|F|$개보다 훨씬 작은 n개이기 때문에, $(x - a_1) \cdots (x - a_n)$으로 나눠도 아무런 문제가 없습니다! 이 곱을 **잘** 계산하면, 곱을 계산하는 데 $\mathcal{O}(n \log^2 n)$ 시간밖에 걸리지 않기 때문에, 전체 시간복잡도는 $\mathcal{O}(\min(n, \deg f)^2 + \deg f \log \deg f + n \log^2 n)$입니다.

식을 잘 보면, 평가할 값의 개수를 절반으로 줄이면, 시간이 절반으로 줄어듭니다. 그러면 매 단계마다 절반으로 줄이는 것은 어떨까요? 각 단계의 다항식을 계산하는 것은 나눌 다항식 $(x - a_1) \cdots (x - a_n)$을 계산하는 도중에 전부 계산할 수 있고, 나누는 과정은 각 깊이마다 $n \log n$보다 적은 시간이 걸리고, 잎에서의 계산 시간은 상수 시간이므로 전체 시간복잡도가 $\mathcal{O}(\deg f \log \deg f + n \log^2 n)$이 됩니다!

다항식의 곱셈, 즉 **특수한 값에 대한 평가**를 가지고 **일반적인 값에 대한 평가**를 빠르게 풀어냈습니다. 즉, 우리는 order가 $\deg f$보다 큰 ω의 자승들을 대입한 값을 가지고 다항식을 빠르게 곱해 오고 있었기 때문에 이는 상당히 재밌는 결과라고 할 수 있습니다.

[3] 물론 지금은 이게 가능한지도 모릅니다.

4.2 보간

조건 $a_i \neq a_j \quad \forall i \neq j$ 하에서, 보간 $(a_1, b_1), \cdots, (a_n, b_n)$의 존재성은 Lagrange의 결과이며, 최소 차수 다항식의 유일성은 위에서 설명한 논리를 그대로 따라갑니다. 보간에서도 평가와 마찬가지로 절반으로 쪼개서 합치는 방법이 있을까요?

이 질문에 답하기 위해서 다음을 만족하는 **최소 차수** 다항식 P_S를 찾기만 하면 될 것 같습니다.

$$P_S(a_i) = \begin{cases} 1 & a_i \in S \\ 0 & a_i \notin S \end{cases}$$

그렇다면, 크기가 절반인 집합 S를 잡은 다음, S와 $T := \{a_1, \cdots, a_n\} \setminus S$에서 보간 문제를 풀어서 각각 f_0와 f_1이라는 결과가 나왔다면, $f_0 P_S + f_1 P_T$가 답이 됩니다. 이제 해야 하는 질문은 과연 P_S를 찾는 것이 쉬울까 하는 것인데, 조금만 생각해 보면 결국 P_S를 찾는 것이 보간 문제를 푸는 것과 별다르지 않은 cost가 든다는 것을 알 수 있습니다. 우리가 마음대로 할 수 있는 것은 (a_i, b_i)들이지 P_S가 아닙니다!

따라서, P_S를 약간 수정해 봅시다.

$$\hat{P}_S(a_i) = \begin{cases} k_i & a_i \in S \\ 0 & a_i \notin S \end{cases} \quad \text{where } k_i \neq 0$$

이렇게 놓으면 S에서 변형된 쌍 $(a_i, b_i k_i^{-1})$으로 보간 문제를 풀고, T에서도 마찬가지로 변형된 쌍으로 풀어서, $f_0 \hat{P}_S + f_1 \hat{P}_T$가 답이 됩니다. 그런데

$$\hat{P}_S := \prod_{a_i \in T} (x - a_i)$$

로 두면 위의 조건을 모두 만족하는 것을 알 수 있습니다. k_i들은 다항식을 평가하는 것이므로, 매 깊이마다 $n \log^2 n$ 시간에 해결할 수 있습니다. 따라서 시간 $\mathcal{O}(n \log^3 n)$에 보간을 해결할 수 있습니다!

5 문제

1. 1주차부터 7주차 자료를 눈으로 쓱 훑어 보세요. 너무 꼼꼼히 읽으실 필요는 없고, "아 맞아 이런 걸 했었지!" 할 수준이면 됩니다.

2. 큰 수의 나눗셈에서 $m^\star$를 구해서 곱했듯이, 똑같은 방법으로 다항식의 역수를 구해 곱하는 방법을 생각해 볼 수 있습니다.

   (a) f/g를 분수식 그대로 잘 변형하여, $\lfloor x^{\deg f}/g(x) \rfloor$와의 연관성을 찾으세요.

   (b) g가 $\deg g = 2^i - 1$을 만족하고 $\deg g_1 < 2^{i-1}$이 되도록 $g = g_0 x^{2^{i-1}} + g_1$로 쓰면

$$\left\lfloor \frac{x^{2^{i+1}-2}}{g(x)} \right\rfloor = \left\lfloor \frac{2h(x)x^{3 \cdot 2^{i-1}-2} - h(x)^2 g(x)}{x^{2^i-2}} \right\rfloor \text{ where } h(x) = \left\lfloor \frac{x^{2^i-2}}{g_0(x)} \right\rfloor$$

임을 증명하세요.

(c) 이 방법으로 구현된 알고리즘이, 본문에 소개된 알고리즘보다 매 단계당 FFT를 1회 적게 사용함을 납득하세요. 그러나 최종 시간은 상수 배만 차이나는데, 그 이유는 FFT를 시행하는 크기가 양쪽 모두 반으로 줄기 때문입니다.

3. 3주차 자료의 subquadratic gcd(HGCD) 부분을 자세히 읽고, 최대공약수를 구하는 HGCD 알고리즘은 곱셈 및 나눗셈**에만** 의존함을 납득하세요. 이 방법으로 다항식 gcd를 계산할 경우 시간복잡도는 $\mathcal{O}(n \log^3 n)$입니다.

4. (조금 느린 키파컵 F번 풀이)

   (a) B보다 작은 양의 정수 n개가 주어졌을 때, 모든 수를 곱하는 시간복잡도 $\mathcal{O}(n \log^2 n)$ 방법이 있음을 보이세요. (Hint: segment tree.)

   (b) HGCD 행렬을 이용하여, 최대공약수가 g일 때 **quadratic** gcd는 시간복잡도 $\mathcal{O}\left(\left(\frac{a+b}{g}\right)^2 \log(a+b)\right)$을 달성함을 보이세요.

5. (전체 평가) $\mathbb{Z}_p$에서 때때로 임의의 수에 대한 값을 구하는 것이 본문에 주어진 로그제곱 알고리즘보다 이득인 경우가 있습니다.

   (a) k가 $p-1$을 나눈다면, $x^k - 1$은 k개의 근을 가짐을 증명하세요. Hint.[4]

   (b) $p - 1 = p_1^{e_1} p_2^{e_2} \cdots$로 쓸 경우, order $p_i^{e_i}$의 원소가 존재함을 보이고, 이 원소들을 다 곱해 order $p-1$인 원소가 존재함을 보이세요.

   (c) 이 원소 ω를 기준으로 FFT를 시행하여 다항식 f에 대해 modulo p에서의 모든 값을 $\mathcal{O}(\deg f + p \log p)$에 얻을 수 있음을 납득하세요.

6. (여러 non-trivial function들의 계산)

   (a) 상수 k에 대해 $x(x+1)(x+2)\cdots(x+k)$를 $\mathcal{O}(k \log^2 k)$ 시간에 계산할 수 있음을 보이세요.

   (b) (a)를 이용하여, $\binom{n}{m} \mod p$를 $\mathcal{O}(\sqrt{n} \log^2 n)$ 시간에 계산할 수 있음을 보이세요. (Hint: $k \approx \sqrt{n}$.)

   (c) $\sum_{i=1}^{n} i^k$을 n에 대한 $(k+1)$차 다항식으로 표현할 수 있음을 보이세요.

   (d) (c)를 이용하여, $\sum_{i=1}^{n} i^k \mod p$를 $\mathcal{O}(k \log^3 k)$ 시간에 계산할 수 있음을 보이세요.

[4] $x^{p-1} - 1$은 $x^k - 1$으로 나누어떨어지고, 따라서 $x^k - 1$을 인수분해하면 irreducible polynomial의 차수가...