
EDITORIAL (보급용)

DOJ Math Contest Vol.1

작성자: rootenter et al.¹

2026.08.22

¹Co-author가 늘어나면 document citation에 1저자만 남고 나머지는 quotient space로 빨려 들어가 영영 찾을 수 없다는 말이 있다. 나는 이 이야기를 무척이나 좋아한다.

총평

4. 그림은 학생 D, R, N이 대화하는 모습을 나타낸 것이다.



제시한 내용이 옳은 학생만을 있는 대로 고른 것은? [3점]

- ① D ② R ③ D, N ④ R, N ⑤ D, R, N

Figure 1: *Apologies for the AI slop image.*

대회 링크: <https://doj.kr/en/contests/mathdoj>

(수정됨333)

이런 답도 없는 대회에 끝까지 참가해주신 모든 분들께 감사드립니다. 근데 B가 저렇게 바로 썰릴 문제는 아니지 않나...?

#	PROBLEM	DIFFICULTY	ACCEPTANCE	SOLVED
A	말랑말랑 계산 직관 트레이닝 summation	Platinum V	75%	23
B	찍사왕 crush	Ruby V	100%	3
C	쿼리는 워수입니까? queryorder	Diamond II	30%	5
D	부호 처리 연습 (1) - Divisor Orthogonality orthogonality	Platinum II	35%	21
E	순열 sqrt	Unrated	0%	2
F	공평한 사다리타기 게임 ladder	Ruby IV	36%	4
G	Yet Another Tree Problem 3 tree	Ruby IV	33%	3
H	Extradimensional Cosmic Phenomenon cosmic	Ruby II	50%	2
I	多次元宇宙融合論 ekdndbd	Ruby III	26%	3

Figure 2: 난이도 조절 실패의 책임은 DADAS Online Judge에 물으시면 되겠습니다 감사합 니다.

A번, D번, F번, I번, H번은 해당 에디토리얼의 작성자(rootenter)가 출제하였습니다. B

번¹은 lunarlity님이, E번²은 pokmui9909님이, C번³과 G번⁴은 dkm110807님께서 출제해주셨습니다. 또 nflight11님, sharaelong님께서도 검수자로서 참여해주셨습니다. 마지막으로 대회 운영과 문제 세팅에 도움을 주신 dadas08님께도 감사의 말씀을 올립니다. 마음 같아서는 모든 문항에 대해 해설을 진행하고 싶었지만 시간적 여유가 없어⁵ 우선 제가 출제했던 문제들에 한정하여 에디토리얼을 작성하였습니다. 그 점에서 양해를 구하고 시작하도록 하겠습니다.

Remake...딱반년만기다려바바

¹Generating function의 shifting을 활용하여 inclusion-exclusion을 취급하는 트릭이 필요합니다. 제가 알고있는 범위 내에선, codeforces나 atcoder, Petrozavodsk Contest, BOJ 등에서도 이와 같은 아이디어를 명시적으로 활용해야하는 문제는 많지 않았습니다.

²다소 복잡한 조합론적 모델링과 inclusion-exclusion 식처리를 필요로 합니다. 저는 검수 기간 내에 풀이하지 못한 문제이기도 합니다.

³짝수의 배신자 2 크아아악

⁴Generating function에 대단히 능숙하다면 아마 보자마자 5분 안에 방정식 형태의 모델링은 끝내지 않을까 싶습니다. 다만 human bias에 의존해서 바로 lagrange inversion으로 들어가게 된다면 (이하 생략)

⁵G번 풀이에 필요한 power projection algorithm부터 유의미하게 서술할 각이 안 잡혔습니다. 올해 여유가 생길 시점에 본 에디토리얼의 remake가 세상 밖으로 나오게 된다면, 반드시 짚고 넘어갈 부분이기도 합니다.

목차

1	말랑말랑 계산 직관 트레이닝 [A]	4
1.1	Solution 1. 아무래도 가장 보편적일 풀이	4
1.2	Solution 2. $\sum$ 에서 식 정리할 때 인덱스는 나중에 고려하세요	5
1.3	Solution 3. 변수 분리법	6
1.4	Solution 4. 귀납 추론	6
2	부호 처리 연습 (1) - Divisor Orthogonality [D]	7
2.1	Solution 1. Prior knowledge...? So cute.	7
2.2	Solution 2. 모르겠으면 일단 그냥	7
2.3	Solution 3. 누적합의 역과정	8
3	공평한 사다리타기 게임 [F]	11
3.1	Part A. 행렬 모델링	11
3.2	Part B. 다항식이 없는 곳에서 저 정도의 DFT를	12
3.3	Part C. FPS Well-Known	14
3.4	입력 제약 관련 해명	14
4	多次元宇宙融合論(다차원우주융합론) [I]	16
4.1	Part B. Analysis on the Spectrum of H and its Uniqueness	17
4.1.1	Solution 1. Various Algebraic Tricks for Random Eigenspaces	18
4.1.2	Solution 2. by MO native	21
4.2	Part A. 다항식에도 스펙트럼이 있다	25
4.2.1	(Wrong?) Solution 2. 어제 내 다항식이 무너졌어,	27
4.2.2	Solution 1. 기본기에 관하여	28
4.2.3	Solution 2. 나는 황족 미적러다	29
4.2.4	이게 그렇게 어려운 건가요?	29
5	Extradimensional Cosmic Phenomenon [H]	30
5.1	Polynomial Algebra	30
5.2	with some Applications	32
5.3	...and its Quotient Algebra	33
5.4	Ideal Basics	35
5.5	Field Extension	37
5.6	함께보면 좋은 연습문제들	41
A	A Solution by a Professional:	43

말랑말랑 계산 직관 트레이닝 [A]

전체로부터의 ‘합’은 그의 대상이 되는 정보의 배열(혹은 나열된 순서)에 관한 성분을 포함하지 않습니다. 그렇기에 관련 문제를 풀 때는 주어진 항들을 재배열하는 과정 자체가 유의미하게 작용할 수밖에 없어요.¹

문제

입력으로 정수 N, M, a, b 가 주어진다. 등차수열 $A_i = ai + b$ 에 대해 다음의 값을 $10^9 + 7$ 로 나눈 나머지를 계산하여라.

$$\sum_{i_M \leq N} \sum_{i_{M-1} \leq i_M} \cdots \sum_{i_1 \leq i_2} A_{i_1}$$

정해 시간복잡도 팩토리얼 전처리 $\mathcal{O}(N + M)$ 및 쿼리당 $\mathcal{O}(1)$.

출제자 rootenter

간단한 문제이지만 수열의 합을 처리하는 다양한 로직을 살펴볼 필요는 있습니다.

1.1 Solution 1. 아무래도 가장 보편적일 풀이

solution writer: nflight11

이항계수 $\binom{n}{r}$ 에 관한 다음과 같은 등식을 이용하면 귀납적으로 임의의 M 에 대한 답을 구할 수 있습니다.

$$\sum_{i=-\infty}^n \binom{i+k}{k} = \binom{n+1}{k+1}$$

편의상 a, b 를 고정해 두고 $s_M(N) := S(N, M, a, b)$ 이라고 정의하겠습니다. 그러면 $s_1(N) = a \frac{N(N+1)}{2} + bN = a \binom{N+1}{2} + b \binom{N}{1}$ 이라는 사실은 어렵지 않게 알 수 있습니다.

이제 여기에 누적합을 한 번 씌워서 $s_2(N) = \sum_{i=1}^N s_1(i)$ 을 계산해 보면, 다음과 같은 식이 나옴 역시 알 수 있습니다.

$$s_2(N) = a \sum_{i=1}^N \binom{i+1}{2} + b \sum_{i=1}^N \binom{i}{1} = a \binom{N+2}{3} + b \binom{N+1}{2}$$

¹보다 나아가서, 역으로 ‘원소들의 합’을 어떤 변환에 대한 invariant로 보거나 그 자체를 기준으로 잡아 수학적 대상(집합 등)을 분류하는 데에 사용하는 것 역시 충분히 합리적일 수 있죠. Maschke's theorem가 앞호우

이로부터 $s_M(N) = a\binom{N+M}{M+1} + b\binom{N+M-1}{M}$ 이라는 추론을 해 볼 수 있으며, 이가 실제로 성립함은 수학적 귀납법을 통하여 증명할 수 있습니다. 증명 과정은 $s_1(N)$ 의 식을 통해 $s_2(N)$ 을 계산하는 방법과 거의 완벽하게 동일하고, 과정은 어렵지 않으니 생략합니다.

1.2 Solution 2. $\sum$ 에서 식 정리할 때 인덱스는 나중에 고려하세요

문제의 식을 다음과 같이 쓰도록 하겠습니다.

$$\sum_{1 \leq i_1 \leq \dots \leq i_M \leq N} A_{i_1}.$$

물론 notation의 차이에 불과하지만, 위처럼 쓰는 것도 꽤나 효과적일 때가 많습니다. 아래와 같이 항들을 분리해봅시다.

$$a \left(\sum_{1 \leq i_1 \leq N} i_1 \cdot \left(\sum_{i_1 \leq i_2 \leq \dots \leq i_M \leq N} 1 \right) \right) + b \left(\sum_{1 \leq i_1 \leq \dots \leq i_M \leq N} 1 \right).$$

다만 이제부터는 편의를 위해 index condition을 Iverson bracket $[-]^2$ 으로 치환하겠습니다.

$$a \underbrace{\sum_{1 \leq i_1 \leq N} i_1 \cdot [i_1 \leq \dots \leq i_M \leq N]}_{[1]} + b \underbrace{\sum [1 \leq i_1 \leq \dots \leq i_M \leq N]}_{[2]}.$$

여기서 항 [2]는 쉽게 처리할 수 있을 것으로 보이네요. $1 \leq i_1 \leq \dots \leq i_M \leq N$ 을 만족하는 자연수의 순서쌍 $(i_1, i_2, \dots, i_M)$ 의 개수를 구하면 충분합니다. 중복조합에 의해,

$$\sum [1 \leq i_1 \leq \dots \leq i_M \leq N] = \binom{N+M-1}{M}.$$

그렇기에 여러분은 이제 항 [1]을 이렇게도 바라볼 수 있습니다:

$$\begin{aligned} \sum_{1 \leq i_1 \leq N} i_1 \cdot [i_1 \leq \dots \leq i_M \leq N] &= \sum [1 \leq i_0 \leq i_1] \cdot [i_1 \leq \dots \leq i_M \leq N] \\ &= \sum [1 \leq i_0 \leq i_1 \leq \dots \leq i_M \leq N] \\ &= \binom{N+M}{M+1}. \end{aligned}$$

그럼 끝났습니다.

$$\therefore \sum_{1 \leq i_1 \leq \dots \leq i_M \leq N} A_{i_1} = a \binom{N+M}{M+1} + b \binom{N+M-1}{M}.$$

²Iverson bracket은 명제가 참이면 1, 거짓이면 0의 값을 가지는 함수를 나타냅니다. 예를 들어 $[1 \leq i \leq N]$ 은 i 가 1 이상 N 이하일 때 1, 그렇지 않을 때 0을 줍니다. 본 문서에서는 앞으로도 특별한 언급 없이 반복해서 차용하겠습니다.

1.3 Solution 3. 변수 분리법

인덱스 사이의 대소 관계를 고려해가면서 문제를 풀 이유가 있나요? 부분적으로 다음을 계산하는 것만을 목표로 하겠습니다:

$$\sum_{1 \leq i_1 \leq \dots \leq i_M \leq N} i_1$$

...원래 다변수 해석에선 대개화만 잘 해도 삶의 질이 올라가는 겁니다.

$$\text{Let. } X_j = i_j - i_{j-1} \quad ; \quad j = 1, \dots, M+1.$$

(단, $i_0 = 1$, $i_{M+1} = N$ 으로 생각하겠습니다.)

$\sum_j X_j = N - 1$ 이고 대칭성에 의해

$$\begin{aligned} \mathbb{E} \left[\sum_{j=1}^{M+1} X_j \right] &= \sum_{j=1}^{M+1} \mathbb{E}[X_j] \\ &= (M+1) \mathbb{E}[X_1] \\ &= N - 1. \end{aligned}$$

즉,

$$\mathbb{E}[i_1] = \mathbb{E}[X_1] + 1 = \frac{N-1}{M+1} + 1 = \frac{M+N}{M+1}.$$

전체 합의 평균을 알았으니 여기서 항의 개수만 곱해지면 되겠네요.

$$\begin{aligned} \therefore \sum_{1 \leq i_1 \leq \dots \leq i_M \leq N} i_1 &= \binom{N+M-1}{M} \frac{N+M}{M+1} \\ &= \binom{N+M}{M+1}. \end{aligned}$$

1.4 Solution 4. 귀납 추론

$M = 1$ 일 때부터 시작해서 $M = 2, 3, \dots$ 에 대해 직접 식을 정리하다보면 규칙이 보입니다. 뭐... 상세 해설은 생략하겠습니다? ³

³솔직히 말하면 한번 정도는 직접 밀어보시는 걸 추천드립니다. 저도 이 문제 검수하면서 이미 두어번 정도는 제 손으로 굴러봤어요. 근데 이걸 또 TeX로 적으라는 건 진짜말안되는거거든요

부호 처리 연습 (1) - Divisor Orthogonality [D]

문제

양의 정수 N 이 주어질 때 다음의 행렬 A 에 대하여 $\det(A)$ 를 계산하자. 이때 행렬 A 의 i 행 j 열 성분은 다음과 같다:

$$A_{ij} = \left(\frac{i}{\gcd(i, j)} \right) \quad (1 \leq i, j \leq N).$$

즉 구하고자하는 값은

$$\begin{vmatrix} \frac{1}{\gcd(1,1)} & \frac{1}{\gcd(1,2)} & \cdots & \frac{1}{\gcd(1,N)} \\ \frac{2}{\gcd(2,1)} & \frac{2}{\gcd(2,2)} & \cdots & \frac{2}{\gcd(2,N)} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{N}{\gcd(N,1)} & \frac{N}{\gcd(N,2)} & \cdots & \frac{N}{\gcd(N,N)} \end{vmatrix}.$$

정해 시간복잡도 $\mathcal{O}(N \log \log N)$

출제자 rootenter

사실 이 문제는 출제자 본인이 가장 못 푸는 유형의 문제입니다.¹ 다음 ~~생은 field of characteristic 2가 항상 보장되는 곳에서~~ 근데 살짝만 비틀면 저만 못 푸는건 아닐 수도 있겠다는 생각이 들더라고요. 무튼 출제 motivation이었습니다.

2.1 Solution 1. Prior knowledge...? So cute.

Appendix A 참조.

2.2 Solution 2. 모르겠으면 일단 그냥

관찰 후 induction은 무적이다.

¹Do read the title.

물론 노가다 식 처리도 실력이긴합니다. 제 개인적인 추천안은 정수의 약배수 관계가 관찰의 경계 케이스에 해당함을 눈치채고, 서로 다른 임의의 두 소수 p, q 에 대해서 $N = p, p^a, pq, p^a q, p^a q^b, \dots$ 일 때로 점차 확장해가며² 식을 직접 미는 것이에요. 이후 가우스소거로 A 를 삼각행렬로 만드는데 성공하면 주대각 성분들만 쭉 곱해주면 되겠죠.³

거기에 더해서 한가지 계산 노하우가 있다면, 어차피 A 의 i 행 j 열 성분은 정말로 (i, j) 에만 의존하니, 각 성분들을 잠시 $f(i, j)$ 로 치환해두는 것이겠네요. 사소하지만 일단 확이 줄어드는 데에 큰 장점이 있고⁴, 문제 상황에 대한 맥락을 노가다 과정 내내 인지할 수 있다는 것 자체가 메리트로 작용합니다. 가끔은 자존심을 굽히고 치환을 열심히 해보는 것도 문제 풀이의 좋은 전략이겠쬬 아무래도?

2.3 Solution 3. 누적합의 역과정

Theorem 2.3.1 (Row-adjusted GCD matrix determinant formula). *Let S be a finite factor-closed set of positive integers, and let $\mu(-, -)$ denote the Möbius function of the divisibility poset $(S, |)$. Suppose that $F(d, n)$ is defined for every $d, n \in S$ satisfying $d | n$. Define the matrix A , whose rows and columns are indexed by S , by*

$$A_{ij} = F(\gcd(i, j), i) \quad (i, j \in S)$$

Then

$$\det A = \prod_{i \in S} \left(\sum_{\substack{j \in S \\ j|i}} \mu(j, i) F(j, i) \right).$$

In particular, since set S is divisor-closed, $\mu(j, i) = \mu(i/j)$ whenever $j | i$.

Proof. As the strategy of A could be revisited to general notion of incidence algebra, **the author of this document leaves the proof to the reader.** $\square$

편의를 위해 $S(N) := \det A$ 로 정의하겠습니다. $F(j, i) = \frac{i}{j}$ 와 같이 정의하면 2.3.1에 의해,

$$S(N) = \det A = \prod_{1 \leq i \leq N} \left(\sum_j \mu(j, i) F(j, i) \zeta(j, i) \right).$$

²이건 어떤 형태로든 일단 짚이 있어야하는 부분입니다. 만일 본인이 이를 무의식적으로 구사하고 있었다면, 그 관찰이 누구에게서나 나올만큼 자명하지는 않다는 걸 꼭 기억합니다.

³몇가지 기본적인 사실 정리: Gaussian elimination을 통해 A 를 triangular matrix로 만들면 그 main diagonal element들의 곱이 $\det A$ 에 해당하게 됩니다. 그러면 정답은 $\prod$ (*어찌구*) 느낌으로 나오겠네요. 물론 근데 (*어찌구*) 라고 하는 항이 multiplicative function으로 나옴을 예상해볼만한가? 라고 물으면 그건 아니에요. 자연스러운 연산의 유일성 측면에서 직전 각주와 연결할만한 직관은 있지만, 이번 대화의 테마와는 괴리가 있으니 넘어가겠습니다.

⁴사실 전 그래서 $f(i, j)$ 대신 $\langle i | j \rangle$ 라는 무근본 노테이션으로 노가다를 전개하긴 했습니다. 그 이후에 좀 더 이리저리 만져봤을 때, 문제 자체의 계산 흐름이 Gram-Schmidt method와 비슷한 결을 따라갈 수밖에 없다... 라는 인상은 있었지만 당장 주목할만한 포인트는 아닙니다.

...그리고 이는 아래를 보다 있어보이게 쓴 것에 불과합니다.

$$\begin{aligned}
S(N) = \det A &= \prod_{1 \leq n \leq N} \left(\sum_{d|n} \mu\left(\frac{n}{d}\right) F(d, n) \right) \\
&= \prod_{1 \leq n \leq N} \left(\sum_{d|n} \mu\left(\frac{n}{d}\right) \frac{n}{d} \right) \\
&= \prod_{1 \leq n \leq N} \left(\sum_{d|n} \mu(d) \cdot d \right)
\end{aligned}$$

여기서 multiplicative function⁵ $f(n) = \sum_{d|n} d \cdot \mu(d)$ 로 세팅하여 $n = p^e$ 만을 대입해보면 $f(n)$ 의 값을 $n \in \mathbb{N}$ 전체에 대해서 확정지을 수 있습니다.⁶

$$\begin{aligned}
f(p^e) &= \sum_{d|p^e} d \cdot \mu(d) \\
&= \sum_{0 \leq k \leq e} p^k \cdot \mu(p^k) \\
&= \begin{cases} 1 & ; \quad e = 0; \\ 1 - p & ; \quad e \geq 1. \end{cases}
\end{aligned}$$

그럼 이어서,

$$\begin{aligned}
S(N) &= \prod_{1 \leq n \leq N} f(n) \\
&= \prod_{1 \leq n \leq N} \prod_{\substack{p|n \\ p \in \mathbb{P}}} (1 - p)
\end{aligned}$$

직전의 식에서 지수항들에 대해 더블카운팅을 하면 되긴 하겠지만... 좀 있어보이게 로그 씌워서 처리하는 것도 가능합니다.

$$\begin{aligned}
\log S(N) &= \sum_{1 \leq n \leq N} \log f(n) \\
&= \sum_{1 \leq n \leq N} \sum_{\substack{p|n \\ p \in \mathbb{P}}} \log(1 - p) \\
&= \sum_{\substack{p \leq N \\ p \in \mathbb{P}}} \sum_{1 \leq n \leq N} [p | n] \log(1 - p) \\
&= \sum_{\substack{p \leq N \\ p \in \mathbb{P}}} \left\lfloor \frac{N}{p} \right\rfloor \log(1 - p).
\end{aligned}$$

⁵Multiplicative function들 사이의 dirichlet convolution은 언제나 다시 multiplicative function을 줍니다. Induced by basic property of (commutative) monoid algebra.

⁶누누이 말하지만 이건 습관의 문제임!! Universal property는 진짜로 조상님이 보장해주니까 괜히 보이는 homomorphism은 최소한의 evaluation으로 그 내부 정보를 전부 잡아 가져가시면 됩니다. (그럴싸한 예시를 하나 더 들어보라 한다면, linear extension theorem 같은 거 생각해보시면 되어요. 5.1.1 참조.)

결과적으로

$$S(N) = \prod_{\substack{p \leq N \\ p \in \mathbb{P}}} (1 - p)^{\lfloor \frac{N}{p} \rfloor}$$

를 얻고, 이는 에라토스테네스의 체를 활용해서 $\mathcal{O}(N \log \log N)$ 에 계산할 수 있습니다.

공평한 사다리타기 게임 [F]

문제

두 양의 정수 N, M 이 주어진다.

‘공평한 사다리타기 게임’의 규칙은 다음과 같다:

- N 명의 참가자 각각에 대응하도록 우선 N 개의 세로줄을 원형으로 긋는다. 편의를 위해 초기에 n 번 참가자에게 배정된 세로줄을 ‘ n 번-세로줄’이라 부르자. ($1 \leq n \leq N$)
- 이후 사전에 주어진 길이 $N-1$ 의 수열 $\{A_n\}$ 에 따라 m 개의 가로줄을 하나씩 그어 내려간다. 그 규칙은 다음과 같다:
 - 먼저 N 개의 세로줄 중 하나를 무작위로 선택한다. 여기서 i 번-세로줄이 선택되었다고 하자.
 - 이어서 i 번-세로줄과 연결할 j 번-세로줄을 선택한다. j 번-세로줄은 i 번-세로줄과의 ‘거리’를 고려하여 $\frac{A_{|j-i|}}{\sum_{n=1}^{N-1} A_n}$ 의 확률로 선택된다. 이때, $A_{N-|j-i|} = A_{|j-i|}$ 임은 보장된다. (단, $i \neq j$.)

M 이하의 모든 양의 정수 m 에 대하여, ‘공평한 사다리타기 게임’에서 m 개의 가로줄을 그을 때 출발 세로선과 도착 세로선이 같은 참가자 수의 기댓값을 998 244 353으로 나눈 나머지를 출력하여라.

정해 시간복잡도 $\mathcal{O}(N \log^2 N)$ ^a

출제자 rootenter

^a...출제자가 채점 환경에 대한 이해가 크게 부족했습니다. 보다 적절한 제한은 $N \leq 5 \cdot 10^5$ 이 아닌 $N \leq 2 \cdot 10^5$ 이 되어야합니다. 곧 다시 언급하겠습니다.

출제 후 만족도가 높았던 소재입니다. 문제를 크게 세 부분으로 나누어 해결하겠습니다.

3.1 Part A. 행렬 모델링

어떤 계의 상태 각각을 basis로 잡고 어떠한 시행 이후 상태가 (직전 상태에 의존하여) 확률적으로 결정될 때, 그러한 전이 전체를 행렬로 나타낼 수 있습니다. 아마 대부분 Markov matrix라는 이름으로라도 어디선가 들어본 적은 있을 것 같네요. 그러한 transfer matrix T 를 모델링하면서 풀이를 시작해보겠습니다.

우선 i -번째 열에서 j -번째 열로 전이할 확률이 곧 전이 행렬 T 의 i 행 j 열 성분에 해당합니다. 이를 T_{ij} 로 나타내겠습니다.

$$T_{ij} = \begin{cases} 1 - \frac{2}{N} & ; \quad i = j; \\ \frac{2A_{|j-i|}}{N \sum_{k=1}^{N-1} A_k}, & ; \quad i \neq j. \end{cases}$$

한편, 문제에서 요구하는 건 각 m 에 대해 m 번의 전이 이후 시작 상태와 같은 위치에 있을 확률의 합입니다. 즉, $\sum_i \mathbf{e}_i^\top T^m \mathbf{e}_i$ 이고, 간단히 표현하면 $\text{tr}(T^m)$ 로도 쓸 수 있습니다. 다만 행렬의 크기가 통상적으로 계산될 수 있다고 알려진 것들과는 차이가 있는 것 같네요. 좀 만만할듯 말듯한 딥러닝 아키텍처도 내부 계산은 768차원짜리로 처리하는데... 그걸 10^5 dim scale에서 M 번이나 곱하라는 건 엔비디아 할아버지가 와도 쉽지 보이고요.

T 가 어떤 특별한 성질을 가지는 건 아닐까요? 일단 성분들이 sparse한 것 같지도 않고¹, 당장 가장 쓰일법한 성질은 모든 행(혹은 열) 정보가 사실상 길이 N 짜리 벡터 하나로 압축된다는 것 정도인데, 그렇다고 행렬곱을 이쁘고 빠르게 처리할 수 있는 건가요? 어차피 우리가 원하는 정보는 행렬의 주대각합이긴 한데...

3.2 Part B. 다항식이 없는 곳에서 저 정도의 DFT를

FFT는 고작 분배법칙 빨리 계산해주는 well-known library 같은 것이 아닙니다. 배운 것이 많고 실제로 경험한 것이 많을수록 자신이 아는 바를 잘 정리해야해요.

Definition 3.2.1 (Discrete Fourier Transform - 일반인용). Let ξ_N be a primitive N -th root of unity. For a vector $\mathbf{x} = (x_0, x_1, \dots, x_{N-1})$, its discrete Fourier transform is the vector $\hat{\mathbf{x}} = (\hat{x}_0, \hat{x}_1, \dots, \hat{x}_{N-1})$ defined by

$$\hat{x}_k = \sum_{j=0}^{N-1} x_j \xi_N^{jk} \quad (0 \leq k < N).$$

The inverse transform is given by

$$x_j = \frac{1}{N} \sum_{k=0}^{N-1} \hat{x}_k \xi_N^{-jk} \quad (0 \leq j < N).$$

...를 좀 멋지게 쓰면

Definition 3.2.2 (Discrete Fourier Transform - 대수버거용). Let G be a finite abelian group. Its Pontryagin dual is

$$\hat{G} := \text{Hom}(G, \mathbb{C}^\times),$$

the group of all one-dimensional representations, or characters, of G . For a function

¹물론 sparse matrix마저도 거듭해서 곱해질 수록 기존의 sparsity를 잃는다는 사실이 잘 알려져있습니다. 그래서 정보의 중복 성분이 많다고 항상 문제가 단순화될 수 있는 건 아니에요.

$f : G \rightarrow \mathbb{C}$, its Fourier transform is the function $\hat{f} : \hat{G} \rightarrow \mathbb{C}$ defined by

$$\hat{f}(\chi) = \sum_{g \in G} f(g) \chi(g).$$

The inverse transform is

$$f(g) = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \hat{f}(\chi) \chi(g)^{-1}.$$

i.e. $G = \mathbb{Z}/N\mathbb{Z}$, every character is of the form

$$\chi_k(j) = \xi_N^{jk} \quad (0 \leq k < N).$$

행렬 T 의 N 개의 eigenvalue를 $\lambda_0, \dots, \lambda_{N-1}$ 이라 하겠습니다. 다음의 사실이 잘 알려져 있습니다:

$$\text{tr}(T) = \sum_{i=0}^{N-1} \lambda_i$$

...네. 오히려 computational linear algebra에 친숙한 사람일수록 어떤 무작위(에 가까운) 행렬의 N 개의 eigenvalue를 구한다는 것은 상당히 비상식적인 일임을 본능적으로나마 알고있을 것입니다. 이유는 여러가지가 있겠지만, 일단 $\mathbb{F}_p$ 에서 정말로 λ_i 가 표현이 되는가하는 문제부터 발목을 잡죠.²

다음을 확인합니다:

Lemma 3.2.3. *Let C be an $N \times N$ circulant matrix given by $C_{ij} = c_{j-i}$, and let ξ_N be a primitive N -th root of unity. For each $0 \leq k < N$,*

$$\mathbf{v}_k = (1, \xi_N^k, \xi_N^{2k}, \dots, \xi_N^{(N-1)k})^\top$$

is an eigenvector of C . More precisely,

$$C\mathbf{v}_k = \left(\sum_{d=0}^{N-1} c_d \xi_N^{kd} \right) \mathbf{v}_k.$$

Proof. The i -th component of $\mathbf{v}_k$ is ξ_N^{ki} . Hence the i -th component of $C\mathbf{v}_k$ is

$$\begin{aligned} (C\mathbf{v}_k)_i &= \sum_{j=0}^{N-1} C_{ij} \xi_N^{kj} \\ &= \sum_{j=0}^{N-1} c_{j-i} \xi_N^{kj}. \end{aligned}$$

²5 참조.

Substitute $d = j - i$. Then $j = i + d$, and since all indices are taken modulo N , we obtain

$$\begin{aligned}(C\mathbf{v}_k)_i &= \sum_{d=0}^{N-1} c_d \xi_N^{k(i+d)} \\ &= \xi_N^{ki} \sum_{d=0}^{N-1} c_d \xi_N^{kd} \\ &= \left(\sum_{d=0}^{N-1} c_d \xi_N^{kd} \right) (\mathbf{v}_k)_i.\end{aligned}$$

This holds for every i , so $\mathbf{v}_k$ is indeed an eigenvector of C . $\square$

Corollary 3.2.3.1. *The eigenvalues of the matrix T are exactly the Fourier coefficients of its first row.*

$\mathbb{F}_p$ 에서 primitive N -th root of unity가 존재함은 $N \mid (p-1)$ 과 동치이므로, generalized Chirp-Z transform을 이용하여 T 의 eigenvalue를 $\mathcal{O}(N \log N)$ 에 **전부** 구할 수 있습니다.

3.3 Part C. FPS Well-Known

그럼 이제 다음과 같은 생성함수를 구해주면 됩니다.

$$\sum_{m=1}^M \left(\sum_{i=0}^{N-1} \lambda_i^m \right) x^m$$

이는 $f(x) = \prod_{i=0}^{N-1} (1 - \lambda_i x)$ 로 정의했을 때

$$-x \frac{f'(x)}{f(x)} = \sum_{m \geq 1} \left(\sum_{i=0}^{N-1} \lambda_i^m \right) x^m$$

의 M 차항까지의 계수와 같습니다.³

$f(x)$ 는 $\mathcal{O}(N \log^2 N)$ 에 계산될 수 있고, 이후 과정은 $\mathcal{O}(N \log N)$ 이므로 문제 해결에 필요한 전체 시간복잡도는 $\mathcal{O}(N \log^2 N)$.

3.4 입력 제약 관련 해명

답도 없는 구현 상수 최적화를 강제해버렸던 점에서, 해당 문제에 접근했던 모든 대회 참가자 분들께 사과드립니다.

이 문제는 주어진 circulant matrix의 symmetricity까지 써가며 시간복잡도를 반절 더 깎는

³4.2.1 등에서 관련 트릭에 대해 보다 자세히 이야기합니다.

것을 의도한 문제는 아녜습니다.⁴ 정해 코드에서는 따로 그런 방식의 최적화를 가한 바는 없지만, 구현에 따른 연산량의 차이를 제대로 고려하지 않았던 점을 인정합니다. 특히 N 의 상한을 $5 \cdot 10^5$ 로 잡았던⁵ 실수는 검수 기간동안 충분히 바로잡을 수 있던 부분이고 동시에 중대한 사안 이기에, 대회시작직전에다우용문제샘플영상만드느라문제올라간것도제대로검수안했냐라는 비판은 겸허히 받아들이도록 하겠습니다.

⁴ 덕분에 살았습니다 대회 때 풀어 주셔서 너무 감사합니다 그리고 진심으로 죄송합니다 다시는 이런 일 없도록 하겠습니다

⁵ 보다 엄밀히, 약수 조건에 의해 $N = 487424$ 가 최대입니다.

多次元宇宙融合論(다차원우주융합론) [I]

네...업슬빙만 해주셔도 고맙죠 당연히...

문제부터 이쁘게 바꾸고 시작하겠습니다:

문제

입력으로 N 개의 정점을 가지는 undirected simple connected graph G 와 수열 $A_0, A_1, \dots, A_{K-1}$ 이 주어진다. 이때 G 의 Laplacian matrix L_G 의 eigenvalue를 $0 = \lambda_0 < \lambda_1 \leq \dots \leq \lambda_{N-1}$ 라 하자. (단, $1 \leq k \leq N-1$ 에 대해 $\sum_{i=1}^{N-1} \lambda_i^{-k} \not\equiv 0 \pmod{p=998\,244\,353}$)임이 보장된다.)

N' 개의 정점을 가지는 **connected complete multipartite graph** H 와 H 의 Laplacian matrix L_H 의 eigenvalue $0 = \mu_0 < \mu_1 \leq \dots \leq \mu_{N'-1}$ 에 대하여, 다음의 다항식^a

$$\frac{1}{NN'} \prod_{\substack{0 \leq i < N \\ 0 \leq j < N' \\ (i,j) \neq (0,0)}} (\lambda_i + \mu_j x) \in \mathbb{F}_p[x]$$

의 0차항부터 $K-1$ 차항까지의 계수가 수열 A_k 와 일치하도록 하는 가능한 H 의 개수를 998 244 353으로 나눈 나머지를 구하여라.

정해 시간복잡도 $\mathcal{O}(N^3 + N' \log^2 N')$

출제자 rootenter

^a G 와 H 의 cartesian product에 matrix-tree theorem을 적용해서 얻을 수 있는 결과입니다. 바로 resultant 박고 들어가서 해석하는 방법도 있긴한데, 개인적으로 그다지 자연스러운 접근처럼 받아들여지지는 않습니다.

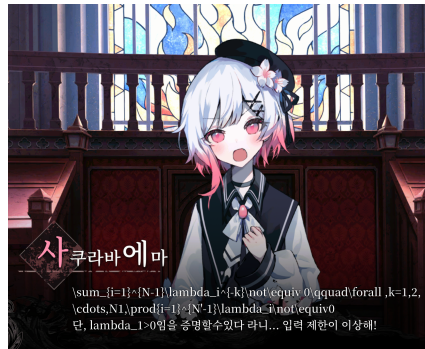


Figure 4.1: Suspicious Integer Constriction.¹

본 문제를 풀이 과정을 두 부분으로 나누어 해설하겠습니다. 근데 뒷 부분을 우선 보는데 spectral graph theory의 감을 잡아가기에는 좋을 거예요. 그런고로...

4.1 Part B. Analysis on the Spectrum of H and its Uniqueness

4.2에서 $h(x)$ 를 계산하는 과정은 마무리되었다고 전제하겠습니다. 본 절에서는 아래의 사실을 증명합니다:

Proposition 4.1.1. 서로 다른 N' 개의 정점을 가지는 (connected) complete multipartite graph $H = K_{\{n_1, \dots, n_k\}}$ 와 H 의 Laplacian matrix L_H 에 대하여 L_H 의 N' 개 eigenvalue 만이 주어질 때 multiset $\{n_1, n_2, \dots, n_k\}$ 를 복원할 수 있으며 동시에 이의 유일성 역시 보장된다. 따라서 가능한 그래프 H 의 개수는

$$\frac{N'!}{\prod_{\alpha} n_{\alpha}! \cdot \prod_{\beta} m_{\beta}!} \cdot^a$$

(단, $\sum_{\alpha} n_{\alpha} = N'$, $m_{\beta} = \sum_{\alpha} [n_{\alpha} = \beta]$.)

^a H 내의 각 independent set 각각의 크기와 그의 multiplicity를 나타내는 multiset이 주어진다면 라벨링만을 고려하면 됩니다. 이는 어렵지 않게 유도 가능한 결과이므로 이를 보이는 과정으로 문단을 더 할애하지는 않겠습니다. (본 식은 cycle type을 고려한 permutation의 개수와 동치임에 주목합니다)

결국 위 명제를 증명하기 위해선 $\{n_1, n_2, \dots, n_k\}$ 와 L_H 의 스펙트럼 사이의 대응 관계를 찾는 것이 주된 목표가 됩니다. 이를 위해 행렬을 미리 세팅해두고 들어가죠.

그래프 H 의 degree matrix D_H 와 adjacency matrix A_H 를 각각 다음과 같이 나타낼 수 있습니다.²

$$D_H = \bigoplus_{\alpha=1}^k (N' - n_{\alpha}) \cdot I_{n_{\alpha}}$$

$$A_H = J_{N'} - \bigoplus_{\alpha=1}^k J_{n_{\alpha}}$$

결과적으로 H 의 Laplacian L_H 는

$$\begin{aligned} L_H &= D_H - A_H \\ &= \left(\bigoplus_{\alpha=1}^k (N' - n_{\alpha}) \cdot I_{n_{\alpha}} \right) - \left(J_{N'} - \bigoplus_{\alpha=1}^k J_{n_{\alpha}} \right) \\ &= \bigoplus_{\alpha=1}^k \left[(N' - n_{\alpha}) \cdot I_{n_{\alpha}} + J_{n_{\alpha}} \right] - J_{N'}. \end{aligned}$$

그럼... 시작해볼까요?

¹해당 제약이 필요하다는 사실은 sharae1ong님께서 검수 과정에서 발견해주셨습니다.

²편의를 위해 $\text{diag}(M_1, \dots, M_k)$ 와 같이 쓰는 대신 $\bigoplus_{\alpha=1}^k M_{\alpha}$ 로 인덱스를 축약해 서술하였음에 유의.

4.1.1 Solution 1. Various Algebraic Tricks for Random Eigenspaces

임의의 행렬로부터 eigenvalue를 이쁘게 뽑아내는 과정은 언제나 주어진 행렬을 여러 부분들로 쪼개는 것이었습니다. 이하 단락은 전부 계산의 영역에 속합니다.

당장 L_H 의 eigenvalue를 전부 계산하기엔 직전 식에서 마지막 $-J_{N'}$ 이라는 항이 대단히 신경쓰이네요. 행렬 $\tilde{L}_H$ 를 미리 정의하고 들어가도록 하겠습니다.

$$\begin{aligned}\tilde{L}_H &= L_H + J_{N'} \\ &= \bigoplus_{\alpha=1}^k \left[(N' - n_\alpha) \cdot I_{n_\alpha} + J_{n_\alpha} \right].\end{aligned}$$

지금부터는 $\tilde{L}_H$ 의 스펙트럼을 근으로 가지는 다항식 $\chi_{\tilde{L}_H}(x)$ 를 계산하고 싶습니다. Characteristic polynomial이란 말조차 사치일지도 모르죠. ~~카역행렬의 동치조건을 15개 이상 읊자 못하는 자는 아 에디를 읽을 자격이 없다.~~³

$$\begin{aligned}\chi_{\tilde{L}_H}(x) &= \det \left(x \cdot I_{N'} - \bigoplus_{\alpha=1}^k \left[(N' - n_\alpha) \cdot I_{n_\alpha} + J_{n_\alpha} \right] \right) \\ &= \det \left(\bigoplus_{\alpha=1}^k \left[(x - N' + n_\alpha) \cdot I_{n_\alpha} - J_{n_\alpha} \right] \right) \\ &= \prod_{\alpha=1}^k \left[\det \left((x - N' + n_\alpha) \cdot I_{n_\alpha} - J_{n_\alpha} \right) \right]\end{aligned}$$

적당히 할 수 있는 만큼 정리한 듯합니다.

지금부터는 다음의 정리로부터 유도되는 성질을 이용해 행렬의 스펙트럼을 빠르게 계산해 보겠습니다.

Lemma 4.1.2 (Matrix determinant lemma). *Let $M \in \text{GL}_n(\mathbb{F})$ and $u, v \in \mathbb{F}^n$. Then the following equation holds:*

$$\det(M + uv^\top) = \det(M) (1 + v^\top M^{-1}u).$$

Proof. Set $w = M^{-1}u$. Factoring M from the matrix gives

$$\det(M + uv^\top) = \det(M) \det(I_n + wv^\top).$$

Write $v = (v_1, \dots, v_n)^\top$. The j -th column of $I_n + wv^\top$ is $\mathbf{e}_j + v_j w$. By multilinearity of the determinant, every term containing w in two or more columns vanishes. Hence

$$\begin{aligned}\det(I_n + wv^\top) &= 1 + \sum_{j=1}^n v_j \det(e_1, \dots, e_{j-1}, w, e_{j+1}, \dots, e_n) \\ &= 1 + \sum_{j=1}^n v_j w_j = 1 + v^\top w.\end{aligned}$$

³물론 농담입니다. 다만 몇개 외워두어서 나쁠 건 없구요. 선형대수학에 약하더라도 적어도 이 단락만큼은 충분히 이해할 수 있도록 editorial을 작성해보죠.

Substituting $w = M^{-1}u$ proves the claim. $\square$

음... 에디가 점점 지루해질 참이니 TeX 차력쇼로 주의를 끌겠습니다.

JUST 계산

직전의 식에서 마지막으로 정리한 부분부터 시작하겠습니다. Matrix determinant lemma에 $u = -\mathbf{1}_{n_\alpha}$, $v = \mathbf{1}_{n_\alpha}$ 을 대입하면,

$$M_\alpha(x) := (x - N' + n_\alpha)I_{n_\alpha} - J_{n_\alpha},$$

$$\begin{aligned}\chi_{\tilde{L}_H}(x) &= \prod_{\alpha=1}^k \det M_\alpha(x) \\ &= \prod_{\alpha=1}^k \left[(x - N' + n_\alpha)^{n_\alpha-1} \cdot (x - N') \right] \\ &= (x - N')^k \prod_{\alpha=1}^k (x - N' + n_\alpha)^{n_\alpha-1}.\end{aligned}$$

한편,

$$R_\alpha(x) := (x - N' + n_\alpha)I_{n_\alpha} - J_{n_\alpha}$$

로 두면 4.1.3에 의해 다음이 성립합니다:

$$R_\alpha(x)\mathbf{1}_{n_\alpha} = (x - N')\mathbf{1}_{n_\alpha}.$$

양변에 $\mathbf{1}_{n_\alpha}^\top R_\alpha(x)^{-1}$ 를 곱하여 정리하면,

$$\mathbf{1}_{n_\alpha}^\top R_\alpha(x)^{-1}\mathbf{1}_{n_\alpha} = \frac{n_\alpha}{x - N'}.$$

이제 4.1.2.2로부터 $\chi_{L_H}(x)$ 역시 closed form으로 나타낼 수 있습니다.

외워.

Corollary 4.1.2.1. *By substituting M with kI_n and $u = v = \mathbf{1}$ at 4.1.2,*

$$\det(k \cdot I_n + \mathbf{1}_n \mathbf{1}_n^\top) = k^{n-1}(k + n),$$

where scalar $k \in \mathbb{F}$.

Corollary 4.1.2.2. *And a more general statement of 4.1.2.1,*

$$\det(M + \mathbf{1}_n \mathbf{1}_n^\top) = \det(M) \left(1 + \mathbf{1}_n^\top M^{-1} \mathbf{1}_n \right),$$

where $M \in \text{GL}_n(\mathbb{F})$.

Lemma 4.1.3. *Let $M \in \text{GL}_n(\mathbb{F})$, then $\mathbf{1}_n$ is an eigenvector of M iff there exists $\lambda \in \mathbb{F}$ such that every row of M has the same sum λ . Moreover, λ is its eigenvalue corresponding to $\mathbf{1}_n$.*

Proof. $M\mathbf{1}_n = \lambda\mathbf{1}_n$ ⁴ $\square$

$$\begin{aligned}\implies \chi_{L_H}(x) &= \det \left(xI_{N'} - \tilde{L}_H + J_{N'} \right) \\ &= \det \left(xI_{N'} - \tilde{L}_H \right) \cdot \left(1 + \mathbf{1}_{N'}^\top \left(xI_{N'} - \tilde{L}_H \right)^{-1} \mathbf{1}_{N'} \right) \\ &= \det \left(xI_{N'} - \tilde{L}_H \right) \cdot \left(1 + \mathbf{1}_{N'}^\top \left(\bigoplus_{\alpha=1}^k \left[(x - N' + n_\alpha) \cdot I_{n_\alpha} - J_{n_\alpha} \right] \right)^{-1} \mathbf{1}_{N'} \right) \\ &= \det \left(xI_{N'} - \tilde{L}_H \right) \cdot \left(1 + \sum_{\alpha=1}^k \left(\mathbf{1}_{n_\alpha}^\top \left[(x - N' + n_\alpha) \cdot I_{n_\alpha} - J_{n_\alpha} \right]^{-1} \mathbf{1}_{n_\alpha} \right) \right) \\ &= \det \left(xI_{N'} - \tilde{L}_H \right) \cdot \left(1 + \sum_{\alpha=1}^k \left(\frac{n_\alpha}{x - N'} \right) \right)\end{aligned}$$

³오른쪽 옆에 정리해둔 것들은 그래도 척추 반사로 나오게끔 외워두시는 걸 권유드려요. 분명 여전히 쉽게 보일 수 있는 결과들이긴 하지만요.

$$\begin{aligned}
&= \chi_{\tilde{L}_H}(x) \cdot \left(1 + \frac{N'}{x - N'}\right) \\
&= (x - N')^k \prod_{\alpha=1}^k (x - N' + n_\alpha)^{n_\alpha-1} \cdot \left(\frac{x}{x - N'}\right) \\
&= \boxed{\boxed{\boxed{x(x - N')^{k-1} \prod_{\alpha=1}^k (x - N' + n_\alpha)^{n_\alpha-1}.}}}
\end{aligned}$$

결과적으로 H 의 전체 스펙트럼 성분은 다음의 multiset으로 나타나며, 4.1.1의 증명이 완결됩니다.

$$\text{Spec}(H) = \left\{0^{(1)}, N'^{(k-1)}\right\} \cup \left(\bigcup_{\alpha=1}^k \left\{(N' - n_\alpha)^{(n_\alpha-1)}\right\}\right)$$

뿐만 아니라, 가능한 스펙트럼의 종류는 많아야 약 N' 개에 불과하기에⁴, multipoint evaluation으로 4.2에서 계산한

$$h(x) = \tau(H) \prod_j (1 + \mu_j x)^{e_j}$$

의 서로 다른 근 $-\mu_j^{-1}$ 들을 모두 구해낼 수 있습니다.⁵ 그리고 separable polynomial⁶ $h_2(x) = \prod_j (x + \mu_j^{-1})$ 를 생각하면 FPS의 연산으로부터

$$\left(\frac{dh}{dx}(x) \cdot h_2(x)\right) \cdot (h(x))^{-1} \Big|_{x=-\mu_j^{-1}}$$

를

$$\frac{dh_2}{dx}(x) \Big|_{x=-\mu_j^{-1}}$$

로 나눈 값이 e_j 가 됩니다.⁷ 이 부분에서 시간복잡도는 $\mathcal{O}(N' \log^2 N')$ 입니다.

⁴여기서 간혹 일부 그래프 문제에서의 최적화 방법론으로 활용되는 sqrt decomposition을 생각해볼 수도 있겠습니 다만... 적어도 이 문제의 풀이로서 요구된 내용은 아닙니다.

⁵ $h(x)$ 의 최소항들만을 구할 수 있는 상황임에도 이것이 가능함에 주목합니다.

⁶여기서 separable이란 multiple root를 가지지 않음을 의미합니다.

⁷음... 어떤 좋은 발상이 존재한다고 주장하기 이전에, 이를 대체할 만한 ‘거의 같은’ 식이 몇가지가 있긴 합니다. 예컨대 $e_j = \lim_{x \rightarrow -\mu_j^{-1}} (x + \mu_j^{-1}) \frac{h'(x)}{h(x)}$ 라던가...? 아니면 $e_j = \lim_{x \rightarrow -\mu_j^{-1}} \frac{\log |h(x)|}{\log |x + \mu_j^{-1}|}$ 도 되긴 하겠네요. 따지고 보면 holomorphic object를 다룬다는 느낌이 대단히 강하죠. (이것이 Residue theorem의 corollary가 아닌가하는 의심은 4.2.3에서부터는 보다 표면적으로 드러낼 만합니다.)

4.1.2 Solution 2. by MO native

solution writer: applebananas

직전 풀이와 본질적으로 크게 어긋나지 않는 풀이입니다. 그러나 생각해볼만한 직관이 다수 존재하여 복붙해서 노테이션 통일 후 첨부합니다. 결론부에 해당하는 4.1.11에서 4.1.1의 증명이 마무리됩니다.

갑작스러운 부탁에도 상당한 분량의 풀이를 즉시 제공해주신 신성고등학교 강지성님께 감사드립니다.

Theorem 4.1.3. Complete multipartite graph $H = K_{\{n_1, \dots, n_k\}}$ 의 L_H 행렬의 고윳값들의 multiset가 주어지면 $\{n_1, \dots, n_k\}$ 의 multiset 또한 유일하게 결정된다.

Proof. 모든 성분이 1인 n 차 정사각행렬을 편의 상 J_n , $n_1 + \dots + n_k = N'$ 라 하며 각 분할을 각각 $V_1, \dots, V_k$ 라 정의하자.

H 는 Complete multipartite graph이므로 서로 다른 분할의 원소끼리는 무조건 간선이 1개 존재해야하며 같은 분할의 원소끼리는 간선이 존재해선 안 된다.

고로, 인접행렬 $A_H = J_{N'} - \text{diag}(J_{n_1}, \dots, J_{n_k})$ 로 나타낼 수 있다.

이를 라플라시안 행렬의 정의에 대입하면 $L_H = D_H - A_H = D_H - J_{N'} + \text{diag}(J_{n_1}, \dots, J_{n_k}) = P - J_{N'}$ 로 쓸 수 있다.

이때 $P = D_H + \text{diag}(J_{n_1}, \dots, J_{n_k})$ 인데 D_H 는 차수행렬로 대각행렬이기에 P 는 여전히 블록 대각행렬이며 각 성분의 경우에는 H 가 Complete multipartite graph이므로 i 번째 대각 블록은 $d_i I_{n_i} + J_{n_i}$ 이고 나머지는 0이다.

따라서 블록 대각행렬의 성질과 H 가 Complete multipartite graph임에 의하면 $P = P^T$, 즉 P 가 대칭행렬임을 알 수 있다.

Lemma 4.1.4. P 와 $J_{N'}$ 는 서로 가환한다.

Proof. $J_{N'} = \mathbf{1}\mathbf{1}^T$ 고 P 의 각 행의 성분들의 합은 H 가 Complete multipartite graph임에 의해 N' 이므로 $P\mathbf{1} = N'\mathbf{1}$ 이다.

따라서, $PJ_{N'} = P\mathbf{1}\mathbf{1}^T = N'\mathbf{1}\mathbf{1}^T = N'J_{N'}$ 이고 $J_{N'}P = \mathbf{1}\mathbf{1}^TP = \mathbf{1}(P^T\mathbf{1})^T = \mathbf{1}(N'\mathbf{1})^T = N'\mathbf{1}\mathbf{1}^T = N'J_{N'}$ 이므로 $PJ_{N'} = J_{N'}P$ 라 위 명제는 참이다. $\square$

고로 Lemma 4.1.4에 의해 임의의 자연수 p 에 대해 $L_H^p = (P - J_{N'})^p = P^p + \sum_{r=1}^p \binom{p}{r} P^{p-r} (-J_{N'})^r$ 다.

Lemma 4.1.5. 임의의 자연수 $r \leq p$ 에 대해 $J_{N'}^r = N'^{r-1}J_{N'}$, $P^{p-r}J_{N'} = N'^{p-r}J_{N'}$ 다.

Proof. 1. $J_{N'}^r = N'^{r-1}J_{N'}$: $J_{N'}^r = (\mathbf{1}\mathbf{1}^T)(\mathbf{1}\mathbf{1}^T) \dots (\mathbf{1}\mathbf{1}^T) = \mathbf{1}(\mathbf{1}^T\mathbf{1})^T(\mathbf{1}^T\mathbf{1})^T \dots (\mathbf{1}^T\mathbf{1})^T\mathbf{1}^T = \mathbf{1}N'^{r-1}\mathbf{1}^T = N'^{r-1}\mathbf{1}\mathbf{1}^T = N'^{r-1}J_{N'}$ 라 위 명제는 참이다.

2. $P^{p-r}J_{N'} = N'^{p-r}J_{N'}$: $P\mathbf{1} = N'\mathbf{1}$ 에 $\mathbf{1}^T$ 를 곱하면 $PJ_{N'} = N'J_{N'}$ 라 $P^{p-r}J_{N'} = P(P \dots (PJ_{N'}) \dots) = N'^{p-r}J_{N'}$ 이므로 위 명제는 참이다. $\square$

Lemma 4.1.6. $L_H^p = P^p - N'^{p-1}J_{N'}$

Proof. 고로 $L_H^p = (P - J_{N'})^p = P^p + \sum_{r=1}^p \binom{p}{r} P^{p-r} (-J_{N'})^r$ 를 Lemma 4.1.5을 이용해 변형하면 $S = \sum_{r=1}^p \binom{p}{r} P^{p-r} (-J_{N'})^r = \sum_{r=1}^p (-1)^r \binom{p}{r} P^{p-r} N'^{r-1} J_{N'} = N'^{p-1} J_{N'} \sum_{r=1}^p \binom{p}{r} (-1)^r$ 인데, 이항정리에 의해 $\sum_{r=0}^p \binom{p}{r} (-1)^r = 0$ 라 $S = -N'^{p-1} J_{N'}$ 이기에 $L_H^p = P^p - N'^{p-1} J_{N'}$ 이므로 위 명제는 참이다. $\square$

Lemma 4.1.7. 그래프 H 의 L_H 행렬의 고윳값들의 multiset이 주어지면, 임의의 자연수 p 에 대해 $\text{tr}(L_H^p)$ 의 값 또한 유일하게 결정된다.

Proof. 고윳값의 성질에 의해 $\text{tr}(L_H) = \sum_{i=1}^{N'} \mu_i$ 인데 고윳값의 성질에 의해 $\text{tr}(L_H^p) = \sum_{i=1}^{N'} \mu_i^p$ 며 고윳값들의 multiset이 주어졌으므로 이 값은 상수이며, 편의상 M_p 라 하자. $\square$

이제 $S_p = \sum_{v \in V} d_v^p$ 라 정의하면 H 는 Complete multipartite graph이므로 이는 $\sum_{i=1}^k n_i d_i^p = \sum_{i=1}^k (N' - d_i) d_i^p = N' \sum_{i=1}^k d_i^p - \sum_{i=1}^k d_i^{p+1}$ 이다.

또한, $T_p = \sum_{i=1}^k d_i^p$ 라 정의하면 위 식을 $T_{p+1} = N' T_p - S_p$, $T_0 = k$, $S_0 = N'$ 로 간략하게 정리할 수 있다.

Lemma 4.1.8. $T_{p+1} = N' T_p - S_p$, $T_0 = k$, $S_0 = N'$ 를 만족하는 수열 T_p 의 일반항은 $T_p = N'^p(k-1) - \sum_{i=1}^{p-1} N'^{p-1-i} S_i$ 다.

Proof. 수학적 귀납법으로 증명하자.

우선 $p = 1$ 인 경우 $T_1 = N'k - N' = N'(k-1)$ 이라 자명하게 참이다.

다음으로 p 일 때 참이라 가정하면 $p+1$ 일 때도 성립함을 보이자.

위 점화식에 일반항을 대입하면 $T_{p+1} = N'(N'^p(k-1) - \sum_{i=1}^{p-1} N'^{p-1-i} S_i) - S_p = N'^{p+1}(k-1) - \sum_{i=1}^{p-1} N'^{p-i} S_i - N'^{p-p} S_p = N'^{p+1}(k-1) - \sum_{i=1}^p N'^{p-i} S_i$ 라 위 명제는 참이다. $\square$

또한, M_p 의 정의와 Lemma 4.1.6에 의해 $M_p = \text{tr}(L_H^p) = \text{tr}(P^p) - N'^{p-1} \text{tr}(J_{N'})$ 인데 $J_{N'}$ 의 정의에 의해 $\text{tr}(J_{N'}) = N'$ 이므로 $M_p = \text{tr}(P^p) - N'^p$ 이다.

이때 P 는 블록 대각행렬이므로 각 블록 행렬 $B_i = d_i I_{n_i} + J_{n_i}$ 에 대해 $\text{tr}(P^p) = \sum_{i=1}^k \text{tr}(B_i^p)$ 이다.

Lemma 4.1.9. $\text{tr}(B_i^p) = n_i d_i^p + N'^p - d_i^p$

Proof. $B_i = d_i I_{n_i} + J_{n_i}$ 인데, I_{n_i} 는 단위행렬이므로 자명히 I_{n_i} 와 J_{n_i} 는 서로 가환한다.

따라서, 위와 같은 논리로 $B_i^p = (d_i I_{n_i} + J_{n_i})^p = \sum_{r=0}^p \binom{p}{r} (d_i I_{n_i})^{p-r} J_{n_i}^r = \sum_{r=0}^p \binom{p}{r} d_i^{p-r} J_{n_i}^r$ 다.

이때 Lemma 4.1.5에 의해 자연수 r 에 대해 $J_{n_i}^r = n_i^{r-1} J_{n_i}$ 가 성립하므로 이를 대입하면 $B_i^p = \binom{p}{0} d_i^p I_{n_i} + \sum_{r=1}^p \binom{p}{r} d_i^{p-r} n_i^{r-1} J_{n_i}$ 다.

이제 양변에 대각합을 취하면 $\text{tr}(B_i^p) = d_i^p \text{tr}(I_{n_i}) + \sum_{r=1}^p \binom{p}{r} d_i^{p-r} n_i^{r-1} \text{tr}(J_{n_i}) = n_i d_i^p + \sum_{r=1}^p \binom{p}{r} d_i^{p-r} n_i^{r-1} \cdot n_i = n_i d_i^p + \sum_{r=1}^p \binom{p}{r} d_i^{p-r} n_i^r$ 다.

그런데 이항 정리에 의해 $\sum_{r=1}^p \binom{p}{r} d_i^{p-r} n_i^r = (d_i + n_i)^p - d_i^p$ 인데 H 가 Complete multipartite graph이기에 $\text{tr}(B_i^p) = n_i d_i^p + N'^p - d_i^p$ 이므로 위 명제는 참이다. $\square$

이제 여기에 Lemma 4.1.9을 대입하면 $\text{tr}(P^p) = \sum_{i=1}^k (n_i d_i^p + N'^p - d_i^p) = S_p + kN'^p - T_p$ 다.

이를 $M_p = \text{tr}(P^p) - N'^p$ 에 대입하면, $M_p = S_p + kN'^p - T_p - N'^p = S_p + (k-1)N'^p - T_p$ 다.

이제 여기에 Lemma 4.1.8를 대입하면 $M_p = S_p + (k-1)N'^p - (k-1)N'^p + \sum_{i=1}^{p-1} N'^{p-1-i} S_i = S_p + \sum_{i=1}^{p-1} N'^{p-1-i} S_i$ 다.

이때 M_p 는 상수이므로 자명히 S_p 는 상수와 S_1 부터 S_{p-1} 들로만 표현이 가능하며 $S_0 = N'$ 이므로 모든 S_i 는 유일하게 결정된다.

Lemma 4.1.10. k 의 값을 수열 T_p 와 무관하게 구할 수 있다.

Proof. 우선 $k = 1$ 인 경우는 자명하므로 $k \geq 2$ 에 대해서만 논하자.

n_i 들 사이에서도 중복이 있을 수 있으니, $S_p = \sum_{i=1}^m m_i \tilde{n}_i \tilde{d}_i^p = \sum_{i=1}^m W_i \tilde{d}_i^p$ 로 준식을 변형할 수 있다.

이는 특성다항식 $S_{p+m} + c_{m-1}S_{p+m-1} + \dots + c_1S_{p+1} + c_0S_p = 0$ 이 성립한다.

이제

$$H_r = \begin{pmatrix} S_1 & S_2 & \cdots & S_r \\ S_2 & S_3 & \cdots & S_{r+1} \\ \vdots & \vdots & \ddots & \vdots \\ S_r & S_{r+1} & \cdots & S_{2r-1} \end{pmatrix}$$

인 한켈 행렬 H_r 을 정의하면, 한켈 행렬의 행렬식의 성질과 위 특성다항식에 의해 $\det\{H_r\} \neq 0$, $\det\{H_{r+1}\} = 0$ 을 만족하는 r 값이 항상 존재하며, 이 값이 m 임을 알 수 있다.

즉, m 은 알고리즘을 통해 구할 수 있다.

$$m \text{이 정해지면 } \begin{pmatrix} S_1 & \cdots & S_m \\ \vdots & \ddots & \vdots \\ S_m & \cdots & S_{2m-1} \end{pmatrix} \begin{pmatrix} c_0 \\ \vdots \\ c_{m-1} \end{pmatrix} = - \begin{pmatrix} S_{m+1} \\ \vdots \\ S_{2m} \end{pmatrix} \text{이므로 특성다항식의 계수 또}$$

한 유일하게 결정되며, 고로 $P(x) = x^m + c_{m-1}x^{m-1} + \dots + c_0 = 0$ 의 해는 자연수며 최대 $N' - 1$ 이므로 유한 시도 내에 결정이 가능하다.

따라서 이를 통해 그래프가 가능한 차수들의 set을 알 수 있다.

$$\text{모든 } \tilde{d}_j \text{는 서로 다른으로, } \begin{pmatrix} \tilde{d}_1 & \tilde{d}_2 & \cdots & \tilde{d}_m \\ \tilde{d}_1^2 & \tilde{d}_2^2 & \cdots & \tilde{d}_m^2 \\ \vdots & \vdots & \ddots & \vdots \\ \tilde{d}_1^m & \tilde{d}_2^m & \cdots & \tilde{d}_m^m \end{pmatrix} \begin{pmatrix} W_1 \\ W_2 \\ \vdots \\ W_m \end{pmatrix} = \begin{pmatrix} S_1 \\ S_2 \\ \vdots \\ S_m \end{pmatrix} \text{인데 이때}$$

$$\text{방테르몽드 행렬의 행렬식이 0이 아니므로 이는 가역행렬이고 따라서 } \begin{pmatrix} W_1 \\ \vdots \\ W_m \end{pmatrix} =$$

$$\begin{pmatrix} \tilde{d}_1 & \cdots & \tilde{d}_m \\ \vdots & \ddots & \vdots \\ \tilde{d}_1^m & \cdots & \tilde{d}_m^m \end{pmatrix}^{-1} \begin{pmatrix} S_1 \\ \vdots \\ S_m \end{pmatrix} \text{로 } W_i \text{들을 유일하게 결정할 수 있으며, } \tilde{n}_j = N' - \tilde{d}_j \text{라 이}$$

또한 유일하게 결정되므로 $m_j = \frac{W_j}{\tilde{n}_j}$ 로 이 또한 유일하게 결정되며 $k = \sum_{j=1}^m m_j$ 또한

유일하게 결정되므로 위 명제는 참이다. $\square$

따라서, Lemma 4.1.8와 Lemma 4.1.10에 의해 T_i 또한 유일하게 결정된다.

즉, T_1 부터 T_k 까지 유일하게 결정되는데 이는 뉴턴의 항등식에 의해 차수 $d_1, \dots, d_k$ 를 근으로 가지는 k 차 다항식 $f(x) = \prod_{i=1}^k (x - d_i)$ 의 계수를 유일하게 결정할 수 있다.

$\mathbb{Z}[x]$ 는 UFD라 인수분해는 유일하므로 $\{d_1, \dots, d_k\}$ 의 multiset은 유일하게 결정되며, H 는 Complete multipartite graph이므로 자명히 $\{n_1, \dots, n_k\}$ 의 multiset 또한 유일하게 결정되기에 위 명제는 참이다. $\square$

Remark 4.1.1. 사실 그냥 Lemma 4.1.10이 증명되면 $\{d_1, \dots, d_k\}$ 의 multiset가 바로 나오므로 위처럼 돌아갈 필요가 없지만, 그냥 뉴턴 항등식 아이디어를 살리고 싶었다...

Theorem 4.1.11. 서로 다른 N' 개의 정점을 가지고 있는 Complete multipartite graph $H = K_{\{n_1, \dots, n_k\}}$ 의 L_H 행렬의 고윳값들의 multiset이 주어졌을 때 가능한 그래프 H 의 개수는 $\{n_1, \dots, n_k\}$ 의 서로 다른 값을 $s_1, \dots, s_m$ 이라 하고 이 값들의 중복도를 각각 $m_1, \dots, m_m$ 이라 하면 $\frac{N'!}{(n_1!n_2!\dots n_k!)\cdot(m_1!m_2!\dots m_m!)}$ 개다.

Proof. Theorem 4.1.3에 의해, 정점을 구별하지 않을 경우 가능한 모든 그래프는 동형이다.

따라서 정점을 배열하는 경우의 수가 답이다.

이는 N' 개의 라벨을 우선 $n_1, n_2, \dots, n_k$ 개만큼 k 개의 조로 분조한 후, 이 조는 구별이 불가능하기에 같은 개수의 조끼리의 중복도 또한 제한하여야하므로 $\frac{N'!}{(n_1!n_2!\dots n_k!)\cdot(m_1!m_2!\dots m_m!)}$ 이기에 위 명제는 참이다. $\square$

답: $\frac{N'!}{(n_1!n_2!\dots n_k!)\cdot(m_1!m_2!\dots m_m!)}$

4.2 Part A. 다항식에도 스펙트럼이 있다

우선 식을 정리합니다.

$$\begin{aligned}
 \frac{1}{NN'} \prod_{\substack{0 \leq i \leq N-1 \\ 0 \leq j \leq N'-1 \\ (i,j) \neq (0,0)}} (\lambda_i + \mu_j x) &= \left[\frac{1}{N} \prod_{\substack{1 \leq i \leq N-1 \\ j=0}} (\lambda_i + \mu_j x) \right] \left[\frac{1}{N'} \prod_{\substack{i=0 \\ 1 \leq j \leq N'-1}} (\lambda_i + \mu_j x) \right] \\
 &\quad \cdot \left[\prod_{\substack{1 \leq i \leq N-1 \\ 1 \leq j \leq N'-1}} (\lambda_i + \mu_j x) \right] \\
 &= \left[\frac{1}{N} \prod_{1 \leq i \leq N-1} \lambda_i \right] \cdot \left[\frac{1}{N'} \prod_{1 \leq j \leq N'-1} \mu_j x \right] \cdot \left[\prod_{\substack{1 \leq i \leq N-1 \\ 1 \leq j \leq N'-1}} (\lambda_i + \mu_j x) \right] \\
 &= \tau(G) \cdot \tau(H) x^{N'-1} \cdot \underbrace{\left[\prod_{\substack{1 \leq i \leq N-1 \\ 1 \leq j \leq N'-1}} (\lambda_i + \mu_j x) \right]}_{=: f(x)}.
 \end{aligned}$$

이때 위 식의 $N' - 1$ 차항은 $\tau(G)\tau(H)f_0$ 와⁸ 같고,

$$f_0 = \prod_{\substack{1 \leq i \leq N-1 \\ 1 \leq j \leq N'-1}} \lambda_i = (N \cdot \tau(G))^{N'-1}$$

임을 알고 있으므로 $\tau(H)$ 는 바로 구해줄 수 있습니다. 결과적으로 문제의 입력으로부터 $f(x) = \prod_{\substack{1 \leq i \leq N-1 \\ 1 \leq j \leq N'-1}} (\lambda_i + \mu_j x)$ 의 N' 차⁹까지의 항들을 뽑아낼 수 있습니다.

이어서 $g(x), h(x) \in \mathbb{F}_p[x]$ 도 다음과 같이 정의합시다:

$$g(x) = \prod_{i=1}^{N-1} (x + \lambda_i), \quad h(x) = \tau(H) \prod_{j=1}^{N'-1} (1 + \mu_j x).$$

$g(x)$ 는 입력으로 주어지는 G 로부터 계산될 수 있습니다. (다만 L_G 의 특성다항식 $\det(xI - L_G)$ 과는 다름에 유의.¹⁰)

우선 알려진 다항식 $f(x), g(x)$ 로부터 $h(x)$ 를 나타낼 수 있는지를 고민해보겠습니다. λ_i 의

⁸필요한 경우 앞으로는 $\mathbb{F}_p[x] \ni f(x) = \sum_i f_i x^i$ 와 같이 다항식의 계수 표현을 사용하겠습니다.

⁹보다 엄밀하게는 $K - N'$ 차. 실제 문제 조건에서는 $K \geq 2N'$ 까지만이 보장되었으므로 앞으로는 $K = 2N'$ 임을 전제하고 논의를 지속하겠습니다.

¹⁰다른게 아니라, 이렇게 두면 부호 세팅 훨씬 편해지잖아요. 능동적인 피계가 됩니다.

값을 직접 구하거나 계산하는 것은 피하기로 하죠.¹¹ 다음의 사실을 관찰합니다:

$$\begin{aligned} f(x) &= \prod_{j=1}^{N'-1} \prod_{i=1}^{N-1} (\lambda_i + \mu_j x) \\ &= \prod_{j=1}^{N'-1} g(\mu_j x) \end{aligned}$$

사람은 기본적으로 곱셈을 별로 좋아하지 않습니다. 다루기 쉬운 형태로 식을 변형하기 위해,

$$\begin{aligned} \hat{f}(x) &= \frac{f'(x)}{f(x)} \\ \hat{g}(x) &= \frac{g'(x)}{g(x)} \\ \hat{h}(x) &= \frac{h'(x)}{h(x)} \end{aligned}$$

를 정의해두겠습니다. 그럼 직전의 식을 열심히 만져보면,

$$\begin{aligned} \hat{f}(x) &= \sum_{j=1}^{N'-1} \mu_j \hat{g}(\mu_j x) \\ &= \sum_{j=1}^{N'-1} \mu_j \sum_{k \geq 0} \hat{g}_k (\mu_j x)^k \\ &= \sum_{k \geq 0} \hat{g}_k \left[\sum_{j=1}^{N'-1} \mu_j^{k+1} \right] x^k, \end{aligned}$$

결과적으로 음이 아닌 정수 k 에 대해 다음이 성립함을 알 수 있습니다.

$$\hat{f}_k = \hat{g}_k \left[\sum_{j=1}^{N'-1} \mu_j^{k+1} \right].$$

문제의 조건에 의해 필요한 범위에서 $\hat{g}_k$ 가 $\mathbb{F}_p$ 에서 0이 될 일은 없습니다!¹² 그럼 바로,

$$\frac{\hat{f}_k}{\hat{g}_k} = \left[\sum_{j=1}^{N'-1} \mu_j^{k+1} \right].$$

$h(x)$ 도 비슷하게 처리해보면,

$$\begin{aligned} \hat{h}(x) &:= \frac{h'(x)}{h(x)} \\ &= \sum_{j=1}^{N'-1} \frac{\mu_j}{1 + \mu_j x}. \end{aligned}$$

¹¹실제로, $\mathbb{F}_p[x]$ 내의 다항식의 근이 $\mathbb{F}_p$ 안에 들어있음이 보장되지 않기 때문에, λ_i 를 modulo p 에서 나타낼 일반적 방법은 없습니다.

¹²그 이유를 알겠나요?

여기서 formal power series의 기본적인 성질에 의해,

$$\begin{aligned}\sum_{j=1}^{N'-1} \frac{\mu_j}{1 + \mu_j x} &= \sum_{j=1}^{N'-1} \mu_j \sum_{k \geq 0} (-\mu_j x)^k \\ &= \sum_{k \geq 0} \left[\sum_{j=1}^{N'-1} \mu_j^{k+1} \right] (-x)^k \\ &= \sum_{k \geq 0} \left[\frac{\hat{f}_k}{\hat{g}_k} \right] (-x)^k.\end{aligned}$$

그럼 결론을 이렇게 정리해볼 수 있겠네요.

$$\therefore [x^k] \hat{h}(x) = (-1)^k \frac{\hat{f}_k}{\hat{g}_k}.$$

이제 $\hat{h}(x)$ 로 $h(x)$ 만 구하면 되나요? 야호!

그렇게 여러분이 알던 세상은 바로 이 자리에서 무너집니다.

4.2.1 (Wrong?) Solution 2. 어제 내 다항식이 무너졌어,

$\hat{h}(x)$ 를 고민도 없이 위와 같이 정의할 수 있었던 건 결국 우리가 로그 연산에 매우 친숙했기 때문입니다. 그리고 여전히 $h(x) = \tau(H) \prod_{j=1}^{N'-1} (1 + \mu_j x)$ 라는 식에서 양변에 로그를 씌우고 미분하는 과정은 열심히 부분분수분해를 가하는 것과 크게 다르지 않죠.¹³ 하지만 $\hat{h}(x)$ 로부터 $h(x)$ 를 역으로 구하는 것은 느낌이 달라보입니다. Log derivative의 역과정을 생각해보죠.

$$h(x) = e^{\int \hat{h}(x) dx}$$

바로 이 지점에서 여러분은 스스로에게 근본적인 질문을 던지게 됩니다:¹⁴

“어 샤갈 적분상수”

이 의문은 꽤나 critical하게 작용할 수밖에 없는 것이, 한동안 여러분은 $\frac{f'(x)}{f(x)}$ 같은 fractional representation을 줄곧 사용해왔으나, polynomial ring $\mathbb{F}_p[x]$ 위에서 식을 정리하고 있었음을 뒤늦게 깨닫기 때문이죠.

...이건 진짜 안 됩니다. 어차피 formal power series의 유일성은 조상님이 보장해줄 것이기 때문에¹⁵ $\exp$ 의 지수부를 $\int_0^x \hat{h}(s) ds + C$ 로 생각하고 양변에 $x = 0$ 수치대입을 하여 양변을 관찰하면 분명 적분상수 C 를 구해낼 수 있을 것입니다.

$$h(0) = e^{\int_0^x \hat{h}(s) ds + C} \Big|_{x=0}$$

그래야만 하겠죠 물론!

$$\iff \tau(H) = e^C \iff C = \log \tau(H) \in ? \mathbb{F}_p$$

¹³Notion of partial fraction decomposition. 여기서 유리식 표현의 유일성을 떠올릴 수만 있다면...

¹⁴출제자와 검수자 모두 문제 해결 과정에서 공통적으로 마주했던 난관이었습니다. 근데 [BOJ 33483]도 사실은...?

¹⁵...좀 드문 케이스이긴 한데, 이 때는 정말로 맞는 말이 되긴 합니다.

ㅋ.

4.2.2 Solution 1. 기본기에 관하여

병목이 생겼던 부분으로 돌아가겠습니다.

$$\frac{h'(x)}{h(x)} = \hat{h}(x)$$

지금까지 우리는 우변의 필요한 차수를 모두 계산하기 위해 $\hat{h}(x)$ 에 관한 정보를 정리해왔습니다. 그리고 지금 여러분이 찾고 싶은 건 $h(x)$ 의 coefficient representation $\sum_i h_i x^i$ 이죠.

근데요, 대체 누가 언제부터 다항식의 분수 표현을 써도 된다고 했죠? $h(x)$ 가 unit이라는 건 누가 귀뜸해준건가요? 원래는 이게 맞죠:

$$h'(x) - h(x) \cdot \hat{h}(x) = 0.$$

...그럼 시작해봅시다.

$X \in \mathbb{F}_p[x]$ 에 대하여 다음을 만족하는 operator¹⁶ $\Theta(-)$ 를 전제합니다:

$$\Theta'(X) = X' \cdot \Theta(X).$$

만약 그러한 $\Theta(-)$ 가 존재하기만 한다면, 아래의 방정식을 생각해볼 수 있습니다.

$$h(x) \cdot \Theta\left(-\int \hat{h}(x)dx\right) = C.$$

곧바로 양변을 미분하여,

$$\left(h'(x) - h(x)\hat{h}(x)\right) \cdot \Theta\left(-\int \hat{h}(x)dx\right) = 0.$$

그리고 이는 뭔가 $\Theta(X(x))$ 의 indeterminate x 에 대한 evaluation의 치역이 $\mathbb{R}^+$ 가 되어야 할 것만 같다는 본능을 따라가면 $h'(x) - h(x) \cdot \hat{h}(x) = 0$ 와 동치임을 확인할 수 있습니다.

음... 제가 방금 뭐라고 했죠? ¹⁷

$$h(x) = \tau(H) \cdot \exp\left(\int \hat{h}(x)dx\right)$$

표준적인 formal power series 구현체는 exp 연산에서 입력 다항식의 상수항이 0일 것을 요구합니다. 적분상수는 그냥 0으로 생각해도 충분하겠네요!

¹⁶...

¹⁷아무일도 없었다.

4.2.3 Solution 2. 나는 황족 미적러다

바로 직전 솔루션을 봤다면 이제 제대로 판단할 수 있겠습니다만

$$h(x) = e^{\int \hat{h}(x) dx + C},$$

이 식은 사실상

$$h(x) = C' e^{\int \hat{h}(x) dx}$$

와 다르지 않습니다. $\mathbb{F}_p[[x]]$ 의 연산은 상상이상으로 자유롭네요.¹⁸

4.2.4 이게 그렇게 어려운 건가요?

네.

...순수하게 formal power series의 combinatorial application 측면에서는 제가 감히 엄두조차 내지 못할 경지에서 뛰노는 **몇몇 인물들이** 떠오르기에, 위에서 서술한 내용이 다른 사람에게 어떻게 읽힐지는 잘 모르겠습니다. 다만 보편적으로 알려진 well-defined object로의 연산이 가해지는 공간이 *아주* 조금만 틀어져도 생길만한 의문은 확실히 여럿 존재합니다. 그 중 일부분을 집어왔다고 생각하면, 단락 전체를 자기 전에 이야기책 읽듯이 눈으로 훑어볼만한 가치는 충분합니다.¹⁹

¹⁸아마 본인이 알고있는 fps 연산의 종류를 읊는데는 6개 이상의 손가락을 필요로 하지 않을 거예요. 애초부터 우리에게 허용된 연산이 그리 많지 않다는 사실에 동의하나요?

¹⁹혹여나 본인이 불면증이 심한 축에 속한다면 바로 이어서 다음 문제도 같이 보시면 되고...요?

Extradimensional Cosmic Phenomenon

[H]

해당 문서의 제목은 ‘EDITORIAL (보급용)’입니다. 달리 말하자면 EDITORIAL (보급용)이라는 뜻이죠. 어떻게하면 필요한 내용을 전부 서술할 수 있지...?

아마 여기까지 정독하신 분들이라면 지금 느끼고 계시겠지만, 이번 MATH DOJ Contest에서 제가 출제한 문제들은 어느정도 비슷한 결을 가진 풀이를 공유하고 있습니다. 그리고 이 H번 같은 경우에는... 앞에서 과하다고 생각될 정도의 어떤 pseudo-intuition 기반의 장문 서술로 떡밥을 계속 던지게 된 계기에 해당하고요.

미리 고해하자면 이 문제는 정해로써 Cantor-Zassenhaus algorithm을 요구합니다.¹ 문제의 난이도가 앞선 문제보다 극단적으로 높아진 것은... 이것으로 충분히 설명이 되리라 생각합니다. 이 알고리즘에 관한 보다 자세한 내용은 kipa님의 [Number Theoretic Algorithms](#)에서 확인하실 수 있습니다. 이부터 revisit하기엔 당장 하고싶은 말이 너무 많아요.

그래서 ‘(유한체) 다항식 인수분해가 나올 구석이 대체 어디있냐’라는 물음에 말끔히 답할 수 있는 수준까지 실력을 끌어올리는 것을 본 단락의 주된 목표로 잡고, 적당한 선에서 에디토리얼을 마무리하도록 하겠습니다.

5.1 Polynomial Algebra

앞에서는 뭔가 있어보이는 theorem이나 lemma 같은 거 나올 때마다 영어로 써서 일부러 거리감을 줬었는데²... 이제부터는 정말 formal로 시작해서 formal로 끝내야한다네요. 우선 앞으로의 이야기는 integral domain³ D 위에서 이루어짐을 기억합니다.

Theorem 5.1.1 (Linear Extension Theorem). F -vector spaces V, W 와 V 의 basis $\mathcal{B}$ 가 주어졌다고 하자. 임의의 map $f : \mathcal{B} \rightarrow W$ 에 대하여 $\varphi|_{\mathcal{B}} = f$ 를 만족하는 linear map $\varphi : V \rightarrow W$ 가 유일하게 존재한다.^a

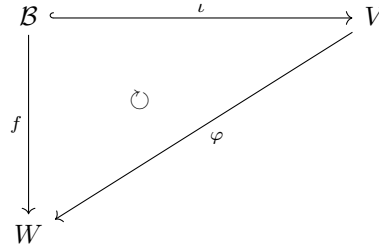
^a선형대수학을 공부하면 초반에 배우게 되는 기본적인 내용에 해당하기에 증명은 생략하겠습니다.

¹이후에는 다항식 CRT 앵강속수. [BOJ 33479] 마냥 막 maximal ideal이니 SES니 뭐니하면서 인수의 중복도까지 따져야하는 상황은 이 문제의 제약에서 발생하지 않습니다. 자세한 내용은 후술.

²Mathematical gatekeeping.

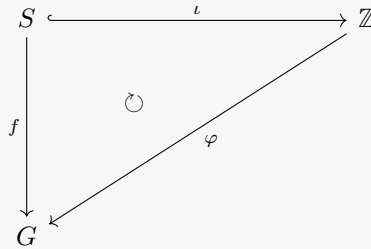
³Integral domain이란 0을 제외한 zero divisor를 가지지 않는 commutative ring을 뜻합니다. 외우기 귀찮으면 ‘뭔가 그럴싸한 수학적인 무언가를 제공할 수 있으면 아무튼 integral domain이다’라고 생각해도 당장은 문제 삼지 않습니다. Cancellation law나 곱셈의 commutativity를 주기 위한 마지노선에 있는 친구이기도 해요.

위 정리를 (inclusion을 ι 라 두면) 아래의 commutative diagram으로 나타낼 수도 있습니다.



간단하게 다른 algebraic structure에서의 적용례를 보고 가겠습니다.

Example 5.1.1. $S = \{1\} \subset \mathbb{Z}$ 라 할 때, 임의의 group G 와 임의의 map $f : S \rightarrow G$ 에 대하여 $\varphi \circ \iota = f$ 를 만족하는 group homomorphism $\varphi : \mathbb{Z} \rightarrow G$ 가 **유일하게** 존재한다.^a



^a이와 같이 structure 선택에 의존적이지 않는 것도 같은(!) 성질을 앞으로 universal property라고도 쓸 것입니다. 읽을 때는 ‘조상님 정리’라는 구어적 표현이 허용됩니다(아님).

함께 polynomial에 대한 이해를 점검하겠습니다.

Example 5.1.2. Commutative R -algebra $\mathcal{A}$ (with multiplicative identity $1_{\mathcal{A}}$)와 임의의 $\alpha \in \mathcal{A}$ 에 대하여 $\mathcal{E}_{\alpha}(x) = \alpha$ 를 만족하는 R -algebra homomorphism

$$\mathcal{E}_{\alpha} : R[x] \longrightarrow \mathcal{A}$$

이 유일하게 존재한다.

Proof. 다항식(..이던 혹은 linear map의 dual basis이던 등등)을 풀어쓰는 아이디어는 언제나 강력했기에...⁴ 다항식 $f(x) = \sum_i f_i x^i$ 에 대하여 $\mathcal{E}_{\alpha}$ 를 다음과 같이 정의합니다:

$$\mathcal{E}_{\alpha} \left(\sum_i f_i x^i \right) = \sum_i f_i \alpha^i$$

$\mathcal{E}_{\alpha}$ 가 R -algebra homomorphism임은 연산 관계에 의해 자명.

한편, 같은 조건을 만족하는 R -algebra homomorphism $\psi : R[x] \rightarrow \mathcal{A}$ 가 있다면

$$\psi \left(\sum_i f_i x^i \right) = \sum_i f_i \psi(x)^i = \sum_i f_i \alpha^i = \mathcal{E}_{\alpha} \left(\sum_i f_i x^i \right).$$

따라서 $\psi = \mathcal{E}_{\alpha}$, 즉 이러한 homomorphism은 (물론) 유일합니다. □

⁴4.2.

그러면 뭐... 애초부터 이렇게 놔도 무방하겠네요.

Definition 5.1.2. Commutative R -algebra $\mathcal{A}$ (with multiplicative identity $1_{\mathcal{A}}$)와 임의의 $\alpha \in \mathcal{A}$ 에 대하여 다음과 같이 정의된 $\mathcal{E}_{\alpha} : R[x] \rightarrow \mathcal{A}$ 는 R -algebra homomorphism이다:

$$\mathcal{E}_{\alpha}(f(x)) = f(\alpha),$$

그리고 이를 evaluation homomorphism (at α)라고 부른다.

또한, $f(x) \in R[x]$ 에 대하여 다음을 만족하는 $\alpha \in R$ 을 root (of $f(x)$)라고 부른다:

$$\mathcal{E}_{\alpha}(f(x)) = f(\alpha) = 0.$$

그리고 잠시 멈추어서 이 구조를 머릿속에 각인해두고, 그제서야 이후 단락을 읽어 내려가 시기를 조심스럽게 권유드립니다. 그럼 준비되셨나요?

5.2 with some Applications

Example 5.2.1 (Division Algorithms in $R[x]$). R 이 commutative ring (with 1)이고 $f(x), g(x) \in R[x]$ 이라 하자. 이때 만약 $g(x)$ 의 leading coefficient가 *unit*이면 다음을 만족하는 $q(x), r(x) \in R[x]$ 는 유일하게 존재한다:

$$f(x) = g(x) \cdot q(x) + r(x) \quad (\deg(r) < \deg(g)).$$

Example 5.2.2 (Remainder Theorem). R 이 commutative ring (with 1)이라 하자. 직전의 예로부터 $\alpha \in R$, $f(x) \in R[x]$ 에 대하여 다음을 만족하는 $q(x) \in R[x]$ 와 $r \in R$ 의 존재성과 유일성은 보장할 수 있다:

$$f(x) = (x - \alpha) \cdot q(x) + r.$$

그리고 양변에 evaluation homomorphism $\mathcal{E}_{\alpha}(-) : R[x] \rightarrow R$ 를 취하면,

$$\begin{aligned} f(\alpha) &= \mathcal{E}_{\alpha}((x - \alpha) \cdot q(x) + r) \\ &= \mathcal{E}_{\alpha}((x - \alpha)) \cdot \mathcal{E}_{\alpha}(q(x)) + \mathcal{E}_{\alpha}(r) \\ &= (\alpha - \alpha) \cdot q(\alpha) + r \\ &= r \end{aligned}$$

Example 5.2.3 (Multipoint Evaluation). Field F 의 서로 다른 원소 $a_0, a_1, \dots, a_{n-1}$ 에 대하여 $V = \{f(x) \in F[x] \mid \deg f < n\}$ 라 하자. 이때 V 는 vector space이므로 각 a_i 에서의 evaluation functional을 $\varepsilon_i = \mathcal{E}_{a_i}|_V \in V^*$ 로 쓸 수 있고, 이때 linear map

$$\mathcal{E} = \prod_{i=0}^{n-1} \varepsilon_i : V \longrightarrow F^n, \quad f \longmapsto (\varepsilon_0(f), \dots, \varepsilon_{n-1}(f))$$

는 isomorphism이다.

Proof. $\mathcal{E}(f) = 0$ 이면 f 는 서로 다른 n 개의 root $a_0, \dots, a_{n-1}$ 을 가집니다. 그런데 $\deg f < n$ 이므로 $f = 0$, 따라서 $\mathcal{E}$ 는 injective. 동시에 $\dim_F V = n = \dim_F F^n$ 이므로 $\mathcal{E}$ 는 isomorphism. $\square$

Example 5.2.4 (Lagrange Interpolation). 위와 같은 $a_0, \dots, a_{n-1}$ 과 임의의 $b_0, b_1, \dots, b_{n-1} \in F$ 에 대하여 $f(a_i) = b_i$ ($0 \leq i \leq n-1$)를 만족하는 $f(x) \in F[x]$ ($\deg f < n$)이 다음과 같은 형태로 존재하며

$$f(x) = \sum_{i=0}^{n-1} b_i \prod_{\substack{0 \leq j < n \\ j \neq i}} \frac{x - a_j}{a_i - a_j},$$

이는 유일하다.

Proof. Example 5.2.3에 의해 $\mathcal{E} : V \rightarrow F^n$ 은 isomorphism이므로 $(b_0, \dots, b_{n-1})$ 의 preimage는 유일하게 존재.

F^n 의 standard basis의 i -번째 원소에 대응하는 V 의 원소는

$$\ell_i(x) = \prod_{\substack{0 \leq j < n \\ j \neq i}} \frac{x - a_j}{a_i - a_j}.$$

따라서 linearity에 의해

$$\mathcal{E}^{-1}(b_0, \dots, b_{n-1}) = \sum_{i=0}^{n-1} b_i \ell_i$$

이고 이의 유일성 역시 자연스럽게 따라옵니다 $\square$

Wall Maria⁵

5.3 ...and its Quotient Algebra

Definition 5.3.1. $D \times (D - \{0\})$ 에 다음과 같은 equivalence relation

$$(a, b) \sim (c, d) \iff ad = bc, \quad (a, b, c, d \in D, \quad b, d \neq 0)$$

을 주고, $a, b \in D, b \neq 0$ 에 대해 (a, b) 의 equivalence class를 앞으로 $[\frac{a}{b}]$ 와 같이 표기하겠습니다. 이때, 이러한 $Q_D = (D \times (D - \{0\})) / \sim$ 를 field of quotients of D 라고 부릅니다.^a

^aField of fractions라고 불리기도 합니다. 우리말로 분수체였나?

⁵Hierarchical filter.

Q_D 의 덧셈과 곱셈 역시 아래와 같이 well-defined.

Definition 5.3.2. $a, b, c, d \in D$ ($b, d \neq 0$)에 대해,

$$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] = \left[\frac{ad + bc}{bd}\right], \quad \left[\frac{a}{b}\right] \cdot \left[\frac{c}{d}\right] = \left[\frac{ac}{bd}\right].$$

여기까지의 세팅이 끝났을 때 우리는 비로소 Q_D 가 정말로 field⁶임을 말할 수 있습니다. 이 부분은 그다지 증명에 어려움이 없을 것이니 바로 다음 단계로 넘어가죠.

위처럼 세팅한 field Q_D 에 대해서는 $D \subseteq Q_D$ 라고 보는게 맞을 것 같습니다. 그리고 정말로, 그렇게 바라보고자 한다면, (injective) ring homomorphism $j : D \rightarrow Q_D$:

$$j(a) = \left[\frac{a}{1}\right]$$

을 생각하는 것이 자연스럽습니다. 그럼 Q_D 는 정말로 D 로부터 identify 되나요?

$$\left[\frac{a}{b}\right] = \left[\frac{a}{1}\right] \cdot \left[\frac{1}{b}\right] = j(a) \cdot j(b)^{-1}, \quad (a, b \in D, b \neq 0)$$

아무래도 그런 것 같네요?⁷ 뿐만 아니라, D 가 field이면 j 가 isomorphism임을 보일 수 있기에 $D = Q_D$ 란 사실도 자연스럽게 성립합니다.

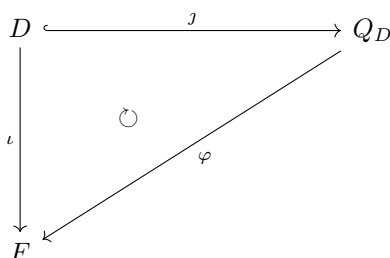
그리고 이제 물어보고 싶은 바는 명확히 정해졌습니다.

Proposition 5.3.3. D 를 subring으로 갖는 field F 와 canonical^a embedding $\iota : D \rightarrow F$ 에 대하여 다음의 조건을 만족하는 field embedding $\varphi : Q_D \rightarrow F$ 이 유일하게 존재한다:

$$\varphi \circ j = \iota.$$

^a~ natural?

Proof. 일단 모르겠으면 다이어그램을 그려,



위 diagram이 commute하려면 $a, b \in D, b \neq 0$ 에 대하여

$$\varphi\left(\left[\frac{a}{b}\right]\right) = \varphi(j(a)j(b)^{-1}) = \iota(a)\iota(b)^{-1}$$

⁶ 모든 nonzero element가 invertible인 commutative ring을 field라고 뜻합니다. 이진... 그래도 외울 수 있잖아요.

⁷ 그리고 이렇게되면 Q_D 라고 하는 것은 그저 우리가 아는 분수 연산보다 좋은 연산 관계를 새로이 보여주는 것입니다.

를 만족해야하며, 따라서 다음과 같이 map φ 를 정의할 수 있습니다:

$$\varphi : Q_D \longrightarrow F, \quad \left[\frac{a}{b} \right] \longmapsto \iota(a)\iota(b)^{-1}.$$

이때 $\left[\frac{a}{b} \right] = \left[\frac{c}{d} \right]$ 라면 equivalence relation의 정의에 의해 $ad = bc$. 여기에 ι 를 가하면

$$\iota(a)\iota(d) = \iota(b)\iota(c).$$

$b, d \neq 0$ 이고 ι 가 injective이므로 $\iota(b), \iota(d) \neq 0$. 양변에 $\iota(b)^{-1}\iota(d)^{-1}$ 을 곱하여 $\iota(a)\iota(b)^{-1} = \iota(c)\iota(d)^{-1}$ 을 얻을 수 있으므로 φ 는 well-defined.

이제 Q_D 에서 정의한 덧셈과 곱셈을 대입하면

$$\begin{aligned} \varphi \left(\left[\frac{a}{b} \right] + \left[\frac{c}{d} \right] \right) &= \varphi \left(\left[\frac{ad+bc}{bd} \right] \right) = \varphi \left(\left[\frac{a}{b} \right] \right) + \varphi \left(\left[\frac{c}{d} \right] \right), \\ \varphi \left(\left[\frac{a}{b} \right] \cdot \left[\frac{c}{d} \right] \right) &= \varphi \left(\left[\frac{ac}{bd} \right] \right) = \varphi \left(\left[\frac{a}{b} \right] \right) \varphi \left(\left[\frac{c}{d} \right] \right). \end{aligned}$$

또한 $\varphi\left(\left[\frac{1}{1}\right]\right) = 1_F$ 이므로 φ 는 ring homomorphism입니다. 나아가 $\varphi\left(\left[\frac{a}{b}\right]\right) = 0$ 이면 $\iota(a) = 0$, 따라서 $a = 0$ 이므로 $\ker \varphi = \{0\}$. 즉, φ 는 field embedding이고,

$$(\varphi \circ j)(a) = \varphi \left(\left[\frac{a}{1} \right] \right) = \iota(a).^8$$

최종적으로 유일성을 보이기 위해 같은 조건을 만족하는 ring homomorphism $\psi : Q_D \rightarrow F$ 를 생각합니다.

$$\psi \left(\left[\frac{a}{b} \right] \right) = \psi(j(a)j(b)^{-1}) = \iota(a)\iota(b)^{-1} = \varphi \left(\left[\frac{a}{b} \right] \right)$$

이므로 $\psi = \varphi$, 즉 이러한 φ 는 **유일합니다**.⁹ □

다만 여전히 갈 길이 멉니다.

5.4 Ideal Basics

Definition 5.4.1. Integral domain D 에 대하여 $p \in D$ 라고 하자. 이때 $p \neq 0$ 이고 $p \notin D^\times$ 이면

1. 다음의 명제가 참이 되도록 하는 p 를 irreducible element (in D)라고 한다:

$$\forall a, b \in D, \quad p = ab \implies a \in D^\times \text{ or } b \in D^\times.$$

2. 다음의 명제가 참이 되도록 하는 p 를 prime element (in D)라고 한다:

$$\forall a, b \in D, \quad p \mid ab \implies p \mid a \text{ or } p \mid b.$$

⁸이처럼 homomorphism에 필요한 정보만을 대입하여 일부 evaluation을 체크해보는 것만으로 전체 mapping 관계를 파악한다는 아이디어는 2.3에서도 활용했습니다.

⁹Universal property. 결국 수학은 누가 누가 더 많은 조상님을 보유하고 있는가에 대한 싸움이라니까요? 그 뭐냐 포켓몬스터 알죠??

물론, 정의로부터 prime element는 항상 irreducible element이기도 합니다.

Definition 5.4.2. Integral domain D 의 ideal이 모두 principal ideal^a이면 그러한 D 를 Principal Ideal Domain(PID)이라고 부른다.

^a원소 하나로 generate되는 ideal. 이를테면 $\langle a \rangle = Da = aD$ 는 $a \in D$ 가 generate하는 principal ideal입니다.

Definition 5.4.3. Commutative ring R 에 대해 다음의 조건들을 만족하는 $\mathfrak{p}$ 를 prime ideal이라고 부른다:

1. $\mathfrak{p} \triangleleft R^a$.
2. 임의의 $a, b \in R$ 에 대하여, $ab \in \mathfrak{p} \iff a \in \mathfrak{p} \text{ or } b \in \mathfrak{p}$.

^aTex 문법의 한계로 기호로 표현하지 못하였는데, $\mathfrak{p} \neq R$ 이어야합니다.

Definition 5.4.4. Commutative ring R 에 대해 다음의 조건들을 만족하는 $\mathfrak{m}$ 을 maximal ideal이라고 부른다:

1. $\mathfrak{m} \triangleleft R^a$.
2. $\mathfrak{m} \leq \mathfrak{n} \leq R$ 인 $\mathfrak{n}$ 에 대하여 $\mathfrak{n} \in \{\mathfrak{m}, R\}$.

^a직전과 유사하게, $\mathfrak{m} \neq R$.

아래 명제부터 시작해보겠습니다.

Proposition 5.4.5. Maximal ideal은 항상 prime ideal이다.

Proof. $\mathfrak{m}$ 이 R 의 maximal ideal이라 하자. 정의에 의해 $R/\mathfrak{m}$ 이 integral domain이면서 동시에 field¹⁰. 한편 어떤 ideal $\mathfrak{p} \in R$ 가 prime ideal인 것과 $R/\mathfrak{p}$ 이 integral domain인 것 역시 동치임은 정의에 의해 자명하므로¹¹, $\mathfrak{m}$ 은 prime ideal. $\square$

때문에,

Corollary 5.4.5.1. Integral domain D 에 대하여 $\text{char}(D)$ 는 0 혹은 prime number.^a

^a즉, D 는 항상 $\mathbb{Z}$ 혹은 $\mathbb{Z}/p\mathbb{Z}$ 와 isomorphic한 subring을... 어?

Corollary 5.4.5.2. F 가 finite field이면 다음을 만족하는 어떤 자연수 n 과 소수 p 가 존재한다:

$$|F| = p^n.$$

5.4.5.2를 말하고 싶어서 좀 오래 끌었습니다. 소인수분해에 대한 직관도 검사검사 전달되었으리라 믿어 의심치 않고요.

¹⁰정말 그런가요?

¹¹정말로 그런가요?

Definition 5.4.6 (필수 아님, 근데 여기까지 온 거 강 보고 가셈). Integral domain D 에 대하여 다음의 성질을 만족하면 UFD(Unique Factorization Domain)라고 부른다.

- (1) 임의의 nonzero nonunit $a \in D$ 는 유한개의 irreducible element들의 곱으로 표현된다. 즉,

$$a = p_1 p_2 \cdots p_n$$

을 만족하는 irreducible elements $p_1, \dots, p_n \in D$ 가 존재한다.

- (2) 위와 같은 표현은 unit과 순서를 제외하면 유일하다. 구체적으로, irreducible elements에 대하여

$$p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$$

이면 $m = n$ 이고, 어떤 permutation $\sigma \in S_n$ 과 units $u_1, \dots, u_n \in D^\times$ 가 존재하여 모든 i 에 대해

$$p_i = u_i q_{\sigma(i)}$$

가 성립한다.

Wall Rose

아래 단부터는 중요하지 않은 내용이 없으니 눌러 읽습니다.

5.5 Field Extension

Definition 5.5.1. E 는 field. 이때 어떤 $\alpha \in E$ 에 대하여

- (1) E 의 subfield F 에 대하여 E 는 F 의 extension field라 한다.^a
- (2) E 의 subring R 에 대하여 $R[\alpha]$ 는 subring of E generated by $R \cup \{\alpha\}$ 로 정의된다.
- (3) E/F 에 대하여 $F(\alpha)$ 를 subfield of E generated by $F \cup \{\alpha\}$ 로 정의된다.

^a그리고 이와 같은 관계를 E/F 로 쓴다.

이 정의를 눈에 좀 익혀보자면 아래 상황을 살펴볼 수 있습니다.

Example 5.5.1. Field extension E/F 와 $\alpha \in E$ 에 대하여,

1. $F[\alpha] = \{f(\alpha) \in E \mid f(x) \in F[x]\}$
2. $F(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \in E \mid f(x), g(x) \in F[x], g(\alpha) \neq 0 \right\}$

...심지어,

Example 5.5.2. $F(\alpha)$ 는 $F[\alpha]$ 의 field of quotients.

이제 아래의 정의를 살펴보겠습니다.

Definition 5.5.2. Field extension E/F 와 $\alpha \in E$ 에 대하여, evaluation homomorphism $\mathcal{E}_\alpha : F[x] \rightarrow E$ 를 생각하자. 이때 $\ker \mathcal{E}_\alpha \neq 0$ 이면 α 를 algebraic element (over F)라고 부르며, 그렇지 않을 경우 transcendental element (over F)라고 부른다.

...물론 다음의 예시도 유효합니다:

Example 5.5.3. Field extension E/F , $\alpha \in E$ 라 하자. 이때 $F[\alpha] = F(\alpha)$ 이면 α 는 algebraic over F .

그리고 직전의 정의에서 언급했던 것과 동일한 setting에서,

Lemma 5.5.3. α 가 algebraic over F 라면

$$F[\alpha] = F(\alpha).$$

Proof. First Isomorphism Theorem에 의해

$$F[x]/\ker \mathcal{E}_\alpha \cong \text{im} \mathcal{E}_\alpha = F[\alpha].$$

그리고 $F[\alpha]$ 는 field E 의 subring, 때문에 $F[\alpha]$ 는 integral domain입니다. 따라서 (정의에 의해) $\ker \mathcal{E}_\alpha$ 는 $F[x]$ 의 prime ideal임은 분명합니다. 한편, PID의 non-zero prime ideal은 항상 maximal ideal이므로 $\ker \mathcal{E}_\alpha$ 는 $F[x]$ 의 maximal ideal. 즉, $F[x]/\ker \mathcal{E}_\alpha$ 는 field이며 $F[\alpha] = F(\alpha)$. $\square$

그리고 직전의 $\ker \mathcal{E}_\alpha$ 는 다음과 같이 정의된 다항식 $\text{irr}(\alpha, F)$ 를 unique generator로 가집니다.

Definition 5.5.4. α 가 algebraic over F 일 때, prime ideal $\mathfrak{p}_\alpha = \{f(x) \in F[x] \mid f(\alpha) = 0\}$ 는 **unique** monic irreducible generator를 가짐을 관찰하자. 그리고 이를 $\text{irr}(\alpha, F)$ 라 표기하고 irreducible polynomial (of α over F)라 부른다.

지금까지 끌어 내려온 관심사는 (드디어 마침내) linear algebra¹²로 porting할 수 있게 되었습니다.

Definition 5.5.5. E/F 가 field extension이면 extension degree of E over F 를 다음과 같이 정의한다:

$$[E : F] = \dim_F E$$

^a

^a E 를 F -vector space라 해석하는데는 조금도 무리가 없습니다. 다소 헛갈린다면 바로 아래에 주어지는 proposition을 참조.

Proposition 5.5.6. E/F 에 대하여 $\alpha \in E$ 가 algebraic over F 이면 $F(\alpha)/F$ 는 finite extension이며^a

$$[F(\alpha) : F] = \deg(\text{irr}(\alpha, F)).$$

¹²...내지는 다항식 차력쇼

$^a[E : F] < \infty$ 이면 E 를 F 의 finite extnesion이라고 부릅니다.

Proof. $n = \deg(\text{irr}(\alpha, F))$ 라 하면 set $\{1, \alpha, \dots, \alpha^{n-1}\}$ 이 (F) linearly independent임은 $\text{irr}(\alpha, F)$ 의 정의에 의해 자명. 즉, $\sum_{i=0}^{n-1} a_i \alpha^i = 0$ 을 만족하려면 $a_0, a_1, \dots, a_{n-1} \in F$ 는 모두 0이어야만 합니다. 그리고 5.2.2의 Remainder Theorem과 5.5.3로부터 $F(\alpha)$ 의 임의의 원소는 어떤 다항식 $f(x) \in F[x]$ 이 존재하여 $\mathcal{E}_\alpha(f(x))$ 로 표현됨을 확인할 수 있습니다. 따라서 $\{1, \alpha, \dots, \alpha^{n-1}\}$ 는 $F(\alpha)$ 의 (F) -basis set.¹³ $\square$

Wall Sina

Theorem 5.5.7 (Kronecker's theorem). *Field F 와 irreducible polynomial $p(x) \in F[x]$ 에 대해 $p(\alpha) = 0$ 인 α 를 포괄하는 F 의 extension field $E = F(\alpha)$ 가 존재한다.*

Proof. $F[x]$ 는 PID이고 $p(x)$ 는 irreducible이므로 $\langle p(x) \rangle$ 는 maximal ideal. 따라서 quotient ring $E = F[x]/\langle p(x) \rangle$ 는 field.

이제 canonical map

$$\iota : F \longrightarrow E, \quad a \longmapsto a + \langle p(x) \rangle$$

를 생각합니다. $p(x)$ 는 nonconstant polynomial이므로 $\langle p(x) \rangle \cap F = \{0\}$ 이고, 따라서 ι 는 injective field homomorphism. 이에 F 를 $\iota(F) \subseteq E$ 와 identify하면 E 를 F 의 extension field로 볼 수 있습니다. E 에서 $\alpha = x + \langle p(x) \rangle$ 로 정의하면 $p(\alpha) = p(x) + \langle p(x) \rangle = 0$. 또한 임의의 $f(x) \in F[x]$ 에 대해 그 residue class는 $f(x) + \langle p(x) \rangle = f(\alpha)$ 로 표현되므로 $E = F[\alpha]$ 입니다. E 가 field이므로 $F[\alpha] = F(\alpha)$, 따라서 $E = F(\alpha)$ 이고 $p(\alpha) = 0$ 을 만족합니다. $\square$

위 정리는 상당히 강력합니다. 당장 적용해볼만한 가벼운 예제가 있다면 아래 정도가 있겠네요.

Example 5.5.4. $F(z)$ 는 field F 위에서 정의된 rational function이 이루는 field. 이때 $x^n - z \in F(z)[x]$ 는 $F(z)$ 위에서 irreducible이므로 $F(z)[x]/\langle x^n - z \rangle$ 는 $F(z)$ 의 extension field. (단, $n \in \mathbb{N}$.)

하지만 문제 풀이를 위해서라면 아래의 내용이 훨씬 중요하겠네요,

Lemma 5.5.8. *임의의 nonzero polynomial $f(x) \in F[x]$ 에 대하여, $n = \deg f$ 라 하면 어떤 F 의 extension field K 와 $\lambda_1, \dots, \lambda_n \in K$ 가 존재하여*

$$f(x) = a \prod_{i=1}^n (x - \lambda_i) \quad (a \in F^\times)$$

로 인수분해된다. 특히 $K = F(\lambda_1, \dots, \lambda_n)$ 로 둘 수 있다.

그리고 다음과 같은 정의는 글의 흐름상 매우매우매우 자연스럽습니다.

Definition 5.5.9. 그러한 extension 중 가장 작은 K/F 를 f 의 splitting field라 한다.

¹³이제는 더이상 우리가 알던 기존의 지식을 `행렬에 대한 무언가의 miscellany` 정도로만 국한시킬 이유가 조금도 없음에 주목합니다.

이제서야 finite field를 제대로 이야기해봅니다. 우선 아래의 사실은 5.4.5.2로부터...

Observation 5.5.10. 2 이상의 정수 p 에 대하여 아래의 명제는 모두 동치이다.^a

1. $\mathbb{Z}/p\mathbb{Z}$ 는 integral domain.
2. $\mathbb{Z}/p\mathbb{Z}$ 는 field.
3. p 는 prime number.

^a가우뚱?한다 싶으면 integral domain과 field의 정의를 슬쩍 보고 오시면 되겠습니다. (Hint: 여기서 zero divisor가 생기지 않을 필요충분조건은...?)

그리고 위의 $\mathbb{Z}/p\mathbb{Z}$ 라고 하는 것은 $\mathbb{F}_p$ 라고도 쓸 수 있으며, 이를 finite field라고도 부름은 아마 많은 분들이 경험적으로나마 알고있는 사실이겠습니다. 그럼 이제 characteristic이 $p > 0$ 으로 유한하면서¹⁴ 실제로 field가 될 수 있는 어떤 대상이 존재하는지, 만약 존재한다면 그것은 어떠한 성질을 가져야하는지를 살펴볼 수밖에 없습니다.

Observation 5.5.11. $\text{char}(F) = 0$ 인 field F 에 대하여 $F[x]$ 의 irreducible polynomial은 separable^a.

^a다항식이 separable이란, 1번 풀이에서도 언급했지만, multiple root를 가지지 않음을 뜻합니다.

Proof. 귀류를 치겠습니다. 만약 irreducible polynomial $f(x) \in F[x]$ 가 multiple root를 가진다면 $\gcd(f, f') \neq 1$. 그런데 f 가 irreducible polynomial이므로 $f \mid f'$ 이어야 하고, $\deg f' < \deg f$ 이므로 $f' = 0$. 따라서 f 는 상수이고 이는 f 가 irreducible이라는 가정에 모순. $\square$

또한, 다음의 사실도 함께 관찰하겠습니다.

Observation 5.5.12. $\text{char}(F) = p > 0$ 인 field F 에 대하여 다음의 $f(x) \in F[x]$ 은 separable polynomial이다:

$$f(x) = x^q - x.$$

(단, $q = p^n$.)

Proof. ...¹⁵

$\square$

그럼....

Definition 5.5.13. Order $q = p^n$ 인 finite field $\mathbb{F}_q$ 는 splitting field of $x^q - x$ over $\mathbb{F}_p$ 로 정의된다.^a

^a원래라면 이의 유일성 역시 함께 따져주어야 합니다만, field isomorphism에 관한 서술을 피해가기 어려워 분량상 생략하였습니다.

오래 기다리셨습니다.

¹⁴물론 p 는 소수.

¹⁵계속 한거잖아요. $f(x)$ 미분해서 $\gcd(f, f') = 1$ 인거 보이셈!!@#!@!

문제

N 개의 정점을 가지는 그래프 G 에 대하여 (finite field) $\mathbb{F}_P$ 위의 laplacian matrix를 L_G , 그리고 N' 개의 정점을 가지는 그래프 H 에 대하여 **quotient ring** $\mathbb{F}_P[x]/\langle x^K - 1 \rangle^a$ 위의 laplacian matrix를 L_H 라 쓰자. 그리고 L_G 의 eigenvalue $\lambda_0, \lambda_1, \dots, \lambda_{N-1}$ 과 L_H 의 eigenvalue $\mu_0(x), \mu_1(x), \dots, \mu_{N'-1}(x)$ 에 대하여(단, $\lambda_0 = \mu_0(x) = 0$), 다음의 다항식

$$\frac{1}{NN'} \prod_{\substack{0 \leq i < N \\ 0 \leq j < N' \\ (i,j) \neq (0,0)}} (\lambda_i + \mu_j(x)) \in \mathbb{F}_P[x]/\langle x^K - 1 \rangle$$

을 구하여라. (단, $\gcd(P, K) = 1$ 임이 보장된다.^{b,c})

출제자 rootenter

^a결국 앞서 언급했던 CRT와 Cantor-Zassenhaus algorithm은 이 친구에 적용해주시면 됩니다. Polynomial $x^K - 1$ 을 irreducible 성분 여럿으로 쪼개어 다시 $\mathbb{F}_P[x]$ 의 quotient를 구해주면 그때 비로소 field가 됩니다.

^b이 조건이 없는 상황에선 단독으로 루비 (최)상위 수준의 난이도를 먹고 들어가는 decomposition reconstruction이 필요합니다. $x^K - 1$ 의 중복근을 허용하게 되면...(이하 생략, 5.6.7, 5.6.8 참고)

^c여담으로, 만약 $K = P - 1$ 이었다면 $x^{P-1} - 1$ 은 separable이고 모든 근이 $\mathbb{F}_P^\times$ 위에 존재합니다. 따라서 $\mathbb{F}_P[x]/\langle x^{P-1} - 1 \rangle$ 은 CRT에 의해 $P - 1$ 개의 $\mathbb{F}_P$ 의 direct product와 isomorphic하고, 각 근에서의 evaluation을 이용하여 F변과 동일하게 DFT를 곧바로 적용할 수도 있습니다 혁!!

5.6 함께보면 좋은 연습문제들

Example 5.6.1. [2025 KAIST 15th ICPC Mock Competition: Misdeed -la bonté de Dieu et l'origine du mal- ([Ruby V](#))]

$\mathbb{F}_q$ 에서의 data point와 (polynomial) functional 사이의 duality가 실제한다면 이들 사이를 오가는 방법은 결국 적절한 homomorphism을 찾는 것 뿐.^a

^a5.2.3과 5.2.4 참조.

Example 5.6.2. [ICPCCamp 2015. Day 4. Grand Prix of China: Tri-color Spanning Tree ([Diamond I](#))]

되는 것은 된다. 행렬 안에 ‘다항식’이라 불리우는 commutative ring $\mathbb{F}_p[x]$ 의 원소를 넣는 것에는 그 어떤 방해도 없습니다.

Example 5.6.3. [제4회 고려대학교 MatKor Cup. 2024 Winter/Spring: 하늘아 군대 잘 가고 ([Ruby V](#))]

Field extension이 가미된 (ternery) FWHT. DFT에 대한 이해도 겸사겸사 끌어올릴 겸 시도해볼만합니다.

Example 5.6.4. [Petrozavodsk Summer 2016. Day 8. DPRK Contest: Easy Homework (Ruby III)^a]

안 되면 되게 하라. $\mathcal{M}_2(\mathbb{F}_p)$ 도 적당히 좋은 성질들이 함께 주어진 (commutative) algebra 입니다. 잘 알려진 discrete logarithm algorithm^b을 그대로 활용하여도 무방합니다.

^a근데 생각해보니까 출처가...?

^bBSGS etc.

Example 5.6.5. [BOJ 25510: Lord of the Characteristic Polynomials (2) (Ruby IV)]

안 되면 되게...어?^a

^aIntegral domain이 만만하구나야,,

Example 5.6.6. [Petrozavodsk Winter 2020. Day 9. Yuhao Du Contest 7: Knowledge-Oriented Problem (Ruby II)]

Spectral graph theory + Combinatorial spanning tree counting.

Example 5.6.7. [제2회 키파컵 B번: Binary Matrix (Ruby II)]

Finite field + Cantor-Zassenhaus algorithm.

Example 5.6.8. [제6회 고려대학교 MatKor Cup: 2025 Winter: 받아안올림 (Ruby II)]

이 문제에서의 후반 처리와 비슷한 아이디어를 요구합니다.^a

^a다항식 인수분해 후 CRT. 다만 중복근을 가질 수 있어서...

A Solution by a Professional:



nflight11

2026. 5. 25. 오전 12:07

저게 멀까



nflight11

2026. 5. 25. 오전 6:11

풀이요

Let $G_{ij} = \gcd(i, j)^{-1}$ and $D_{ij} = i\delta_{ij}$ then $A = DG$ so $\det A = \det D \det G = N! \det G$.
Let another matrix B as $B_{id} = [d|i]$ when $[i]$ is Iverson bracket then $B \in \text{SL}_N(\mathbb{Z})$ since it is triangular with unit main diagonal so there uniquely exists E with $E = \det G$ and $G = BEB^T$, that is, $E = B^{-1}G(B^{-1})^T$.
If we assume E as diagonal. Then $\gcd(i, j)^{-1} = G_{ij} = \sum_x B_{ix} E_{xx} B_{jx} = \sum_{x|\gcd(i,j)} E_{xx} = \sum_{x|\gcd(i,j)} e_x$. We can use Möbius inversion to get value of e_x because $n^{-1} = \sum_{x|n} e_x$. $e_n = \sum_{x|n} \mu(x) (1/(n/x))^{-1} = n^{-1} \sum_{x|n} x \mu(x)$. Of course e is multiplicative so

$$e_n = \prod_{p|n} e_{p^{v_p}} = \prod_{p|n} \left(p^{-v_p} \sum_{m=0}^{v_p} p^m \mu(p^m) \right) = \prod_{p|n} \left(p^{-v_p} \sum_{m=0}^1 p^m \mu(p^m) \right) = \prod_{p|n} p^{-v_p} (1-p) = n^{-1} \prod_{p|n} (1-p).$$

Thus, diagonal matrix E with its diagonal entry are $n^{-1} \prod_{p|n} (1-p)$ actually satisfies $G = BEB^T$.
 $\det G = \det E = \prod_1^N e_n = N!^{-1} \prod_{n=1}^N \prod_{p|n} (1-p)$ so $\det A = N! \det G$.

$$\det A = \prod_{n=1}^N \prod_{p|n} (1-p) = \prod_{p \leq N} (1-p)^{1/N/p}.$$

It can be calculated in $\mathcal{O}(N)$ time for precompute prime table and $\mathcal{O}(\pi(N) \log P) = \mathcal{O}(N \log P / \log N)$ time to calculate products, so overall time is $\mathcal{O}(N \log P / \log N)$.
Sample code is as follows.

```

1 N = int(input()); mod = 10**9+7
2 if N == 1: print(1); exit(0)
3 table = [i%2==1 for i in range(1+N)]; table[1], table[2] = False, True
4 ret = pow(1-2, N//2, mod)
5 for p in range(3, 1+N, 2):
6     if table[p]:
7         ret *= pow(1-p, N//p, mod); ret %= mod
8         for q in range(p*p, 1+N, p): table[q] = False
9 print(ret)

```



아무래도 PE맞인데



rootenter

2026. 5. 25. 오전 7:48

개쩐다
어디서 똥거한 건 아닌데 zz
결국 손바닥 안이군



lunarlity

2026. 5. 25. 오후 12:50

아하 (수정됨)
뭔가맷코컵의난이도가 높아진이유가
안봐도알거같은요

what