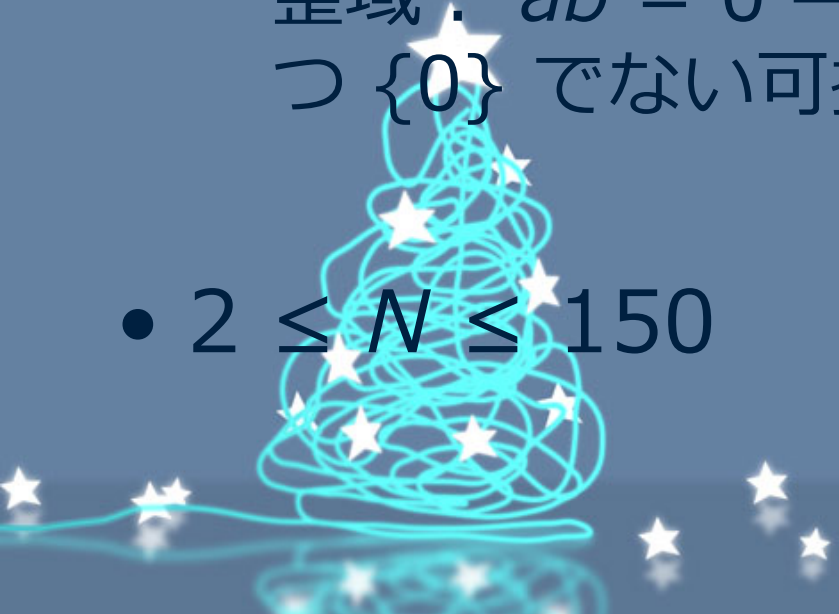
C: integral domain

問題概要

- N 元整域を 1 つ作り足し算と掛け算の票を出力せよ
  - 環：足し算と掛け算が定まった集合
  - 可換環：掛け算が可換な環
  - 整域： $ab = 0 \Rightarrow a = 0$ or $b = 0$ が成り立つ $\{0\}$ でない可換環
- $2 \leq N \leq 150$



注意

- N が素数なら mod N での足し算と掛け算を行えばよいが，N が素数でないときにも解はある
  - 例： $N = 4$

f	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

g	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

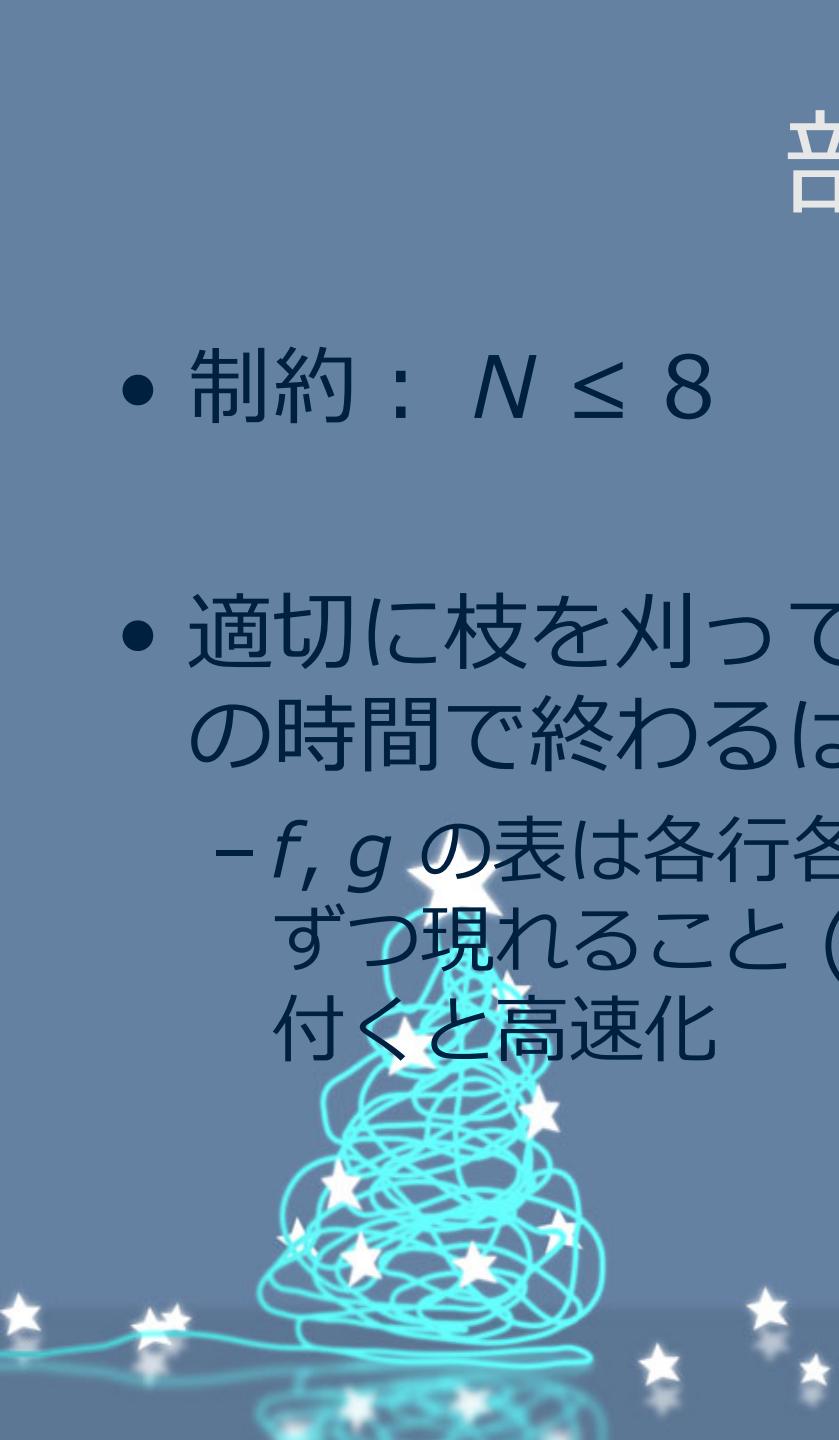
数学の問題です

- 満点獲得のためにはいろいろな知識が要ります
- 部分点だけなら無理ではないですが大変です

部分点

- 制約： $N \leq 8$

- 適切に枝を刈って全探索すればそこそこの時間で終わるはずので解を埋め込める
  - f, g の表は各行各列で 0 から N - 1 が 1 回ずつ現れること (g の 0 の部分を除く) に気付くと高速化



知識・考察

- 有限集合は整域ならば体
  - a ($\neq 0$) 倍写像は単射 (整域だから)
  - 単射は全射 (有限集合だから)
  - ということは特に 1 に行くので a の乗法の逆元が存在

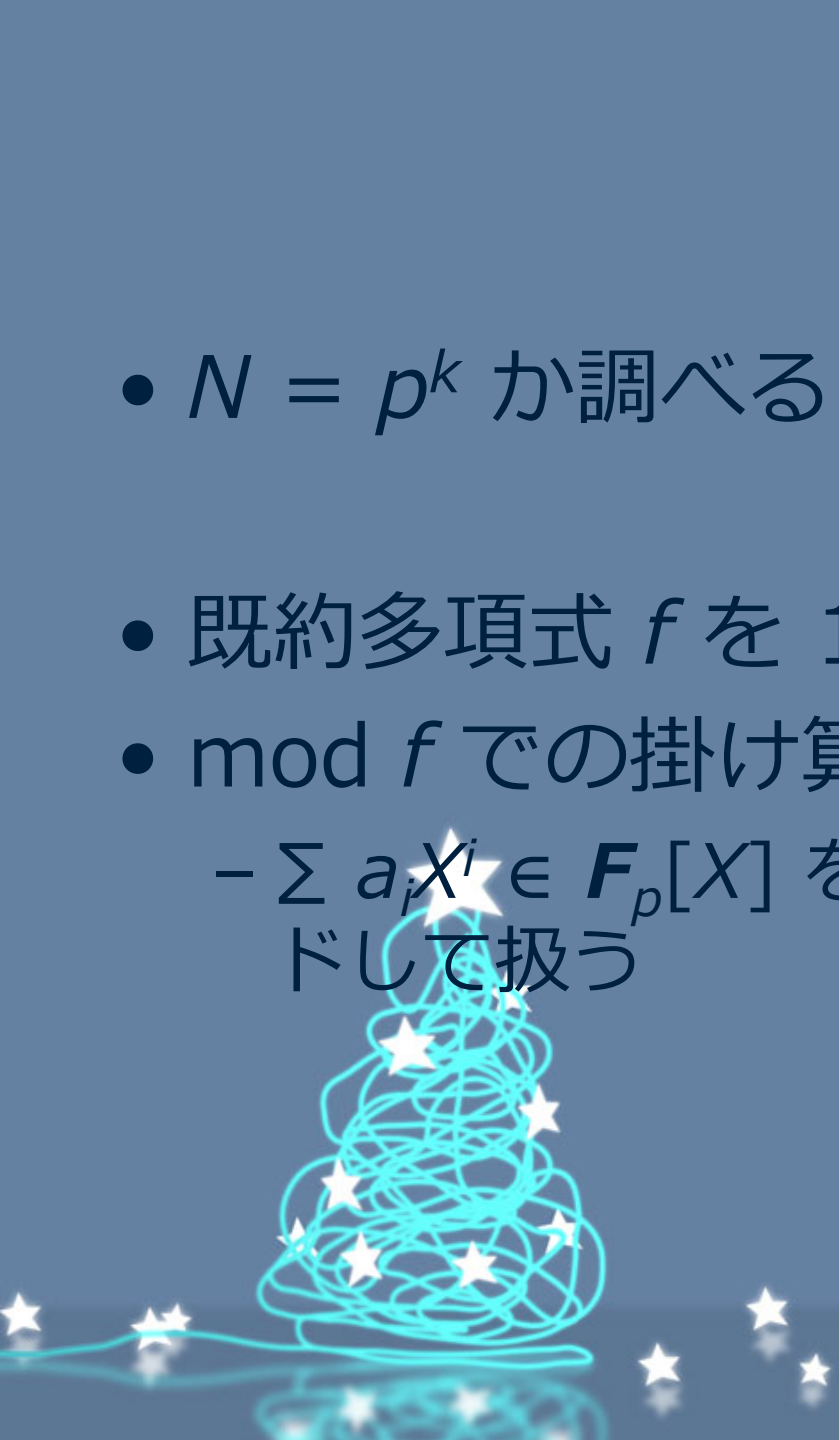
知識・考察

- 有限体の元の個数は p^k (p は素数，k は正の整数) に限る
  - 標数を p とすれば $\boldsymbol{F}_p$ ベクトル空間だから
    - $\boldsymbol{F}_p$ は mod p での足し算・掛け算による有限体
- 元の個数 p^k の有限体は存在する
  - $\boldsymbol{F}_p$ 係数の k 次既約多項式 f を 1 つとって，$\boldsymbol{F}_p[X] / (f)$ を考えればよい
    - 既約多項式の存在は数え上げで示せる
  - 同型を除いて一意であることも知られている

解法

- $N = p^k$ か調べる

- 既約多項式 f を 1 つ求める
- mod f での掛け算などをして答えを出力
  - $\Sigma\, a_i X^i \in \boldsymbol{F}_p[X]$ を整数 $\Sigma\, a_i p^i$ にでもエンコードして扱う

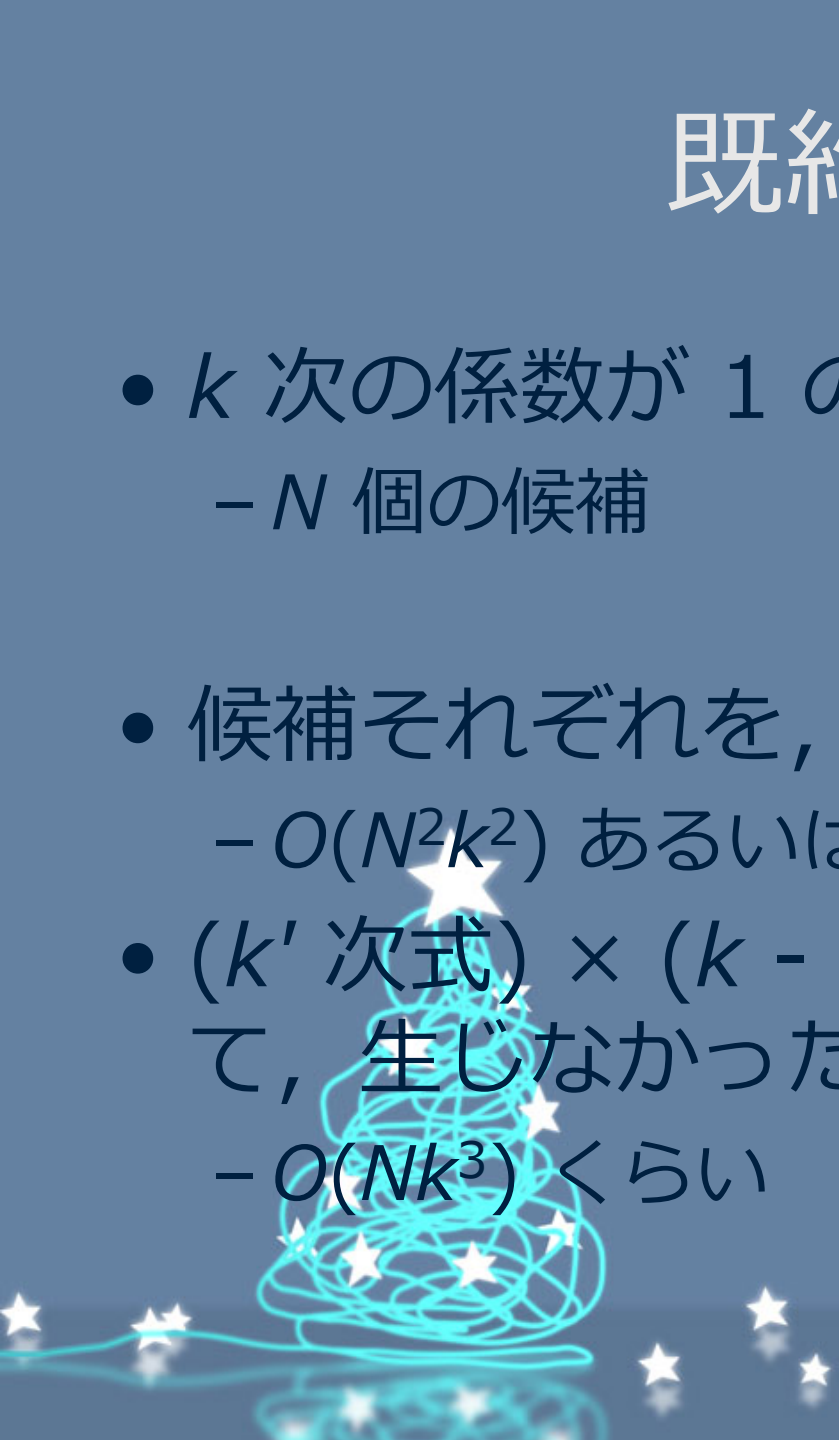


多項式の計算

- 掛け算・割り算ともに $O((\text{次数})^2)$ 時間かかってよい
  - 係数が体の元なので割り算も簡単

既約多項式

- k 次の係数が 1 のもののみ考えればよい
  - N 個の候補
- 候補それぞれを，低次の式で試し割り
  - $O(N^2k^2)$ あるいは $O(N\sqrt{N}\,k^2)$ くらい
- (k' 次式) × (k - k' 次式) をすべて生成して，生じなかったものを拾う
  - $O(Nk^3)$ くらい

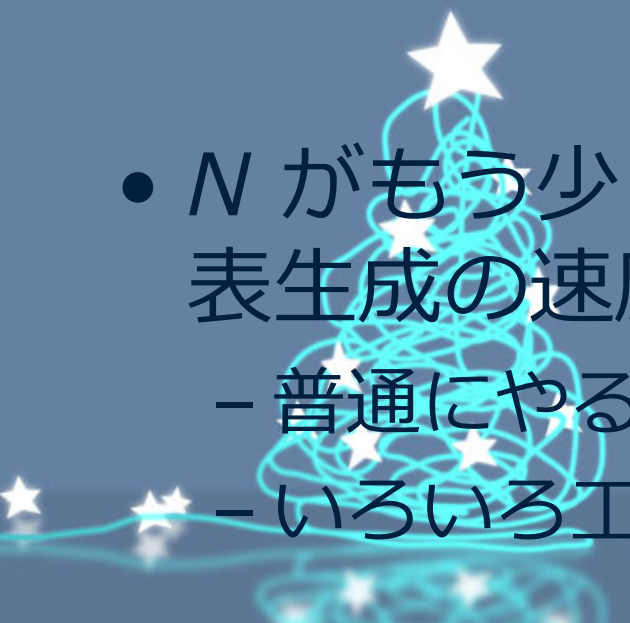


既約多項式

- 手計算で求めて埋め込んでもよい
  - 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 3^2, 3^3, 3^4, 5^2, 5^3, 7^2, 11^2 だけなんとかすればよいので意外となんとかなる

おまけ

- $N \leq 150$ だった事情
  - 出力ファイルのサイズを抑えるため
  - 出力チェッカの速度
    - 整域かどうかは $O(N^2)$ で判定できますが面倒かつバグのリスクがあるので $O(N^3)$ を書きました
- N がもう少し大きいと足し算表・掛け算表生成の速度が要求できた
  - 普通にやると $O(N^2k^2)$
  - いろいろ工夫すると $O(N^2)$



結果

- 総提出数： 111
- 提出者数： 41
- 正解者数： 6
- 最初の正解： omeometo (00:32:19)