多項式の解の個数

問題作成：北川
解法作成：安達・北川
解説：北川

問題概要

- 整数係数多項式 f の mod P での零点の個数を求めよ

だめな解法

- $0 \leqq z < P$ を満たす全ての整数に対して $f(z)=0$ か試す
- P は 10^9 くらいになるので無理

想定解法

- 複数の z に対して一度に f(z)=0 かを判定したい
- 「f(a)=0 ⇔ f(z) が z−a で割り切れる」ことを利用する
- **f(z)** と z(z−1)(z−2)…(z−P+1) との GCD が取れればその次数が答え
- 実は、z(z−1)(z−2)…(z−P+1) =z^P**-z** になる(フェルマーの小定理)

GCDの計算

- GCDを普通に計算すると O(max(P, deg f)^3) くらいかかる
- z^P-z と f のGCDを計算したいが、やっぱり P が大きい
- z^p-z を f で前もって割っておく
- $z^{n+m} \% f = (z^n \% f)(z^m \% f) \% f$
- $z^n \% f$ の次数は deg f 以下
- → 繰り返し二乗法 O((deg f)² log P)

コーナーケース

- $a_N \neq 0$ と書いてあるが、a_N % P $\neq$ 0とは言っていない(サンプルにある)
- 基本的に答えはN以下になるが、f = 0 のときに P になる

結果

- 総提出数: 16
- 提出者数: 3
- 正解者数:0

- Judge solution
  - 約100行