Вказівки щодо розв'язання завдання № 25 відбірково-тренувальних зборів команди міста Києва

1. Шаховий клуб

Нехай M — кількість гравців в клубі. Розглянемо простішу задачу, в якій рівень гри кожного гравця – число від 1 до M, і жодна пара гравців не має однакового рівня гри. Впорядкуємо всіх шахістів за рівнем гри. Розглянемо події у порядку надходження. В кожний момент часу розглянемо послідовність X_1, X_2, ... , X_M величин віку гравців з рівнем гри 1, 2, ... , M з тим зауваженням, що вік певного гравця вважатимемо нульовим, якщо він ще не прийшов до клубу на момент події. Таке припущення еквівалентне відсутності гравця: його ніколи не виберуть як супротивника. На початку розгляду послідовність X_1, X_2, ... , X_M містить лише нулі, а подія першого типу полягає у зміні величини деякого числа X_i послідовності з 0 на певне натуральне число.

Нехай k та X_k — рівень гри та “поточний вік” гравця з деякої події другого типу. Тоді його суперником буде гравець з силою гри $s(k) = \min \{j \mid j > k,\ X_j > X_k\}$, якщо ця множина не порожня.

Побудуємо *дерево відрізків (інтервалів)* над послідовністю X_1, X_2, ... , X_M, у якій кожна вершина зберігає максимальне значення X_j на відповідному відрізку індексів:

- кореню дерева відповідає відрізок індексів [1.. M], тобто вся послідовність;
- кожній вершині, якій відповідає відрізок довжини, більшої за 1, має дві дочірніх вершини, що є коренями піддерева відрізків на лівій і правій половині (рекурсивно).

Дерево відрізків дозволяє швидко змінювати значення X_i з підтриманням властивості, виділеної у тексті підкресленням, за $O(\log_2 M)$ операцій таким чином:

1. Змінимо значення максимуму у відповідному листі;
2. Для кожної вершини на шляху від листа до кореня дерева змінимо значення максимуму на більше з двох дочірніх вершин.

Також дерево відрізків дозволяє знайти найменше t, при якому $X_t > z$ при даному z (якщо воно існує), за допомогою наступного алгоритму.

1. Починаємо з повного дерева (всього відрізку);
2. Якщо поточне піддерево — лист, ми знайшли відповідь і припиняємо виконання алгоритму;
3. Якщо максимум в лівій половині відрізку більше ніж z, оголошуємо ліве піддерево поточним, інакше оголошуємо праве піддерево поточним
4. Переходимо до кроку 2.

Глибина дерева відрізків є $O(\log_2 M)$, тому обидва алгоритми мають складність $O(\log_2 M)$.

Складніше реалізувати запит на пошук $s(k)$. Розглянемо такий алгоритм:

1. Починаємо розгляд з кореня дерева.
2. Повторюємо для поточного піддерева:

- якщо k не належить до поточного піддерева, то жодна з його вершин не може бути відповіддю;
- якщо k належить до правого піддерева поточного піддерева, оголошуємо праве піддерево поточним (у цьому випадку жодна з вершин лівого піддерева не може бути відповіддю);
- інакше, тобто якщо максимум X_j в лівому піддереву більший за X_k, рекурсивно знаходимо $s(k)$ для лівого піддерева. Якщо відповідь не існує в лівому піддереві, то повертаємо найменше t з правого піддерева, при якому $X_t > X_k$.

Кількість рекурсивних викликів алгоритму пошуку $s(k)$ є $O(\log_2 M)$. Ключовим спостереженням є те, що пошук найменшого допустимого t правого піддерева може відбутися не більше одного разу, тому також потребує $O(\log_2 M)$ часу. Тому загальна складність дорівнює $O(\log_2 M)$.

Зведемо початкову задачу до щойно розв'язаної.

1. Впорядкуємо гравців за зростанням рівня гри, а при рівності — за зростанням віку (наприклад, швидким методом Хоара);
2. Замінимо рівень гри кожного гравця на його позицію у впорядкованій таким чином послідовності.

Вперше на Київських міських учнівських олімпіадах з інформатики використання дерева відрізків передбачалося у 2007 році (II тур, задача 5 «Комарі»).

2. Факторіали

Подамо $N!$ добутком $2^m \cdot 5^n \cdot N_0$, де N_0 не кратне ні двом, ні п'ятьом,

$$m = [N/2] + [N/2^2] + [N/2^3] + \ldots$$
$$n = [N/5] + [N/5^2] + [N/5^3] + \ldots$$

де $[x]$ — ціла частина числа x. Легко бачити, що $n \le m$.

Міркування щодо m такі. У добутку $N!=1\cdot 2\cdot\ldots\cdot N$ кожне друге число кратне 2, кожне четверте — кратне числу $4 = 2^2$, кожне восьме — кратне числу $8 = 2^3$ і т.і. Серед чисел 1, 2, … , N саме $[N/2]$ кратні 2. Поділивши кожне парне число на 2, отримаємо у добутку $[N/2^2]$ парних чисел (тих, що спочатку були кратні 4). Поділивши й ці парні числа на 2, то отримаємо $[N/2^3]$ парних чисел (тих, що спочатку були кратні 8)… Міркування щодо n аналогічні.

Шуканим кодом буде $(N_0 \cdot 2^{m-n}) \bmod 1000$ (лишок при діленні на 1000). Розглянемо таку допоміжну задачу: підрахувати $(N!/p^{\max}) \bmod p^k$, де p — просте число, а $(N!/p^{\max})$ — це $N!$, поділене на p максимальну можливу кількість разів, так щоб результат все ще був цілим, k — довільне натуральне число. Спочатку маємо:

$$\frac{N!}{p^{\max}} = \left(1\cdot 2\cdot\ldots\cdot(p-1)\cdot\frac{p}{p^{\max}}\right)\left((p+1)\cdot(p+2)\cdot\ldots\cdot(2p-1)\cdot\frac{2p}{p^{\max}}\right)\ldots(\ldots\cdot N)$$

В кожній великій дужці p множників, окрім, можливо, останньої, де множників може бути менше (якщо N не кратне p). Надалі вважатимемо, що N не кратне p: це не суттєво для подальших міркувань. Перші p – 1 множник у дужці не ділиться на p, але p-ий ділиться. Запишемо такі p-ті множники окремо наприкінці виразу:

$$\frac{N!}{p^{\max}} = 1\cdot 2\cdot\ldots\cdot(p-1)\cdot(p+1)\cdot\ldots\cdot(2p-1)\cdot(2p+1)\cdot\ldots\cdot(\ldots\cdot N)\cdot\left(\frac{p}{p^{\max}}\cdot\frac{2p}{p^{\max}}\cdot\ldots\cdot\frac{\left[N/p\right]p}{p^{\max}}\right). \quad (1)$$

З рівності: $\frac{x\cdot p}{p^{\max}} = \frac{x}{p^{\max}}$ виплаває: $\frac{p}{p^{\max}}\cdot\frac{2p}{p^{\max}}\cdot\ldots\cdot\frac{\left[N/p\right]p}{p^{\max}} = \frac{1}{p^{\max}}\cdot\frac{2}{p^{\max}}\cdot\ldots\cdot\frac{\left[N/p\right]}{p^{\max}} = \frac{\left[N/p\right]!}{p^{\max}}$.
Тут *степінь* max *у знаменнику кожного дробу свій* і є найбільшим невід'ємним цілим числом, при якому відповідне відношення є натуральним числом.

Нас цікавить не $N!/p^{\max}$, а $(N!/p^{\max}) \bmod p^k$, тому усі множники більші за p^k можна замінити на їхню остачу від ділення на p^k: $ap^k + b = b \pmod{p^k}$. Першу частину подання (1) перетворимо на добуток багатьох однакових множників:

$$\frac{N!}{p^{\max}} \overset{\left(\bmod p^k\right)}{\equiv} \left(1\cdot 2\cdot\ldots\cdot(p-1)\cdot(p+1)\cdot\ldots\cdot\left(p^k-1\right)\right)^{\left[\frac{N}{p^k}\right]}\cdot\left(1\cdot 2\cdot\ldots\cdot(p-1)\cdot(p+1)\cdot\ldots\cdot N \bmod p^k\right)\cdot\frac{\left[N/p\right]!}{p^{\max}}.$$

Якщо N кратне p^k, то друга група множників, виділена дужками, відсутня.
Позначимо:

- $B_{p,k} = \mathbf{(}1\cdot 2 \cdots (p-1)\,(p+1) \cdots (2p-1)\,(2p+1) \cdots (p^k-1)\mathbf{)} \bmod p^k$;
- $S_{M,p,k} = \mathbf{(}1\cdot 2 \cdots (p-1)\,(p+1) \cdots M\mathbf{)} \bmod p^k$.

Тоді: $\frac{N!}{p^{\max}} \bmod p = \left(B_{p,k}^{\left[\frac{N}{p^k}\right]}\cdot S_{N \bmod p^k,p,k}\cdot\frac{\left[N/p\right]!}{p^{\max}}\right) \bmod p$.

$B_{p,k}$ обчислимо так:

```
Bp,k = 1
для всіх i від 1 до p^k при i не кратному p:
   Bp,k = (Bp,k * i) mod p^k
```

$S_{M,p,k}$ обчислимо так:

```
SM,p,k = 1
для всіх i від 1 до M при i не кратному p:
   SM,p,k = (SM,p,k * i) mod p^k
```

Тоді $(N!/p^{\max}) \bmod p^k$ можна обчислити таким чином:

```
calcMod(N, p, k)
   якщо N = 0, то
       повернути 1

   повернути (
              Bp,k в степені (N div p^k) за модулем p^k *
              S(N mod p^k),p,k *
              calcMod(N div p, p, k)
             ) mod p^k
```

В даному випадку треба використовувати *алгоритм швидкого підняття до степеня* за модулем:

$$x^n \bmod m = \begin{cases} 1, & n = 0 \\ \left(x^{n/2}\right)^2 \bmod m, & n \vdots 2 \\ \left(x \cdot x^{n-1}\right) \bmod m, & (n-1) \vdots 2 \end{cases}$$

Використовуючи цю рекурентну формулу можна порахувати $x^n \bmod m$ за $O(\log n)$.

Тепер відомо, як обчислити $A = (N!/2^{\max}) \bmod 2^3$ і $B = (N!/5^{\max}) \bmod 5^3$. Звернемо увагу, що $N!/2^{\max} = N_0 \cdot 5^n$ і $N!/5^{\max} = N_0 \cdot 2^m$.

Постає логічне питання: чи можна, знаючи $(N_0 \cdot 5^n) \bmod 2^3$ і величину n, знайти $N_0 \bmod 2^3$? На щастя, в нашому випадку відповідь: «так».

Число 5^n — непарне, а тому — взаємно просте з 2^3:

$$\text{НСД}(5^n, 2^3) = 1 = 5^n a + 2^3 b \qquad (2)$$

при певних цілих a, b. Теорему про подання найбільшого спільного дільника (НСД) такою сумою доводять при логічно послідовному викладі теорії цілих чисел і многочленів у курсі вищої алгебри для студентів вищих навчальних закладів. Для учнів загально освітніх шкіл такий матеріал подано, наприклад, у таких виданнях:

- Вибрані питання елементарної математики/ За ред. чл.-кор. АН УРСР А.В.Скорохода. — Київ: Вища школа, 1982. — 455 с.;
- О.Б.Рудик. Початки алгебри, аналізу, аналітичної геометрії і теорії ймовірностей. Тернопіль: Навчальна книга – Богдан, 2005, 416 с.

Помноживши усі частини рівностей (2) на A, отримаємо таке твердження: *існує* єдиний з точністю до кратного 2^3 розв'язок N_0 рівняння: $N_0 \cdot 5^n = A \pmod{2^3}$.

Число N_0 — непарне, тому лишок його при діленні на 8 належить до множини {1, 3, 5, 7}. Ми можемо перебрати усі 4 варіанти значень і перевірити, при якому значенні справджується рівність (2). Таким чином ми можемо визначити A_0 — лишок від ділення N_0 на 2^3 . Аналогічно ми можемо визначити B_0 — лишок від ділення N_0 на 5^3, перебравши 100 лишків при діленні на 125, що не кратні 5.

Знаючи лишки від ділення N_0 на 2^3 і на 5^3, можна обчислити лишок від ділення N_0 на $2^3 \cdot 5^3 = 1000$. Для цього достатньо перебрати 1000 можливих лишків від 0 до 999 і перевірити, чи при діленні на 2^3 лишок буде A_0 , а при діленні на 5^3 лишок буде B_0. Існування розв'язку випливає з китайської теореми про лишки. Учням, не знайомим з цією теоремою, можна запропонувати такі міркування:

- $5 \cdot 0 = 0$, $5 \cdot 1 = 5$, $5 \cdot 2 \overset{8}{\equiv} 2$, $5 \cdot 3 \overset{8}{\equiv} 7$, $5 \cdot 4 \overset{8}{\equiv} 4$, $5 \cdot 5 \overset{8}{\equiv} 1$, $5 \cdot 6 \overset{8}{\equiv} 6$, $5 \cdot 7 \overset{8}{\equiv} 3$;
- розв'язати рівняння: $B_0 + 125b = A_0 + 8a$ відносно цілих a,b можна перебором 8 лишків b при діленні на 8 до досягнення кратності 8 таких виразів:

$B_0 + 125b - A_0 \overset{8}{\equiv} B_0 + 5b - A_0$.

Як уже зазначено, остаточна відповідь має вигляд: $(N_0 \cdot 2^{m-n}) \bmod 1000$.