Спасительная загадка

Автор задачи и разработчик: Даниил Орешников

В задаче был дан массив, полученный из некоторого другого массива a вычитанием из него некоторого его циклического сдвига. Требовалось восстановить все возможные величины сдвига, для которых это возможно.

В первой подгруппе можно было перебрать все возможные массивы и величины сдвига. Действительно, если подходящее a существует, не теряя общности можно взять его первый элемент равным 0 и, используя b, восстановить его элементы по порядку. Если какой-то элемент остался не восстановленным, можно принять его также равным нулю, и восстанавливать дальше.

Можно заметить, что такое решение работает за $\mathcal{O}(n^2)$, если просто перебирать элементы по очереди, чтобы найти первый еще не восстановленный. Это же решение проходит и пятую подгруппу. Для первой подгруппы достаточно было написать любой менее оптимальный перебор, например, за время $\mathcal{O}(n^3)$ или дольше.

Дальше можно было заметить, что если выбрать первый элемент массива a равным нулю, и начать восстанавливать его элементы как $a_{i+x} = a_i - b_i$, если известна величина сдвига. Таким образом, можно восстановить элементы a_{i+x}, a_{i+2x}, и так далее. Рано или поздно эта последовательность вернется в исходный элемент a_i по кругу. Необходимым и достаточным условием на то, что все эти элементы можно восстановить — что сумма использованных элементов b равна 0, если мы начали с a_i и вернулись к нему же.

На самом деле, если n и x взаимно просты, то такая последовательность восстановлений обойдет все элементы a и вернется в исходный индекс. Если же нет, то весь массив a разобьется на $\gcd(n, x)$ «циклов», которые можно восстанавливать независимо друг от друга.

Поэтому в случае, когда $n \in \mathbb{P}$, все возможные сдвиги x взаимно просты с n, и достаточно проверить, что сумма элементов b равна нулю, тогда все сдвиги возможны.

А в подгруппе, в которой $n = 2^k$, наибольший общий делитель с произвольным x может быть толкьо равен 2^t для $t \leqslant k$. Чтобы проверить, какие сдвиги x возможны, надо проверить, какие сдвиги 2^t возможны, все сдвиги с таким же gcd с n будут тоже возможны. А сдвиг 2^t возможен, когда для каждого остатка $r < 2^t$ верно, что $b_r + b_{2^t+r} + b_{2\cdot 2^t+r} + \ldots = 0$.

Такое условие можно посчитать для каждого t несложной динамикой. Пусть $\texttt{sum}[t][r]$ — указанная сумма. Тогда $\texttt{sum}[t][r] = \texttt{sum}[t+1][r] + \texttt{sum}[t+1][2^t + r]$. Подсчет такой динамики займет $\sum\limits_{t=0}^{k} 2^k \approx 2n$ времени.

Для полного решения требовалось для каждого возможного делителя n определить, может ли он быть корректным сдвигом. Тогда любой x, gcd которого с n равен этому делителю, будет тоже корректным.

В четвертой подгруппе достаточно малое количество b не равно нулю, поэтому можно было для каждого делителя n определить, какие из них входят в соответствующие «циклы». Для определенного делителя d смотрим, какие остатки дают ненулевые b_i по модулю d, группируем по остаткам, и проверяем, что сумма в каждой группе равна нулю.

Для последних двух подгрупп можно было воспользоваться динамикой, аналогичной подгруппе с $n = 2^k$. Если для каждого d — делителя n, найти некоторое простое число p в его разложении на простые ($d = p \cdot c$), можно пересчитывать динамику $\texttt{sum}[c][r]$ как

$$\texttt{sum}[c][r] = \sum_{i=0}^{p-1} \texttt{sum}[d][c \cdot i + r].$$

Время работы такого пересчета равно $\sum\limits_{d|n} \min\_\text{prime}(d)$, что близко к линейному от n времени работы. Осталось только быстро находить минимальное простое в разложении каждого делителя n. Если делать это за $\sqrt{d}$, можно было решить предпоследнюю группу, а если воспользоваться линейным решетом Эратосфена, получалось полное решение.