Домашнее задание 12. Теория чисел
Автор: *Головко Денис*, Б05–225

Загадка 1.

Решение.

Определим переменную x и будем последовательно проходить значения от 1 до n. Создадим переменную ans, в которую будем накапливать значения выражения $\left\lfloor \frac{n}{x} \right\rfloor$. Этот процесс позволит нам учесть все числа, которые делятся на x, вплоть до $\left\lfloor \frac{n}{x} \right\rfloor \cdot x$, включая x, $2x$, $3x$, и так далее. Это гарантирует, что мы рассмотрим все числа, имеющие x в качестве делителя, и только их.

Асимптотика. $O(n)$

Загадка 2.

Решение.

Найдем все простые числа до n с помощью решета Эратосфена $O(n \log \log n)$ времени.

Для каждого простого числа p из найденных ранее, проверим, делится ли число $n^2 + i$ на p, для всех i от 0 до n. Если делится, то $n^2 + i$ составное и его можно исключить из списка простых чисел.

Вместо явного исключения каждого числа, используем массив булевых значений длиной $n+1$, где каждый индекс i соответствует числу n^2+i. Изначально все значения в массиве устанавливаем в false.

Для каждого простого числа p, если $n^2 + i$ делится на p, устанавливаем значение в массиве булевых значений на индексе i в true.

Проходим по массиву булевых значений и выбираем индексы, которые остались false, тем самым определяя простые числа в интервале.

Таким образом, мы получаем список всех простых чисел в интервале $[n^2, n^2+n]$ с асимптотикой $O(n \log \log n)$, что соответствует теореме о распределении простых чисел.

Асимптотика. $O(n \log \log n)$

Загадка 4.

Решение.

Рассмотрим уравнение $x^n + y^n = z^n$. Преобразуем его в форму $x^n - z^n + y^n = 0$ и определим две переменные: U будет равняться $x^n - y^n$, а V будет соответствовать z^n. Так, мы получаем $U + V = 0$. Мы хотим выяснить, сколько существует комбинаций для достижения каждой пары значений U и V, что позволит нам находить ответы за время $O(m)$.

Для этого введем функцию f_l, которая будет представлять количество решений уравнения $k^n = l$ в $\mathbb{Z}_m$. Эту функцию можно вычислить за $O(m \log n)$. Далее мы составляем два многочлена: $X = f_0 + f_1 x + \ldots + f_{m-1} x^{m-1}$ и $Z = f_0 + f_{m-1} x + \ldots + f_1 x^{m-1}$. Произведение этих многочленов соответствует уравнению $x^n - y^n = U$. Таким образом, суммируя коэффициенты при x^i (где $i < m$) и при x^{i+m} в произведении $X \cdot Z$, мы можем вычислить количество комбинаций для достижения значения $U = i$. Число возможных комбинаций для получения $V = i$ уже известно и равно f_i, значит, мы решили загадку.

Асимптотика. $O(m \log n + m \log m) = O(N \log N)$, *где* $N = \max\{n, m\}$

Загадка 5.

Решение.

Рассмотрим загадку построения массива dp[X][Y], где X – количество используемых разрешенных цифр, а Y – их сумма. Мы хотим вычислить dp[n / 2][Y] для всех подходящих Y. Разгадкой будет сумма квадратов этих значений: $\sum_{y \in Y} dp[n/2][y]^2$, где Y обозначает набор допустимых значений сумм.

Чтобы упростить расчеты и избежать подсчета dp[.][.] за $O(n^2)$, воспользуемся многочленом: $P(x) = d_1 + d_2 \cdot x + \ldots + d_k \cdot x^{k-1}$. Коэффициенты этого многочлена при x^r соответствуют dp[1][r + 1]. Возведение этого многочлена в m-ую степень даст коэффициенты, равные dp[m][.]. Докажем это по индукции. База уже установлена. Предположим, что коэффициенты $P^m = c_1 + c_2 \cdot x + \ldots + c_{m(k-1)+1} \cdot x^{m(k-1)}$ соответствуют dp[m][.]. Тогда $P^{m+1} = P^m \cdot P$, где коэффициент при x^{r-1} равен $e_r = \sum_{i,j;i+j=r} c_i \cdot d_j$. Здесь c_i – количество последовательностей длиной m с суммой i, а d_j – количество последовательностей длиной 1 с суммой j. Их произведение равно количеству последовательностей длиной m + 1 с суммой i + j = r.

Используя метод быстрого возведения в степень и FFT для перемножения многочленов, мы можем вычислить dp[n/2][.] за $O(\log(k) \cdot k + O(\log(2 \cdot k) \cdot 2k + \ldots + O(\log(\frac{n}{2}) \cdot \frac{n}{2})) = \ldots = O(n \log n)$, тем самым решив загадку.

Асимптотика. $O(n \log n)$

Загадка 7.

Решение.

Перефразируем загадку и будем находить недопустимые позиции для вхождения подстроки p в строку s. Недопустимая позиция определяется как такая, что символ $p[j]$ не соответствует символам в s, находящимся в пределах окрестности размера k от позиции $i + j$.

Для решения загадки создадим массив stepanov[a][r], отображающий позиции в s, на которых символ a отсутствует в подстроке s[stepanov[a][r] : stepanov[a][r] + $2k$]. Элементы массива упорядочены так, что stepanov[a][1] < stepanov[a][2] < ... < stepanov[a][kulapin[a] − 1], где kulapin[a] обозначает количество таких недопустимых позиций для символа a.

Позиция i в s является недопустимой для символа $a = p[j]$, если существует l такое, что stepanov[a][l] = $i+j-k$. Следовательно, значение i может быть вычислено как stepanov[a][l]$-j+k$. Мы хотим подсчитать все такие недопустимые позиции i для каждого символа.

Для каждого символа a в алфавите Σ определим: $P_a(x) = \sum_{0 \leqslant d \leqslant m-1 \text{ и } p[d]=a} x^d$ и $Q_a(x) = \sum_{i=1}^{\text{kulapin}[a]-1} x^{N-(k+\text{stepanov}[a][i])}$, где N — достаточно большое число, чтобы предотвратить перекрытие коэффициентов при умножении, то есть $N = O(n)$ и удовлетворяющее неравенству $N \geqslant k + 2m$. Произведение $P_a \cdot Q_a$ даст нам все недопустимые позиции i для символа a.

Наконец, обнаружив плохие позиции для каждого символа в Σ, мы исключаем их из общего количества позиций в s, чтобы найти допустимые позиции для вхождения p.

Асимптотика. $O(|\Sigma| \cdot n \log n)$*, поскольку для каждого символа из* Σ *мы проводим умножение многочленов с помощью FFT*

Загадка 8.

Решение.

Вспомним лемму, которая устанавливает критерий Лежандра для квадратичных вычетов и невычетов:

Лемма. Для $a \in \mathbb{Z}_p^*$*, a является квадратичным вычетом, если* $a^{\frac{p-1}{2}} \equiv 1 \mod p$*, и квадратичным невычетом, если* $a^{\frac{p-1}{2}} \equiv -1 \mod p$.

Используя эту лемму, можно показать, что если $p \equiv 3 \mod 4$, то -1 является квадратичным невычетом, потому что $(-1)^{\frac{p-1}{2}} \equiv -1 \mod p$. Аналогично, если $p \equiv 1 \mod 4$, можно найти квадратичный невычет путем поиска элемента a, для которого $a^2 \equiv -1 \mod p$. Приведу алгоритм поиска квадратного корня:

Если $p \equiv 3 \mod 4$, квадратный корень a может быть найден как $\pm a^{\frac{p+1}{4}} \mod p$.

Если $p \equiv 1 \mod 4$, представляем p как $p = 1 + m \cdot 2^s$, где m нечетно.

Инициализируем $u_0 = a^m$ и $v_0 = a^{\frac{m+1}{2}}$, где $v_0^2 \equiv a \cdot u_0 \mod p$. Находим произвольный квадратичный вычет b и вычисляем $c = b^m$, так что $c^{2^{s-1}} \equiv -1 \mod p$. Далее итеративно обновляем u_i и v_i до тех пор, пока u_i не станет равным 1, что указывает на то, что v_i является квадратным корнем из a.

Существование детерминированного полиномиального алгоритма для извлечения квадратных корней означает, что можно эффективно проверить, является ли элемент a квадратичным вычетом, выполнив возведение в степень и сравнение. Если такой алгоритм существует, то мы можем также проверить, является ли a квадратичным невычетом, не обнаружив корня. Это означает, что существование одного из алгоритмов подразумевает возможность выполнения другого, так как оба сводятся к возведению в степень в поле $\mathbb{Z}_p$, что может быть выполнено за полиномиальное время относительно $\log p$, то есть загадки равносильны.

Асимптотика. $O\left(poly(\log p)\right)$