Вторая лига. Теория чисел

Разбор задач

В рамках этого разбора под делением ($/$, $\frac{a}{b}$) подразумевается целочисленное деление, если не сказано другого.

Задача A. Простые числа (2)

Задача на реализацию решета Эратосфена. Стоит заметить, что Time Limit на этой задаче достаточно строгий, поэтому некоторые правильные решения могли не проходить все тесты. Однако, если написать решето достаточно оптимально и/или ускорить вывод можно набрать полный балл.

Время - $O(n * \log\log n)$.

Память - $O(n)$.

Задача B. Делимость на 3

Пусть (n_i) – последовательность остатков элементов последовательности, заданной в условии.

Рассмотрим элемент последовательности n_i.

$$n_i \;=\; (n_{i-1} * 10^c \;+ i) \;\%\; 3, \text{при } i \neq 1$$

Известно, что $N \;\%\; 3 = S(N) \;\%\; 3$. Где $S(N)$ – сумма цифр числа N. Это несложно доказать самостоятельно.

Нам не важно каким является число c, так как умножение на 10^c не влияет на остаток, согласно описанному свойству.

То есть, n_i $\text{однозначно определяется по паре}$ n_{i-1} и $i \;\%\; 3$. Так как количество таких различных пар равно 9, можно вручную исследовать последовательность и обнаружить цикл.

$$1, 0, 0, 1, 0, 0, 1, 0, 0, 1, \ldots$$

Период равен $(1, 0, 0)$, начинается с первого элемента, его длина равна 3. Так как нулю не равен только первый элемент, то нам достаточно от общего числа элементов отнять количество циклов присутствующих в последовательности (возможно, последний цикл будет не полным). То есть, ответ равен $N - (N + 2)/3$.

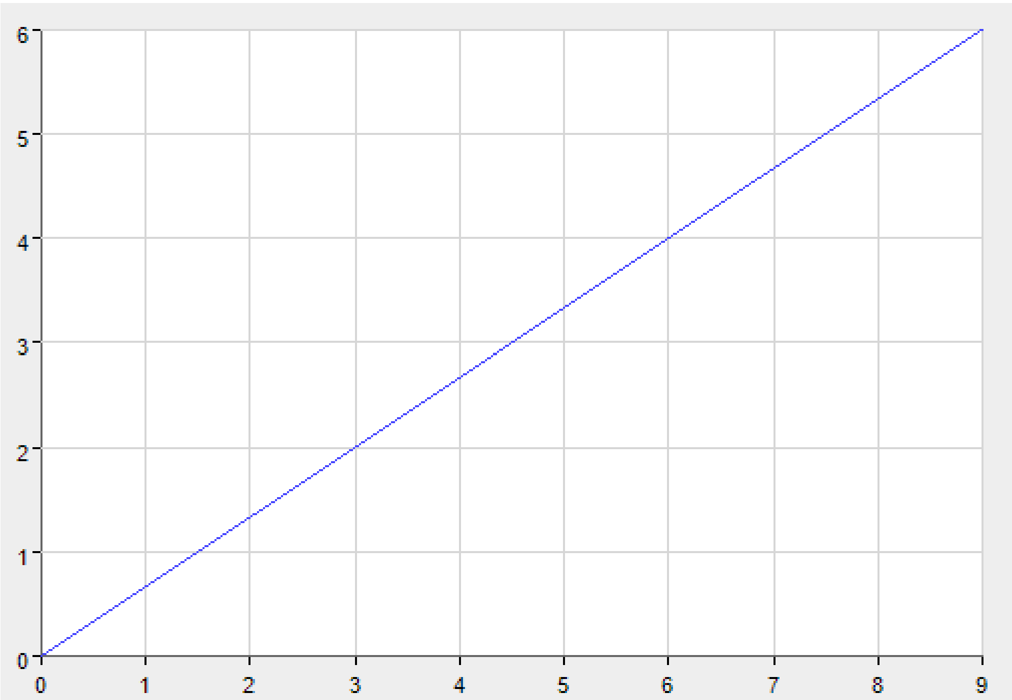
Время - $O(1)$. Память - $O(1)$.

Задача C. Отрезок

Для случаев, когда отрезок параллелен одной из осей, ответ очевиден и равен длине отрезка, увеличенной на единицу.

Рассмотрим остальные случаи. Не нарушая общности, предположим, что первый конец отрезка лежит в начале координат, а второй – в первой четверти координатной плоскости и имеет координаты (x, y).

Рассмотрим пример для $x = 9, y = 6$.



Что бы найти точку на отрезке, с наименьшими целочисленными координатами (не считая $(0, 0)$), необходимо найти отношение координат второго конца отрезка и представить в виде сокращенной дроби.

$$\frac{\Delta x}{\Delta y} = \frac{9}{6} = \frac{3}{2}.$$

Мы получили точку $(3, 2)$.

Понятно, что точки $(3k, 2k)$, где k: $(k \in Z, 3k \leq 9)$, так же принадлежат отрезку. Таких точек будет $\gcd(x, y)$. Ответом будет $\gcd(x, y) + 1$, так как следует учесть еще и точку $(0, 0)$.

Время - $O(\log \min(n, m))$.

Память - $O(1)$.

Задача D. Прості числа царства Ерудит

В задаче просят проверять равно ли количество делителей числа трем. Понятно, что числа, у которых ровно три делителя, это квадраты простых чисел.

То есть, нам нужно быстро проверять, является ли число N квадратом простого.

Способ 1.

Проверяем является ли N квадратом целого. Если да, проверяем является ли $\sqrt{N}$ простым. Время - $O(\mathrm{q} * \sqrt[4]{N})$. Память - $O(1)$.

Способ 2.

Запоминаем все квадраты простых чисел. Для каждого N, запускаем бинарный поиск для проверки принадлежности числа массиву (вместо массива и бинарного поиска можно использовать set из stl). Время - $O(\mathrm{q} * \log \frac{N}{\log N} + N * \log \log N)$. Память - $O(N)$.

Задача E. НОД и НОК

Вспомним представление НОД и НОК.

$$
\begin{aligned}
N &= 2^{\alpha_1} * 3^{\alpha_2} * 5^{\alpha_3} * \ldots \\
M &= 2^{\beta_1} * 3^{\beta_2} * 5^{\beta_3} * \ldots \\
\text{НОД}(N, M) &= 2^{\min(\alpha_1, \beta_1)} * 3^{\min(\alpha_2, \beta_2)} * 5^{\min(\alpha_3, \beta_3)} * \ldots \\
\text{НОК}(N, M) &= 2^{\max(\alpha_1, \beta_1)} * 3^{\max(\alpha_2, \beta_2)} * 5^{\max(\alpha_3, \beta_3)} * \ldots \\
&\alpha_i, \beta_i \geq 0
\end{aligned}
$$

Найдем каноническое разложения $\text{НОД}(N, M)$ и $\text{НОК}(N, M)$ и рассмотрим каждое простое число в них.

Пусть p_i – рассматриваемое простое число.

α_i – степень, в которой p_i входит в разложение $\text{НОД}(N, M)$.

β_i – степень, в которой p_i входит в разложение $\text{НОД}(N, M)$.

$\alpha_i + \beta_i > 0$, иначе нет смысла рассматривать p_i.

Теперь можно рассмотреть 3 случая:

1. $\alpha_i < \beta_i$. В этом случае мы получаем 2 варианта разложения. Либо N содержит в разложении p_i в степени β_i, а M - p_i в степени α_i, либо наоборот.
2. $\alpha_i = \beta_i$. И M, и N содержат p_i в равных степенях.
3. $\alpha_i > \beta_i$. Таких пар M и N не существует.

Подытожим. Если существуют α_i и β_i такие, что $\alpha_i > \beta_i$, то ответ равен 0, иначе ответ равен 2^t, где t - количество α_i и β_i таких, что $\alpha_i < \beta_i$. Время - $O(\sqrt{\max(\text{НОД}(N,M),\text{НОК}(N,M))})$.

Память - $O(\log\max(\text{НОД}(N,M),\text{НОК}(N,M)))$.

Задача F. Нова гра

В задаче необходимо найти число, у которого минимальный делитель, отличный от 1, наибольший, среди всех чисел на отрезке.

Очевидно, что минимальный делитель, отличный от 1, это наименьший простой делитель.

Понятно, что если на отрезке есть хотя бы одно простое число, то наибольшее среди них – искомое. Это следует из того, что никакое число с отрезка не может иметь наименьший простой делитель большим, чем наибольшее простое число с этого отрезка.

Так как мы знаем, что интервал между соседними простыми числами достаточно мал, по сравнению с самими числами, мы можем сформировать алгоритм поиска нужного числа.

Начинаем двигаться с правого конца отрезка, при этом запоминая наибольший минимальный простой делитель, среди тех чисел, которые прошли. Если текущее число оказалось простым, то проход по отрезку нужно оборвать. Если на отрезке не оказалось простого числа – мы запомнили нужную нам величину. Ответом будет найденная величина минус 1, так как ведущий начинает с 2.

Если $d(n) = p_{n+1} - p_n$, где p_i – i-тое простое.

Время - $O(d\left(\frac{B}{\ln B}\right)\sqrt{B})$. Память - $O(1)$.

Задача G. Многочлен

Предположим, что мы раскрыли скобки и у нас получился полином какой-то степени. Понятно, что если мы подставим 1 вместо X, то мы получим сумму коэффициентов. Изначальное выражение эквивалентно разложенному. То есть, нам нужно найти значение заданного выражения при $X = 1$ по заданному модулю и это будет ответом. Время - $O(1)$. Память - $O(1)$.

Задача H. Марсианские факториалы

В рамках разбора этой задачи в нижних индексах указывается основание системы счисления, если не указывается – подразумевается десятичная система счисления.

Давайте разберемся, «откуда берутся» нули в конце числа в системе счисления по основанию K.

Рассмотрим следующие тождества:

$$10_K = K_{10}$$

$$10 \ldots 0_K = \ 10_K^t \ = K_{10}^t, t \ \in N$$

$$p_K * 10_K^t \ = p_{10} * K_{10}^t, t \ \in N, p \ \in N, \text{в конце } p \text{ нет нулей}$$

То есть, для нахождения количества нулей в конце числа в системе счисления по основанию K, нам нужно вычислить максимальную степень числа K, на которую наше число делиться.

Однако, явно вычислить факториал мы не имеем возможности, поэтому давайте придумаем оптимальный способ вычисления.

Рассмотрим каноническое разложение K:

$$K = p_1^{\alpha_1} * p_2^{\alpha_2} * \ldots * p_s^{\alpha_s}$$

Понятно, что в разложении $N!$, нас интересуют только простые, которые есть в разложении K.

$$N! = \ p_1^{\beta_1} * p_2^{\beta_2} * \ldots * p_s^{\beta_s} * t$$

Тогда искомая степень равна $\min(\frac{\beta_1}{\alpha_1}, \frac{\beta_2}{\alpha_2}, \dots, \frac{\beta_s}{\alpha_s})$.

Осталось научиться быстро считать β_i.

Зафиксируем p_i. В последовательности натуральных чисел каждое p_i число, имеет в разложении p_i, каждое ${p_i}^2$ – имеет ${p_i}^2$ и т. д.

Итого $\beta_i = \frac{N}{p_i} + \frac{N}{{p_i}^2} + \dots + \frac{N}{{p_i}^r}$.

Время - $O(\log K * \log N + \sqrt{K})$. Память - $O(\log K)$.

Задача I. A^B mod C

Обычное быстрое поднесение в степень по модулю не даст полный балл на C++, так как возникает переполнение типов при умножении.

Одним из возможных решений этой проблемы является применение идеи быстрого поднесения в степень для умножения.

Заменив умножение на суммирование, получаем уже не совсем быстрое умножение по модулю, однако оно помогает нам избежать переполнения. Время - $O(\log A * \log B)$. Память - $O(1)$.

Задача J. Гарні числа

Если число не делится ни на один квадрат натурального числа, отличного от 1, то будем называть это число свободным от квадратов.

То, что произведение всех заданных чисел не свободно от квадратов, эквивалентно тому, что существуют два заданных числа, которые имеют общий делитель отличный от 1, либо какое-то заданное число не свободно от квадратов (возможно, оба случая одновременно).

В первом случае достаточно рассмотреть все попарные НОДы.

Разберемся со вторым случаем. Если число M не свободно от квадратов, то его можно представить в виде $M = x^2 * y$. Снова получаем два случая:

2. $y < \sqrt[3]{M}$. Тогда за $O(\sqrt[3]{M})$ мы можем найти x (если такой есть).
3. $y < \sqrt[3]{M}$. Тогда за $O(\sqrt[3]{M})$ мы можем “исключить” y и проверить является ли квадратом, то что осталось.

Время - $O(N^2 \log M + N * \sqrt[3]{M})$. Память - $O(N)$.