Обозначения

$\sum_{i=1}^{n} a_i = a_1 + a_2 + \ldots + a_n$

$\prod_{i=1}^{n} a_i = a_1 \cdot a_2 \cdot \ldots \cdot a_n$

$f(n) = \mathcal{O}(g(n))$ — существуют такие числа a и b, что для всех n: $f(n) \le a + bg(n)$.

$a \equiv b \pmod{m}$ — a и b имеют одинаковые остатки при делении на m.

Задачи

Определение. Функция Эйлера $\varphi(n)$ — количество натуральных чисел не больших n, которые взаимно просты с n.

Если число n имеет разложение на простые числа в виде $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$, то

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right)$$

или иначе говоря

$$(p_1 - 1) \cdot p_1^{a_1 - 1} \cdot (p_2 - 1) \cdot p_2^{a_2 - 1} \cdot \ldots \cdot (p_k - 1) \cdot p_k^{a_k - 1}$$

Определение. (*Теорема Эйлера*) Для любого числа k взаимно простого с n, $k^{\varphi(n)} \equiv 1 \pmod{n}$.

Частный случай этой теоремы при простом n называется *малой теоремой Ферма*. Этот случай примечателен тем, что $\varphi(p) = p - 1$ для простого p, поэтому теорема принимает совсем простой вид.

Задача 1. Найти количество натуральных чисел, которые меньше n и взаимно просты с числом m, за $\mathcal{O}(\sqrt{m})$.

Задача 2. Найти сумму НОД по всем подотрезкам массива натуральных чисел, не больших C, за $\mathcal{O}(n \log C)$.

Задача 3. Найти сумму НОД по всем непустым подмножествам массива из n натуральных чисел, не больших C, за $\mathcal{O}(n + C \log C)$. Ответ найдите по модулю $10^9 + 7$.

Задача 4. Найдите сумму всех простых чисел от 1 до n за $\mathcal{O}(n \log \log n)$ времени и $\mathcal{O}(\sqrt{n})$ памяти.

Задача 5. Докажите, что в процессе работы расширенного алгоритма Евклида все x_i не превосходят b_i по модулю, а все y_i не превосходят a_i по модулю. Из чего следует, что если входные данные алгоритма Евклида помещаются в какой-то тип данных, то и во время вычислений не произойдет никаких переполнений.

Задача 6. Перемножьте два числа a и b по модулю $m \le 10^{18}$ на C++ без использования `int128` за

a) $\mathcal{O}(\log m)$

b) $\mathcal{O}(1)$

Задача 7. За $\mathcal{O}(n)$ для каждого числа от 1 до n найдите:

a. Количество его делителей.

b. Сумму его делителей.

c. Функцию Эйлера от него.

Задача 8. Дан массив a длины n. Необходимо для каждого k от 1 до n посчитать сумму элементов массива a на позициях, делящихся на k ($a_0 + a_k + a_{2k} + \ldots$) за a) $\mathcal{O}(n \log n)$ b) $\mathcal{O}(n \log \log n)$.

Задача 9. Назовем суммирующей функцией Эйлера $\varphi_\Sigma(n)$ сумму всех натуральных чисел, не больших n, которые взаимно просты с n. Придумайте формулу для $\varphi_\Sigma(n)$.

Задача 10. Назовём натуральное число кубастым, если его можно представить в виде $a^3 \cdot b$ для каких-то натуральных $a > 1, b \ge 1$. Найти количество кубастых чисел, не больших $n \le 10^{18}$.

Задача 11. a) Даны числа $a_1, a_2, \ldots, a_n$, а также простой модуль p. Необходимо найти обратные по модулю p ко всем a_i за $\mathcal{O}(n + \log p)$.

b) Найдите обратные ко всем числам от 1 до n по простому модулю p ($n < p$) за $\mathcal{O}(n)$.

Задача 12. Даны два числа a и b. Проверьте, влезает ли их произведение в тип `long long`.

Задача 13. Пусть $n \ge p$. Обозначим за $n!_p$ число, полученное из $n!$ делением его на p пока делится. Посчитайте $n!_p$ по модулю p за a) $\mathcal{O}(p \log_p n)$ b) $\mathcal{O}(p + \log_p n)$.

Задача 14. Дан массив a длины $n \le 10^6$ ($1 \le a_i \le 10^7$). Необходимо найти пару его элементов с наименьшим значением НОКа.

Задача 15. (*) Научитесь выполнять n запросов поиска дискретного логарифма (найти такое x_i, что $a_i^{x_i} \equiv b_i \pmod{p}$) по простому модулю p за $\mathcal{O}\left(\sqrt{p \cdot n} + n \log p\right)$.

Задача 16. (**) Найдите количество простых чисел от 1 до n за $\mathcal{O}(n^{2/3})$.

Задача 17. (***) Докажите, что количество делителей $d(n)$ числа n — это субполиномиальная величина. То есть для любого $\varepsilon > 0$ верно, что $\frac{d(n)}{n^\varepsilon} \to 0$ при $n \to +\infty$ (иными словами, $d(n) = o(n^\varepsilon)$).

Задача 18. (******) Правда ли, что для любого натурального n существует натуральное $m \neq n$, такое что $\varphi(n) = \varphi(m)$?