24 Программа EulerPhi

Задача. Бобу требуется написать программу, которая определяет количество различных простых делителей заданного натурального числа n. Число n может быть очень большим, его факторизация затруднена. Однако Боб может воспользоваться программой `EulerPhi`, которая выполняется на суперкомпьютере Трента и за приемлемое время находит значение функции Эйлера от n. Помогите Бобу, используя следующие дополнительные данные: число простых делителей нечетно и все они имеют вид $2^s r + 1$, где s — натуральное число, общее для всех делителей, r — нечетное число.

Решение. Пусть

$$n = \prod_{i=1}^{k} p_i^{e_i},$$

где k — нечетное, p_i — различные простые, $p_i = 2^s r_i + 1$. Значение функции Эйлера

$$\varphi(n) = \prod_{i=1}^{k} p_i^{e_i - 1}(p_i - 1)$$

и

$$d = \gcd(n, \varphi(n)) = \prod_{i=1}^{k} p_i^{e_i - 1}.$$

Поэтому

$$\frac{\varphi(n)}{d} = \prod_{i=1}^{k}(p_i - 1) = 2^{sk} r',$$

$$\frac{n}{d} = \prod_{i=1}^{k} p_i = \prod_{i=1}^{k}(2^s r_i + 1) = 2^s r'' + 1,$$

где $r' = r_1 r_2 \ldots r_k$ и $r'' = r_1 + r_2 + \ldots + r_k + 2^s r'''$ — нечетные.

Определяя максимальную степень 2, на которую делится $\frac{n}{d} - 1$, находим s. Определяя максимальную степень 2, на которую делится $\frac{\varphi(n)}{d}$, находим sk. После этого находим $k = \frac{sk}{s}$. □

Обсуждение. На самом деле можно обойтись без дополнительных данных о делителях n. Более того, с помощью программы `EulerPhi` можно определить не только число делителей, но и сами делители. Оказывается, что Г. Миллер и М. Рабин в статьях, посвященных тесту простоты, который впоследствии был назван тестом Миллера — Рабина, попутно (прямо или косвенно) доказали следующие факты:

Теорема (Миллер, 1976). Если выполнена расширенная гипотеза Римана, то существует алгоритм, который по паре $(n, \varphi(n))$ находит нетривиальный делитель n за время $O((\log n)^6)$.

Теорема (Рабин, 1980). Существует вероятностный алгоритм, который по паре $(n, \varphi(n))$ находит нетривиальный делитель n за среднее время $O((\log n)^6)$.