Об одном признаке делимости чисел в двоичной системе счисления

Еникеев Разиль Радикович

ассистент

Институт вычислительной математики и информационных технологий

Казанский (Приволжский) федеральный университет, Казань, Россия

E-mail: renikeev@kpfu.ru

Научный руководитель *— Ишмухаметов Шамиль Талгатович*

Еще со школы известны быстрые способы проверки делимости одного числа на другое, представленных в десятичной системе счисления. Например, делимость числа a на 2, 5, 10: необходимо, чтобы последний десятичный разряд a делился на соответсвующее число; делимость числа a на 3 и 9: необходимо, чтобы сумма цифр a делилась на соответствующее число.

Однако, в подобных критериях используется представление чисел в десятичной системе счисления, что затрудняет применение этих признаков для вычислений на компьютере, в котором числа хранятся в двоичной системе. Также из этих примеров видно, что признаки делимости отличаются друг от друга, а это опять же затрудняет реализацию вычисления остатка по модулю на компьютере.

В нашей работе предлагается общий признак делимости a на нечетное число b, где a представлено в двоичной системе счисления.

Рассмотрим число $a = (a_n a_{n-1} \dots a_1 a_0)_2 = \sum_{i=0}^{n} a_i 2^i$. Остаток от деления a на b можно найти по формуле

$$a \bmod b = \left(\sum_{i=0}^{n} (a_i 2^i \bmod b) \right) \bmod b. \tag{1}$$

Рассмотрим в (1) равный единице i-й бит числа a и перенесем этот бит на j-ую ($i > j$) позицию (j-й бит сохраняется), или по-другому заменим 2^i на 2^j, сохранив остаток от деления, тогда имеем

$$\begin{aligned} 2^i &\equiv 2^j \pmod b, \\ 2^{i-j} &\equiv 1 \pmod b. \end{aligned} \tag{2}$$

Определим *шаг сдвига с сохранением остатка*, или *шаг*, как минимальное натуральное число $s = i - j$, удовлетворяющее (2). Например, для 3 значение шага равно 2. Из формулы (1) видно, что на s можно сдвинуть и i-й бит, равный нулю, с сохранением значения

остататка от деления на b. Следовательно, можно произвольный i-й ($i \geq s$) бит сдвинуть на s бит вправо, сохраняя значение остатка от деления. Такой сдвиг можно выполнять до тех пор, пока $i \geq s$. Тогда, записав $a = (a'_m \dots a'_0)_{2^s}$, получим следующий признак делимости

$$a \bmod b = \left(\sum_{i=0}^{m} a'_i \right) \bmod b. \tag{3}$$

Например, для $b = 3$ мы суммируем числа длины 2 бита.

Описанный выше способ эффективен для вычисления человеком, а для эффективной реализации на компьютере лучше всего представить a в виде $a = (a'_m \dots a'_0)_{2^{ks}}$, где k — натуральное число, а ks — наибольшее кратное числа s, не превосходящее длины машинного слова. Для этого представления будет выполняться признак делимости (3), но в то же время количество слагаемых будет меньше. Таким образом, вычисление остатка деления произвольного большого числа можно свести к суммированию чисел длины ks.

По теореме Эйлера шаг s для нечетного числа b существует всегда [1], а следовательно предлагаемый признак делимости можно применять при вычислениях по модулю произвольного нечетного числа, меняя лишь значение шага.

Преимущества предложенного метода: возможность распараллеливания алгоритма и эффективная реализация на компьютерах.

Недостаток предложенного метода — для эффективной реализации на компьютере необходимо выбирать в качестве модуля такие числа, шаг которых будет малым (менее 32 или 64).

Наиболее эффективным применением предложенного признака является нахождение остатка от деления длинного числа (произвольно высокой точности) на малое. Эта задача может возникнуть в следующих ситуациях: алгоритмы на основе китайской теоремы об остатках [2], проверка наличия малых делителей в тестах простоты длинных чисел [2], первый шаг при удалении ложных делителей [3].

Литература

1. Виноградов И. М. Основы теории чисел. М.: Наука, 1981.
2. Ишмухаметов Ш. Т. Методы факторизации натуральных чисел. Казань: Казанский университет, 2011.
3. Sorenson J. Two fast GCD algorithms // J. Algorithms. 1994. V. 16, № 1. P. 110–144.