Секция «Математическая логика, алгебра и теория чисел»

О наибольшем количестве шагов в алгоритме SJWA вычисления НОД

Научный руководитель – Ишмухаметов Шамиль Талгатович

Долгов Дмитрий Александрович

Аспирант

Казанский (Приволжский) федеральный университет, Институт вычислительной математики и информационных технологий, Казань, Россия

E-mail: DADolgoff@yandex.ru

К-арный алгоритм - один из наиболее быстрых алгоритмов вычисления НОД натуральных чисел [1]. Пусть $u > v > 0$ - нечетные натуральные числа, натуральное число $k < v$, числа $m = \lfloor\sqrt{k}\rfloor$, $rk = \sqrt{k}$. На каждом шаге произвольного к-арного алгоритма необходимо искать коэффициенты x, y, такие что $xu+yv = 0\ (mod\ k)$ для фиксированного целого k: $\alpha gcd(u, v) = gcd(v, |(xu + yv)/k|)$. Целое число α является побочным множителем. Алгоритм *SJWA* – один из вариантов к-арного алгоритма, который не накапливает побочных множителей в ходе работы: $gcd(u, v) = gcd(|(x_1u + y_1v)/k|, |(x_2u + y_2v)/k|)$ [2].

Для вычисления наибольшего количества шагов в алгоритме *SJWA* можно воспользоваться техникой Ламе. Но для этого необходимо найти наибольшее нечетное значение к-арной редукции, получаемой на текущем шаге алгоритма. Отсюда можно сформулировать следующую задачу.

Пусть $T = T(m)$ – целое число, причем $1 \leqslant T \leqslant 2$ и число $u = vm - T$. Пусть число k не является полным квадратом. Требуется найти наибольшее нечетное значение функции f, область значения которой – натуральные числа

$$f(n_s, d_s, n_{s+1}, d_{s+1}) = \frac{-d_s(vm - T) + vn_s}{n_s d_{s+1} - d_s n_{s+1}}, \tag{1}$$

а также значения переменных $n_s, d_s, n_{s+1}, d_{s+1}$, при которых достигается это наибольшее значение с учетом следующих условий

$$\begin{cases} 1 \leqslant n_{s+1} \leqslant m, \\ 2 \leqslant |d_s| \leqslant |d_{s+1}| \leqslant m, \\ m \leqslant n_s \leqslant k, \\ m^2 < k < (m+1)^2. \end{cases} \tag{2}$$

Все переменные и параметры являются дискретными, поэтому у нас возникает задача дискретной оптимизации. Переменные n_s, n_{s+1}, d_s, d_{s+1} зависят от чисел k, u, v, то есть сами являются функциями. Решение $d_3 = -(m-1)$, $d_4 = m$, $n_3 = m+1$, $n_4 = 1$, $k = m^2 + 2m - 1$ не удовлетворяет условию задачи выбора наибольшего нечетного значения функции f.

Нетрудно заметить, что сформилированная задача максимизации функции f является задачей нелинейной оптимизации, для которой можно проверить условия Каруша – Куна – Таккера. Применению этих условий, а также приминению техники Ламе при решении исходной **теоретико-числовой задачи** поиска наибольшего количества шагов в алгоритме *SJWA* и будет посвящен доклад.

Источники и литература

1) Sorrenson J. Two fast GCD Algorithms // J.Alg., 16. 1994. No 1. pp.110-144.

2) Sedjelmaci S. M. Jebelean–Weber's algorithm without spurious factors // Information Processing Letters, 102. 2007. No 6. pp. 247-252.