Секция «Математическая логика, алгебра и теория чисел»

О новом k-арном алгоритме 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: regist.gymnast@yandex.ru

К-арный алгоритм - один из наиболее быстрых алгоритмов вычисления НОД натуральных чисел [1]. Пусть $u > v > 0$ - нечетные натуральные числа, натуральное число $k \in (2, v)$. На каждом шаге произвольного k-арного алгоритма необходимо найти коэффициенты x, y такие что $xu + yv = 0 \ (mod\ k)$ для фиксированного целого k. В предложенном k-арном алгоритме используется два различных шага редукции: один шаг алгоритма Евклида с выбором наименьшего по модулю остатка чередуется с одним шагом k-арного алгоритма. В рамках последнего задействуется (представленная ниже) модификация алгоритма поиска коэффициентов $M - JWA$ [2], позволяющая искать числа x, y, причем для их поиска она использует не исходные числа u, v, а минимально возможные числа u', v', для которых выполняется соотношение

$$\left|\frac{v}{u} - \frac{v'}{u'}\right| < \frac{1}{k}. \tag{1}$$

Это позволяет оперировать числами меньшего размера для нахождения чисел x, y. Предлагаемый k-арный алгоритм не накапливает побочных множителей, поскольку числа x, y, вычисляемые во время работы k-арного алгоритма, удовлетворяют лемме Седжелмаси [2]. В докладе будет представлена оценка количества шагов алгоритма в худшем случае, а также оценка сложности алгоритма в худшем случае.

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.

Иллюстрации

Algorithm 1 Поиск коэффициентов x,y

$u' = \lfloor u/2^t \rfloor$, $v' = \lfloor v/2^t \rfloor$, $t \in [1, \lfloor \log(v) \rfloor]$
$r = v/u \ mod\ k$
$f_1 = (n_1, d_1) = (k, 0)$
$f_2 = (n_2, d_2) = (r, 1)$
while $n_2 > s$ **do**
    $f_1 = f_1 - \lfloor n_1/n_2 \rfloor f_2$
    $swap(f_1, f_2)$
return $\begin{pmatrix} n_1 & d_1 \\ n_2 & d_2 \end{pmatrix}$

Рис. Алгоритм поиска коэффициентов x,y