Секция «Математическая логика, алгебра и теория чисел»

О среднем числе шагов в к-арном алгоритме Соренсона с правым сдвигом с фиксированным знаменателем

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

Алгоритм Соренсона - один из наиболее быстрых алгоритмов вычисления НОД натуральных чисел [2]. Пусть $u > v$, $u,\ v \in \mathbb{N}$, $\gcd(u,v) = 1$. Необходимо найти коэффициенты $x,\ y \in \mathbb{Z}^{\neq 0}$: $xu - yv \ = 0 \mod k$ для некоторого фиксированного $k \in \mathbb{N}^{\geqslant 2}$, $\gcd(u,k) = \gcd(v,k) = 1$. Справедлива формула: $\alpha \gcd(u,v) = \gcd(v,(xu-yv)/k)$, $\alpha \in \mathbb{N}$. Число $\frac{u}{v}$ можно разложить в к-арную цепную дробь

$$\frac{u}{v} = \frac{y_1}{x_1} + \cfrac{k_1}{\frac{y_2}{x_2} + \cfrac{k_2}{\ddots + \cfrac{k_{n-1}}{y_n}}} = \langle (y_1,x_1,k_1);(y_2,x_2,k_2),\cdots (y_n,x_n,k_n)\rangle$$

длины n, в которой $\frac{y_2}{x_2}$, ..., $\frac{y_n}{x_n} \in \mathbb{Q}^{\neq 0}$, $\frac{y_1}{x_1} \in \mathbb{Q}$, $k_i \in \mathbb{Z}^{\geq 2}$, $i \geqslant 1$. В алгоритме Соренсона $k_i = k$, x_i и y_i — коэффициенты на i шаге алгоритма, $u_i x_i - v_i y_i = 0 \mod k$.

Обозначим континуант как $[g_1,...,g_n]$, где $g_i = (y_i,x_i,k_i)$, $i \in \overline{1,n}$. Для континуантов к-арных цепных дробей справедливо: $[\,] = 1$, $[g_1] = y_1$, $[g_1,g_2] = y_1y_2 + k_1x_1x_2$.

Предложение 1. *Пусть* $\frac{u}{v} = \langle g_1; g_2, g_3, \cdots g_n\rangle$, $n \geqslant 3$, $m \geqslant 1$, *тогда*

1) $[g_1,...,g_n] = y_n\,[g_1,...,g_{n-1}] + k_{n-1}x_{n-1}x_n\,[g_1,...,g_{n-2}]$.
2) $[g_1,g_2,\cdots g_n] = y_1\,[g_2,\cdots g_n] + k_1x_1x_2\,[g_3,\cdots g_n]$
3) $[g_1,...,g_n] = [g_1,...,g_m]\,[g_{m+1},...,g_n] + k_mx_mx_{m+1}\,[g_1,...,g_{m-1}]\,[g_{m+2},...,g_n]$
4) $[g_1,...,g_n] = [g_n,...,g_1]$, *если* $k_i = k_j$ *при* $i \neq j$.
5) *Если* $\frac{u}{v} \geqslant 1$, *то* $\frac{u}{v} = \frac{[g_1;g_2,g_3,\cdots g_n]}{x_1[g_2,g_3,\cdots g_n]}$, *иначе* $\frac{u}{v} = \frac{x_1[g_2,g_3,\cdots g_n]}{[g_1;g_2,g_3,\cdots g_n]}$.

Пусть $x_i = 1$, $y_i > 0$, $r(u)$ — количество решений уравнения $u = RR' + kTT'$ в натуральных числах. Рассмотрим дробь $\frac{v}{u}$. Тогда, $\sum_{1<v<u} n(v) = 2r(u) + \frac{3}{2}\phi(u)$, сумма берется по взаимно простым u, v [1]. Число решений уравнения $u = RR' + kTT'$ можно записать в виде $\sum\limits_{\substack{1\leqslant d<u \\ u-d=0 \mod k}} \tau_2(d)\tau_2(\frac{u-d}{k})$, где $\tau_2(u)$ — функция числа делителей.

Также в докладе будет рассказано об обобщениях теоремы Хейльбронна, о максимальном значении континуанта при ограничениях $1 \leqslant |x_i|, |y_i| \leqslant \lfloor\sqrt{k}\rfloor$ и некоторых связанных с этим результатах.

Источники и литература

1) Heilbronn H. On the average length of a class of finite continued fractions// Number Theory and Analysis. 1968. pp. 87-96.
2) Sorrenson J. Two fast GCD Algorithms // J.Alg., 16. 1994. No 1. pp.110-144.