Секция «Математическая логика, алгебра и теория чисел»

Обобщенный бинарный алгоритм вычисления НОД без побочных множителей

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

K-арный алгоритм - один из наиболее быстрых алгоритмов вычисления НОД [2,3]. Пусть $u > v > 0$ - нечетные натуральные числа. Нужно найти коэффициенты α, β, такие что $\alpha u + \beta v = 0 \ (mod\ k)$ для фиксированного целого k: $\gamma gcd(u, v) = gcd(v, |(\alpha u + \beta v)/k|)$, γ — побочный множитель. При $k = 2^m$, получаем обобщенный бинарный алгоритм.

T-остаток u_t - последние t бит числа u: $u\ mod\ 2^t$ [1]. Находим линейную комбинацию t-остатков чисел u, v, где $(\alpha * u_t + \beta * v_t) = 0 \pmod{2^s}$: $(\alpha * u_t + \beta * v_t)/2^s$. Коэффициенты находим с помощью последовательностей A_i, B_i, C_i, $A_1 = \max(u_t, v_t)$, $B_1 = \min(u_t, v_t)$:

$$C_i = (max(A_i, B_i) \pm min(A_i, B_i))/2^{s_i}, s_i : 2^{s_i} | C_i, 2^{s_i+1} \not| C_i$$
$$A_i = min(A_{i-1}, B_{i-1}),\ B_i = C_{i-1}, i > 1 \quad (1)$$

Если в случае вычитания в (1) $C_i = 0$ или в случае сложения $A_i = B_i = C_i = 1$, то заканчиваем построение последовательностей. Теорема 1 описывает поиск коэффициентов для чисел u, v для случая сложения, похожая теорема есть и для случая вычитания.

Теорема 1.

$$\alpha_1 = 1,\ \beta_1 = 1, \alpha_2 = 1,\ \beta_2 = 2^{s_1} + 1$$

$$\alpha_i = \begin{cases} 1,\ \textit{если } B_1 < C_z,\ 1 \le z \le i-1 \\ \alpha_l * 2^{\sum_{z=l+1}^{i-1} s_z} + \alpha_{i-1}, \textit{если } A_i = C_l,\ l < i-1 \end{cases}$$

$$\beta_i = \begin{cases} 2^{\sum_{z=1}^{i-1} s_z} + \beta_{i-1},\ \textit{если } B_1 < C_z,\ 1 \le z \le i-1 \\ \beta_l * 2^{\sum_{z=l+1}^{i-1} s_z} + \beta_{i-1}, \textit{если } A_i = C_l,\ , l < i-1, B_i = C_{i-1} \end{cases}$$

Если $\log_2 u - \log_2 v > s$, то запускаем 1 шаг алгоритма Евклида, s — параметр.

Теорема 2. *1. Пусть C_m=0 для случая вычитания или $A_m = B_m = C_m = 1$ для случая сложения. Тогда,* $\gcd(u, v) = \gcd(\frac{|\alpha_m u + \beta_m v|}{2^t}, \frac{|\alpha_{m-1} u + \beta_{m-1} v|}{2^t})$.

2. Сложность алгоритма поиска коэффициентов в худшем случае в случае вычитания равна $O(t^2)$. Сложность алгоритма НОД в худшем случае в случае вычитания с фиксированным $k = t$ без учета шага алгоритма Евклида равна $O(n^2)$, где $\log_2 u = \log_2 v = n$.

Источники и литература

1) Dolgov D. GCD calculation in the search task of pseudoprime and strong pseudoprime numbers // Lobachevskii Journal of Mathematics, 37. 2016. No 1. pp. 733-738.
2) Sorrenson J. Two fast GCD Algorithms // J.Alg., 16. 1994. No 1. pp.110-144.
3) Weber K. The accelerated integer GCD algorithm // ACM Transacations of Math.Software, 21. 1995. No 1. pp. 1-12.