Секция «Математическая логика, алгебра и теория чисел»

Быстрое умножение целых чисел

Трегубова Анна Андреевна
Студент (специалист)
Московский государственный университет имени М.В.Ломоносова,
Механико-математический факультет, Кафедра теории чисел, Москва, Россия
E-mail: ann-tr@yandex.ru

Определение.
Дискретным преобразованием Фурье называется отображение, сопоставляющее каждому набору $x = (x_0, x_1, ..., x_{k-1}) \in \mathbb{R}$ некоторый другой набор $(\hat{x}_0, \hat{x}_1, ..., \hat{x}_{k-1}) \in \mathbb{R}$ такой, что

$$\hat{x}_i = \sum_{j=0}^{k-1} x_j g^{ij}, \qquad i = 0, ..., k-1.$$

Пусть $k = 2^s$, тогда следующий алгоритм вычисляет преобразование Фурье за $2^{s+1}(s+1)$ арифметических операций.
Для каждого целого числа $v = 2^{s-1}i_1 + ... + 2i_{s-1} + i_s$ символом v^* будем обозначать $v* = 2^{s-1}i_s + ... + 2i_2 + i_1$,

Алгоритм быстрого преобразования Фурье
Дано: $x = (x_0, x_1, ..., x_{k-1})$.
Найти: $\hat{x} = (\hat{x}_0, \hat{x}_1, ..., \hat{x}_{k-1})$.
g- примитивный корень из 1, степени k, т.е. $g^k = 1$.

1) Строим матрицу $A = (a_{u,v})$, где $0 \le u \le s, 0 \le v \le 2^s - 1$ по следующему правилу $\forall \quad 0 \le v \le 2^s - 1$:
положим:
$$a_{0,v} = x_{v*}$$

2) для $0 < u \le s$, при всех v, $0 \le v$

Источники и литература

а) Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов
б) О.Н.Герман, Ю.В.Нестеренко Теоретико-числовые методы в криптографии
в) Кибернетический сборник Новая серия выпуск 10 под ред. А. А. Ляпунова изд. Мир, Москва 1973
г) A. Schonhage and V. Strassen, «Schnelle Multiplikation grosser Zahlen», Computing 7 (1971), pp. 281—292.