

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
имени М.В. ЛОМОНОСОВА

МЕХАНИКО - МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

ОТЗЫВ НА ДИПЛОМНУЮ РАБОТУ

студентки 5 курса Трегубовой Анны Андреевны

**Руководитель:** профессор Нестеренко Ю.В.

**Тема:** Быстрое умножение целых чисел.

Как известно, два  $n$ -значных целых числа можно перемножить выполнив существенно меньше, чем  $n^2$  операций умножения цифр. Впервые такой алгоритм был предложен в 1962г. А.А. Карацубой. Алгоритм Карацубы требовал  $O(n^{\log_2 3})$  умножений. В 1965г. А.Тоом усовершенствовал алгоритм Карацубы. Для перемножения двух  $n$ -значных целых чисел алгоритм Тоома требовал  $O(n^{1+\varepsilon})$  умножений при любом фиксированном  $\varepsilon > 0$ . Постоянная в  $O(\ )$  зависит от  $\varepsilon$ . В 1971г. А. Шёнхаге и Ф. Штрассен предложили ещё более быстрый алгоритм умножения. Ему требуется  $O(n \log n \log \log n)$  операций умножения. Этот алгоритм рекурсивно использует быстрое преобразование Фурье над кольцом вычетов целых чисел по модулю  $2^m + 1$ . Дальнейшее усовершенствование алгоритма умножения было выполнено в 2007 году когда М.Фюрер предложил алгоритм, требующий  $O(n \ln n 2^{\log^* n})$  умножений, а  $\log^* n$  - сколь угодно длинная, но фиксированная итерация логарифма. Существует гипотеза, утверждающая, что для некоторого алгоритма сложность умножения имеет оценку  $O(n \log n)$  операций умножения.

В дипломной работе была поставлена задача найти алгоритм быстрого преобразования Фурье, не использующий рекурсий и на этой основе построить алгоритм умножения целых чисел, подобный алгоритму Шёнхаге-Штрассена. Эта задача была успешно решена А. Трегубовой. Алгоритм без рекурсии был построен, см. Алгоритм 2 и теорему 1. Такой же алгоритм с заменой примитивного элемента может использоваться и для быстрого вычисления обратного преобразования Фурье. А.Трегубовой удалось получить короткое и элегантное доказательство корректности построенного алгоритма. Структурно он оказался проще, а верхняя оценка его сложности оказалась точнее, чем в алгоритмах, указанных в литературе. Я полагаю, что дипломная работа А.Трегубовой заслуживает отличной оценки и после некоторой доработки текста может быть опубликована.

профессор Ю.В.Нестеренко