**Амер Исмаил Ф. О. Разработка эффективных алгоритмов вычисления НОД натуральных чисел для криптографии и теории чисел**

ОГЛАВЛЕНИЕ ДИССЕРТАЦИИ

кандидат наук Амер Исмаил Ф. О.

Введение

Глава 1. Обзор алгоритмов вычисления наибольшего общего делителя (НОД) натуральных чисел и оценки их

сложности

1.1 Классический алгоритм Евклида

1.1.1 Расширенный алгоритм Евклида

1.1.2 Оценка производительности алгоритма Евклида

1.2 Бинарный алгоритм вычисления НОД

1.3 fc-арный алгоритм Евклида

1.4 Аппроксимирующий к-арный алгоритм

Глава 2. Программирование к-арного метода вычисления НОД

натуральных чисел

2.1 Методика экспериментальных вычислений

2.2 Исследование значений коэффициента редукции в зависимости

от к

2.3 Поиск подходящей пары (х,у) в fc-арном алгоритме

2.4 Методы ускорение процедуры поиска пары (х,у) в fc-арном алгоритме

2.5 Время вычисления НОД при использовании предтаблиц обратных элементов

2.6 Анализ значений х и у и выбор способа перебopa пар (х,у)

2.7 Использование предтаблиц значений х и у для заданных

значений а и b

2.8 Сдвиг интервала значений у

2.9 Экспериментальные результаты времени при сдвиге области значений у

2.10 Вычисления с большим сдвигом области значений у

2.11 Смешанный алгоритм на основе к-арного алгоритма и схемы Евклида

Стр.

2.12 Выводы по главе

Глава 3. Исследование аппроксимирующего к-арного

алгоритма вычисления НОД

3.1 Базовая схема аппроксимирующего алгоритма

3.2 Программирование аппроксимирующего ^-арного алгоритма в МРП1

3.3 Расчет времени и среднего числа итераций АКА

3.3.1 Оценка производительности вычисления НОД для

Ь = 330 бит

3.3.2 Оценка производительности вычисления НОД для

Ь = 825 бит

3.3.3 Оценка производительности вычисления НОД для

Ь = 1650 бит

3.4 Ускорение аппроксимирующего алгоритма

3.4.1 Ускоренное вычисление параметра г = А/В

3.4.2 Оценка времени вычисления НОД по новой схеме

3.4.3 Оптимизация вычисления параметра а и аппроксимирующей дроби Фарея

3.4.4 Построение аппроксимирующей дроби методом Фарея

3.4.5 Оценка трудоемкости процедуры Фарея

3.4.6 Вычисление параметра С = (Ах + Ву)/к

3.5 Приложения аппроксимирующего алгоритма

3.5.1 Тест простоты Миллера-Рабина

3.5.2 Поиск строго псевдопростых чисел

3.5.3 Экспериментальные результаты

3.6 Выводы по Главе

Заключение

Список сокращений и условных обозначений

Список литературы

Список рисунков

Стр.

Список таблиц

Приложение А. Коды программного комплекса