**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ**

**РОССИЙСКОЙ ФЕДЕРАЦИИ**

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ

УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ

(национальный исследовательский университет)»

**Институт (Филиал) 8 Кафедра Кафедра 806 «Вычислительная математика и программирование»**

**Группа м80-407б-18 Направление подготовки ?**

**Профиль ?**

**Квалификация бакалавр**

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА**

**БАКАЛАВРА**

На тему: Алгоритмы факторизации больших чисел.

Автор ВКРБ\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (\_\_\_\_\_\_\_\_\_\_)

(фамилия, имя, отчество полностью)

Руководитель (\_\_\_\_\_\_\_\_\_\_)

(фамилия, имя, отчество полностью)

Консультант (\_\_\_\_\_\_\_\_\_\_)

(фамилия, имя, отчество полностью)

Консультант (\_\_\_\_\_\_\_\_\_\_)

(фамилия, имя, отчество полностью)

Рецензент (\_\_\_\_\_\_\_\_\_\_)

(фамилия, имя, отчество полностью)

**К защите допустить**

Заведующий кафедрой 806 (\_\_\_\_\_\_\_\_\_)

(№ каф) (фамилия, имя, отчество полностью)

\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_г.

Москва 2022

Содержание:

1. Введение
2. Модульная арифметика
3. Нахождение простых чисел.
   1. Решето Эратосфена
   2. Решето Аткина
   3. Символ Лежандра
   4. Теорема Тоннели-Шенкса
4. Основные экспоненциальные алгоритмы
   1. P-1 метод Полларда
   2. P+1 метод Вильямса
5. Метод квадратичного решета
   1. Отбор факторной базы
   2. Применение символа Лежандра и алгоритма Тоннели-Шенкса
   3. Генерирующий полином
   4. Этап просеивания
   5. Составление матрицы
   6. Решение матрицы в конечном поле
   7. GCD
6. Асимптотика алгоритма и сравнение его с другими
7. Возможные улучшения
   1. Параллельное вычисление на этапе просеивания
   2. Решение матрицы используя битовые срезы
   3. Метод факторизации GNFS

**Введение**

В настоящее время в любых сетях используется шифрование информации для защиты от вмешательства третьих лиц. Для шифрования используются различные криптосистемы, такие как RSA. Тот факт, что задача факторизации больших чисел есть задача предполагаемой большой вычислительной сложности, лежит в основе различных криптосистем. Факторизация или разложение на множители целых чисел–одна из древнейших проблем теории чисел. Методы факторизации целых чисел затрагивают такие области математики, как теория чисел, модульная арифметика, решение матричных уравнений. В настоящей работе рассматриваются и анализируются некоторые известные методы факторизации. При решении задачи факторизации затрагивается ряд других задач, непосредственно связанных с ней, таких как тесты на простоту и генерация больших простых чисел.

Пусть число n целое и составное, под термином факторизация будем иметь в виду нахождение чисел отличных от единицы и самого числа, произведение которых будет давать нам искомое число n. В случае, когда таких чисел нет, число n будет считаться простым, имеющим в качестве делителя само себя и единицу. В данной работе будут рассмотрены алгоритмы факторизации чисел, а также теоремы и алгоритмы, необходимые для проведения факторизации чисел.

**Модульная арифметика.**

Прежде чем переходить к непосредственной факторизации, стоит оговорить о некоторых понятиях, которые будут в дальнейшем использоваться в разборе принципов работы тех или иных алгоритмов.

Пусть Z обозначает множество целых чисел, а – целое число. Условие, что целое число a делится нацело на b, будем записывать через

Определение 1.1 Говорят, что два целых числа a и b сравнимы по модулю p, записывается,

если

Отношение по модулю натурального числа обладает свойствами:

1. Симметричность
2. Рефлективность
3. Транзитивность