**САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ**

**ПЕТРА ВЕЛИКОГО**

**Институт компьютерных наук и технологий**

**Кафедра «Распределенные вычисления и компьютерные сети»**

**Курсовая работа**

на тему: Метод Сильвера-Полига-Хеллмана

по дисциплине: Основы компьютерной алгебры

Выполнил студент

гр. 23507/1 <*подпись*> В.Б.Борисов

Руководитель

доц. кафедры <*подпись*> П.В.Трифонов

«\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2015 г.

Санкт-Петербург

2015

СОДЕРЖАНИЕ

[Введение 3](#_Toc429616064)

[Основная часть 3](#_Toc429616065)

[Постановка задачи 3](#_Toc429616066)

[Описание алгоритма 3](#_Toc429616067)

[Тестирование 4](#_Toc429616068)

[Заключение 4](#_Toc429616069)

[Список литературы 4](#_Toc429616070)

Введение

**Алгоритм Полига — Хеллмана** (также называемый *алгоритм Сильвера — Полига — Хеллмана*) — [детерминированный алгоритм](https://ru.wikipedia.org/wiki/%D0%94%D0%B5%D1%82%D0%B5%D1%80%D0%BC%D0%B8%D0%BD%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D1%8B%D0%B9_%D0%B0%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC) [дискретного логарифмирования](https://ru.wikipedia.org/wiki/%D0%94%D0%B8%D1%81%D0%BA%D1%80%D0%B5%D1%82%D0%BD%D0%BE%D0%B5_%D0%BB%D0%BE%D0%B3%D0%B0%D1%80%D0%B8%D1%84%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) в [кольце вычетов](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BB%D1%8C%D1%86%D0%BE_%D0%B2%D1%8B%D1%87%D0%B5%D1%82%D0%BE%D0%B2) по модулю [простого числа](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%81%D1%82%D0%BE%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%BE). Одной из особенностью алгоритма является то, что для [простых](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%81%D1%82%D0%BE%D0%B5_%D1%87%D0%B8%D1%81%D0%BB%D0%BE) чисел специального вида можно находить дискретный логарифм за [полиномиальное](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D0%B0%D1%81%D1%81_P) время.

Алгоритм Полига—Хеллмана крайне эффективен, если p-1 раскладывается на небольшие простые множители. Это очень важно учитывать при выборе параметров криптографических схем. Иначе схема будет ненадёжной.

# Основная часть

# Постановка задачи

Реализовать метод Сильвера-Полига-Хеллмана по модулю сколь угодно большого простого числа на языке С++.

# Описание алгоритма

Пусть задано сравнение

|  |  |
| --- | --- |
| a^x\equiv b\pmod{p}, |  |

и известно разложение числа p-1 на простые множители:

|  |  |
| --- | --- |
| p-1=\prod\limits_{i=1}^{k}q_i^{\alpha_i}. |  |

Необходимо найти число x,\;0\leq x < p-1, удовлетворяющее сравнению.

Составить таблицу значений , где =,

Вычислить

Для i от 1 до k

Пусть

Где

Тогда верно сравнение:

Вывод верхнего сравнения:

С помощью таблицы, составленной на шаге 1, находим Для j от 1 до . Рассматриваем сравнение

Решение опять же находится по таблице

Конец цикла по j

Конец цикла по i

Найдя для всех i, находим

По китайской теореме об остатках

# Тестирование

Чтобы убедиться в правильности написанной программы были проведены тесты, которые показали не только корректные результаты, но и время работы алгоритма. Ниже приведена таблица результатов.

|  |  |  |
| --- | --- | --- |
| Входные данные | Результат | Время работы алгоритма в секундах |
| 3 13 17 | 4 | 0 |
| 2 5 7237 | 4085 | 0.015 |
| 2 40 37 | Нет решений | 0.015 |
| 71 210 251 | 197 | 0.015 |
| 123123 123123 999997 | 1 | 0.078 |
| 1231231 1231231 1982354 | 1 | 0.156 |

# Заключение

Алгоритм и длинная арифметика к нему реализованы на C++. Программа протестирована так и на малых, так и на больших числах. Проверено корректность вычислений с помощью программного пакета Maple. Поставленная задача решена.

# Список литературы

[1] П.В Трифонов, Построение и анализ алгоритмов