Отчёт по лабораторной работе №8.  
Целочисленная арифметика многократной точности

Студент: Асеинова Елизавета, 1132236897

Группа: НФИмд-01-23

Преподаватель: Кулябов Дмитрий Сергеевич,

д-р.ф.-м.н., проф.

Москва 2023

Содержание

# 1 Цель работы

Целью данной лабораторной работы является ознакомление с алгоритмами по воплощению целочисленной арифметики многократной точности, а также программная реализация данных алгоритмов.

# 2 Задание

Реализовать рассмотренные в инструкции к лабораторной работе алгоритмы программно.

Алгоритмы:

1. Сложение неотрицательных целых чисел
2. Вычитание неотрицательных целых чисел
3. Умножение неотрицательных целых чисел столбиком
4. Быстрый столбик
5. Деление многоразрядных целых чисел

# 3 Теоретическое введение

В данной лабораторной работе предметом нашего изучения стали алгоритмы по воплощению целочисленной арифметики многократной точности.

## 3.1 Арифметика многократной точности

Арифметика многократной точности — это операции (базовые арифметические действия, элементарные математические функции и пр.) над числами большой разрядности, т.е. числами, разрядность которых превышает длину машинного слова универсальных процессоров общего назначения (более 128 бит)

В современных асимметричных криптосистемах в качестве ключей, как правило, используются целые числа длиной 1000 и более битов. Для задания чисел такого размера не подходит ни один стандартный целочисленный тип данных современных языков программирования.

При работе с большими целыми числами знак такого числа удобно хранить в отдельной переменной. Например, при умножении двух чисел знак произведения вычисляется отдельно.

Далее нами были рассмотрены алгоритмы по воплощению целочисленной арифметики многократной точности.

# 4 Выполнение лабораторной работы

В соответствии с заданием, была написана программа по воплощению алгоритма Ро-метода Полларда для задач дискретного логарифмирования.

Программный код и результаты выполнения программ представлен ниже.

## 4.1 Вспомогательные действия

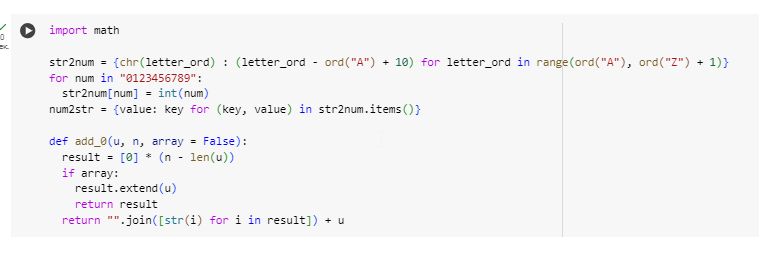


Figure 1: Вспомогательные действия для удобства дальнейших вычислений

## 4.2 Алгоритм 1. Сложение неотрицательных целых чисел. Реализация



Figure 2: Алгоритм 1. Сложение неотрицательных целых чисел

## 4.3 Алгоритм 2. Вычитание неотрицательных целых чисел. Реализация



Figure 3: Алгоритм 2. Вычитание неотрицательных целых чисел

## 4.4 Алгоритм 3. Умножение неотрицательных целых чисел столбиком. Реализация



Figure 4: Алгоритм 3. Умножение неотрицательных целых чисел столбиком

## 4.5 Алгоритм 4. Быстрый столбик. Реализация

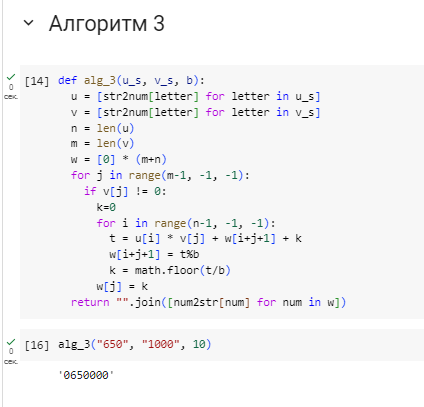


Figure 5: Алгоритм 4. Быстрый столбик

## 4.6 Алгоритм 5. Деление многоразрядных целых чисел. Реализация

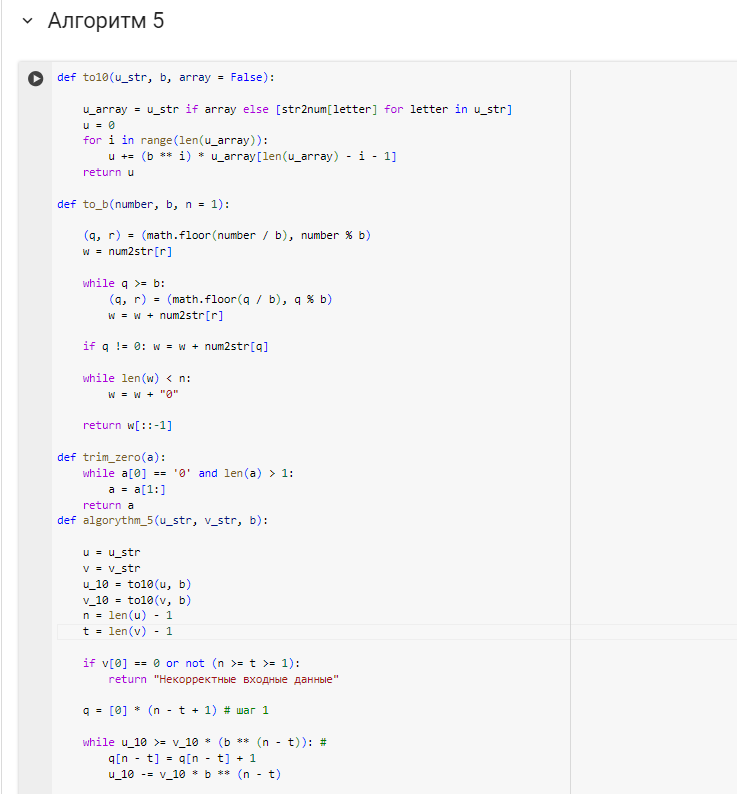


Figure 6: Алгоритм 5. Деление многоразрядных целых чисел

## 4.7 Алгоритм 5. Деление многоразрядных целых чисел. Реализация

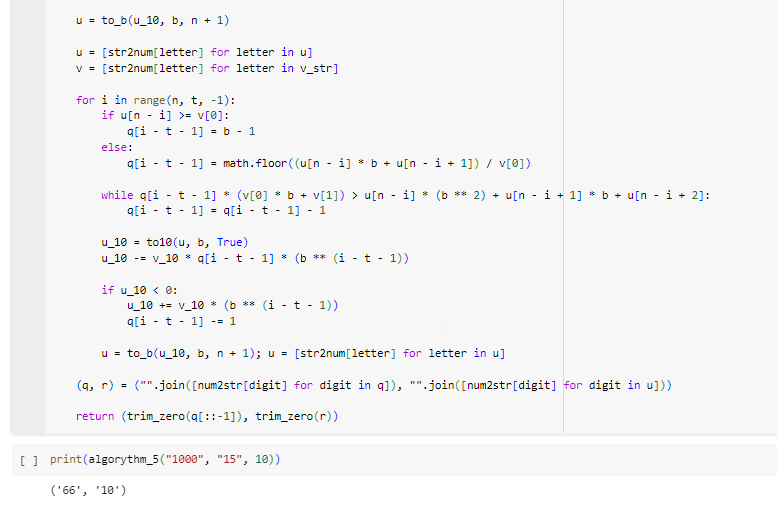


Figure 7: Алгоритм 5. Деление многоразрядных целых чисел

# 5 Выводы

Таким образом, была достигнута цель, поставленная в начале лабораторной работы: в результате выполнения данной лабораторной работы нам удалось осуществить программно алгоритмы, рассмотренные в описании к лабораторной работе, а также мы осуществили программно данные алгоритмы.

# Список литературы