Лабораторнаяя работа №8.  
Целочисленная арифметика многократной точности

Студентка: Царитова Нина Аведиковна

Группа: НФИмд-02-23

Преподаватель: Кулябов Дмитрий Сергеевич,

д-р.ф.-м.н., проф.

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.

## 3.2 Сложение неотрицательных целых чисел

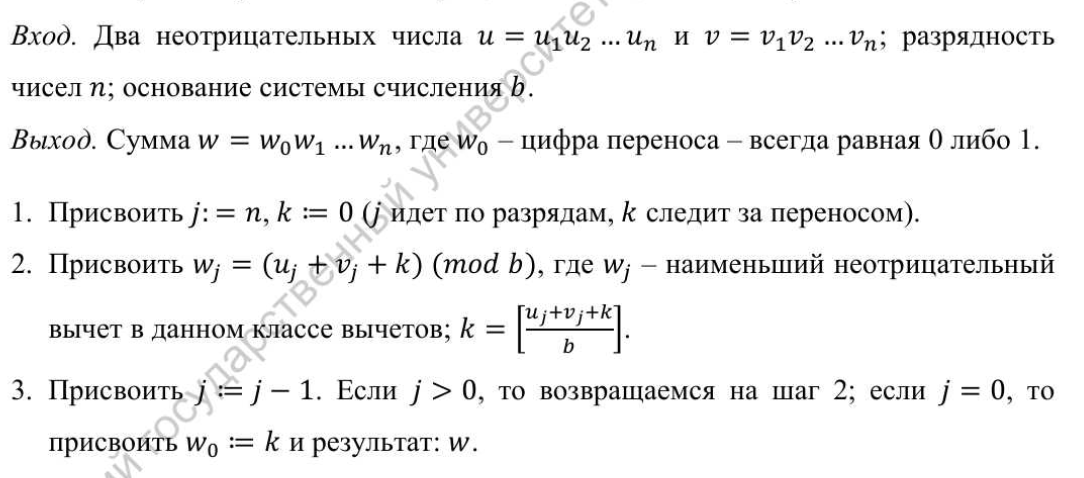


Figure 1: Алгоритм 1. Сложение неотрицательных целых чисел

## 3.3 Вычитание неотрицательных целых чисел

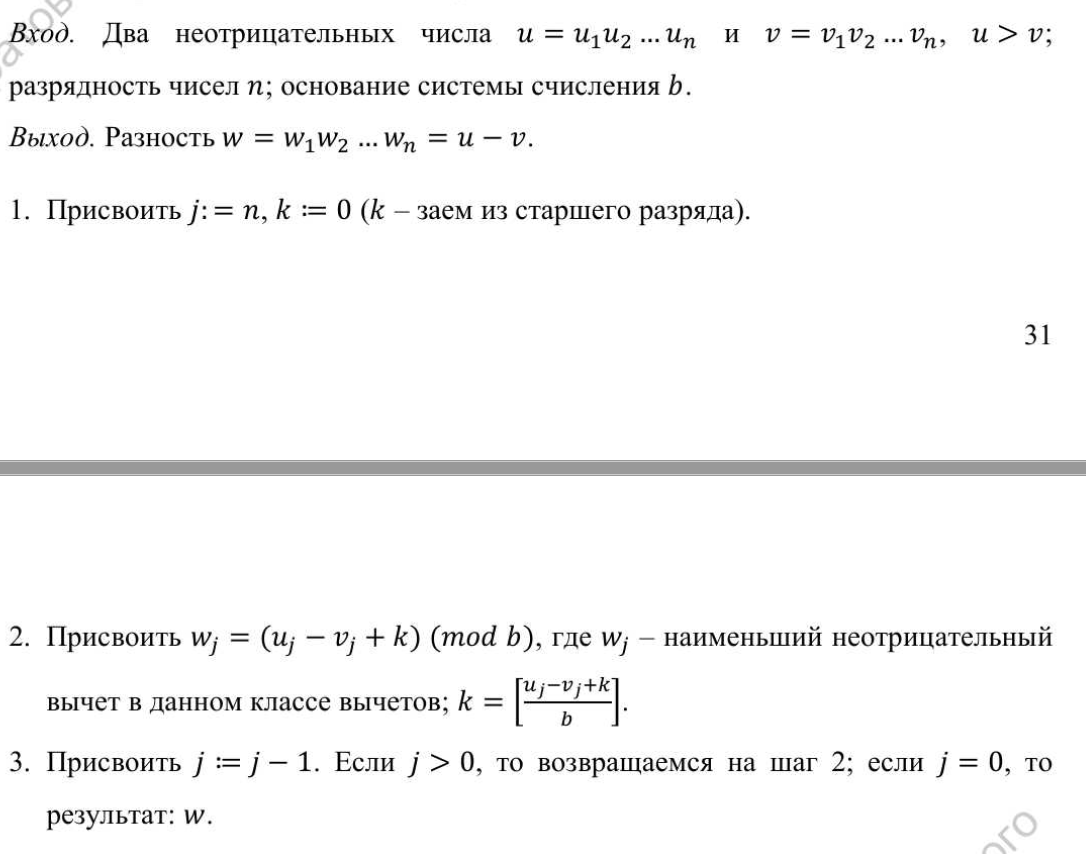


Figure 2: Алгоритм 2. Вычитание неотрицательных целых чисел

## 3.4 Умножение неотрицательных целых чисел столбиком

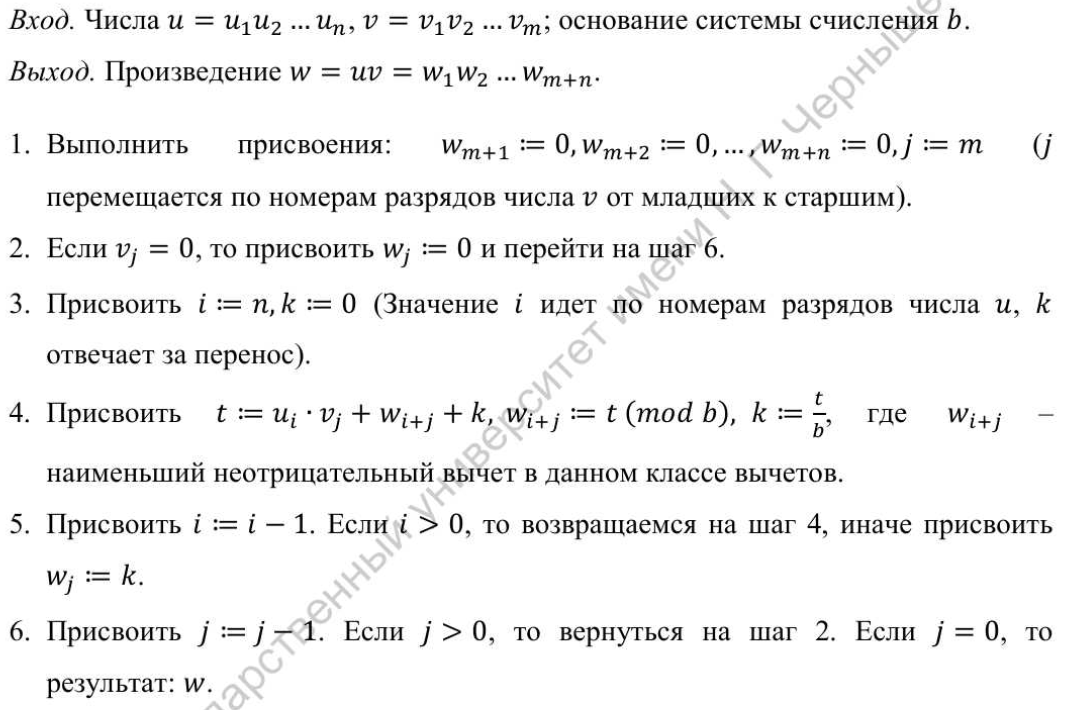


Figure 3: Алгоритм 3. Умножение неотрицательных целых чисел столбиком

## 3.5 Быстрый столбик

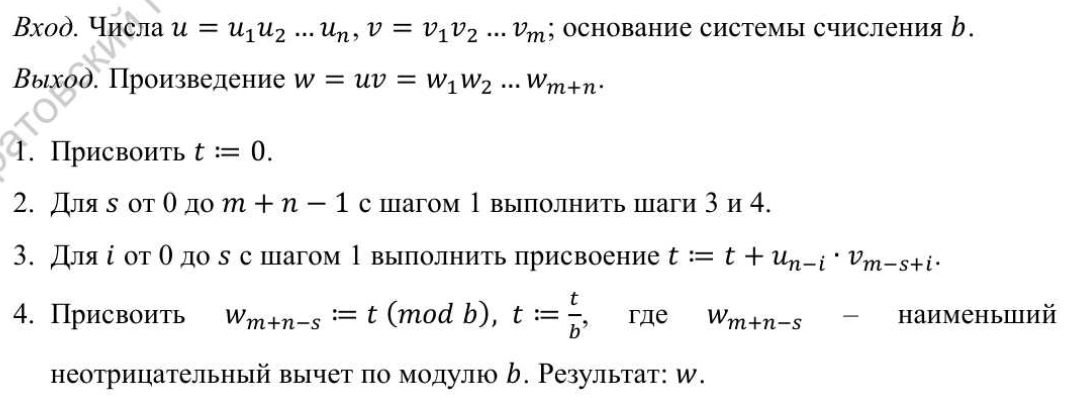


Figure 4: Алгоритм 4. Быстрый столбик

## 3.6 Деление многоразрядных целых чисел

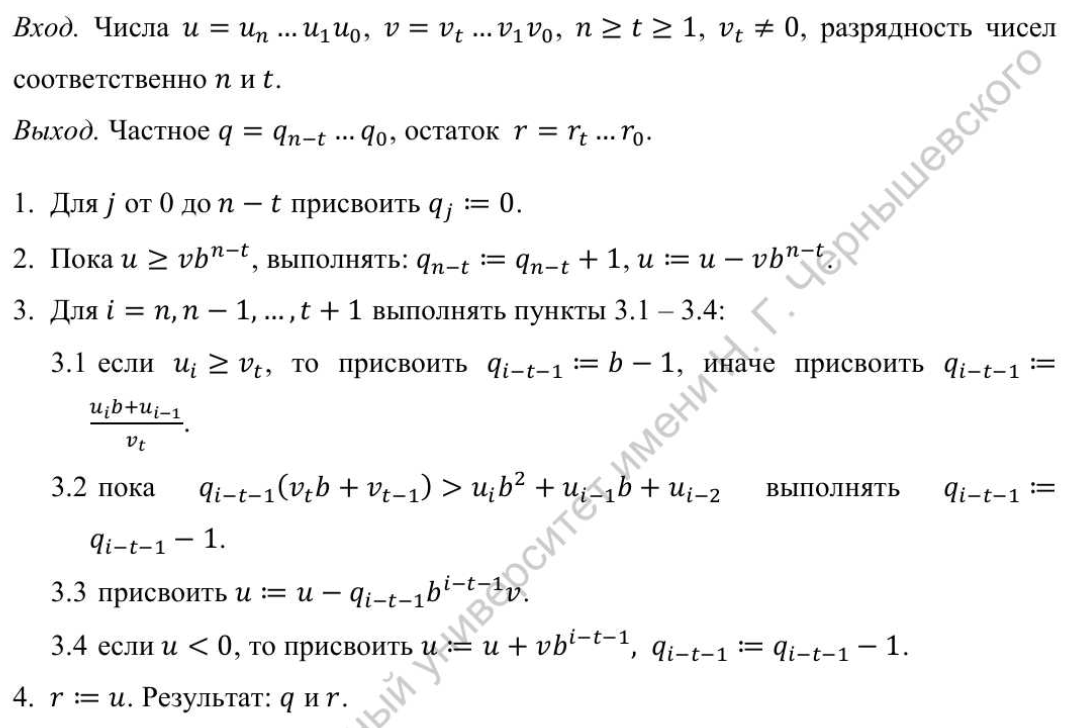


Figure 5: Алгоритм 5. Деление многоразрядных целых чисел

# 4 Выполнение лабораторной работы

В соответствии с заданием, были написаны программы по воплощению алгоритмов, представленных в описании к лабораторной работе.

Программный код и результаты выполнения программ представлены ниже.

## 4.1 Вспомогательные действия

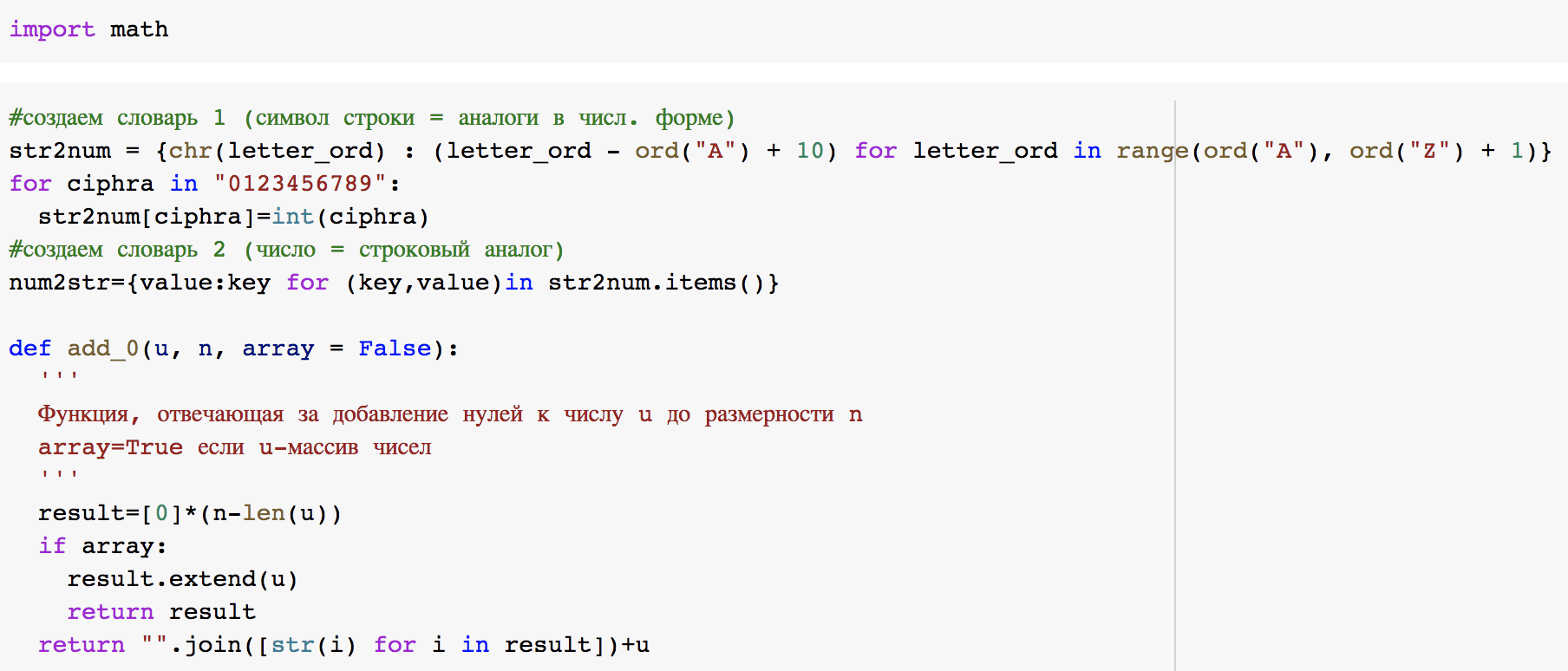


Figure 6: Вспомогательные действия для удобства дальнейших вычислений

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

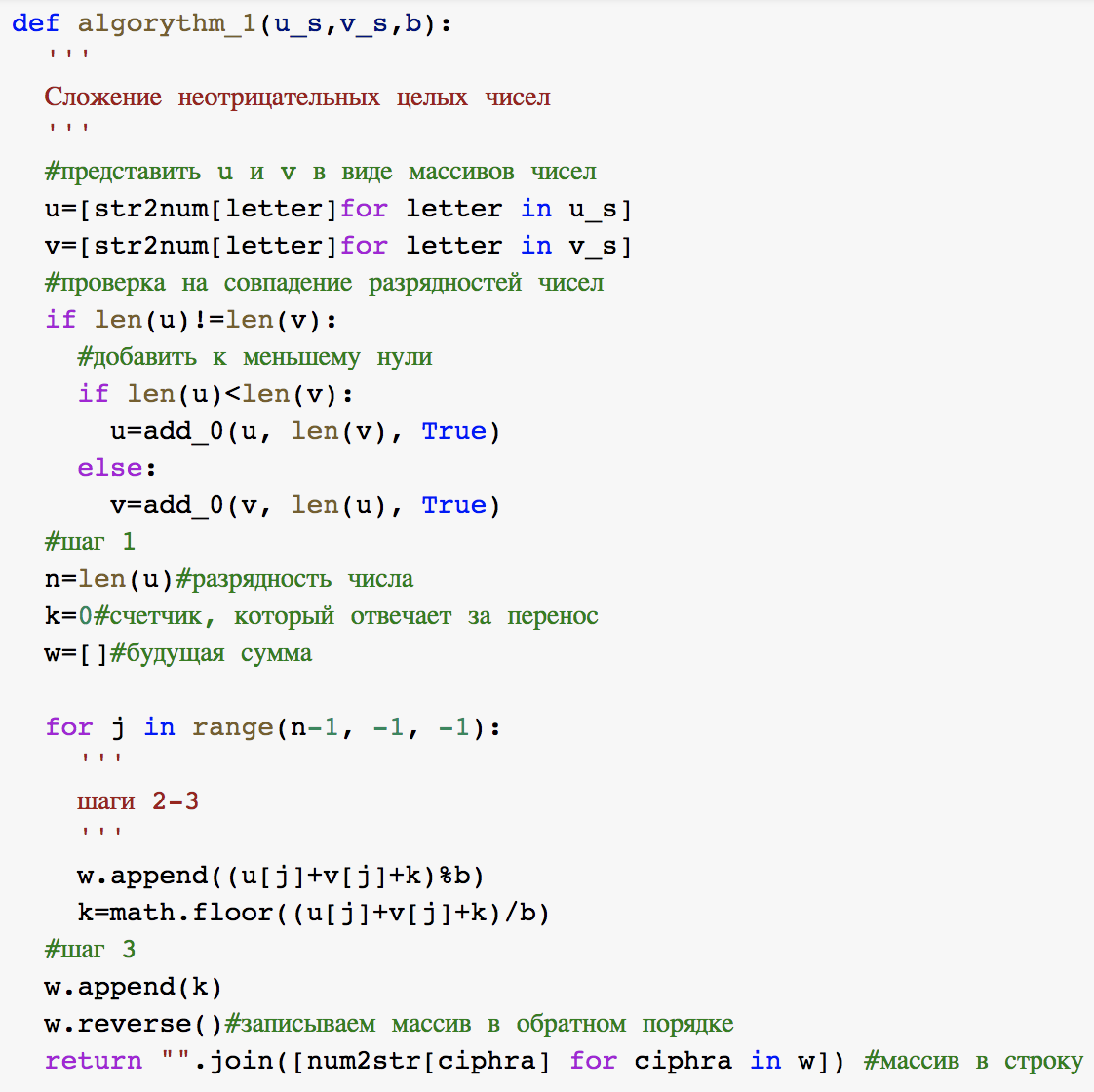


Figure 7: Алгоритм 1. Сложение неотрицательных целых чисел

## 4.3 Алгоритм 1. Сложение неотрицательных целых чисел. Результат

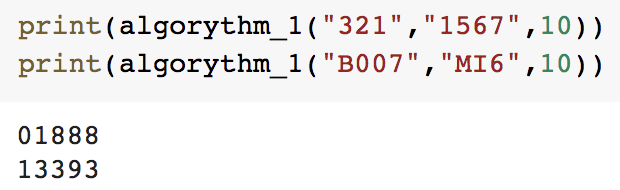


Figure 8: Алгоритм 1. Сложение неотрицательных целых чисел

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

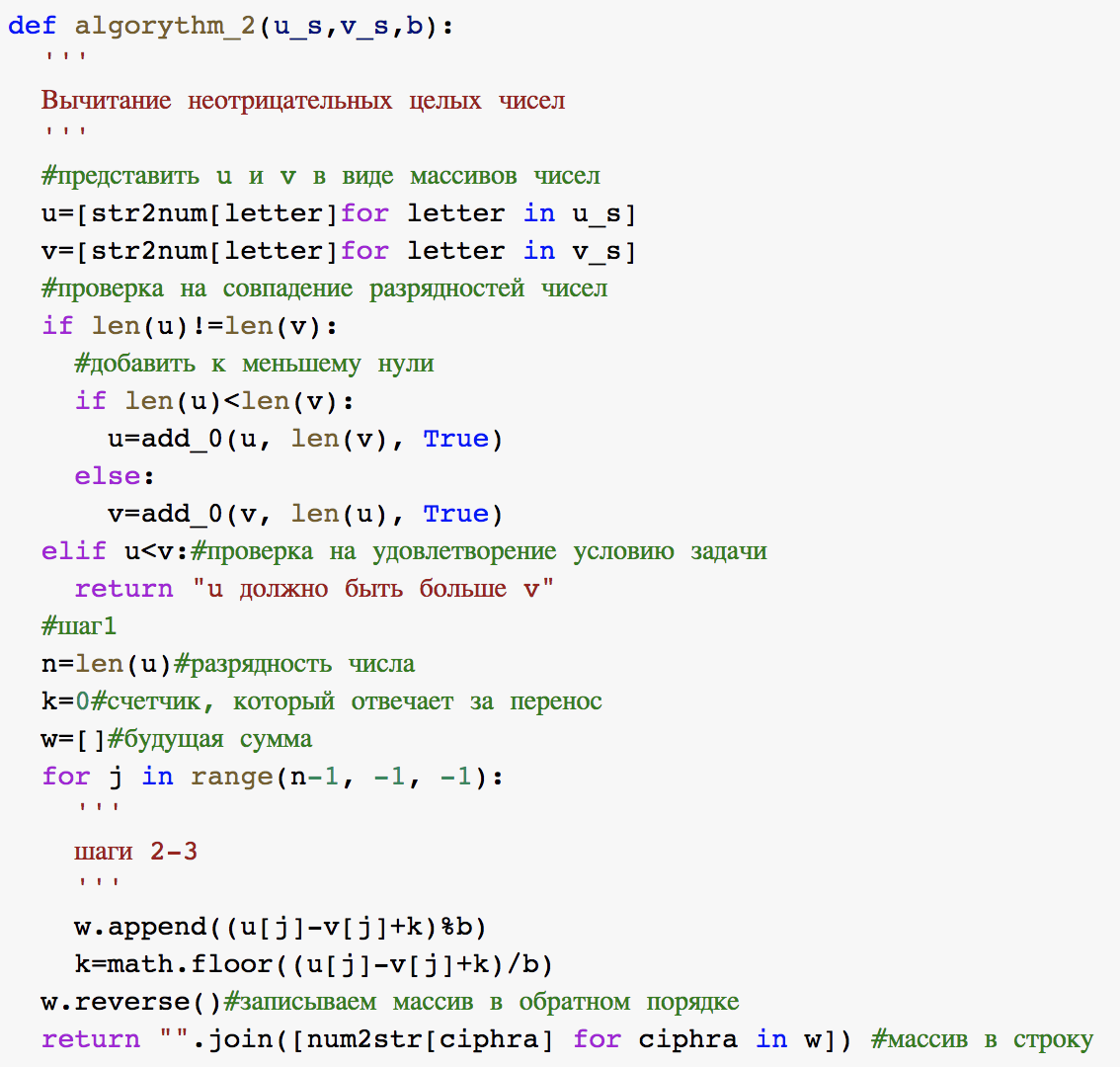


Figure 9: Алгоритм 2. Вычитание неотрицательных целых чисел

## 4.5 Алгоритм 2. Вычитание неотрицательных целых чисел. Результат

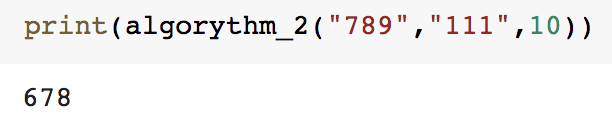


Figure 10: Алгоритм 2. Вычитание неотрицательных целых чисел

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

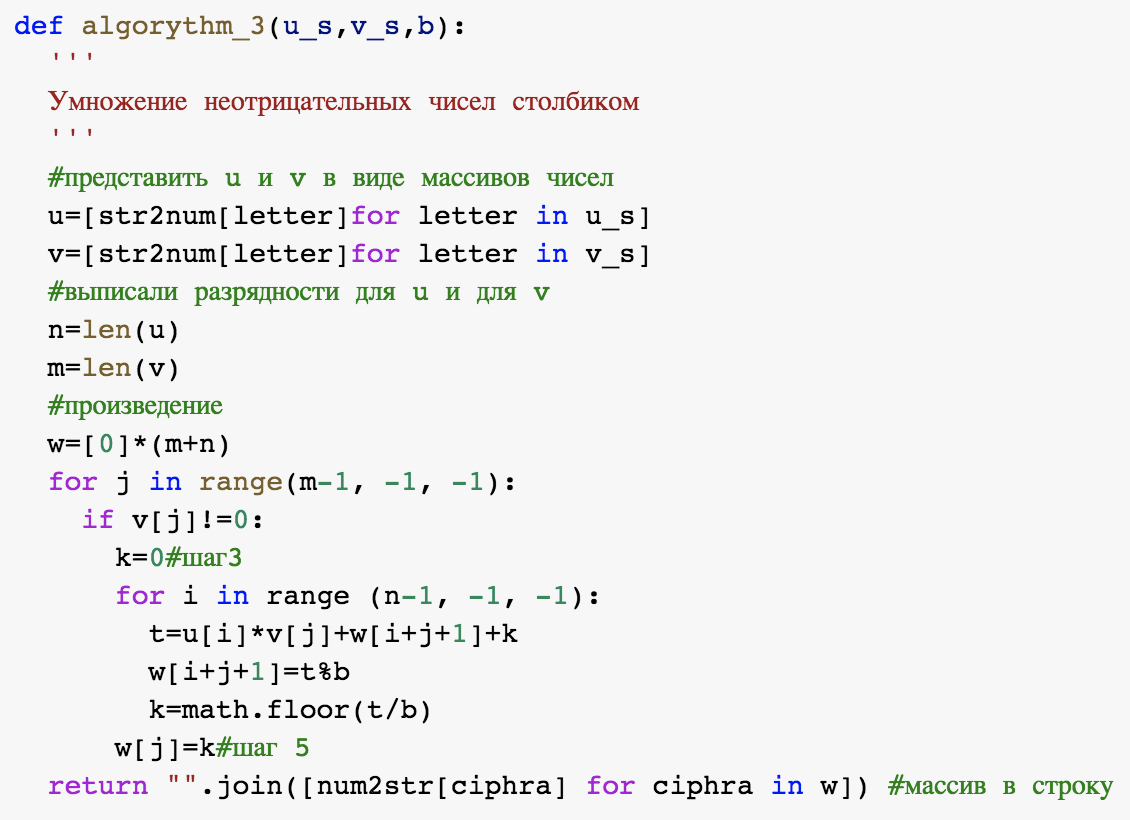


Figure 11: Алгоритм 3. Умножение неотрицательных целых чисел столбиком

## 4.7 Алгоритм 3. Умножение неотрицательных целых чисел столбиком. Результат

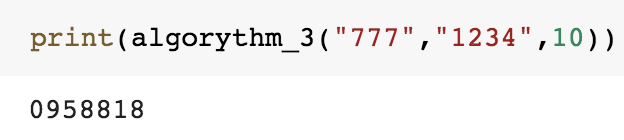


Figure 12: Алгоритм 3. Умножение неотрицательных целых чисел столбиком

## 4.8 Алгоритм 4. Быстрый столбик. Реализация

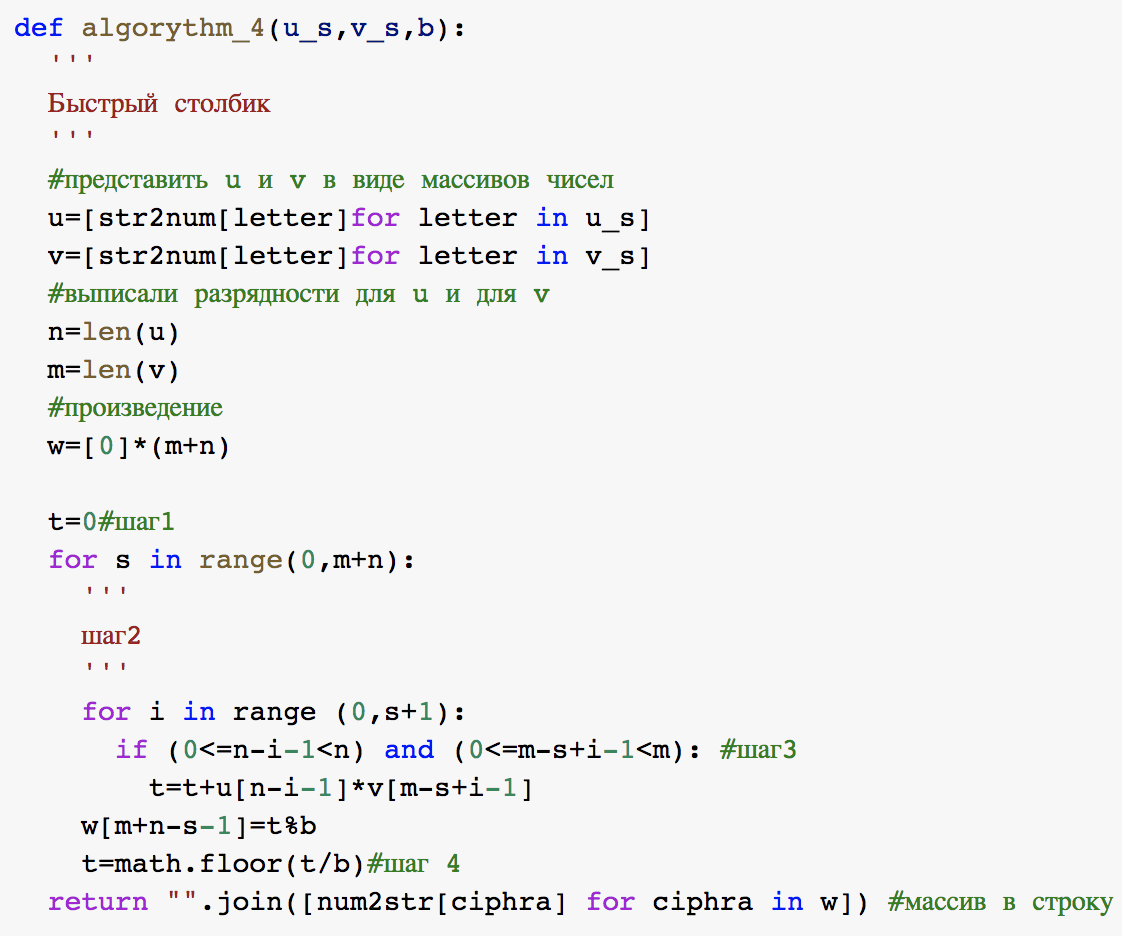


Figure 13: Алгоритм 4. Быстрый столбик

## 4.9 Алгоритм 4. Быстрый столбик. Результат

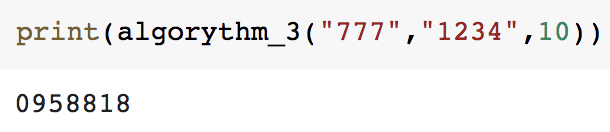


Figure 14: Алгоритм 4. Быстрый столбик

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

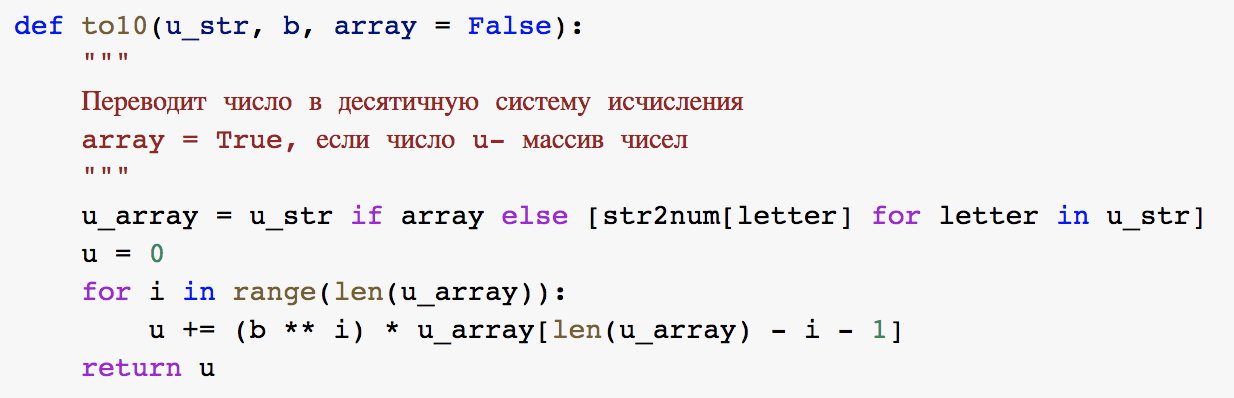


Figure 15: Алгоритм 5. Деление многоразрядных целых чисел

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

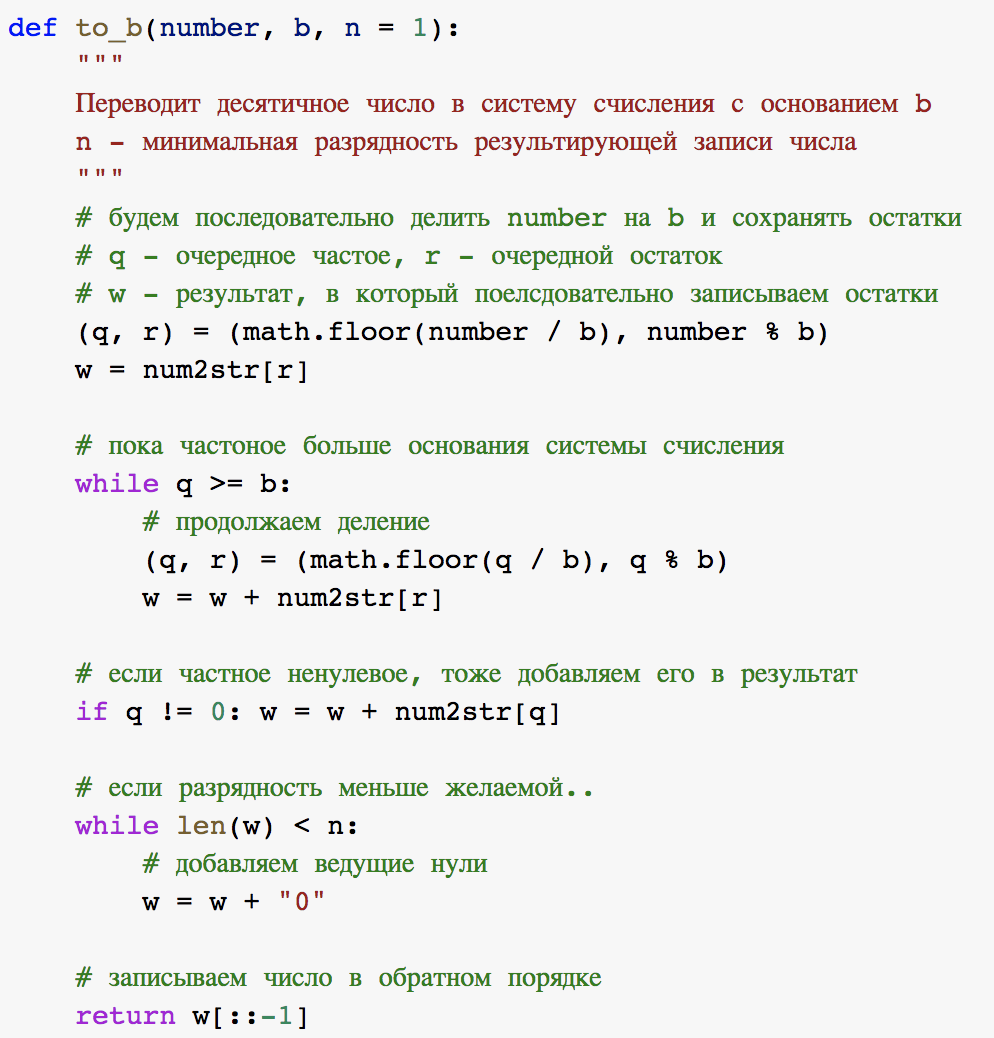


Figure 16: Алгоритм 5. Деление многоразрядных целых чисел

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

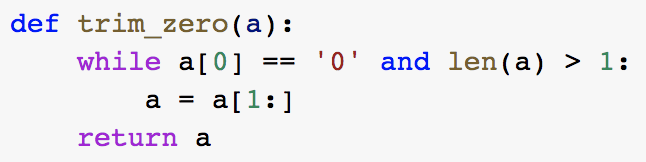


Figure 17: Алгоритм 5. Деление многоразрядных целых чисел

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

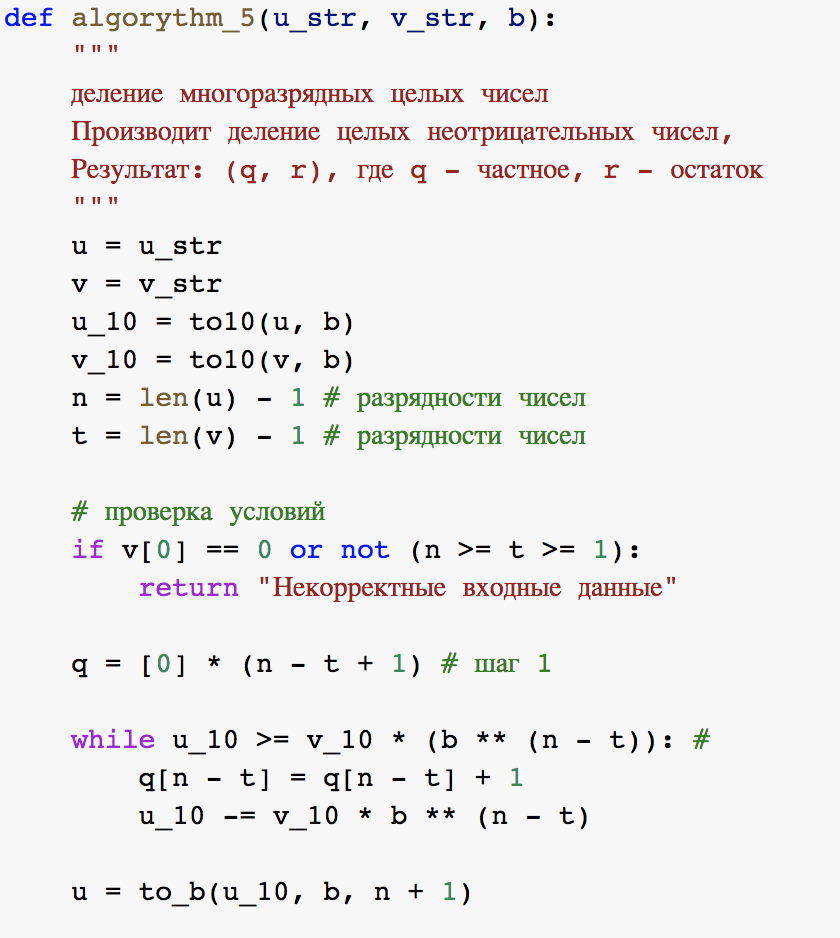


Figure 18: Алгоритм 5. Деление многоразрядных целых чисел

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

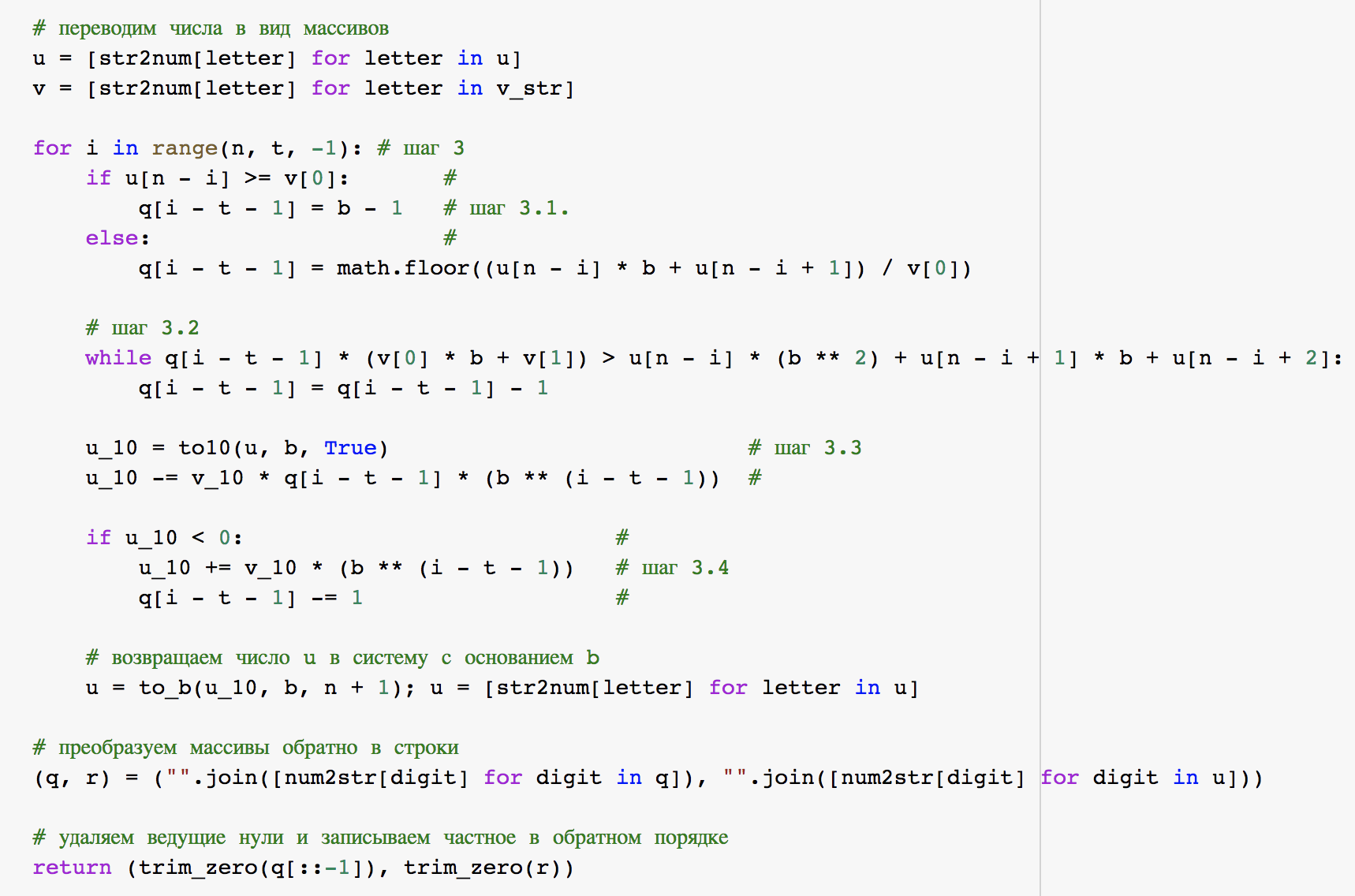


Figure 19: Алгоритм 5. Деление многоразрядных целых чисел

## 4.15 Алгоритм 5. Деление многоразрядных целых чисел. Результат



Figure 20: 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

1. Бубнов С.А. Лабораторный практикум по основам криптографии: учебно-методическое пособие. Саратов; http://elibrary.sgu.ru/uch\_lit/656.pdf: Саратовский государственный университет им. Н.Г. Чернышевского, 2012.
2. Исупов К.С. Методы и алгоритмы организации высокоточных вычислений в арифметике остаточных классов для универсальных процессорных платформ: phdthesis. Вятский государственный университет, 2014.
3. Панкратова И.А. Теоретико-числовые методы в криптографии: учебное пособие. Томск: Томский государственный университет, 2009. С. 120.