Отчёт по лабораторной работе 8

Целочисленная арифметика многократной точности

Воробьев Александр Олегович

Содержание

# Цель работы

Ознакомление с алгоритмами целочисленной арифметики многократной точности, а также их последующая программная реализация.

# Теоретические сведения

Высокоточная (длинная) арифметика — это операции (базовые арифметические действия, элементарные математические функции и пр.) над числами большой разрядности (многоразрядными числами), 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. Представление чисел в формате с плавающей точкой позволяет задать очень большие числа (например, тип long double языка C++ – до ), но не удовлетворяет требованию абсолютной точности, характерному для криптографических приложений. Поэтому большие целые числа представляются в криптографических пакетах в виде последовательности цифр в некоторой системе счисления (обозначим основание системы счисления ): где .

Основание системы счисления выбирается так, чтобы существовали машинные команды для работы с однозначными и двузначными числами; как правило, равно , или .

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

Далее при описании алгоритмов квадратные скобки означают, что берётся целая часть числа.

## Сложение неотрицательных целых чисел

\*Вход. Два неотрицательных числа и ; разрядность чисел ; основание системы счисления .

\*Выход. Сумма , где - цифра переноса, всегда равная либо .

1. Присвоить ( *идет по разрядам, следит за переносом*).
2. Присвоить , где .
3. Присвоить . Если , то возвращаемся на шаг 2; если , то присвоить и результат: .

## Вычитание неотрицательных целых чисел

\*Вход. Два неотрицательных числа и , ; разрядность чисел ; основание системы счисления .

\*Выход. Разность .

1. Присвоить ( – заём из старшего разряда).
2. Присвоить ; .
3. Присвоить . Если , то возвращаемся на шаг 2; если , то результат: .

## Умножение неотрицательных целых чисел столбиком

\*Вход. Числа , ; основание системы счисления .

\*Выход. Произведение .

1. Выполнить присвоения: ( *перемещается по номерам разрядов числа от младших к старшим*).
2. Если , то присвоить и перейти на шаг 6.
3. Присвоить (*значение идет по номерам разрядов числа , отвечает за перенос*).
4. Присвоить .
5. Присвоить . Если , то возвращаемся на шаг 4, иначе присвоить .
6. Присвоить . Если , то вернуться на шаг 2. Если , то результат: .

## Быстрый столбик

\*Вход. Числа , ; основание системы счисления .

\*Выход. Произведение .

1. Присвоить .
2. Для от до с шагом 1 выполнить шаги 3 и 4.
3. Для от до с шагом 1 выполнить присвоение .
4. Присвоить . Результат: .

## Деление многоразрядных целых чисел

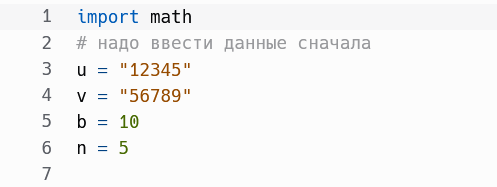
\*Вход. Числа , .

\*Выход. Частное , остаток .

1. Для от до присвоить .
2. Пока , выполнять: .
3. Для выполнять пункты 3.1 – 3.4: 3.1. если , то присвоить , иначе присвоить . 3.2. пока выполнять . 3.3. присвоить . 3.4. если , то присвоить , .
4. . Результат: и .

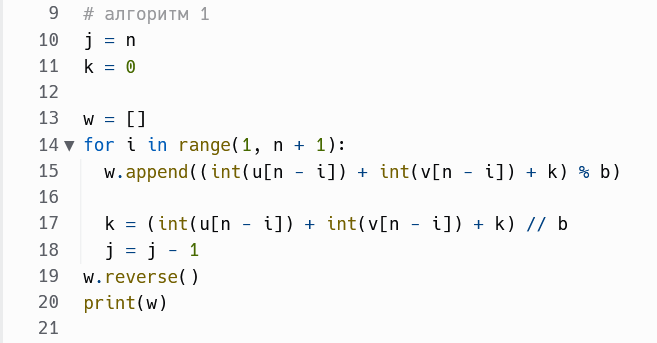
# Выполнение лабораторной работы

1. Написал блок данных (рис. -@fig:001)



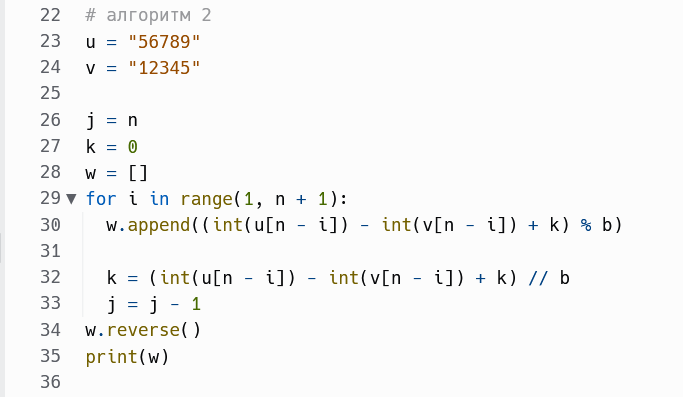
Начальные данные

1. Написал алгоритм сложения неотрицательных целых чисел (рис. -@fig:002)



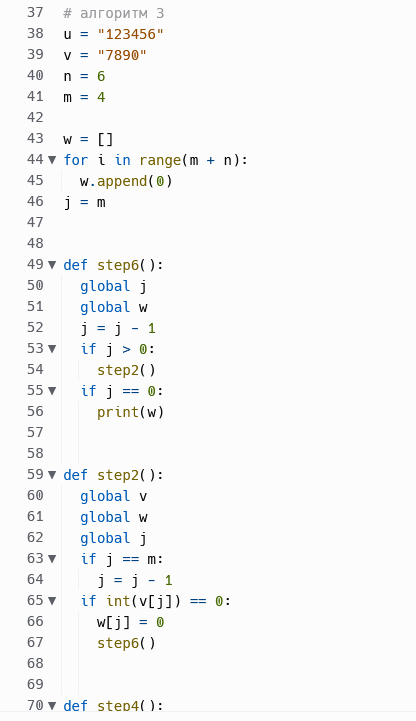
Алгоритм Сложение неотрицательных целых чисел

1. Написал алгоритм вычитания неотрицательных целых чисел (рис. -@fig:003)

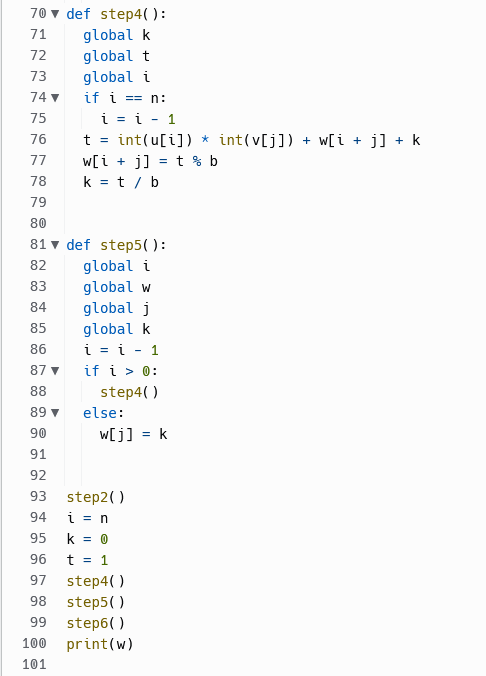


Алгоритм вычитания неотрицательных целых чисел

1. Написал алгоритм умножения неотрицательных целых чисел столбиком(рис. -@fig:004)(рис. -@fig:005)

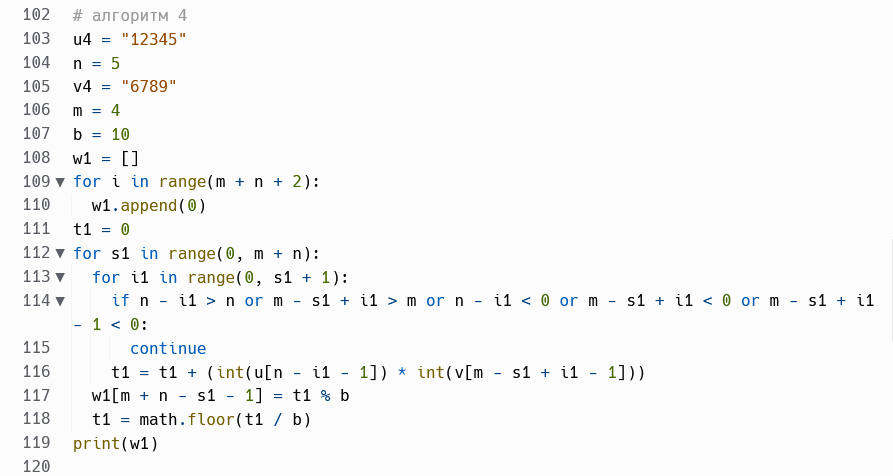


Алгоритм умножения неотрицательных целых чисел столбиком первая часть



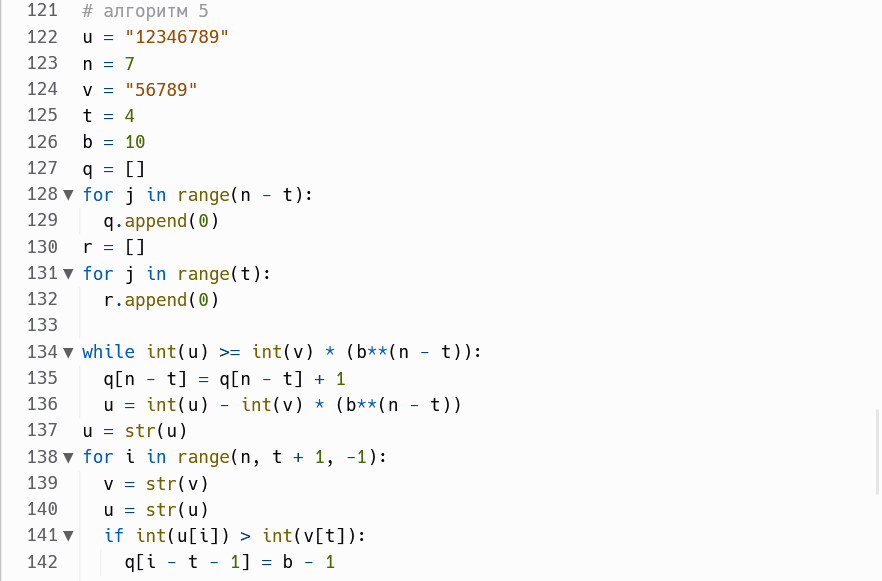
Алгоритм умножения неотрицательных целых чисел столбиком вторая часть

1. Написал алгоритм быстрого столбика (рис. -@fig:006)

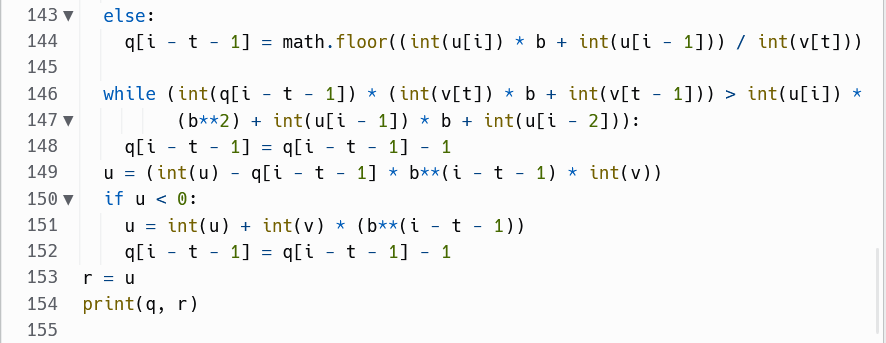


Алгоритм быстрого столбика

1. Написал алгоритм деления многоразрядных целых чисел (рис. -@fig:007)(рис. -@fig:008)

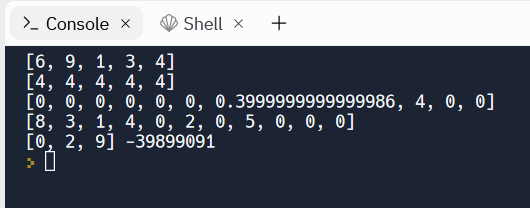


Алгоритм деления многоразрядных целых чисел



Алгоритм деления многоразрядных целых чисел

1. Получил результат (рис. -@fig:009)



Результат алгоритмов

# Выводы

Изучал задачу представления больших чисел, познакомились с вычислительными алгоритмами и реализовали их.

# Список литературы

1. [Длинная арифметика от Microsoft](https://habr.com/ru/post/207754/)