Санкт-Петербургский Национальный Исследовательский Университет Информационных Технологий, Механики и Оптики

Кафедра Систем Управления и Информатики

# Лабораторная работа №2 Вариант №5

Выполнил (и:)

Бахтина А.В.,

Шевченко К.В.,

Шимченко А.С

Проверил Мусаев А.А.

Санкт-Петербург,

2023

ВВЕДЕНИЕ

Целью работы является изучение алгоритмов хеширования и его методов (деления, умножения и сложения). В задании необходимо показать алгоритмы хеширования по методу деления и CRC-32.

ЗАДАНИЕ 1

**1.1 Алгоритм деления**

В начале создается список из символов в формате цифр юникода (рисунок 1). Далее преобразовывается множество целых неотрицательных чисел k в диапазон значений m. В итоге с использованием хэш-функции вычисляется остаток от деления данной операцией (рисунок 2). В данном алгоритме получается вывод списка из хэша для каждого символа (рисунок 3).

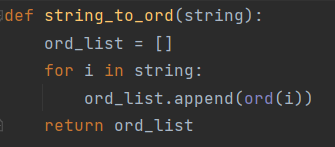


Рисунок 1 – Список из символов

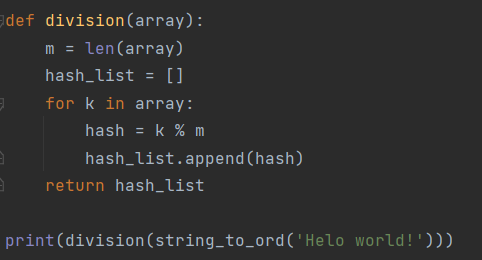


Рисунок 2 – Алгоритм деления



Рисунок 3 – Вывод работы алгоритма

**1.2 Алгоритм CRC-32**

Алгоритм CRC32 представлен в отражённой форме (со сдвигом вправо) с обратным полиномом. Проверка не одного, а сразу 8 бит осуществляется с помощью таблицы предвычисленных значений на основе образующего полинома 0xEDB88320 (рисунок 4). После работы этой части алгоритма в таблице находятся 256 32-битных значений. Алгоритм инициализирует регистр значением 0xFFFFFFFF, так как при инициализации нулевым значением он будет иметь «слепое пятно» в отношении нулевых байтов в начале сообщения и не сможет оценить их количество. Байты данных поступают в нижние 8 бит значения CRC, проверяется нижний бит значения и инвертируется конечное значение (рисунок 5). Алгоритм выводит результат работы функции crc32 в шестнадцатеричной системе счисления (рисунок 6).

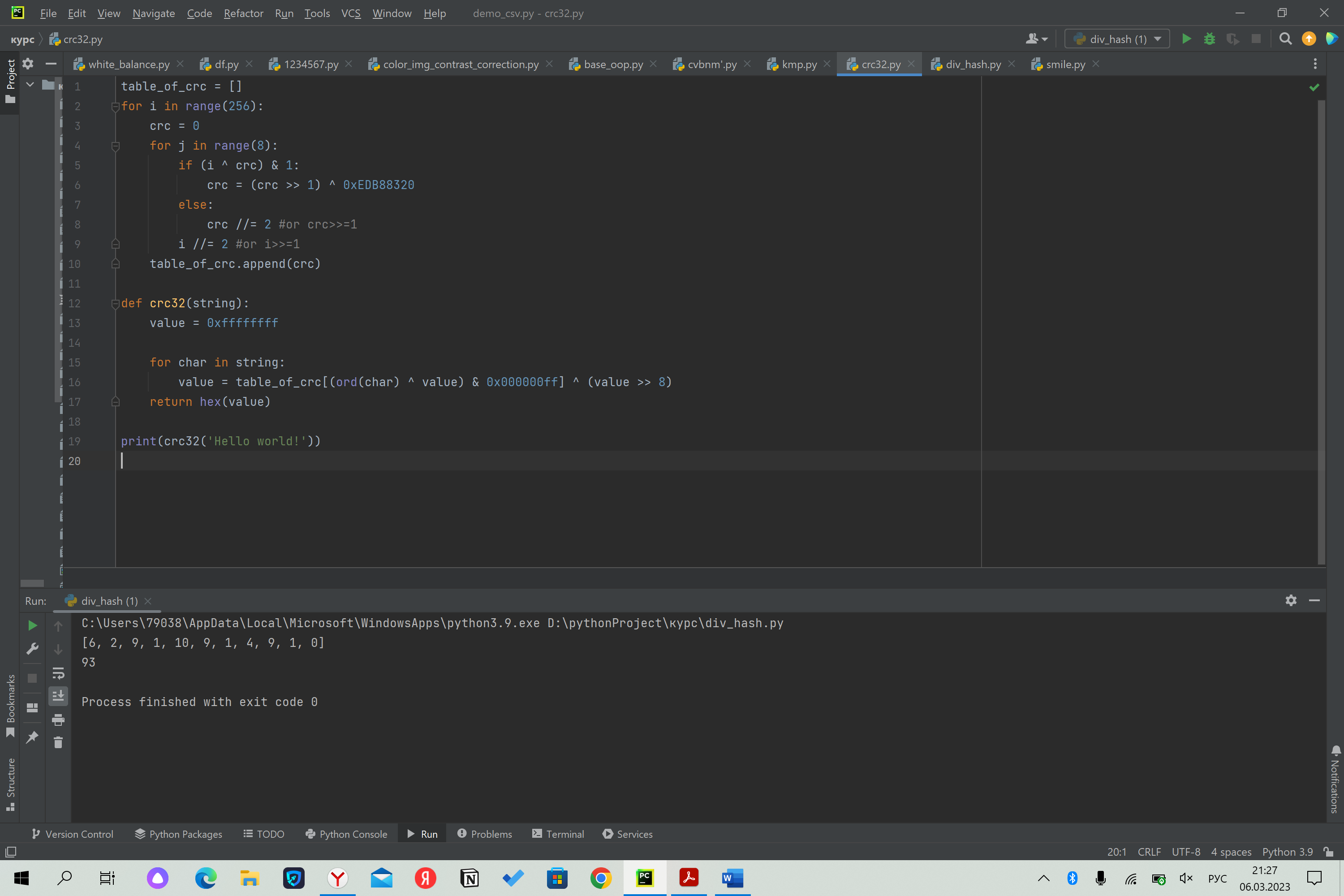


Рисунок 4 – Таблица предвычисленных значений

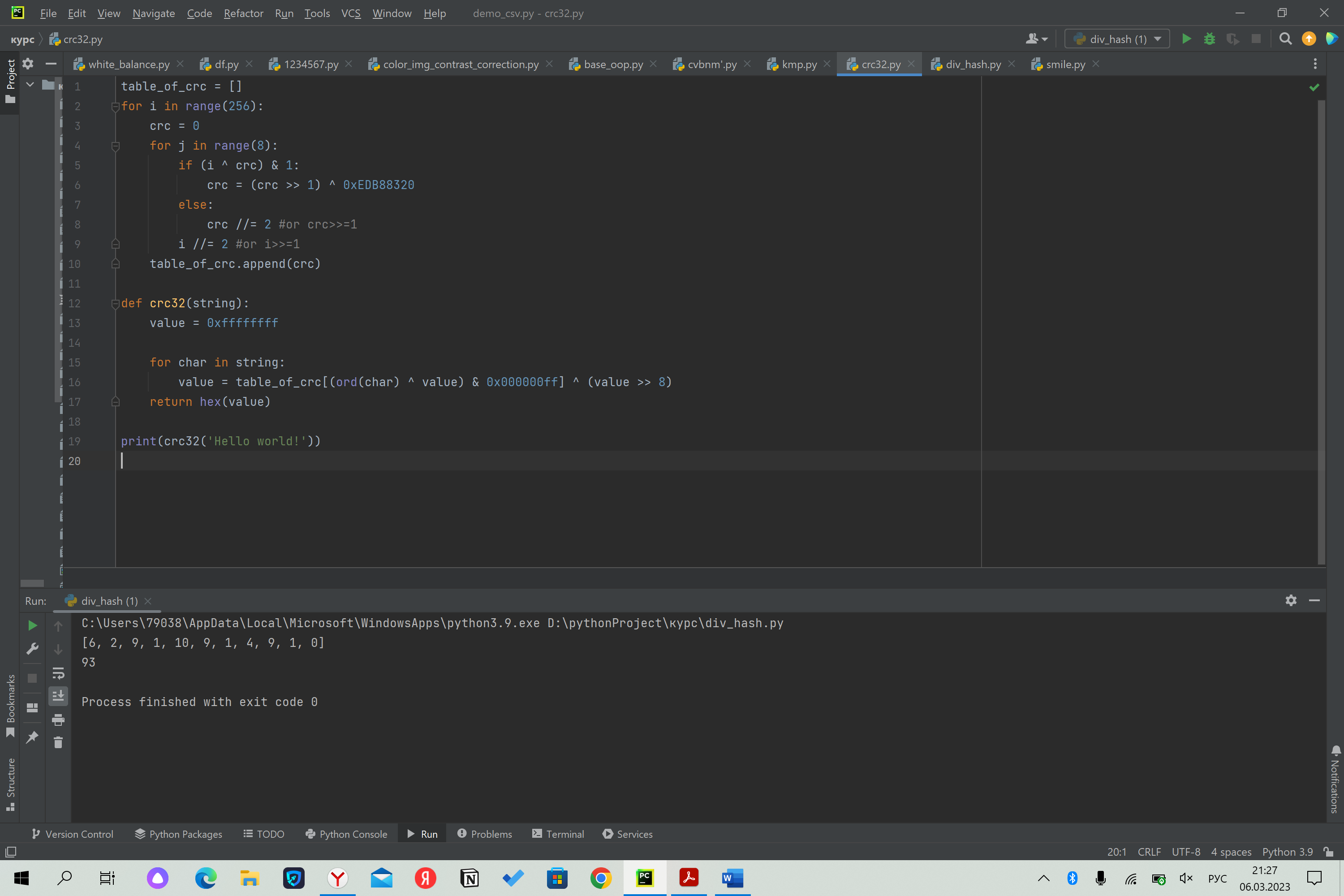


Рисунок 5 – Алгоритм CRC32

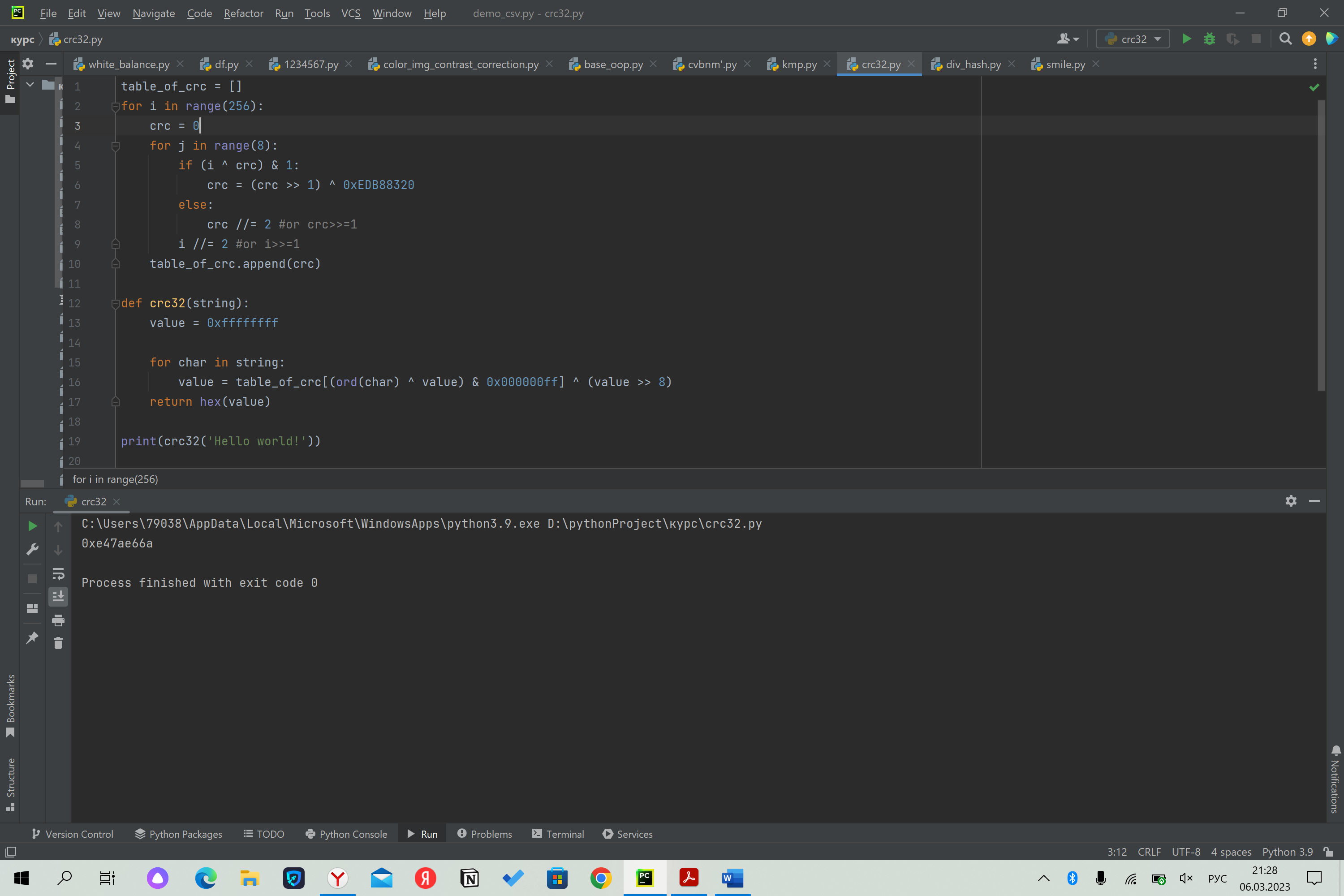


Рисунок 6 – Вывод работы алгоритма

ЗАКЛЮЧЕНИЕ

В ходе работы была выполнена основная цель - изучение алгоритмов хеширования и его методов (деления, умножения и сложения). Было выполнено задание для закрепления теории: показать алгоритмы хеширования по методу деления и CRC-32.

СПИСОК ЛИТЕРАТУРЫ

1. GitHub [Электронный ресурс] – URL: <https://github.com/al-shimchenko/ads> (дата обращения: 06.03.2023)