|  |  |
| --- | --- |
| **Российский университет транспорта (МИИТ)**  **Институт транспортной техники и систем управления**  **Кафедра «Управление и защита информации»** | |
| **Отчет**  **по практическому заданию**  **по теме «Возведение в степень по модулю числа»**  **по дисциплине «Криптографические методы защиты информации»** | |
|  | Выполнил:  Студент группы ТКИ-342  Белов С.В.  Проверил:  Доцент кафедры УиЗи, к.т.н., с.н.с.  Михалевич И.Ф. |
| Москва 2023 | |

**Оглавление**

[Задание 5](#_Toc129209461)

[Исходные данные 5](#_Toc129209462)

[1. Способы преобразования и проверки правильности преобразования 6](#_Toc129209463)

[1.1 Метод разбиения (breakdown method) 6](#_Toc129209464)

[1.2 Преобразование чисел методом вычисления значений полиномов (многочленов) 6](#_Toc129209465)

[1.3 Метод преобразования числа ручным пересчётом 6](#_Toc129209466)

[1.4 Схема Горнера 7](#_Toc129209467)

[2. Преобразование и проверка для двоичной системы 8](#_Toc129209468)

[2.1 Вычисление значений числа ДР 8](#_Toc129209469)

[2.1.1 Метод деления 8](#_Toc129209471)

[2.1.2 Проверка методом Полинома и Горнера 8](#_Toc129209472)

[2.2 Вычисление значений числа ДЗ 8](#_Toc129209473)

[2.2.1 Метод деления 9](#_Toc129209476)

[2.2.2 Проверка методом Полинома и Горнера 9](#_Toc129209477)

[2.3 Вычисление значений числа ДР+ДЗ 9](#_Toc129209478)

[2.3.1 Метод деления 10](#_Toc129209483)

[2.3.2 Проверка методом Полинома и Горнера 10](#_Toc129209484)

[3. Проверка и преобразование для троичной системы 10](#_Toc129209485)

[3.1 Вычисление значений числа ДР 10](#_Toc129209486)

[3.1.1 Метод деления 11](#_Toc129209488)

[3.1.2 Проверка методом Полинома и Горнера 11](#_Toc129209489)

[3.2 Вычисление значений числа ДЗ 11](#_Toc129209490)

[3.2.1 Метод деления 12](#_Toc129209495)

[3.2.2 Проверка методом Полинома и Горнера 12](#_Toc129209496)

[3.3 Вычисление значений числа ДР+ДЗ 12](#_Toc129209497)

[3.3.1 Метод деления 13](#_Toc129209504)

[3.3.2 Проверка методом Полинома и Горнера 13](#_Toc129209505)

[4. Проверка и преобразование для четверичной системы 13](#_Toc129209506)

[4.1 Вычисление значений числа ДР 13](#_Toc129209507)

[4.1.1 Метод деления 14](#_Toc129209509)

[4.1.2 Проверка методом Полинома и Горнера 14](#_Toc129209510)

[4.2 Вычисление значений числа ДЗ 14](#_Toc129209511)

[4.2.1 Метод деления 15](#_Toc129209516)

[4.2.2 Проверка методом Полинома и Горнера 15](#_Toc129209517)

[4.3 Вычисление значений числа ДР+ДЗ 15](#_Toc129209518)

[4.3.1 Метод деления 16](#_Toc129209525)

[4.3.2 Проверка методом Полинома и Горнера 16](#_Toc129209526)

[5. Проверка и преобразование для восьмеричной системы 16](#_Toc129209527)

[5.1 Вычисление значений числа ДР 16](#_Toc129209528)

[5.1.1 Метод деления 17](#_Toc129209530)

[5.1.2 Проверка методом Полинома и Горнера 17](#_Toc129209531)

[5.2 Вычисление значений числа ДЗ 18](#_Toc129209532)

[5.2.1 Метод деления 18](#_Toc129209537)

[5.2.2 Проверка методом Полинома и Горнера 18](#_Toc129209538)

[5.3 Вычисление значений числа ДР+ДЗ 19](#_Toc129209539)

[5.3.1 Метод деления 19](#_Toc129209546)

[5.3.2 Проверка методом Полинома и Горнера 19](#_Toc129209547)

[6. Проверка и преобразование для шестнадцатеричной системы 20](#_Toc129209548)

[6.1 Вычисление значений числа ДР 20](#_Toc129209549)

[6.1.1 Метод деления 20](#_Toc129209551)

[6.1.2 Проверка методом Полинома и Горнера 21](#_Toc129209552)

[6.2 Вычисление значений числа ДЗ 21](#_Toc129209553)

[6.2.1 Метод деления 22](#_Toc129209558)

[6.2.2 Проверка методом Полинома и Горнера 22](#_Toc129209559)

[6.3 Вычисление значений числа ДР+ДЗ 22](#_Toc129209560)

[6.3.1 Метод деления 23](#_Toc129209567)

[6.3.2 Проверка методом Полинома и Горнера 23](#_Toc129209568)

[Заключение 24](#_Toc129209569)

# Задание

Записать свой день рождения и текущий день выполнения задания в формате д.м.г.

Представить запись в п. 1 в формате восьмиразрядных десятичных чисел дмг(конкатенация).

Найти сумму чисел, отражающих день рождения и текущий день выполнения задания.

Преобразовать каждое число, полученное в пунктах 2 и 3, в двоичные числа.

Произвести суммирование чисел п. 2 в двоичной системе.

Сверить число, полученное в п. 5 с числом, полученным в п. 4 для числа из п.3.

Произвести обратное преобразование результата, полученного в п. 6, в десятичное число. Сверить результат с числом в п. 3.

Повторить действия п. п. 4 -7 для троичных чисел.

Повторить действия п. п. 4 -7 для четверичных чисел.

Повторить действия п. п. 4 -7 для восьмеричных чисел.

Повторить действия п. п. 4 -7 для шестнадцатеричных чисел.

Оформить отчет.

# Исходные данные





# Способы преобразования и проверки правильности преобразования

## Метод разбиения (breakdown method)

Преобразуемое число последовательно делим на основание целевой системы счисления. Следующее деление использует частное предыдущей операции. Так продолжается до тех пор, пока остаток в пределах целевой системы счисления и частное не достигнут значения 0. Полученные остатки заполняют разряды в целевой системе счисления, начиная с самого младшего разряда.

## Преобразование чисел методом вычисления значений полиномов (многочленов)

Полином (греч. пολυ - «много» + лат. nomen «имя»). Полином от одной переменной есть конечная формальная сумма вида:

|  |  |
| --- | --- |
| , |  |

где: - фиксированные коэффициенты, - степень полинома, – основание системы счисления.

Наблюдение: значение нулевого разряда полинома всегда равно значению коэффициента при его нулевом элементе.

Определение: нулевой элемент полинома называется свободным членом

Оценки сложности алгоритмов

n – кол-во бит числа.

## Метод преобразования числа ручным пересчётом

Правила преобразования двоичного числа в *k* -ричные числа с основаниями :

* исходная двоичная последовательность разделяется на группы по *k* двоичных символов справа налево;
* старшая группа символов может дополняться до общего размера в *k* символов необходимым числом нулей слева.

## Схема Горнера

Альтернативой полиномиальному методу перевода чисел в десятичную форму является схема Горнера. По схеме Горнера легко перевести в десятичное число любое число по основанию *p*, представив его в виде алгебраического многочлена *n*-й степени:

|  |  |
| --- | --- |
| = |  |

Для перевода числа не требуется операция возведения в степень *n*, достаточно произвести *n* операций умножения и *n* операций сложения, не прибегая к операциям возведения в степень.

|  |  |
| --- | --- |
| = |  |

1. Цифру в старшем разряде умножить на основание *p*;
2. к результату добавить цифру в предыдущем разряде;
3. результат умножить на основание *p*;
4. повторить операции 2, 3 к цифрам в остальных разрядах;
5. на операции с цифрой в нулевом разряде получено число в десятичной записи.

# Преобразование и проверка для двоичной системы

## 2.1 Вычисление значений числа ДР





### Метод деления



### Проверка методом Полинома и Горнера



## 2.2 Вычисление значений числа ДЗ





### Метод деления



### Проверка методом Полинома и Горнера



## 2.3 Вычисление значений числа ДР+ДЗ









### Метод деления



### Проверка методом Полинома и Горнера



# Проверка и преобразование для троичной системы

## 3.1 Вычисление значений числа ДР





### Метод деления



### Проверка методом Полинома и Горнера



## 3.2 Вычисление значений числа ДЗ









### Метод деления



### Проверка методом Полинома и Горнера



## 3.3 Вычисление значений числа ДР+ДЗ










### Метод деления



### Проверка методом Полинома и Горнера



# Проверка и преобразование для четверичной системы

## 4.1 Вычисление значений числа ДР





### Метод деления



### Проверка методом Полинома и Горнера



## 4.2 Вычисление значений числа ДЗ









### Метод деления



### Проверка методом Полинома и Горнера



## 4.3 Вычисление значений числа ДР+ДЗ










### Метод деления



### Проверка методом Полинома и Горнера



# Проверка и преобразование для восьмеричной системы

## 5.1 Вычисление значений числа ДР





### Метод деления



### Проверка методом Полинома и Горнера



## 5.2 Вычисление значений числа ДЗ









### Метод деления



### Проверка методом Полинома и Горнера



## 5.3 Вычисление значений числа ДР+ДЗ










### Метод деления



### Проверка методом Полинома и Горнера



# Проверка и преобразование для шестнадцатеричной системы

## 6.1 Вычисление значений числа ДР





### Метод деления



### Проверка методом Полинома и Горнера



## 6.2 Вычисление значений числа ДЗ









### Метод деления



### Проверка методом Полинома и Горнера



## 6.3 Вычисление значений числа ДР+ДЗ










### Метод деления



### Проверка методом Полинома и Горнера



# Заключение

В ходе решения практического задания были преобразованы в различные системы счисления следующие значения: ДР – день рождения, ДЗ – день выполнения задания. Применялись следующие методы: разбиения (деления), полиномов, многочлена, по схеме Горнера, «ручным» пересчетом. Все значения были перепроверены и соответствуют исходным данным.