|  |  |
| --- | --- |
| **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  Дроздов А.Д.  Проверил:  Доцент кафедры УиЗи, к.т.н., с.н.с.  Михалевич И.Ф. |
| Москва 2023 | |

**Оглавление**

[1. Теоретическая часть 3](#_Toc128233466)

[1.1. Основной метод вычисления степени по модулю числа 3](#_Toc128233467)

[1.2. Альтернативные методы вычисления 3](#_Toc128233468)

[1.3. Вопросы оценки сложности алгоритмов 3](#_Toc128233469)

[2. Практическая часть 3](#_Toc128233470)

[2.1. Результаты вычисление 3](#_Toc128233471)

[2.2. Сравнение сложности алгоритмов вычисления 3](#_Toc128233472)

[Заключение 3](#_Toc128233473)

# Задание

Номер варианта: 4.

Вычислить:

|  |  |
| --- | --- |
|  | (1) |
|  | (2) |
|  | (3) |
|  | (4) |
|  | (5) |
|  | (6) |

Исходные данные:

|  |  |
| --- | --- |
|  | (7) |
|  | (8) |

Провести анализ сложности выполненных расчетов для каждого из примененных алгоритмов.

# Теоретическая часть

## Бинарный алгоритм возведения в степень по модулю числа

Бинарный алгоритм – это один из методов, позволяющий возвести число в степень по заданному модулю с помощью разложения степени в двоичное число.

Исходное выражение:

|  |  |
| --- | --- |
|  | (9) |

Для возведения числа в степень по заданному модулю необходимо степень из десятичной системы счисления перевести в двоичную и представить исходное выражение следующим образом, где – степени разложенного (степени двойки)

|  |  |
| --- | --- |
|  | (10) |

Выполняем вышеуказанные преобразования до тех пор, пока результат не будет найден.

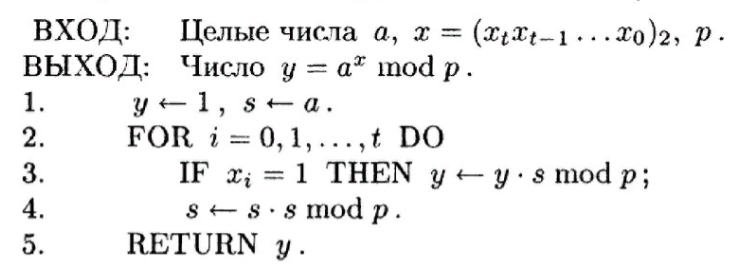


Рисунок 1 – Псевдокод бинарного алгоритма

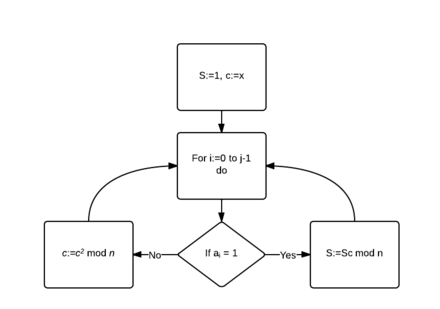


Рисунок 2 – Блок-схема бинарного алгоритма

## 1.2. Альтернативный алгоритм быстрого возведения в степень по модулю числа – Китайская теорема об остатках

Пусть необходимо возвести число в степени по модулю :

|  |  |
| --- | --- |
|  | (11) |

Тогда выражение можно разложить на простые множители , при и построить следующую систему:

|  |  |
| --- | --- |
|  | (12) |

Теперь можно представить как где – целое число

|  |  |
| --- | --- |
|  | (13) |

Подставляя одно уравнение в другое, получим результат.

## Оценки сложности алгоритмов

n – кол-во бит числа.

Бинарный алгоритм имеет сложность 1.5n умножения двух чисел, 1.5n операций деления числа 2n-битовых чисел на n-битовое число.

Для алгоритма с применением китайской теоремы об остатках сложность .

# Практическая часть

## Результаты вычисление

### 2.3.1. Вычисление заданных выражений с помощью бинарного алгоритма

Число , степень .

|  |  |
| --- | --- |
|  | (14) |
|  | (15) |
|  | (16) |

Выражение 1:

|  |  |
| --- | --- |
|  | (17) |
|  | (18) |
|  | (19) |
|  | (20) |
|  | (21) |
|  | (22) |

Подставляем полученные значения и получаем результат:

|  |  |
| --- | --- |
|  | (23) |

Выражение 2:

|  |  |
| --- | --- |
|  | (24) |
|  | (25) |
|  | (26) |
|  | (27) |
|  | (28) |
|  | (29) |

Подставляем полученные значения и получаем результат:

|  |  |
| --- | --- |
|  | (30) |

Выражение 3:

|  |  |
| --- | --- |
|  | (31) |
|  | (32) |
|  | (33) |
|  | (34) |
|  | (35) |
|  | (36) |

Подставляем полученные значения и получаем результат:

|  |  |
| --- | --- |
|  | (37) |

Выражение 4:

|  |  |
| --- | --- |
|  | (38) |
|  | (39) |
|  | (40) |
|  | (41) |
|  | (42) |
|  | (43) |

Подставляем полученные значения и получаем результат:

|  |  |
| --- | --- |
|  | (44) |

Выражение 5:

|  |  |
| --- | --- |
|  | (45) |
|  | (46) |
|  | (47) |
|  | (48) |
|  | (49) |
|  | (50) |

Подставляем полученные значения и получаем результат:

|  |  |
| --- | --- |
|  | (51) |

Выражение 6:

|  |  |
| --- | --- |
|  | (52) |
|  | (53) |
|  | (54) |
|  | (55) |
|  | (56) |
|  | (57) |

Подставляем полученные значения и получаем результат:

|  |  |
| --- | --- |
|  | (58) |

# Заключение

Текст заключения.