|  |  |
| --- | --- |
| **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**

[Задание 3](#_Toc129028125)

[1. Теоретическая часть 4](#_Toc129028126)

[1.1. Бинарный алгоритм возведения в степень по модулю числа 4](#_Toc129028127)

[1.2. Альтернативный алгоритм быстрого возведения в степень по модулю числа – Китайская теорема об остатках 5](#_Toc129028128)

[1.3. Оценки сложности алгоритмов 5](#_Toc129028129)

[2. Практическая часть 6](#_Toc129028130)

[2.1. Вычисление с помощью бинарного алгоритма 6](#_Toc129028131)

[2.2. Вычисление с помощью китайской теореме об остатках 8](#_Toc129028132)

[Заключение 9](#_Toc129028133)

# Задание

Номер варианта: 4.

Вычислить:

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Исходные данные:

|  |  |
| --- | --- |
|  |  |
|  |  |

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:

|  |  |
| --- | --- |
|  |  |

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)

|  |  |
| --- | --- |
|  |  |

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

|  |
| --- |
|  |
| 1. – Псевдокод бинарного алгоритма |

|  |
| --- |
| Алгоритмы быстрого возведения в степень по модулю - Wikiwand |
| 1. – 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 :

|  |  |
| --- | --- |
|  |  |

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

|  |  |
| --- | --- |
|  |  |

Вычеты c использованием малой теоремы Ферма, где .

Теперь можно представить как где – целое число

|  |  |
| --- | --- |
|  |  |

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

## Вычисление с помощью бинарного алгоритма

Число , степень .

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |

Выражение 1:

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Подставляем полученные значения и получаем результат:

|  |  |
| --- | --- |
|  |  |

Выражение 2:

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Подставляем полученные значения и получаем результат:

|  |  |
| --- | --- |
|  |  |

Выражение 3:

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Подставляем полученные значения и получаем результат:

|  |  |
| --- | --- |
|  |  |

Выражение 4:

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Подставляем полученные значения и получаем результат:

|  |  |
| --- | --- |
|  |  |

Выражение 5:

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Подставляем полученные значения и получаем результат:

|  |  |
| --- | --- |
|  |  |

Выражение 6:

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Подставляем полученные значения и получаем результат:

|  |  |
| --- | --- |
|  |  |

## Вычисление с помощью китайской теореме об остатках

Число , степень .

По китайской теореме об остатках сначала необходимо значение модуля представить, как произведение взаимно простых чисел. Поэтому возьмем выражение 2, в котором представим следующим образом.

Выражение 2:

|  |  |
| --- | --- |
|  |  |
|  |  |

Тогда по теореме получим систему:

|  |  |
| --- | --- |
|  |  |
|  |  |

Подставит из первого уравнения во второе:

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Заключение

В результате выполнения практической работы было рассмотрено два алгоритма быстрого возведения числа в степень по модулю. При вычислении заданных выражений вышеуказанными способами можно убедиться в том, что бинарный алгоритм универсален и подходит для выражения любой сложности, а метод с использованием китайской теоремы об остатках применим только в том случае, когда модуль раскладывается на взаимно простые сомножители.