УО «Белорусский государственный университет информатики и радиоэлектроники»

Кафедра ПОИТ

Отчет по лабораторной работе №3

по предмету «Теория информации»

Выполнил:

Крутько А.А.

гр. 251004

Проверила:

Болтак С.В.

Минск 2024

1. **Быстрое возведение в степень по модулю:**

57 mod 22 = 5\*56 mod 22 = 5 \* (53)2 mod 22 = 5 \* (5 \* 52)2 mod 22 = 3

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| А1 (основание степени) | Z(степень) | X(результат) | Модуль | Шаги выполнения |
| 5 | 7 | 1 | 22 | 0 |
| 5 | 6 | 1\*5 mod 22 = 5 | 22 | 1 |
| 5 \* 5 mod 22 = 3 | 3 | 5 | 22 | 2 |
| 3 | 2 | 5 \* 3 mod 22 = 15 | 22 | 3 |
| 3 \* 3 mod 22 = 9 | 1 | 15 | 22 | 4 |
| 9 | 0 | 15 \* 9 mod 22 = 135 mod 22 = 3 | 22 | 5 |

1. **Поиск всех первообразных корней числа**

Простое p – 11

Ищем от [2; p – 1] => [2; 10]

|  |  |  |
| --- | --- | --- |
| 2 | mod 11 = 25 mod 11 = 10 | mod 11 = 22 mod 11 = 4 |
| 3 | mod 11 = 35 mod 11 = 1 | mod 11 = 32 mod 11 = 9 |
| 4 | mod 11 = 45 mod 11 = 1 | mod 11 = 42 mod 11 = 5 |
| 5 | mod 11 = 55 mod 11 = 1 | mod 11 = 52 mod 11 = 3 |
| 6 | mod 11 = 65 mod 11 = 10 | mod 11 = 62 mod 11 = 3 |
| 7 | mod 11 = 75 mod 11 = 10 | mod 11 = 72 mod 11 = 5 |
| 8 | mod 11 = 85 mod 11 = 10 | mod 11 = 82 mod 11 = 9 |
| 9 | mod 11 = 95 mod 11 = 1 | mod 11 = 92 mod 11 = 4 |
| 10 | mod 11 = 105 mod 11 = 10 | mod 11 = 102 mod 11 = 1 |

Ответ: у числа p = 11 имеется 4 первообразных корня

1. **Пример работы расширенного алгоритма Евклида**