1. **Пример работы алгоритма быстрого возведения в степень с модульной арифметикой**

**45 mod 9 = 7**

|  |  |  |  |
| --- | --- | --- | --- |
| Шаги выполнения | Основание | Z(степень) | результат |
| 0 | 4 | 5 | (4 \* 4) mod 9 = 7 |
| 1 | 7 | 4 | (7 \* 7) mod 9 = 4 |
| 2 | 4 | 1 | (4 \* 4) mod 9 = 7 |

1. **Пример поиска всех первообразных корней**

Задано простое p = 7.

Количество первообразных .

Проверяем по степеням от 1 до p-1

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

1. **Пример работы расширенного алгоритма Евклида для взаимно простых чисел**

**x\*a + y\*b = 1, a = 11, b =19**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **итерация** | **a** | **b** | **x** | **y** | **q** |
| 0 | 11 | 19 | 7 | -4 | 1 |
| 1 | 19 | 11 | -4 | 7 | 1 |
| 2 | 11 | 8 | 3 | -4 | 1 |
| 3 | 8 | 3 | -1 | 3 | 1 |
| 4 | 3 | 2 | 1 | -1 | 1 |
| 5 | 2 | 1 | 0 | 1 | 1 |
| 6 | 1 | 0 | 1 | 0 | 1 |