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

**25 mod 3 = 2**

|  |  |  |  |
| --- | --- | --- | --- |
| Шаги выполнения | Основание | Z(степень) | результат |
| 0 | 2 | 5 | (2 \* 2) mod 3 = 1 |
| 1 | 1 | 4 | (1 \* 1) mod 3 = 1 |
| 2 | 2 | 1 | (2 \* 1) mod 3 = 2 |

1. **Пример поиска всех первообразных корней**

Задано простое p = 7.

Количество первообразных .

Проверяем по степеням от 2 до p-1

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

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

**x1 \* a + x2 \* y = 1; a = 419, b = 167, НОД(a, b) = 1**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| i | qi-1 | ri | x1 | x2 |
| 0 |  | 419 | 1 | 0 |
| 1 |  | 167 | 0 | 1 |
| 2 | 419/167 = 2 | 419 - 2\*167 = 85 | 1 - 2\*0 = 1 | 0 - 2\*1 = -2 |
| 3 | 167/85 = 1 | 167 - 1\*85 = 82 | 0 - 1\*1 = -1 | 1 – 1\*(-2) = 3 |
| 4 | 85/82 = 1 | 85 - 1\*82 = 3 | 1 - 1\*(-1) = 2 | -2 - 1\*3 = -5 |
| 5 | 82/3 = 27 | 82 - 27\*3 = 1 | -1 - 27\*2 = -55 | 3 - 27\*(-5) = 138 |
| 6 | 3/1 = 3 | 3 - 3\*1 = 0 | 2 - 3\*(-55) = 167 | -5 - 3\*138 = -419 |