1. **Пример работы алгоритма быстрого возведения в степень**

75 mod 4, т.е. a=7, z=5, n = 4

|  |  |  |  |
| --- | --- | --- | --- |
| **a (основание степени)** | **Z (степень)** | **X (результат)** | **Итерация** |
| 7 | 5 | 1 | 0 |
| 7 | 4 | 3 | 1 |
| 1 | 2 | 3 | 2 |
| 1 | 1 | 3 | 3 |
| 1 | 0 | 3 | 4 |

Ответ: 75 mod 4 = 3

1. **Пример поиска случайного первообразного корня**

p=53, p – 1 = 52 = 22 \* 13

|  |  |  |
| --- | --- | --- |
| **g** | **g^26 mod 53** | **Первообразный** |
| 2 | 52 | Да |
| 3 | 52 | Да |
| 4 | 1 | Нет |
| 5 | 52 | Да |
| 6 | 52 | Да |
| 7 | 1 | Нет |
| 8 | 52 | Да |
| 9 | 1 | Нет |
| 10 | 52 | Да |
| 11 | 52 | Да |
| 12 | 52 | Да |
| 13 | 52 | Да |
| 14 | 1 | Нет |
| 15 | 52 | Да |
| 16 | 1 | Нет |
| 17 | 52 | Да |
| 18 | 52 | Да |
| 19 | 52 | Да |
| 20 | 52 | Да |
| 21 | 1 | Нет |
| 22 | 52 | Да |
| 23 | 52 | Да |
| 24 | 52 | Да |
| 25 | 1 | Нет |
| 26 | 52 | Да |
| 27 | 1 | Нет |
| 28 | 52 | Да |
| 29 | 52 | Да |
| 30 | 52 | Да |
| 31 | 1 | Нет |
| 32 | 52 | Да |
| 33 | 52 | Да |
| 34 | 52 | Да |
| 35 | 1 | Нет |
| 36 | 52 | Да |
| 37 | 52 | Да |
| 38 | 52 | Да |
| 39 | 1 | Нет |
| 40 | 52 | Да |
| 41 | 52 | Да |
| 42 | 1 | Нет |
| 43 | 52 | Да |
| 44 | 52 | Да |
| 45 | 1 | Нет |
| 46 | 52 | Да |
| 47 | 52 | Да |
| 48 | 52 | Да |
| 49 | 1 | Нет |
| 50 | 52 | Да |
| 51 | 52 | Да |
| 52 | 1 | Нет |

2, 3, 5, 6, 8, 10, 11, 12, 13, 15, 17, 18, 19, 20, 22, 23, 24, 26, 28, 29, 30, 32, 33, 34, 36, 37, 38, 40, 41, 43, 44, 46, 47, 48, 50, 51 – первообразные корни

1. **Пример работы расширенного алгоритма Евклида**

**x1\*a + y1\*b = нод(a,b), a = 161, b = 28, нод(a,b) = 7**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **итерация** | **q** | **a0** | **a1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 161 | 28 | 1 | 0 | 0 | 1 |
| 1 | 5 | 28 | 21 | 0 | 1 | 1 | -5 |
| 2 | 1 | 21 | 7 | 1 | -1 | -5 | 6 |
| 3 | 3 | 7 | 0 | -1 | 4 | 6 | -23 |