1. **Алгоритм возведения в степень**

x = az mod m

a = 24; z = 33; m = 41

|  |  |  |  |
| --- | --- | --- | --- |
| а1(основание степени) | Z(степень) | х(результат) | Шаги выполнения |
| 24 | 33 | 1 | 0 |
| 24 | 32 | 1\*24 mod 41 = 24 | 1 |
| 24 \* 24 mod 41 = 2 | 16 | 24 | 2 |
| 2 \* 2 mod 41 = 4 | 8 | 24 | 3 |
| 4 \* 4 mod 41 = 16 | 4 | 24 | 4 |
| 16 \* 16 mod 41 = 10 | 2 | 24 | 5 |
| 10 \* 10 mod 41 = 18 | 1 | 24 | 6 |
| 18 | 0 | 24\*18 mod 41 = 22 | 7 |

2433 mod 41 = 24 \* 2432 mod 41 = 24 \* 216 mod 41 = 24 \* 48 mod 41 =

= 24 \* 164 mod 41 = 24 \* 102 mod 41 = 24 \* 181 mod 41 = 22

1. **Поиск первообразных корней**

Условие для первообразного корня:

(

p простое, поэтому

Для поиска всех первообразных корней пройдемся по интервалу [2, p-1] и найдем те числа, которые соответствуют условию.

Пусть p = 73 => p-1 = 72. Простые делители p-1 = {q0=2, q1=3}.

|  |  |  |  |
| --- | --- | --- | --- |
| gi |  |  | Является ли первообразным корнем или нет? |
| 2 | 1 | 64 | Нет |
| 3 | 1 | 1 | Нет |
| 4 | 1 | 8 | Нет |
| 5 | 72 | 8 | Да |
| 6 | 1 | 64 | Нет |
| 7 | 72 | 1 | Нет |
| 8 | 1 | 1 | Нет |
| 9 | 1 | 1 | Нет |
| 10 | 72 | 1 | Нет |
| 11 | 72 | 8 | Да |
| 12 | 1 | 8 | Нет |
| 13 | 72 | 64 | Да |
| 14 | 72 | 64 | Да |
| 15 | 72 | 8 | Да |
| 16 | 1 | 64 | Нет |
| 17 | 72 | 1 | Нет |
| 18 | 1 | 64 | Нет |
| 19 | 1 | 64 | Нет |
| 20 | 72 | 64 | Да |
| 21 | 72 | 1 | Нет |
| 22 | 72 | 1 | Нет |
| 23 | 1 | 8 | Нет |
| 24 | 1 | 1 | Нет |
| 25 | 1 | 64 | Нет |
| 26 | 72 | 8 | Да |
| 27 | 1 | 1 | Нет |
| 28 | 72 | 8 | Да |
| 29 | 72 | 64 | Да |
| 30 | 72 | 1 | Нет |
| 31 | 72 | 64 | Да |
| 32 | 1 | 8 | Нет |
| 33 | 72 | 8 | Да |
| 34 | 72 | 64 | Да |
| 35 | 1 | 8 | Нет |
| 36 | 1 | 8 | Нет |
| 37 | 1 | 8 | Нет |
| 38 | 1 | 8 | Нет |
| 39 | 72 | 64 | Да |
| 40 | 72 | 8 | Да |
| 41 | 1 | 8 | Нет |
| 42 | 72 | 64 | Да |
| 43 | 72 | 1 | Нет |
| 44 | 72 | 64 | Да |
| 45 | 72 | 8 | Да |
| 46 | 1 | 1 | Нет |
| 47 | 72 | 8 | Да |
| 48 | 1 | 64 | Нет |
| 49 | 1 | 1 | Нет |
| 50 | 1 | 8 | Нет |
| 51 | 72 | 1 | Нет |
| 52 | 72 | 1 | Нет |
| 53 | 72 | 64 | Да |
| 54 | 1 | 64 | Нет |
| 55 | 1 | 64 | Нет |
| 56 | 72 | 1 | Нет |
| 57 | 1 | 64 | Нет |
| 58 | 72 | 8 | Да |
| 59 | 72 | 64 | Да |
| 60 | 72 | 64 | Да |
| 61 | 1 | 8 | Нет |
| 62 | 72 | 8 | Да |
| 63 | 72 | 1 | Нет |
| 64 | 1 | 1 | Нет |
| 65 | 1 | 1 | Нет |
| 66 | 72 | 1 | Нет |
| 67 | 1 | 64 | Нет |
| 68 | 72 | 8 | Да |
| 69 | 1 | 8 | Нет |
| 70 | 1 | 1 | Нет |
| 71 | 1 | 64 | Нет |
| 72 | 1 | 1 | Нет |

Множество первообразных корней для p=73 => = {5, 11, 13, 14, 15, 20, 26, 28, 29, 31, 33, 34, 39, 40, 42, 44, 45, 47, 53, 58, 59, 60, 62, 68}

1. **Расширенный алгоритм Евклида**

Пусть

**a = 403**(делители {1, 13, 31, 403});

**b = 718**(делители {1, 2, 359, 718})

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Итерация** | **q** | **d0** | **d1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 403 | 718 | 1 | 0 | 0 | 1 |
| 1 | 0 | 718 | 403 | 0 | 1 | 1 | 0 |
| 2 | 1 | 403 | 315 | 1 | -1 | 0 | 1 |
| 3 | 1 | 315 | 88 | -1 | 2 | 1 | -1 |
| 4 | 3 | 88 | 51 | 2 | -7 | -1 | 4 |
| 5 | 1 | 51 | 37 | -7 | 9 | 4 | -5 |
| 6 | 1 | 37 | 14 | 9 | -16 | -5 | 9 |
| 7 | 2 | 14 | 9 | -16 | 41 | 9 | -23 |
| 8 | 1 | 9 | 5 | 41 | -57 | -23 | 32 |
| 9 | 1 | 5 | 4 | -57 | 98 | 32 | -55 |
| 10 | 1 | 4 | 1 | 98 | -155 | -55 | 87 |
| 11 | 4 | 1 | 0 | -155 | 718 | 87 | -403 |

**x1 = -155; y1 = 87**

**(-155) \* 403 + 87 \* 718 = 1**