1. **Алгоритм возведения в степень**

x = az mod m

a = 44; z = 29; m = 53

|  |  |  |  |
| --- | --- | --- | --- |
| а1(основание степени) | Z(степень) | х(результат) | Шаги выполнения |
| 44 | 29 | 1 | 0 |
| 44 | 28 | 1\*44 mod 53 = 44 | 1 |
| 44 \* 44 mod 53 = 28 | 14 | 44 | 2 |
| 28 \* 28 mod 53 = 42 | 7 | 44 | 3 |
| 42 | 6 | 44\*42 mod 53 = 46 | 4 |
| 42 \* 42 mod 53 = 15 | 3 | 46 | 5 |
| 15 | 2 | 46 \* 15 mod 53 = 1 | 6 |
| 15 \* 15 mod 53 = 13 | 1 | 1 | 7 |
| 13 | 0 | 1 \* 13 mod 53 = 13 | 8 |

4429 mod 53 = 44 \* 4428 mod 53 = 44 \* 2814 mod 53 = 44 \* 427 mod 53 =

= 44 \* 42 \* 426 mod 53 = 46 \* 153 mod 53 = 46 \* 15 \* 152 mod 53 = 1 \* 131 mod 53 = 13

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 = 59 => p-1 = 58. Простые делители p-1 = {q0=2, q1=29}.

|  |  |  |  |
| --- | --- | --- | --- |
| gi |  |  | Первообразный корень? |
| 2 | 58 | 4 | + |
| 3 | 1 | 9 | - |
| 4 | 1 | 16 | - |
| 5 | 1 | 25 | - |
| 6 | 58 | 36 | + |
| 7 | 1 | 49 | - |
| 8 | 58 | 5 | + |
| 9 | 1 | 22 | - |
| 10 | 58 | 41 | + |
| 11 | 58 | 3 | + |
| 12 | 1 | 26 | - |
| 13 | 58 | 51 | + |
| 14 | 58 | 19 | + |
| 15 | 1 | 48 | - |
| 16 | 1 | 20 | - |
| 17 | 1 | 53 | - |
| 18 | 58 | 29 | + |
| 19 | 1 | 7 | - |
| 20 | 1 | 46 | - |
| 21 | 1 | 28 | - |
| 22 | 1 | 12 | - |
| 23 | 58 | 57 | + |
| 24 | 58 | 45 | + |
| 25 | 1 | 35 | - |
| 26 | 1 | 27 | - |
| 27 | 1 | 21 | - |
| 28 | 1 | 17 | - |
| 29 | 1 | 15 | - |
| 30 | 58 | 15 | + |
| 31 | 58 | 17 | + |
| 32 | 58 | 21 | + |
| 33 | 58 | 27 | + |
| 34 | 58 | 35 | + |
| 35 | 1 | 45 | - |
| 36 | 1 | 57 | - |
| 37 | 58 | 12 | + |
| 38 | 58 | 28 | + |
| 39 | 58 | 46 | + |
| 40 | 58 | 7 | + |
| 41 | 1 | 29 | - |
| 42 | 58 | 53 | + |
| 43 | 58 | 20 | + |
| 44 | 58 | 48 | + |
| 45 | 1 | 19 | - |
| 46 | 1 | 51 | - |
| 47 | 58 | 26 | + |
| 48 | 1 | 3 | - |
| 49 | 1 | 41 | - |
| 50 | 58 | 22 | + |
| 51 | 1 | 5 | - |
| 52 | 58 | 49 | + |
| 53 | 1 | 36 | - |
| 54 | 58 | 25 | + |
| 55 | 58 | 16 | + |
| 56 | 58 | 9 | + |
| 57 | 1 | 4 | - |
| 58 | 58 | 1 | - |

1. **Расширенный алгоритм Евклида**

Пусть

**a = 442**(делители {1, 2, 13, 17, 26, 34, 221, 442});

**b = 805**(делители {1, 5, 7, 23, 35, 115, 161, 805})

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Итерация** | **q** | **d0** | **d1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 442 | 805 | 1 | 0 | 0 | 1 |
| 1 | 0 | 805 | 442 | 0 | 1 | 1 | 0 |
| 2 | 1 | 442 | 363 | 1 | -1 | 0 | 1 |
| 3 | 1 | 363 | 79 | -1 | 2 | 1 | -1 |
| 4 | 4 | 79 | 47 | 2 | -9 | -1 | 5 |
| 5 | 1 | 47 | 32 | -9 | 11 | 5 | -6 |
| 6 | 1 | 32 | 15 | 11 | -20 | -6 | 11 |
| 7 | 2 | 15 | 2 | -20 | 51 | 11 | -28 |
| 8 | 7 | 2 | 1 | 51 | -377 | -28 | 207 |
| 9 | 2 | 1 | 0 | -377 | 805 | 207 | -442 |

**x1 = -377;**

**y1 = 207;**

**(-377) \* 442 + 207 \* 805 = 1**