# Алгоритм возведения в степень

x = az mod m

a = 4; z = 9; m = 11

|  |  |  |  |
| --- | --- | --- | --- |
| а1(основание степени) | Z(степень) | х(результат) | Шаги  выполнения |
| 4 | 9 | 1 | 0 |
| 4 | 8 | 1\*4 mod 11 = 4 | 1 |
| 4 \* 4 mod 11 = 5 | 4 | 4 | 2 |
| 5 \* 5 mod 11 = 3 | 2 | 4 | 3 |
| 3 \* 3 mod 11 = 9 | 1 | 9 | 4 |
| 9 | 0 | 4\*9 mod 11 = 3 | 5 |

49 mod 11 = 4 \* 48 mod 11 = 4 \* 54 mod 11 = 4 \* 32 mod 11 = 4 \* 9 mod 11 = 3

# Поиск первообразных корней

Пусть p = 37 => p-1 = 36. Простые делители p-1 = {q0=2, q1=3}.

|  |  |  |  |
| --- | --- | --- | --- |
| gi | 𝑝−1  𝑔 𝑞0 = 𝑔18  𝑖 𝑖 | 𝑝−1  𝑔 𝑞1 = 𝑔12  𝑖 𝑖 | Массив g |
| 2 | 36 | 26 | {2} |
| 3 | 1 | 37 | {2} |
| 4 | 1 | 37 | {2} |
| 5 | 36 | 10 | {2, 5} |
| 6 | 36 | 1 | {2, 5} |
| 7 | 1 | 10 | {2, 5} |
| 8 | 36 | 1 | {2, 5} |
| 9 | 1 | 26 | {2, 5} |
| 10 | 1 | 1 | {2, 5} |
| 11 | 1 | 1 | {2, 5} |
| 12 | 1 | 26 | {2, 5} |
| 13 | 36 | 10 | {2, 5, 13} |
| 14 | 36 | 1 | {2, 5, 13} |
| 15 | 36 | 26 | {2, 5, 13, 15} |
| 16 | 1 | 26 | {2, 5, 13, 15} |
| 17 | 36 | 26 | {2, 5, 13, 15, 17} |

|  |  |  |  |
| --- | --- | --- | --- |
| 18 | 36 | 10 | {2, 5, 13, 15, 17, 18} |
| 19 | 36 | 10 | {2, 5, 13, 15, 17, 18, 19} |
| 20 | 36 | 26 | {2, 5, 13, 15, 17, 18, 19, 20} |
| 21 | 1 | 26 | {2, 5, 13, 15, 17, 18, 19, 20} |
| 22 | 36 | 26 | {2, 5, 13, 15, 17, 18, 19, 20, 22} |
| 23 | 36 | 1 | {2, 5, 13, 15, 17, 18, 19, 20, 22} |
| 24 | 36 | 10 | {2, 5, 13, 15, 17, 18, 19, 20, 22, 24} |
| 25 | 1 | 26 | {2, 5, 13, 15, 17, 18, 19, 20, 22, 24} |
| 26 | 1 | 1 | {2, 5, 13, 15, 17, 18, 19, 20, 22, 24} |
| 27 | 1 | 1 | {2, 5, 13, 15, 17, 18, 19, 20, 22, 24} |
| 28 | 1 | 26 | {2, 5, 13, 15, 17, 18, 19, 20, 22, 24} |
| 29 | 36 | 1 | {2, 5, 13, 15, 17, 18, 19, 20, 22, 24} |
| 30 | 1 | 10 | {2, 5, 13, 15, 17, 18, 19, 20, 22, 24} |
| 31 | 36 | 1 | {2, 5, 13, 15, 17, 18, 19, 20, 22, 24} |
| 32 | 36 | 10 | {2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32} |
| 33 | 1 | 10 | {2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32} |
| 34 | 1 | 10 | {2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32} |
| 35 | 36 | 26 | {2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35} |
| 36 | 1 | 1 | {2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35} |

Множество первообразных корней для p=37 => = {2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35}

# Расширенный алгоритм Евклида

Пусть

**a = 126**(делители {1, 2, 3, 7});

**b = 277**(делители {1, 277})

НОД(𝒂, 𝒃) = 𝟏

𝑥1 ∗ 𝑎 + 𝑦1 ∗ 𝑏 = НОД(𝑎, 𝑏)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Итерация** | **q** | **a₀** | **a₁** | **x₀** | **x₁** | **y₀** | **y₁** |
| 0 | – | 277 | 126 | 1 | 0 | 0 | 1 |
| 1 | 2 | 126 | 25 | 0 | 1 | 1 | -2 |
| 2 | 5 | 25 | 1 | 1 | -5 | -2 | 11 |
| 3 | 25 | 1 | 0 | -5 | 126 | 11 | -277 |

**x1 = -5; y1 = 11**

**126 \* 11 + (-5) \* 277 = 1**