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

a1 = 11, z = 23(10111), n = 71

|  |  |  |  |
| --- | --- | --- | --- |
| **а1(основание степени)** | **z(степень)** | **х(результат)** | **Шаги выполнения** |
| 11 | 23 | 1 | 0 |
| 11 | 22 | (1 \* 11) mod 71 = 11 | 1 |
| (11 \* 11) mod 71 = 50 | 11 | 11 (22 – четное) | 2 |
| 50 | 10 | (11 \* 50) mod 71 = 53 | 3 |
| (50 \* 50) mod 71 = 15 | 5 | 53 (10 – четное) | 4 |
| 15 | 4 | (53 \* 15) mod 71 = 14 | 5 |
| (15 \* 15) mod 71 = 12 | 2 | 14 (4 – четное) | 6 |
| (12 \* 12) mod 71 = 2 | 1 | 14 (4 – четное) | 7 |
| 2 | 0 | (14 \* 2) mod 71 = 28 | 8 |

1123 mod 71 = 28

**2.** **Пример поиска случайного первообразного корня**

p = 31, p – 1 = 30 = 2 \* 3 \* 5

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **g** | **g^30/2 mod 31** | **g^30/3 mod 31** | **g^30/5 mod 31** | **Первообразный** |
| 2 | 1 | 1 | 1 | - |
| 3 | 30 | 25 | 16 | + |
| 4 | 1 | 1 | 1 | - |
| 5 | 1 | 1 | 1 | - |
| 6 | 30 | 25 | 1 | - |
| 7 | 30 | 25 | 16 | + |
| 8 | 30 | 1 | 16 | - |
| 9 | 1 | 25 | 16 | - |
| 10 | 1 | 1 | 1 | - |
| 11 | 30 | 25 | 16 | + |
| 12 | 30 | 25 | 16 | + |
| 13 | 30 | 25 | 16 | + |
| 14 | 30 | 25 | 16 | + |
| 15 | 1 | 1 | 1 | - |
| 16 | 1 | 1 | 1 | - |
| 17 | 30 | 25 | 16 | + |
| 18 | 30 | 25 | 16 | + |
| 19 | 30 | 25 | 16 | + |
| 20 | 1 | 1 | 1 | - |
| 21 | 30 | 25 | 16 | + |
| 22 | 30 | 25 | 16 | + |
| 23 | 30 | 25 | 16 | + |
| 24 | 1 | 25 | 16 | - |
| 25 | 1 | 1 | 1 | - |
| 26 | 30 | 25 | 16 | + |
| 27 | 1 | 25 | 16 | - |
| 28 | 30 | 25 | 16 | + |
| 29 | 30 | 25 | 16 | + |
| 30 | 1 | 1 | 1 | - |

3, 7, 11, 12, 13, 14, 17, 18, 19, 21, 22, 23, 26, 28, 29 – первообразные корни

**3.** **Пример работы расширенного алгоритма Евклида**

a = 31, b = 71

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Итерация** | **q** | **a0** | **a1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 31 | 71 | 1 | 0 | 0 | 1 |
| 1 | 0 | 71 | 31 | 0 | 1 | 1 | 0 |
| 2 | 2 | 31 | 9 | 1 | -2 | 0 | 1 |
| 3 | 3 | 9 | 4 | -2 | 7 | 1 | -3 |
| 4 | 2 | 4 | 1 | 7 | -16 | -3 | 7 |
| 5 | 4 | 1 | 0 | -16 | 71 | 7 | -31 |

x = -16, y = 7

31 \* (-16) + 71 \* 7 = -496 + 497 = 1