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

а = 7, z = 83(10100112), n = 101

|  |  |  |  |
| --- | --- | --- | --- |
| **а1(основание степени)** | **z(степень)** | **х(результат)** | **Шаги выполнения** |
| 7 | 83 | 1 | 0 |
| 7 | 83 | 7 | 1 |
| 49 | 41 | 40 | 2 |
| 78 | 20 | 40 | 3 |
| 24 | 10 | 40 | 4 |
| 71 | 5 | 12 | 5 |
| 92 | 2 | 12 | 6 |
| 81 | 1 | 63 | 7 |

783 mod 101 = 63

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

p = 41, p – 1 = 40 = 23 · 5

|  |  |  |  |
| --- | --- | --- | --- |
| **g** | **g^40/2 mod 41** | **g^40/5 mod 41** | **Первообразный** |
| 2 | 1 | 1 | - |
| 3 | 40 | 1 | - |
| 4 | 1 | 18 | - |
| 5 | 1 | 18 | - |
| 6 | 40 | 10 | + |
| 7 | 40 | 37 | + |
| 8 | 1 | 16 | - |
| 9 | 1 | 1 | - |
| 10 | 1 | 16 | - |
| 11 | 40 | 16 | + |
| 12 | 1 | 8 | - |
| 13 | 1 | 36 | - |
| 14 | 40 | 36 | + |
| 15 | 1 | 8 | - |
| 16 | 1 | 36 | - |
| 17 | 40 | 10 | + |
| 18 | 1 | 37 | - |
| 19 | 40 | 37 | + |
| 20 | 1 | 16 | - |
| 21 | 1 | 18 | - |
| 22 | 1 | 18 | - |
| 23 | 40 | 8 | + |
| 24 | 1 | 8 | - |
| 25 | 1 | 16 | - |
| 26 | 1 | 36 | - |
| 27 | 40 | 36 | - |
| 28 | 40 | 16 | + |
| 29 | 1 | 10 | - |
| 30 | 1 | 10 | - |
| 31 | 40 | 8 | + |
| 32 | 1 | 37 | - |
| 33 | 1 | 37 | - |
| 34 | 40 | 16 | + |
| 35 | 1 | 36 | - |
| 36 | 1 | 36 | - |
| 37 | 40 | 10 | + |
| 38 | 1 | 8 | - |
| 39 | 40 | 18 | + |
| 40 | 1 | 1 | - |

Первообразные корни по модулю 41 (g, для которых обе проверки ≠ 1):

{6, 7, 11, 14, 17, 19, 23, 27, 28, 31, 34, 37, 39}

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

a = 299, b = 107

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Итерация** | **q** | **a0** | **a1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 299 | 107 | 1 | 0 | 0 | 1 |
| 1 | 2 | 107 | 85 | 0 | 1 | 1 | -2 |
| 2 | 1 | 85 | 22 | 1 | -1 | -2 | 3 |
| 3 | 3 | 22 | 19 | -1 | 4 | 3 | -11 |
| 4 | 1 | 19 | 3 | 4 | -5 | -11 | 14 |
| 5 | 6 | 3 | 1 | -5 | 34 | 14 | -95 |
| 6 | 3 | 1 | 0 | 34 | -107 | -95 | 299 |

x = 34, y = -95

31 \* 299 + (-95) \* 107 = 10166 – 10165 = 1