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

a1 = 5, z = 13 (1101), n = 23

|  |  |  |  |
| --- | --- | --- | --- |
| **а1(основание степени)** | **z(степень)** | **х(результат)** | **Шаги выполнения** |
| 5 | 13 | 1 | 0 |
| 5 | 12 | (1 \* 5) mod 23 = 5 | 1 |
| (5 \* 5) mod 23 = 2 | 6 | 5 (12 – четное) | 2 |
| (2 \* 2) mod 23 = 4 | 3 | 5 (6 – четное) | 3 |
| 4 | 2 | (5 \* 4) mod 23 = 20 | 4 |
| (4 \* 4) mod 23 = 16 | 1 | 20 (2 – четное) | 5 |
|  | 0 | (20 \* 16) mod 23 = 21 | 6 |

513 mod 23 = 21

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

p = 13, p – 1 = 12 = 2 \* 2 \* 3

|  |  |  |  |
| --- | --- | --- | --- |
| **g** | **g^12/2 mod 13** | **g^12/3 mod 13** | **Первообразный** |
| 2 | 12 | 3 | + |
| 3 | 1 | 3 | - |
| 4 | 1 | 9 | - |
| 5 | 12 | 1 | - |
| 6 | 12 | 9 | + |
| 7 | 12 | 9 | + |
| 8 | 12 | 1 | - |
| 9 | 1 | 9 | - |
| 10 | 1 | 3 | - |
| 11 | 12 | 3 | + |
| 12 | 1 | 1 | - |

2, 6, 7, 11 – первообразные корни

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

a = 17, b = 43

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Итерация** | **q** | **a0** | **a1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 17 | 43 | 1 | 0 | 0 | 1 |
| 1 | 0 | 43 | 17 | 0 | 1 | 1 | 0 |
| 2 | 2 | 17 | 9 | 1 | -2 | 0 | 1 |
| 3 | 1 | 9 | 8 | -2 | 3 | 1 | -1 |
| 4 | 1 | 8 | 1 | 3 | -5 | -1 | 2 |
| 5 | 8 | 1 | 0 | -5 | 43 | 2 | -17 |

x = -5, y = 2

17 \* (-5) + 43 \* 2 = -85 + 86 = 1