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

a1 = 88, z = 14 (1110), n = 42

|  |  |  |  |
| --- | --- | --- | --- |
| **а1(основание степени)** | **z(степень)** | **х(результат)** | **Шаги выполнения** |
| 88 | 14 | 1 | 0 |
| (88 \* 88) mod 42 = 16 | 7 | 1 (14 - четное) | 1 |
| 16 | 6 | (1 \* 16) mod 42 = 16 | 2 |
| (16 \* 16) mod 42 = 4 | 3 | 16 (6 – четное) | 3 |
| 4 | 2 | (16 \* 4) mod 42 = 22 | 4 |
| (4 \* 4) mod 42 = 16 | 1 | 22 (2 – четное) | 5 |
|  | 0 | (22 \* 16) mod 42 = 16 | 6 |

8814 mod 42 = 16

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

p = 23, p – 1 = 22 = 2 \* 11

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

5, 7, 10, 11, 14, 15, 17, 19, 20, 21 – первообразные корни

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

a = 52, b = 777

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Итерация** | **q** | **a0** | **a1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 52 | 777 | 1 | 0 | 0 | 1 |
| 1 | 0 | 777 | 52 | 0 | 1 | 1 | 0 |
| 2 | 14 | 52 | 49 | 1 | -14 | 0 | 1 |
| 3 | 1 | 49 | 3 | -14 | 15 | 1 | -1 |
| 4 | 16 | 3 | 1 | 15 | -254 | -1 | 17 |
| 5 | 3 | 1 | 0 | -254 | 777 | 17 | -52 |

x = -254, y = 17

52 \* (-254) + 777 \* 17 = -13208 + 13209 = 1