1. **Пример работы алгоритма быстрого возведения в степень**   
   54 mod 3, т.е. a=5, z=4, n = 3

|  |  |  |  |
| --- | --- | --- | --- |
| **а (основание степени)** | **Z(степень)** | **X(результат)** | **итерация** |
| 5 | 4 | 1 | 0 |
| 1 | 2 | 1 | 1 |
| 1 | 1 | 1 | 2 |
| 1 | 0 | 1 | 3 |

Ответ: 54 mod 3=1

1. **Пример поиска случайного первообразного корня**p=17, p – 1 = 16 = 24

|  |  |  |
| --- | --- | --- |
| **g** | **g^8 mod 17** | **Является первообразным** |
| 2 | 1 | Нет |
| 3 | 16 | Да |
| 4 | 1 | Нет |
| 5 | 16 | Да |
| 6 | 16 | Да |
| 7 | 16 | Да |
| 8 | 16 | Да |
| 9 | 1 | Нет |
| 10 | 16 | Да |
| 11 | 16 | да |
| 12 | 16 | Да |
| 13 | 16 | Да |
| 14 | 1 | Нет |
| 15 | 1 | Нет |
| 16 | 1 | Нет |

3,5,6,7,8,10,11,12,13– первообразные корни

1. **Пример работы расширенного алгоритма Евклида**

**x1\*a + y1\*b = нод(a,b), a = 630, b = 147, нод(a,b) = 21**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **итерация** | **q** | **a0** | **a1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 630 | 147 | 1 | 0 | 0 | 1 |
| 1 | 4 | 147 | 42 | 0 | 1 | 1 | -4 |
| 2 | 3 | 42 | 21 | 1 | -3 | -4 | 13 |
| 3 | 2 | 21 | 0 | -3 | 7 | 13 | -30 |