1. **Пример работы алгоритма быстрого возведения в степень**   
   76 mod 5, т.е. a=7, z=6, n = 5

|  |  |  |  |
| --- | --- | --- | --- |
| **а (основание степени)** | **Z(степень)** | **X(результат)** | **итерация** |
| 7 | 6 | 1 | 0 |
| 4 | 3 | 1 | 1 |
| 4 | 2 | 4 | 2 |
| 1 | 1 | 4 | 3 |
| 1 | 0 | 4 | 4 |

Ответ: 4

***Проверка с помощью калькулятора:*** 76 = 117649, отнимаем 4 и получаем ровное деление на 5 без остатка.

1. **Пример поиска случайного первообразного корня**
2. **Пример работы расширенного алгоритма Евклида**

**x1\*a + y1\*b = нод(a,b), a = 731, b = 504, нод(a,b) = 1**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **итерация** | **q** | **a0** | **a1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 731 | 504 | 1 | 0 | 0 | 1 |
| 1 | 1 | 504 | 227 | 0 | 1 | 1 | -1 |
| 2 | 2 | 227 | 50 | 1 | -2 | -1 | 3 |
| 3 | 4 | 50 | 27 | -2 | 9 | 3 | -13 |
| 4 | 1 | 27 | 23 | 9 | -11 | -13 | 16 |
| 5 | 1 | 23 | 4 | -11 | 20 | 16 | -29 |
| 6 | 5 | 4 | 3 | 20 | -111 | -29 | 161 |
| 7 | 1 | 3 | 1 | -111 | 131 | 161 | -190 |