

1. Пример работы алгоритма быстрого возведения в степень

$7^6 \bmod 5$, 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: $7^6 \bmod 5=4$

2. Пример поиска случайного первообразного корня

$p=11$, $p - 1 = 10 = 2*5$

| g | $g^{10/2} \bmod 11$ | $g^{10/5} \bmod 11$ | Является первообразным |
|----|---------------------|---------------------|------------------------|
| 2 | 10 | 4 | да |
| 3 | 1 | 9 | нет |
| 4 | 1 | 5 | нет |
| 5 | 1 | 3 | нет |
| 6 | 10 | 3 | да |
| 7 | 10 | 5 | да |
| 8 | 10 | 9 | да |
| 9 | 1 | 4 | нет |
| 10 | 10 | 1 | нет |

2, 6, 7, 8 – первообразные корни

3. Пример работы расширенного алгоритма Евклида

$x_1*a + y_1*b = \text{нод}(a,b)$, $a = 731$, $b = 504$, $\text{нод}(a,b) = 1$

| итерация | q | a_0 | a_1 | x_0 | x_1 | y_0 | y_1 |
|----------|---|-------|-------|-------|-------|-------|-------|
| 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 |