

1. Пример работы алгоритма быстрого возведения в степень

$5^4 \bmod 3$, 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: $5^4 \bmod 3 = 1$

2. Пример поиска случайного первообразного корня

$p=7$, $p-1 = 6 = 2 \cdot 3$

g	$g^{6/2} \bmod 7$	$g^{6/3} \bmod 7$	Является первообразным
2	1	4	Нет
3	6	2	Да
4	1	2	Нет
5	6	4	Да
6	6	1	Нет

3, 5 – первообразные корни

3. Пример работы расширенного алгоритма Евклида

$x_1 \cdot a + y_1 \cdot b = \text{нод}(a, b)$, $a = 17$, $b = 13$, $\text{нод}(a, b) = 1$

итерация	q	a_0	a_1	x_0	x_1	y_0	y_1
0	-	17	13	1	0	0	1
1	1	13	4	0	1	1	-1
2	3	4	1	1	-3	-1	4
3	4	1	0	-3	13	4	-17