1. Пример работы алгоритма быстрого возведения в степень с модульной арифметикой

$x = a^z \bmod m$
$a = 3, z = 7, m = 5$
$3^7 * \bmod 5 = 3 * 3^6 \bmod 5 = 3 * (3^3)^2 \bmod 5 = 3 * (3 * 3^2)^2 \bmod 5 = 2$

a1 (основание степени)	z (степень)	x (результат)	Шаги выполнения
3	7	1	0
3	6	(1 * 3) mod 5 = 3	1
(3 * 3) mod 5 = 4	3	3	2
4	2	(3 * 4) mod 5 = 2	3
(4 * 4) mod 5 = 1	1	2	4
1	0	(2 * 1) mod 5 = 2	5

$x = 3^7 * \bmod 5 = 2$

2. Пример поиска случайного первообразного корня

Задано простое p = 13.

Ищем простые делители: p – 1 = 12 = 2 * 2 * 3.

Простые делители: 2 и 3.

Число будет первообразным корнем, если $g^{\frac{p-1}{q}} \not\equiv 1 \bmod p$, где g – возможный первообразный корень, а q – простой делитель.

g			Первообразный корень
2	2 ^ (12/2) mod 13 = 12	2 ^ (12/3) mod 13 = 3	да
3	3 ^ (12/2) mod 13 = 1	3 ^ (12/3) mod 13 = 3	нет
4	4 ^ (12/2) mod 13 = 1	4 ^ (12/3) mod 13 = 9	нет
5	5 ^ (12/2) mod 13 = 12	5 ^ (12/3) mod 13 = 1	нет
6	6 ^ (12/2) mod 13 = 12	6 ^ (12/3) mod 13 = 9	да
7	7 ^ (12/2) mod 13 = 12	7 ^ (12/3) mod 13 = 9	да
8	8 ^ (12/2) mod 13 = 12	8 ^ (12/3) mod 13 = 1	нет
9	9 ^ (12/2) mod 13 = 1	9 ^ (12/3) mod 13 = 9	нет
10	10 ^ (12/2) mod 13 = 1	10 ^ (12/3) mod 13 = 3	нет
11	11 ^ (12/2) mod 13 = 12	11 ^ (12/3) mod 13 = 3	да
12	12 ^ (12/2) mod 13 = 1	12 ^ (12/3) mod 13 = 1	нет

Первообразные корни: 2, 6, 7, 11.

3. Пример работы расширенного алгоритма Евклида с взаимно простыми числами

$x_1 * a + y_1 * b = НОД\ (a, b)$,
$a = 123, b = 101, (a, b) = 1$

Итерация	q	a_0	a_1	x_0	x_1	y_0	y_1
0	-	123	101	1	0	0	1
1	1	101	22	0	1	1	-1
2	4	22	13	1	-4	-1	5
3	1	13	9	-4	5	5	-6
4	1	9	4	5	-9	-6	11
5	2	4	1	-9	23	11	-28
6	4	1	0	23	-101	-28	123

$x_1 = 23, y_1 = -28;$
$23 * 123 + (-28) * 101 = 1.$