1) Алгоритм возведения в степень

$x = a^z \bmod m$

a = 8; z = 7; m = 13

a1(основание степени)	Z(степень)	x(результат)	Шаги выполнения
8	7	1	0
8	6	1*8 mod 13 = 8	1
8 * 8 mod 13 = 12	3	8	2
12	2	8 * 12 mod 13 = 5	3
12 * 12 mod 13 = 1	1	5	4
1	0	5 * 1 mod 13 = 5	5

$8^7 \bmod 13 = 8 * 8^6 \bmod 13 = 8 * 12^3 \bmod 13 = 8 * 12 * 12^2 \bmod 13 =$
$= 5 * 12^2 \bmod 13 = 5 * 1 \bmod 13 = 5$

2) Поиск первообразных корней

Условие для первообразного корня:

$$(g^{\varphi(p)} = 1\ mod\ p)\ AND\ (g^l \neq 1\ mod\ p; 1 \leq l \leq \varphi(p) - 1)$$

p простое, поэтому $\varphi(p) = p - 1$

Для поиска всех первообразных корней пройдемся по интервалу [2, p-1] и найдем те числа, которые соответствуют условию.

Пусть p = 29 => p-1 = 28. Простые делители p-1 = {q_0=2, q_1=7}.

g_i	$g_i^{\frac{p-1}{q_0}} = g_i^{14}$	$g_i^{\frac{p-1}{q_1}} = g_i^{4}$	Массив g
2	28	16	{2}
3	28	23	{2,3}
4	1	24	{2,3}
5	1	16	{2,3}
6	1	20	{2, 3}
7	1	23	{2, 3}
8	28	7	{2, 3, 8}
9	1	7	{2, 3, 8}
10	28	24	{2, 3, 8, 10}
11	28	25	{2, 3, 8, 10, 11}
12	28	1	{2, 3, 8, 10, 11}
13	1	25	{2, 3, 8, 10, 11}
14	28	20	{2, 3, 8, 10, 11, 14}
15	28	20	{2, 3, 8, 10, 11, 14, 15}
16	1	25	{2, 3, 8, 10, 11, 14, 15}
17	28	1	{2, 3, 8, 10, 11, 14, 15}

18	28	25	{2, 3, 8, 10, 11, 14, 15, 18}
19	28	24	{2, 3, 8, 10, 11, 14, 15, 18, 19}
20	1	7	{2, 3, 8, 10, 11, 14, 15, 18, 19}
21	28	7	{2, 3, 8, 10, 11, 14, 15, 18, 19, 21}
22	1	23	{2, 3, 8, 10, 11, 14, 15, 18, 19, 21}
23	1	20	{2, 3, 8, 10, 11, 14, 15, 18, 19, 21}
24	1	16	{2, 3, 8, 10, 11, 14, 15, 18, 19, 21}
25	1	24	{2, 3, 8, 10, 11, 14, 15, 18, 19, 21}
26	28	23	{2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26}
27	28	16	{2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27}
28	1	1	{2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27}

Множество первообразных корней для p=29 => = {2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27}

3) Расширенный алгоритм Евклида

Пусть

a = 482(делители {1, 2, 241, 482});

b = 715(делители {1, 5, 11, 13, 55, 65, 143, 715})

НОД$(\boldsymbol{a}, \boldsymbol{b}) = \mathbf{1}$

$$x_1 * a + y_1 * b = \text{НОД}(a, b)$$

итерация	**q**	$\mathbf{d_0}$	$\mathbf{d_1}$	$\mathbf{x_0}$	$\mathbf{x_1}$	$\mathbf{y_0}$	$\mathbf{y_1}$
0	-	482	715	1	0	0	1
1	0	715	482	0	1	1	0
2	1	482	233	1	-1	0	1
3	2	233	16	-1	3	1	-2
4	14	16	9	3	-43	-2	29
5	1	9	7	-43	46	29	-31
6	1	7	2	46	-89	-31	60
7	3	2	1	-89	313	60	-211

x1 = 313; y1 = -211

313 * 482 + (-211) * 715 = 1