1. **Пример работы алгоритма быстрого возведения в степень по модулю**

12^19 mod 37 = ?

x = 1

12 mod 37 = 12

x = x * 12 mod 37 = 12

12^2 mod 37 = 144 mod 37 = 33

x = x * 33 mod 37 = 26

12^4 mod 37 = (12^2 mod 37)^2 mod 37 = 33^2 mod 37 = 16

12^8 mod 37 = (12^4 mod 37)^2 mod 37 = 16^2 mod 37 = 34

12^16 mod 37 = (12^8 mod 37)^2 mod 37 = 34^2 mod 37 = 9

x = x * 9 mod 37 = 12

12^19 mod 37 = x = 12

2. **Пример поиска случайного первообразного корня**

Пусть простое число p = 19

Простые делители (p-1) = 18 = 2*3*3

2^(18/2) mod 19 = 18	подходит	11^(18/2) mod 19 = 1	Не подходит
2^(18/3) mod 19 = 7		11^(18/3) mod 19	
3^(18/2) mod 19 = 18	подходит	12^(18/2) mod 19 = 18	Не подходит
3^(18/3) mod 19 = 7		12^(18/3) mod 19 = 1	
4^(18/2) mod 19 = 1	Не подходит	13^(18/2) mod 19 = 18	подходит
4^(18/3) mod 19		13^(18/3) mod 19 = 11	
5^(18/2) mod 19 = 1	Не подходит	14^(18/2) mod 19 = 18	подходит
5^(18/3) mod 19		14^(18/3) mod 19 = 7	
6^(18/2) mod 19 = 1	Не подходит	15^(18/2) mod 19 = 18	подходит
6^(18/3) mod 19		15^(18/3) mod 19 = 11	
7^(18/2) mod 19 = 1	Не подходит	16^(18/2) mod 19 = 1	Не подходит
7^(18/3) mod 19		16^(18/3) mod 19	
8^(18/2) mod 19 = 18	Не подходит	17^(18/2) mod 19 = 1	Не подходит
8^(18/3) mod 19 = 1		17^(18/3) mod 19	
9^(18/2) mod 19 = 1	Не подходит	18^(18/2) mod 19 = 18	Не подходит
9^(18/3) mod 19		18^(18/3) mod 19 = 1	
10^(18/2) mod 19 = 18	подходит		
10^(18/3) mod 19 = 11			

Первообразные: 2, 3, 10, 13, 14, 15.

3. **Пример работы расширенного алгоритма Евклида**

x_1*a + y_1*b = (a,b), a =513, b =987

итерация	**q**	**d_0**	**d_1**	**x_0**	**x_1**	**y_0**	**y_1**
0	-	513	987	1	0	0	1
1	0	987	513	0	1	1	0
2	1	513	474	1	-1	0	1
3	1	474	39	-1	2	1	-1
4	12	39	6	2	-25	-1	13
5	6	6	3	-25	152	13	-79
6	2	3	0	152	-329	-79	171

X_1 = 152 y_1 = -79

513 * 152 + 987 * (-79) = 3