**Примеры работы алгоритмов**

**1. Алгоритм быстрого возведения в степень**

**Вычисление:** 57 mod  3   
**Параметры:** a=5,z=7, n=3

| **а (основание)** | **Z (степень)** | **X (результат)** | **Итерация** |
| --- | --- | --- | --- |
| 5 | 7 | 1 | 0 |
| 1 | 3 | 2 | 1 |
| 1 | 1 | 2 | 2 |
| 1 | 0 | 2 | 3 |

**Ответ:** 57 mod  3 =2

**2. Поиск первообразного корня**

**Параметры:** p=7*,* p−1=6=2×3. Проверка g от 2 до 6:

| **g** | **g3 mod  7** | **g2 mod  7** | **Первообразный?** |
| --- | --- | --- | --- |
| 2 | 1 | 4 | Нет |
| 3 | 6 | 2 | Да |
| 4 | 1 | 1 | Нет |
| 5 | 6 | 4 | Да |
| 6 | 6 | 1 | Нет |

**Первообразные корни:** 3, 5.

**3. Расширенный алгоритм Евклида**

**Найти:** *x* и y такие, что 28x+16y = НОД(28,16) = 4

| **Итерация** | **q** | **a₀** | **a₁** | **x₀** | **x₁** | **y₀** | **y₁** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | — | 28 | 16 | 1 | 0 | 0 | 1 |
| 1 | 1 | 16 | 12 | 0 | 1 | 1 | -1 |
| 2 | 1 | 12 | 4 | 1 | -1 | -1 | 2 |
| 3 | 3 | 4 | 0 | -1 | — | 2 | — |

**Решение:**  
x=−1*x*=−1, y=2*y*=2.  
**Проверка:** 28×(−1)+16×2=−28+32=4.