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

|  |  |  |  |
| --- | --- | --- | --- |
| а1(основание степени) | Z(степень) | х(результат) | Шаги выполнения |
| 4 | 11 | 1 | 0 |
| 4 | 10 | 1\*4=4 | 1 |
| (4\*4) mod9 = 7 | 5 | 4 | 2 |
| 7 | 4 | (4\*7) mod 9=1 | 3 |
| (7\*7) mod 9 = 4 | 2 | 1 | 4 |
| (4\*4) mod 9 = 7 | 1 | 1 | 5 |
| 7 | 0 | 1\*7=7 | 6 |

1. **Пример поиска случайного первообразного корня**

Задано простое p = 19

Ищем простые делители p-1 = 18 = 2 \* 3 \* 3

1-я степень = 18/3 = 6

2-я степень = 18/2 = 9

|  |  |  |  |
| --- | --- | --- | --- |
| **g** | **g^6 mod 19** | **g^9 mod 19** | **Первообразный** |
| 2 | 7 | 18 | + |
| 3 | 7 | 18 | + |
| 4 | 11 | 1 | - |
| 5 | 7 | 1 | - |
| 6 | 11 | 1 | - |
| 7 | 1 | 1 | - |
| 8 | 1 | 18 | - |
| 9 | 11 | 1 | - |
| 10 | 11 | 18 | + |
| 11 | 1 | 1 | - |
| 12 | 1 | 18 | - |
| 13 | 11 | 18 | + |
| 14 | 7 | 18 | + |
| 15 | 11 | 18 | + |
| 16 | 7 | 1 | - |
| 17 | 7 | 1 | - |
| 18 | 1 | 18 | - |

**Первообразные корни – 2, 3, 10, 13, 14,15**

1. **Пример работы расширенного алгоритма Евклида**

**x1\*a + y1\*b = НОД(a,b), a = 13, b = 23, (a,b) = 1**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **итерация** | **a** | **b** | **q** | **r** | **x0** | **x1** | **y0** | **y1** |
| 0 | 13 | 23 | - | - | 1 | 0 | 0 | 1 |
| 1 | 23 | 13 | 1 | 23 mod 13 = 10 | 0 | 1 – 1 \* 0 = 1 | 1 | 0 – 1 \* 1 = -1 |
| 2 | 13 | 10 | 13 / 10 = 1 | 13 mod 10 = 3 | 1 | 0 – 1 \* 1 = -1 | -1 | 1 – 1 \* (-1) = 2 |
| 3 | 10 | 3 | 10/3 = 3 | 10 mod 3 =1 | -1 | 1-3\*(-1) = 4 | 2 | -1 -3\*2=-7 |
|  |  |  |  |  |  |  |  |  |

**x1 = -4 y1 = -7**

**(-7) \* 13 + 4 \* 23 = 1**