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

|  |  |  |  |
| --- | --- | --- | --- |
| А (основание степени) | Z (степень) | Х (результат) | Шаги выполнения |
| 6 | 9 | 1 | 0 |
| 6 | 8 | (1 \* 6) mod 19 = 6 | 1 |
| (6\*6) mod 19 = 17 | 4 | 6 | 2 |
| (17\*17) mod 19 = 4 | 2 | 6 | 3 |
| (4\*4) mod 19 = 16 | 1 | 6 | 4 |
|  | 0 | (16\*6) mod 19 = 1 | 5 |

1. **Пример поиска случайного первообразного корня**

Задано простое p = 11

Ищем простые делители p-1 = 10 = 2 \* 5

|  |  |  |  |
| --- | --- | --- | --- |
| **g** | **g^10/2 mod 11** | **g^10/5 mod 11** | **Первообразный** |
| 2 | 10 | 4 | + |
| 3 | 1 | 9 | - |
| 4 | 1 | 5 | - |
| 5 | 10 | 3 | - |
| 6 | 10 | 3 | + |
| 7 | 10 | 5 | + |
| 8 | 10 | 9 | - |
| 9 | 1 | 4 | - |
| 10 | 1 | 1 | - |

**Первообразные корни – 2, 6, 7.**

1. **Пример работы расширенного алгоритма Евклида**

**x1\*a + y1\*b = НОД(a,b), a = 17, b = 5, (a,b) = 1**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **итерация** | **q** | **a0** | **a1** | **x0** | **x1** | **y0** | **y1** |
| 0 | — | 5 | 17 | 1 | 0 | 0 | 1 |
| 1 | 3 | 17 | 5 | 0 | 1 | 1 | 0 |
| 2 | 2 | 5 | 2 | 1 | -3 | 0 | 1 |
| 3 | 2 | 2 | 1 | -3 | 7 | 1 | -2 |
| 4 | — | 1 | 0 | 7 | — | -2 | — |
| 0 | — | 5 | 17 | 1 | 0 | 0 | 1 |
| 1 | 3 | 17 | 5 | 0 | 1 | 1 | 0 |

**x1 = -2 y1 = 7**

**(-2) \* 17 + 7 \* 5 = 1**