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

a = 4, z = 5, n = 15

**45= 4\*44 = 4\*(16)2 mod 15 = 4\*(1)2 mod 15** = **4\*1 mod 15 = 4**

|  |  |  |  |
| --- | --- | --- | --- |
| а1(основание степени) | Z(степень) | х(результат) | Шаги выполнения |
| 4 | 5 | 1 | 0 |
| 4 | 4 | 1\*4=4 | 1 |
| 4\*4 mod 15 = 1 | 2 | 4 | 2 |
| 1\*1 mod 15 = 1 | 1 | 4 | 3 |
| 4\*1 mod 15 = 4 | 0 | 4\*1=4 | 4 |

1. **Пример поиска случайного первообразного корня**

Задано простое p = 13

Ищем простые делители p-1 = 12 = 6 \* 2 => 3 и 2

|  |  |  |  |
| --- | --- | --- | --- |
| **Корни** | **g12/3 mod 13** | **g12/2 mod 13** | **Подходит?** |
| 2 | 3 | 12 | Да |
| 3 | 3 | 1 | Нет |
| 4 | 9 | 1 | Нет |
| 5 | 1 | 12 | Нет |
| 6 | 9 | 12 | Да |
| 7 | 9 | 12 | Да |
| 8 | 1 | 12 | Нет |
| 9 | 9 | 1 | Нет |
| 10 | 3 | 1 | Нет |
| 11 | 3 | 12 | Да |
| 12 | 1 | 1 | Нет |

Ответ: 2, 6, 7, 11

1. **Пример работы расширенного алгоритма**

**x0\*a + y0\*b = нод(a,b), a = 991, b = 313, (a,b) = 1**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **итерация** | **q** | **a** | **b** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 991 | 313 | 1 | 0 | 0 | 1 |
| 1 | 3 | 313 | 52 | 0 | 1 | 1 | -3 |
| 2 | 6 | 52 | 1 | 1 | -6 | -3 | 19 |
| 3 | 52 | 1 | 0 | -6 | 313 | 19 | -987 |

**x0 = -6 y0 = 25**

**-6 \* 991 + 19 \* 313 = -5946 + 5947 = 1**