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

Пусть a1 = 4, Z = 15, n = 13.

415 mod 13 = 12

|  |  |  |  |
| --- | --- | --- | --- |
| Шаги выполнения | а1(основание степени) | Z(степень) | х(результат) |
| 0 | 4 | 15 | 1 |
| 1 | 4 | 15 – 1 = 14 | (1 \* 4) mod 13 = 4 |
| 2 | (4 \* 4) mod 13 = 3 | 14 / 2 = 7 | 4 |
| 3 | 3 | 7 – 1 = 6 | (4 \* 3) mod 13 = 12 |
| 4 | (3 \* 3) mod 13 = 9 | 6 / 2 = 3 | 12 |
| 5 | 9 | 3 – 1 = 2 | (12 \* 9) mod 13 = 4 |
| 6 | (9 \* 9) mod 13 = 3 | 2 / 2 = 1 | 4 |
| 7 | 3 | 1 – 1 = 0 | (4 \* 3) mod 13 = 12 |

1. **Пример поиска случайного первообразного корня**

Пусть p = 13

Простые делители p – 1 = 12 = 2 \* 2 \* 3

|  |  |  |  |
| --- | --- | --- | --- |
| g | g12/2 mod 13 | g12/3 mod 13 | Первообразный |
| 2 | 12 | 3 | да |
| 3 | 1 | 3 | нет |
| 4 | 1 | 9 | нет |
| 5 | 12 | 1 | нет |
| 6 | 12 | 9 | да |
| 7 | 12 | 9 | да |
| 8 | 12 | 1 | нет |
| 9 | 1 | 9 | нет |
| 10 | 1 | 3 | нет |
| 11 | 12 | 3 | да |
| 12 | 1 | 1 | нет |

1. **Пример работы расширенного алгоритма Евклида**

x1\* a + y1\* b = НОД(a, b), a = 413, b = 612, (a, b) = 1

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **итерация** | **q** | **a0** | **a1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 413 | 612 | 1 | 0 | 0 | 1 |
| 1 | 0 | 612 | 413 | 0 | 1 | 1 | 0 |
| 2 | 1 | 413 | 199 | 1 | -1 | 0 | 1 |
| 3 | 2 | 199 | 15 | -1 | 3 | 1 | -2 |
| 4 | 13 | 15 | 4 | 3 | -40 | -2 | 27 |
| 5 | 3 | 4 | 3 | -40 | 123 | 27 | -83 |
| 6 | 1 | 3 | 1 | 123 | -163 | -83 | 110 |
| 7 | 3 | 1 | 0 | -163 | 612 | 110 | -413 |

x1 = -163 y1 = 110

-163 \* 413 + 110 \* 612 = 1