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

Пусть a1 = 6, Z = 13, n = 11.

613 mod 11 = 7

|  |  |  |  |
| --- | --- | --- | --- |
| Шаги выполнения | а1(основание степени) | Z(степень) | х(результат) |
| 0 | 6 | 13 | 1 |
| 1 | 6 | 13 – 1 = 12 | (1 \* 6) mod 11 = 6 |
| 2 | (6 \* 6) mod 11 = 3 | 12 / 2 = 6 | 6 |
| 4 | (3 \* 3) mod 11 = 9 | 6 / 2 = 3 | 6 |
| 5 | 9 | 3 – 1 = 2 | (6 \* 9) mod 11 = 10 |
| 6 | (9 \* 9) mod 11 = 3 | 2 / 2 = 1 | 10 |
| 7 | 3 | 1 – 1 = 0 | (10 \* 3) mod 11 = 7 |

1. **Пример поиска случайного первообразного корня**

Пусть p = 19

Простые делители p – 1 = 18 = 2 \* 3 \* 3

|  |  |  |  |
| --- | --- | --- | --- |
| g | g18/2 mod 19 | g18/3 mod 19 | Первообразный |
| 2 | 18 | 7 | да |
| 3 | 18 | 7 | да |
| 4 | 1 | 11 | нет |
| 5 | 1 | 7 | нет |
| 6 | 1 | 11 | нет |
| 7 | 1 | 1 | нет |
| 8 | 18 | 1 | нет |
| 9 | 1 | 11 | нет |
| 10 | 18 | 11 | да |
| 11 | 1 | 1 | нет |
| 12 | 18 | 1 | нет |
| 13 | 18 | 11 | да |
| 14 | 18 | 7 | нет |
| 15 | 18 | 11 | да |
| 16 | 1 | 7 | нет |
| 17 | 1 | 7 | нет |
| 18 | 18 | 1 | нет |

1. **Пример работы расширенного алгоритма Евклида**

x1\* a + y1\* b = НОД(a, b), a = 342, b = 607, (a, b) = 1

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **итерация** | **q** | **a0** | **a1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 342 | 607 | 1 | 0 | 0 | 1 |
| 1 | 0 | 607 | 342 | 0 | 1 | 1 | 0 |
| 2 | 1 | 342 | 265 | 1 | -1 | 0 | 1 |
| 3 | 1 | 265 | 77 | -1 | 2 | 1 | -1 |
| 4 | 3 | 77 | 34 | 2 | -7 | -1 | 4 |
| 5 | 2 | 34 | 9 | -7 | 16 | 4 | -9 |
| 6 | 3 | 9 | 7 | 16 | -55 | -9 | 31 |
| 7 | 1 | 7 | 2 | -55 | 71 | 31 | -40 |
| 8 | 3 | 2 | 1 | 71 | -268 | -40 | 151 |
| 9 | 2 | 1 | 0 | -268 | -465 | 151 | 342 |

x1 = 268 y1 = 151

151 \* 607 + (-268) \* 342 = 1