**Пример работы алгоритма быстрого возведения в степень**

|  |  |  |  |
| --- | --- | --- | --- |
| а1(основание степени) | z1(степень) | х(результат) | Шаги выполнения |
| 4 | 12 | 1 | 0 |
| 4\*4 mod 7 = 2 | 6 | 1 | 1 |
| 2\*2 mod 7 = 4 | 3 | 1 | 2 |
| 4 | 2 | 1\*4 mod 7 = 4 | 3 |
| 4\*4 mod 7 = 2 | 1 | 4 | 4 |
| 2 | 0 | 4\*2 mod 7 = 1 | 5 |

**Пример поиска первообразных корней**

p = 13

p-1 = 12 = 2 \* 6 = 2 \* 2 \* 3; Простые делители = [2, 3]

q = [2, 6, 7, 11], где q – первообразный корень

**Пример работы расширенного алгоритма Евклида**

Коэффициенты Безу:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **итерация** | **q** | **a0** | **a1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 43 | 61 | 1 | 0 | 0 | 1 |
| 1 | 0 | 61 | 43 | 0 | 1 | 1 | 0 |
| 2 | 1 | 43 | 18 | 1 | -1 | 0 | 1 |
| 3 | 2 | 18 | 7 | -1 | 3 | 1 | -2 |
| 4 | 2 | 7 | 4 | 3 | -7 | -2 | 5 |
| 5 | 1 | 4 | 3 | -7 | 10 | 5 | -7 |
| 6 | 1 | 3 | ***1*** | 10 | ***-17*** | -7 | ***12*** |
| 7 | 3 | 1 | 0 | -17 | 61 | 12 | -43 |