**3 РАСЧЁТЫ**

**Быстрое возведение в степень**

Степень 0:

Степень 1:

Степень 2:

Степень 3:

Степень 4:

**Первообразный корень по модулю**

Первообразный корень g по модулю m – это такое целое число, что

Нахождение первообразного корня по модулю 7.

**Расширенный алгоритм Евклида**

Расширенный алгоритм Евклида позволяет найти наибольший общий делитель и коэффициенты из леммы Безу. Лемма Безу гласит о том, что для любых целых чисел a и b есть такие целые числа x и y, для которых верно равенство 𝒂 ∗ 𝒙 + 𝒃 ∗ 𝒚 = (𝒂, 𝒃).

Пусть a = 21, b = 8. НОД(a, b) = 1

xn = xn – 2 – q \* xn - 1

yn = yn – 2 – q \* yn - 1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **q** | **a** | **b** | **r** | **xn** | **yn** |
| - | 21 | 8 | - | 1 | 0 |
| - | 21 | 8 | - | 0 | 1 |
| 2 | 21 | 8 | 5 | 1 | -2 |
| 1 | 8 | 5 | 3 | -1 | 3 |
| 1 | 5 | 3 | 2 | 2 | -5 |
| 1 | 3 | 2 | **1** | **-3** | **8** |
| 2 | 2 | 1 | **0** | **-** | **-** |

-3 \* 21 + 8 \* 8 = -63 + 64 = 1