1. **Пример работы алгоритма быстрого возведения в степень** (без модульной арифметики, студент должен привести пример с модульной арифметикой)

**25= 2\*24 = 2\*(4)2 = 2\*(16)1** = 32

|  |  |  |  |
| --- | --- | --- | --- |
| а1(основание степени) | Z(степень) | х(результат) | Шаги выполнения |
| 2 | 5 | 1 | 0 |
| 2 | 4 | 1\*2=2 | 1 |
| 2\*2=4 | 2 | 2 | 2 |
| 4\*4=16 | 1 | 2 | 3 |
| 16 | 0 | 16\*2 | 4 |

1. **Пример поиска случайного первообразного корня** (студент должен привести пример поиска всех первообразных корней по заданному модулю)

Задано простое p = 7

Ищем простые делители p-1 = 6 = 2\*3

Проверяем является ли случайное число 3 первообразным корнем по модулю 7:

36/2 mod 7 = 6; 36/3 mod 7 = 2. Число 3 является первообразным по модулю 7.

1. **Пример работы расширенного алгоритма Евклида** (числа не взаимно простые, студент должен привести пример с взаимно простыми числами)

**x1\*a + y1\*b = нод(a,b), a = 612, b = 342, (a,b) = 18**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **итерация** | **q** | **a0** | **a1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 342 | 612 | 1 | 0 | 0 | 1 |
| 1 | 0 | 612 | 342 | 0 | 1 | 1 | 0 |
| 2 | 1 | 342 | 270 | 1 | -1 | 0 | 1 |
| 3 | 1 | 270 | 72 | -1 | 2 | 1 | -1 |
| 4 | 3 | 72 | 54 | 2 | -7 | -1 | 4 |
| 5 | 1 | 54 | 18 | -7 | 9 | 4 | -5 |
| 6 | 3 | 18 | 0 | 9 | -34 | -5 | 19 |

**x1 = 9 y1 = -5**

**9 \* 342 + (-5) \* 612 = 18**