**Лабораторная работа 3 | Вариант 3 | Столбов Кирилл 251001**

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

**1111 mod 13 = (11 \* ((11 \* (112 mod 13)2) mod 13)2 mod 13) mod 13 = 6**

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

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

Задано простое p = 113

Ищем простые делители p-1 = 112 = 24 \* 7

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**

**x1\*a + y1\*b = 1, a = 385, b = 612,**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **итерация** | **q** | **a0** | **a1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 385 | 612 | 1 | 0 | 0 | 1 |
| 1 | 1 | 227 | 385 | 0 | 1 | 1 | -1 |
| 2 | 1 | 158 | 227 | 1 | -1 | -1 | 2 |
| 3 | 1 | 69 | 158 | -1 | 2 | 2 | -3 |
| 4 | 2 | 20 | 69 | 2 | -5 | -3 | 8 |
| 5 | 3 | 9 | 20 | -5 | 17 | 8 | -27 |
| 6 | 2 | 2 | 9 | 17 | -39 | -27 | 62 |
| 7 | 4 | 1 | 2 | -39 | 173 | 62 | -275 |

**x1 = 9 y1 = -5**

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