УО «Белорусский государственный университет информатики и радиоэлектроники»

Кафедра ПОИТ

Отчет по лабораторной работе № 3

по предмету «Теория информации»

Вариант 2

Выполнил:

Калинкович А.Д

Гр. 351003

Проверил:

Болтак С. В.

Минск 20 25

1. **Пример работы алгоритма быстрого возведения в степень с модульной арифметикой**:

**753 mod 23 = (732 mod 23 \* 716 mod 23 \* 74 mod 23 \* 7 mod 23) mod 23**

|  |  |  |  |
| --- | --- | --- | --- |
| а1(основание степени) | Z(степень) | х(результат) | Шаги выполнения |
| 7 | 1 | 7 mod 23 = 7 | 0 |
| 7 mod 23 | 2 | (7 \* 7) mod 23 = 26;  72 mod 23 = 26 | 1 |
| 72 mod 23 | 2 | (26 \* 26) mod 23 = 9;  74 mod 23 = 9; | 2 |
| 74 mod 23 | 2 | (9 \* 9) mod 23 = 12;  78 mod 23 = 12; | 3 |
| 78 mod 23 | 2 | (12 \* 12) mod 23 = 6;  716 mod 23 = 6; | 4 |
| 716 mod 23 | 2 | (6 \* 6) mod 23 = 13;  732 mod 23 = 13; | 5 |

7 mod 23 = 7;

74 mod 23 = 9;

716 mod 23 = 6;

732 mod 23 = 13;

(13 \* 6 \* 9 \* 7) mod 23 = 753 mod 23**;**

((13 \* 6) mod 23 \* (9 \* 7) mod 23) mod 23 = (78 mod 23 \* 63 mod 23) mod 23 = (9 \* 17) mod 23 = 15;

1. **Пример поиска всех первообразных корней по заданному модулю**

1) Задано простое p = 41

2) Ищем простые делители p - 1 = phi = 40 => 2, 5

3) Итерируем от 1 до p – 1 = 40, проверяя все значения в соответствии с условием

for g = 1 to p – 1 do:

3.1) Итерируем по простым делителями и проверяем условие,

foreach factor in (2,5):

g (phi / factor) mod p != 1

Если результат возведения в степень будет равен 1 по модулю p – значит порядок числа **g** меньше **p – 1** и он не является первообразным корнем.

Возможные степени:

Exp1 = 40 / 2 = 20 ;

Exp2 = 40 / 5 = 8;

Вычисления:  
**g = 1:**

* 120  mod  41=1
* 18 mod  41=1
* Не является первообразным корнем.

**g = 2:**

* 220 mod  41=40
* 28 mod  41=10
* Первообразный корень.

**g = 3:**

* 320 mod  41=1
* 38 mod  41=37
* Не является первообразным корнем.

**g = 4:**

* 420 mod  41=1
* 48 mod  41=18
* Не является первообразным корнем.

**g = 5:**

* 520 mod  41=40520 mod41=40
* 58 mod  41=958mod41=9
* Первообразный корень.

**g = 6:**

* 620 mod  41=40620 mod41=40
* 68 mod  41=1068mod41=10
* Первообразный корень.

**g = 7:**

* 720 mod  41=40720 mod41=40
* 78 mod  41=3878mod41=38
* Первообразный корень.

**g = 8:**

* 820 mod  41=1820 mod41=1
* 88 mod  41=1088mod41=10
* Не является первообразным корнем.

**g = 9:**

* 920 mod  41=1920 mod41=1
* 98 mod  41=198mod41=1
* Не является первообразным корнем.

**g = 10:**

* 1020 mod  41=11020 mod41=1
* 108 mod  41=1108mod41=1
* Не является первообразным корнем.

**g = 11:**

* 1120 mod  41=401120 mod41=40
* 118 mod  41=18118mod41=18
* Первообразный корень.

**g = 12:**

* 1220 mod  41=40
* 128 mod  41=37
* Первообразный корень.

**g = 13:**

* 1320 mod  41=40
* 138 mod  41=38
* Первообразный корень.

**g = 14:**

* 1420 mod  41=1
* 148 mod  41=18
* Не является первообразным корнем.

**g = 15:**

* 1520 mod  41=40
* 158 mod  41=37
* Первообразный корень.

**g = 16:**

* 1620 mod  41=1
* 168 mod  41=10
* Не является первообразным корнем.

**g = 17:**

* 1720 mod  41=40
* 178 mod  41=38
* Первообразный корень.

**g = 18:**

* 1820  mod  41=1
* 188 mod  41=37
* Не является первообразным корнем.

**g = 19:**

* 1920  mod  41=40
* 198 mod  41=18
* Первообразный корень.

**g = 20 :**

* 2020 mod  41=1
* 208 mod  41=37
* Не является первообразным корнем.

**g = 21:**

* 2120  mod  41=12120 mod41=1
* 218 mod  41=38218mod41=38
* Не является первообразным корнем.

**g = 22:**

* 2220  mod  41=402220 mod41=40
* 228 mod  41=10228mod41=10
* Первообразный корень.

**g = 23:**

* 2320  mod  41=12320 mod41=1
* 238 mod  41=18238mod41=18
* Не является первообразным корнем.

**g = 24:**

* 2420  mod  41=402420 mod41=40
* 248 mod  41=37248mod41=37
* Первообразный корень.

**g = 25:**

* 2520 mod  41=12520 mod41=1
* 258 mod  41=38258mod41=38
* Не является первообразным корнем.

**g = 26:**

* 2620  mod  41=40
* 268 mod  41=10
* Первообразный корень.

**g = 27:**

* 2720  mod  41=1
* 278 mod  41=37
* Не является первообразным корнем.

**g = 28:**

* 2820  mod  41=40
* 288 mod  41=18
* Первообразный корень.

**g = 29:**

* 2920  mod  41=40
* 298 mod  41=38
* Первообразный корень.

**g = 30:**

* 3020  mod  41=40
* 308 mod  41=37
* Первообразный корень.

**g = 31:**

* 3120  mod  41=1
* 318 mod  41=10
* Не является первообразным корнем.

**g = 32:**

* 3220  mod  41=1
* 328 mod  41=18
* Не является первообразным корнем.

**g = 33:**

* 3320  mod  41=1
* 338 mod  41=37
* Не является первообразным корнем.

**g = 34:**

* 3420  mod  41=40
* 348 mod  41=10
* Первообразный корень.

**g = 35:**

* 3520  mod  41=40
* 358 mod  41=18
* Первообразный корень.

**g = 36:**

* 3620  mod  41=1
* 368 mod  41=38
* Не является первообразным корнем.

**g = 37:**

* 3720  mod  41=1
* 378 mod  41=37
* Не является первообразным корнем.

**g = 38:**

* 3820  mod  41=1
* 388 mod  41=18
* Не является первообразным корнем.

**g = 39:**

* 3920  mod  41=1
* 398 mod  41=10
* Не является первообразным корнем.

**g = 40:**

* 4020  mod  41=1
* 408 mod  41=1
* Не является первообразным корнем.

**Итоговый список первообразных корней по модулю 41:**

6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35

Количество первообразных корней: 16 (что соответствует ϕ(40) = 16).

1. **Пример работы расширенного алгоритма Евклида с взаимно простыми числами**

**x1\*a + y1\*b = нод(a,b), a = 43, b = 13**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **итерация** | **q** | **a0** | **a1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 43 | 13 | 1 | 0 | 0 | 1 |
| 1 | 3 | 13 | 4 | 0 | 1 | 1 | -3 |
| 2 | 3 | 4 | 1 | 1 | -3 | -3 | 10 |
| 3 | 4 | 1 | 0 | -3 | 13 | 10 | -43 |

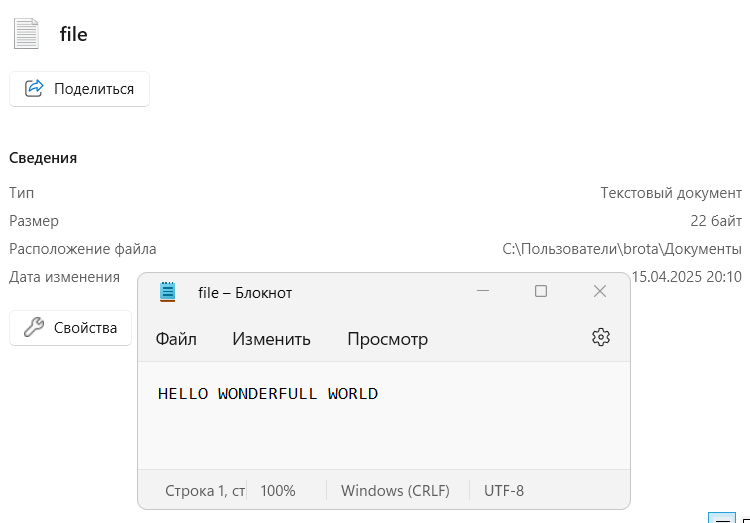
**x1 = -3**

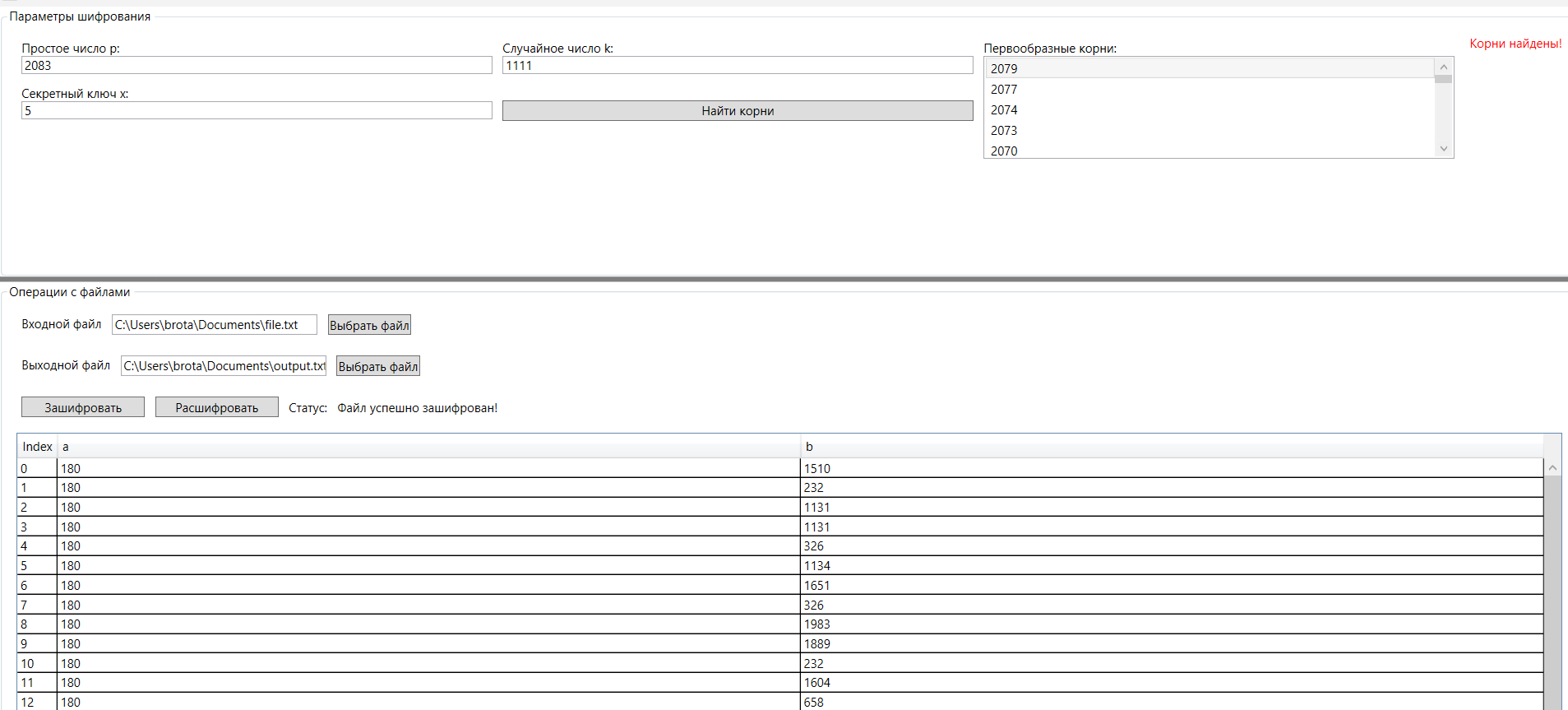
**y1 = 10**

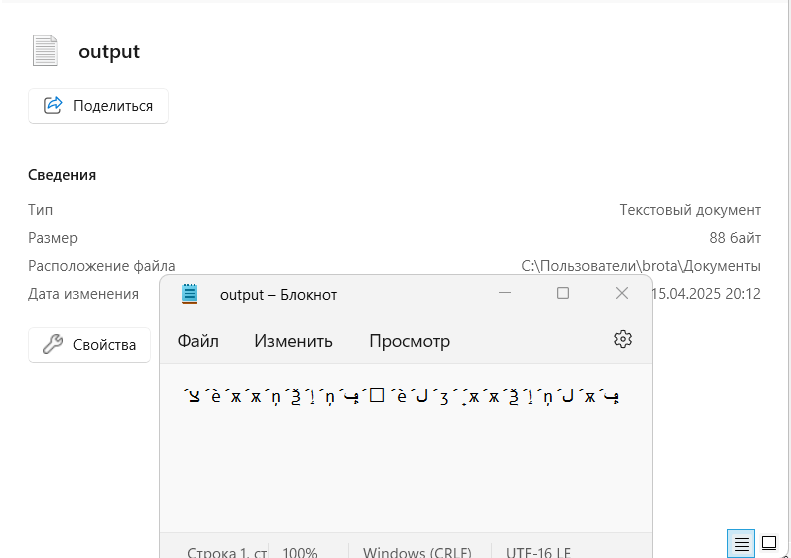
**-3 \* 43 + 13 \* 10 = 1**

Пример работы программы:

1. Текстовый документ:







Пример расшифровки:

