

**МИНОБРНАУКИ РОССИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«МИРЭА – Российский технологический университет»**

|  |
| --- |
| **РТУ МИРЭА** |
|  |
| **Институт кибербезопасности и цифровых технологий (ИКБ)** |
|  |
| КБ-2 «Информационно-аналитические системы кибербезопасности» |

**ОТЧЕТ О ВЫПОЛНЕНИИ ИНДИВИДУАЛЬНОГО ЗАДАНИЯ №1**

**В РАМКАХ ДИСЦИПЛИНЫ «МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ»**

Выполнил:

Студент 4-ого курса

Учебной группы БИСО-02-22

Зубарев В.С.

1. Проверить на простоту два произвольных целых числа разрядностью не менее 5.

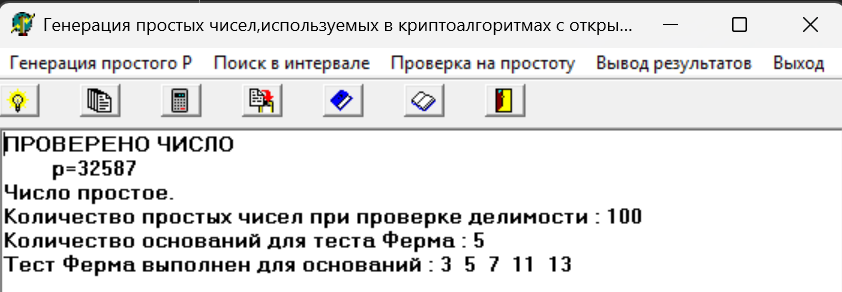


Рисунок 1 – Проверка случайно-выбранного первого числа

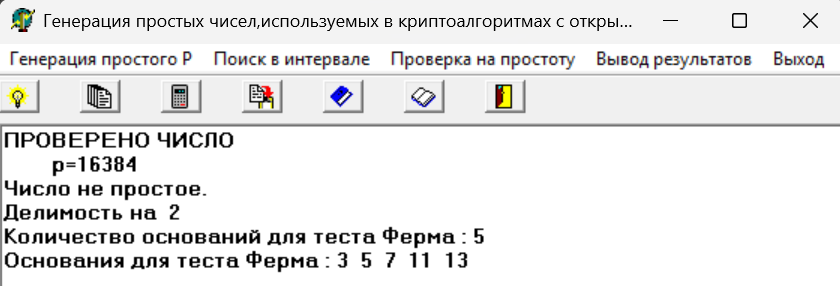


Рисунок 2 - Проверка случайно-выбранного второго числа

1. Распределение простых чисел.
   1. Задан интервал вида [х, x + L], при заданных х = 2000, L = 500, количество простых чисел для деления 5—15, количество оснований 1—2.



Рисунок 3 - Поиск в интервале (кол-во простых - 15, основания - 1)

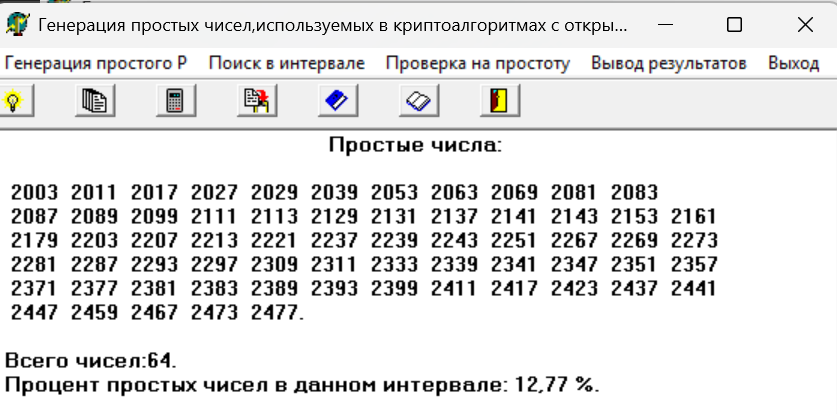


Рисунок 4 - Поиск в интервале (кол-во простых - 15, основания - 2)

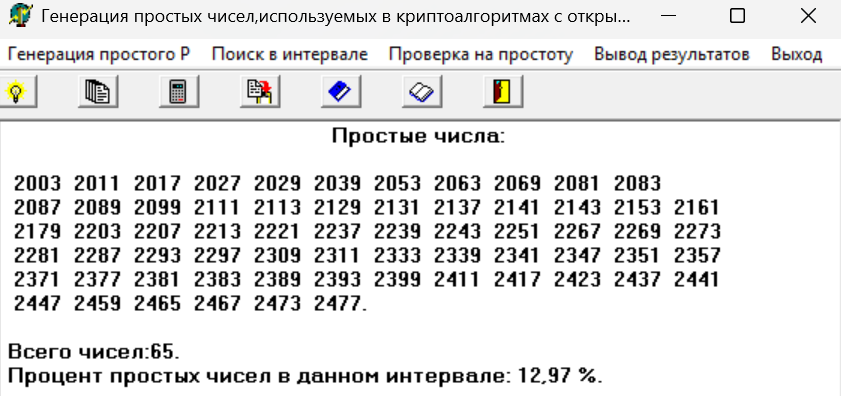


Рисунок 5 - Поиск в интервале (кол-во простых - 0, основания - 1)

* + 1. Вычислить количество простых чисел в интервале
    2. Сравнить с величиной .
    3. При каких условиях к .
       - Достаточно большое x ()
       - Достаточно большое L относительно x.
  1. Найти в интервале (1000, 1000 + 300) все простые числа. Задано: количество простых чисел для деления 5—20, количество оснований 1—3.

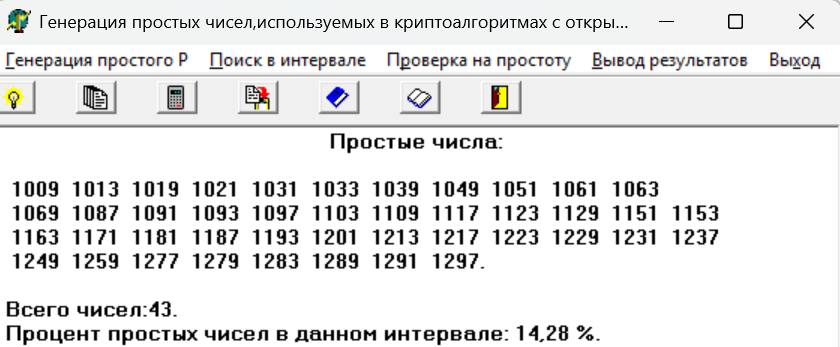


Рисунок 6 - Все простые числа в интервале от [1000,1300] (простые числа – 20, основания – 1)

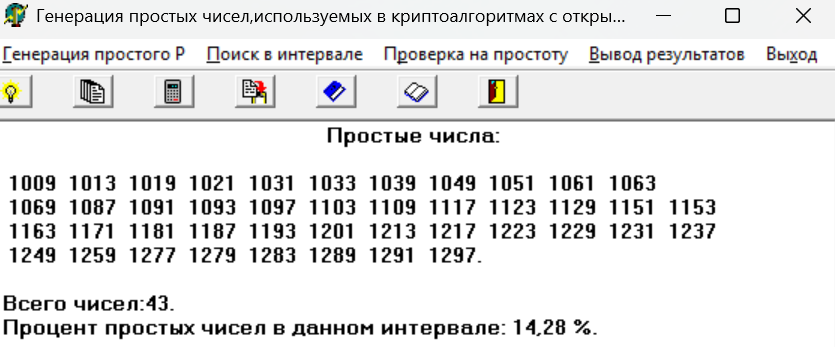


Рисунок 7 - Все простые числа в интервале от [1000,1300] (простые числа – 20, основания – 3)

* + 1. Пусть L(i) — разность между двумя соседними простыми числами. Построить гистограмму для L(i).

Рисунок 8 - Гистограмма распределения L(i)

* + 1. Вычислить выборочное среднее .
    2. Сравнить с величиной , где х — середина интервала.
  1. Для заданного набора чисел {k} оценить относительную погрешность формулы для k-го простого числа: p(k) = k/ ln(k), k = {10, 15, 20, 30, 35}.

|  |  |  |  |
| --- | --- | --- | --- |
| Значение формулы | Ср.Знач | Абс.Погр | Относ.Погр |
| 4,342944819 | 1005 | 1000,657055 | 0,995678662 |
| 5,539040596 | 1007,5 | 1001,960959 | 0,994502193 |
| 6,676164014 | 1010 | 1003,323836 | 0,993389937 |
| 8,820423114 | 1015 | 1006,179577 | 0,991309928 |
| 9,844324492 | 1017,5 | 1007,655676 | 0,990324988 |

Таблица 1 - вычисление относительной погрешности

1. Методы генерации простых чисел.
   1. В интервале (500, 500 + 200) построить график относительного количества натуральных чисел, проходящих «решето Эратосфена», т.е. не делящихся на первые k простых. Расчет производится для всех k <= 10.

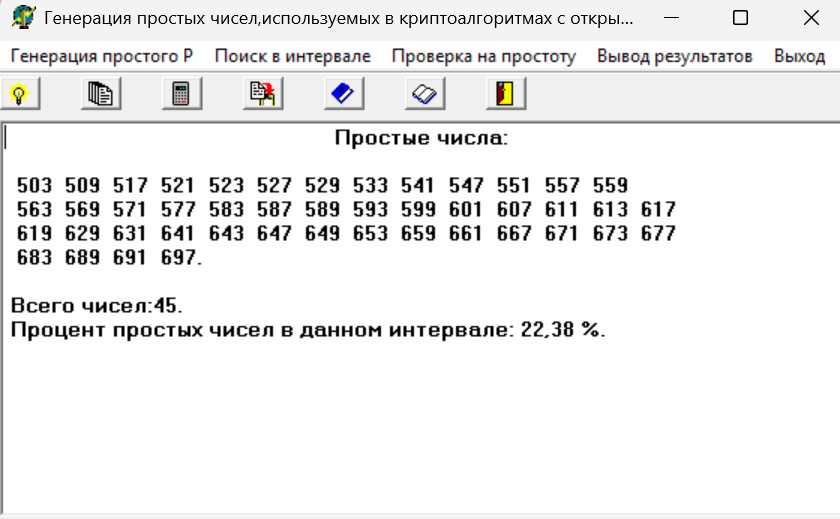


Рисунок 9 - Все простые числа проходящие через "Решето Эратосфена" на интервале

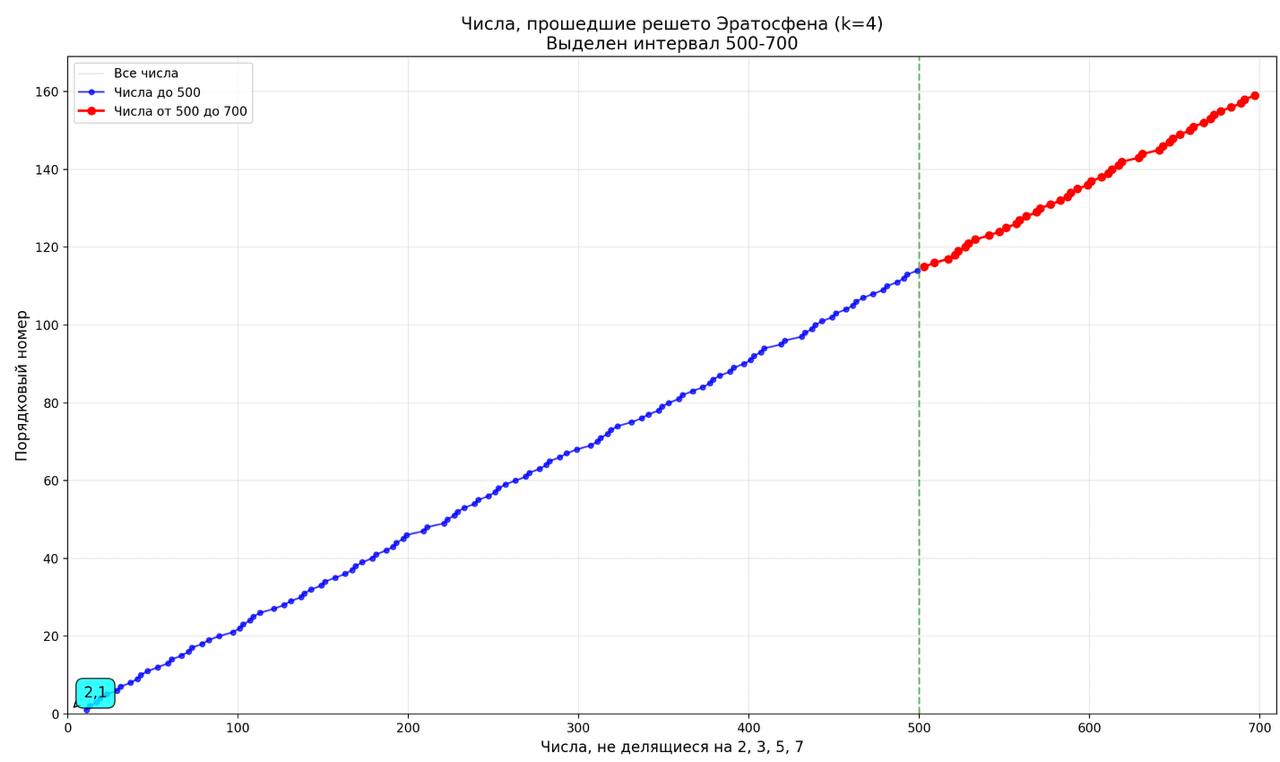


Рисунок 10 – График распределения простых чисел на интервале

* 1. Для интервала (1500, 1500 + 300):
     1. Рассчитать точное количество Р0 простых чисел в интервале, т.е. при проверке задать только тест на делимость. Количество первых простых чисел для деления определяется из расчета максимальное число для деления равно квадратному корню из максимального значения интервала;

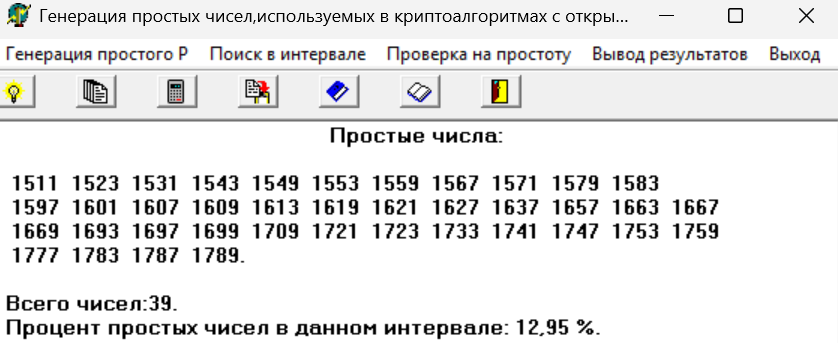


Рисунок 11 - Все простые в интервале при пробном делении на первые 13 простых

* + 1. Составить тест с небольшим количеством пробных делений и одним основанием в тесте Ферма. Вычислить количество Р1 вероятно простых чисел, удовлетворяющих этому тесту;

Малая теорема Ферма

Пусть , где p – простое число, a – натуральное целое число не кратное p, тогда n – проверяемое число, для которого необходимо найти такое a, при котором . Если такое a найдено, то n – достоверно составное число. В случае если n – следует считать вероятно простым.

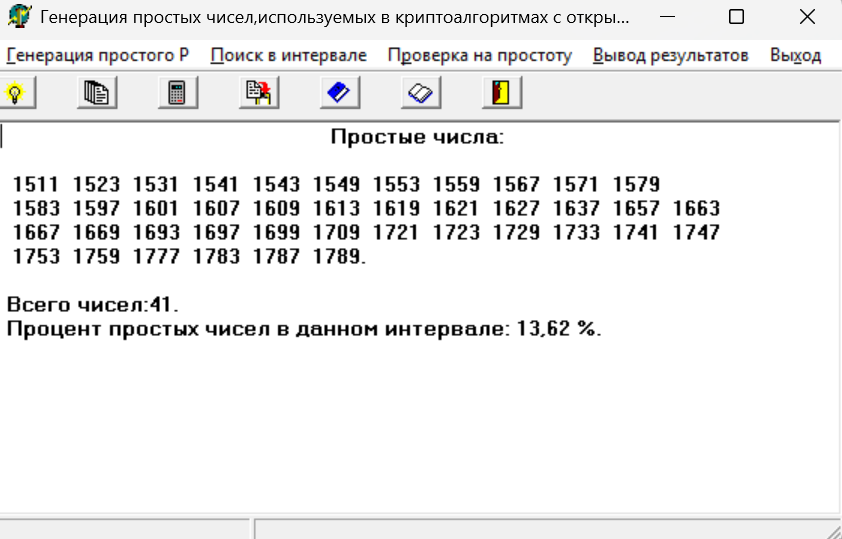


Рисунок 12 - Тест Ферма(1)

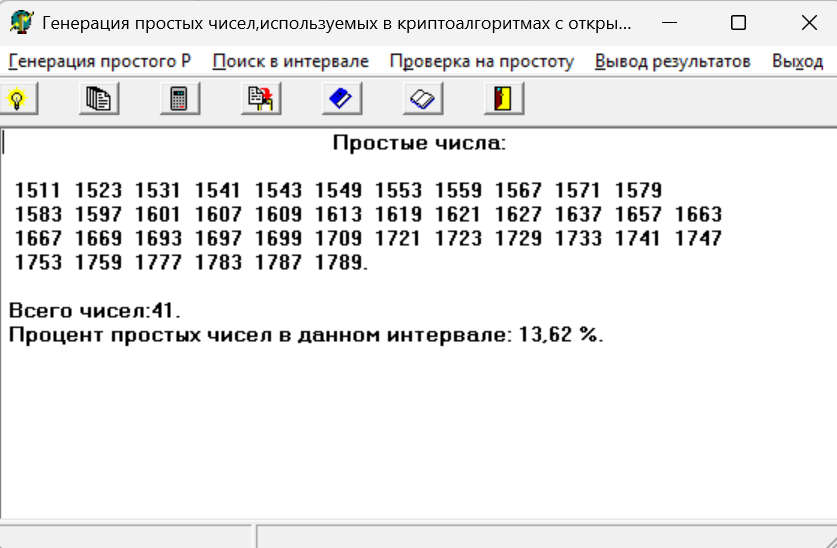


Рисунок 13 - Тест пробных делений (3)

Количество

* + 1. Составить тест с большим, чем в предыдущем случае, количеством пробных делений и двумя или тремя основаниями в тесте Ферма. Вычислить количество Р2 вероятно простых чисел, удовлетворяющих этому тесту. Проанализировать полученные данные.

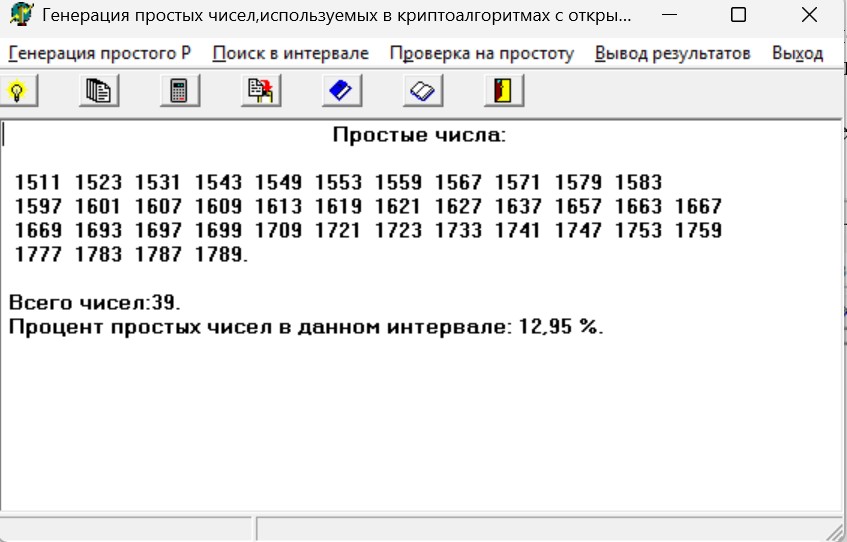


Рисунок 14 - Тест Ферма(3)

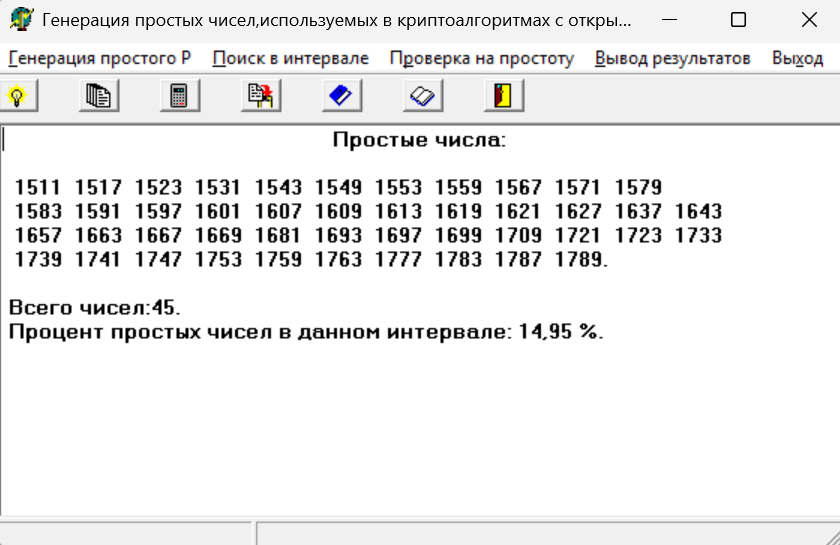


Рисунок 15 - Пробные деления (10)

Количество

* 1. Известно, что в заданном интервале имеются числа Кармайкла. Найти их. Варианты интервалов:

Числа Кармайка –такое число n, для которого при любом a взаимно простым с n .

Теория поиска чисел Кармайкла.

* + - * 1. Определяем границы интервала
        2. Выделяем все нечетные числа n
        3. Для каждого числа строим разложение на простые множители вида
        4. Если в разложении встречаются , где k >1 – число не является числом Кармайкла
        5. Для каждого проверяем
        6. Если все условия выполнены – число Кармайкла

В контексте работы поиск чисел Кармайкла – это нахождение различий между тестами пробных делений и тестами Ферма с одним основанием, проходящим по множеству простых чисел до ближайшего простого числа, не превышающего , где N – верхняя граница интервала.

* + 1. (1050, 1050 + 100);

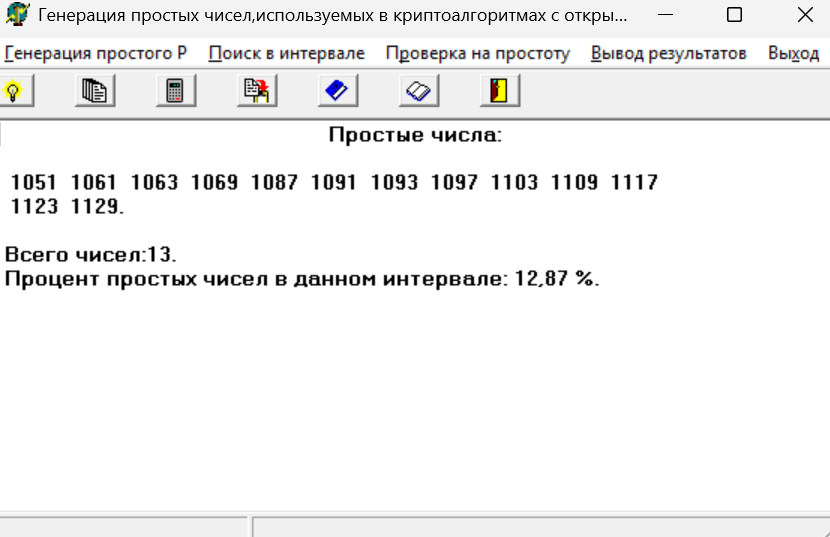


Рисунок 16 - Тест пробных делений (100)

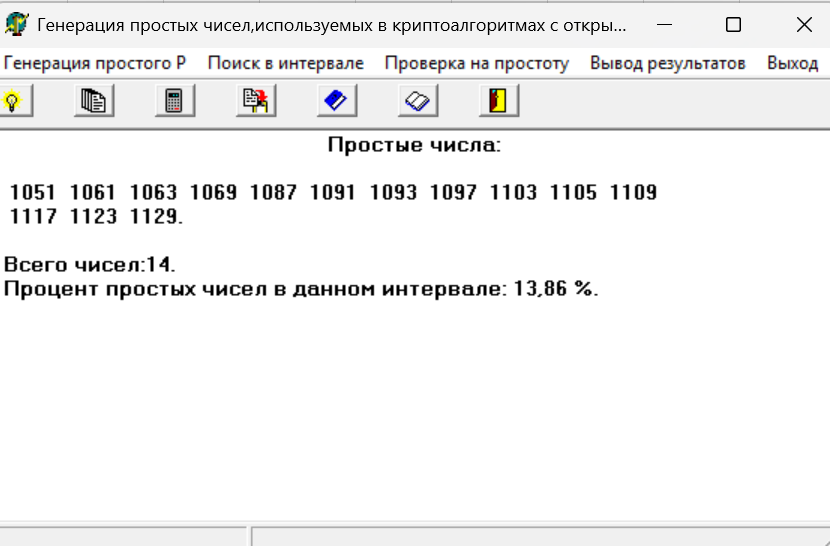


Рисунок 17 - тест Ферма (основание = 3)

В данном интервале число Кармайкла – 1105

Проверка

* + 1. (1700, 1700 + 100);

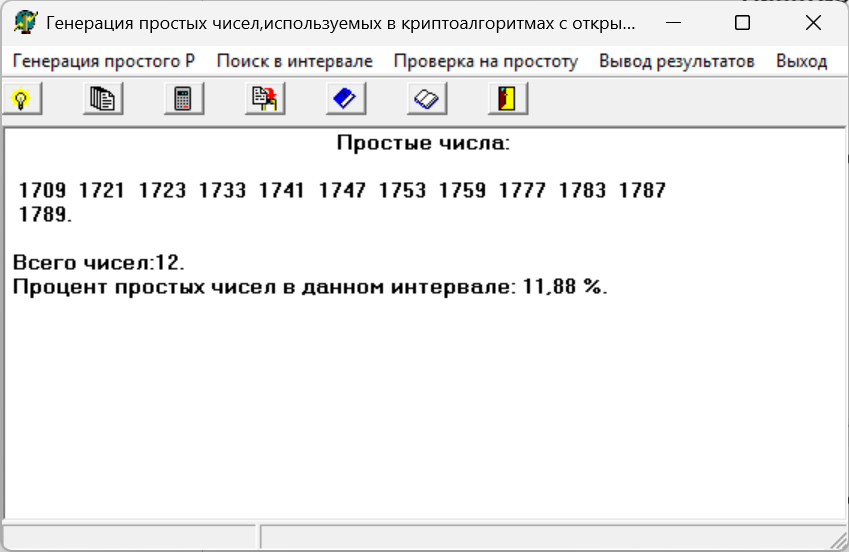


Рисунок 18 - Тест пробных делений (100)

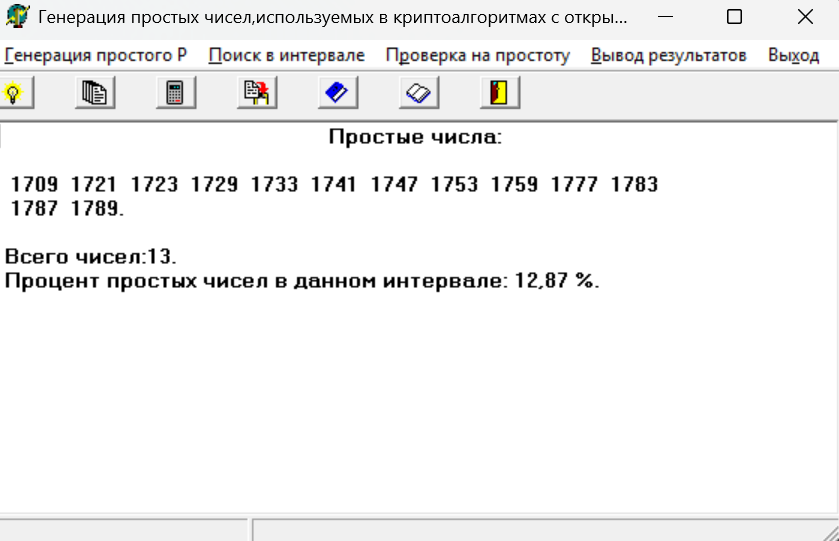


Рисунок 19 - тест Ферма (основание = 5)

В данном интервале число Кармайкла – 1729

Проверка

* + 1. (2400, 2400 + 100)

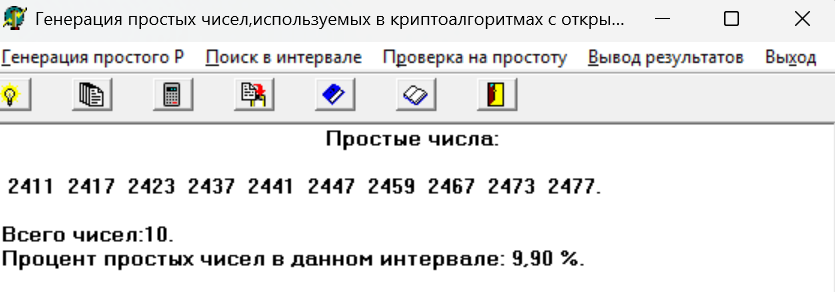


Рисунок 20 - Тест пробных делений (100)

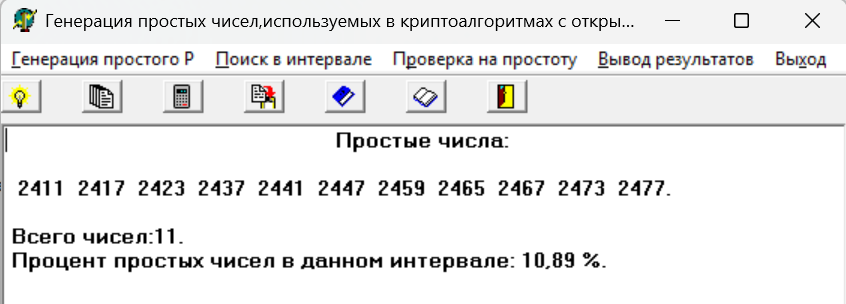


Рисунок 21 - Тест Ферма (основание = 3)

В данном интервале число Кармайкла – 2465

Проверка

Вывод: тест Ферма может выдавать псевдо-простые числа, которые необходимо исключать формулой Кармайкла.