МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

ІКТА

кафедра ЗІ



**З В І Т**

до лабораторної роботи №4

з курсу: «Основи криптографічного захисту інформації»

на тему: «Генерація простих чисел, що використовуються в

асиметричних системах шифрування»

Виконав: ст. гр. УІ-42

Симоненко Д.С.

Прийняв: Шандра З.А.

Львів – 2017

**Мета роботи:** вивчення методів генерації простих чисел, що використовуються в системах шифрування з відкритим ключем, та перевірка чисел на простоту.

Тестуванням деякого числа *n* на простоту це перевірка чи є дане число *n* простим, чи ні. Для цього достатньо перевірити всі можливі прості дільники цього числа за винятком самого числа *n*. Така можливість пов’язана з тим відомим фактом теорії чисел, що будь-яке натуральне число *n* можна єдиним способом представити у вигляді добутку степенів простих чисел, тобто *n* = П *pn*p, де *np* – кількість простих чисел, рівних *p*, присутніх у поданні числа *n* .

Якщо остача від ділення числа *n* на деякий можливий простий його дільник дорівнює нулю, то таке число *m* не є простим.

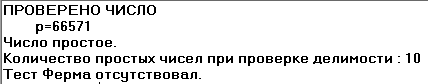
Всі можливі прості дільники числа *n*, які слід перевірити, знаходяться в межах від 2 до *n*div 2. Для великого числа *n* така перевірка може тривати занадто довго. Тому важливе значення мають різні методи скорочення терміну перевірки.

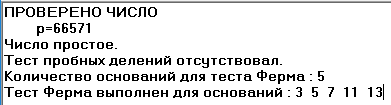
Один із методів пов’язаний з тим, що дільники числа завжди зустрічаються парами. Наприклад, число 144 має своїм дільником число 3, тобто 144 mod 3 = 0. Але дільник 3 обов’язково супроводжується також дільником 48, оскільки 48 \* 3 = 144. Таким чином, зрозуміло, що перевіривши дільник 3, немає потреби перевіряти супутній дільник 48.

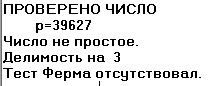
Остаточний висновок за таких умов полягає в тому, що при тестуванні числа *n* на простоту достатньо перевірити тих можливих простих дільників, які знаходяться в межах від 2 до *n*. При цьому відмітимо, що певне спрощення процесу перевірки з алгоритмічної точки зору буде досягнуто, якщо серед можливих дільників в указаних межах не вибирати тільки простих, а натомість перевіряти всі поспіль.

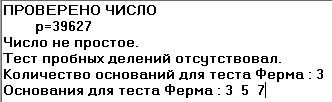
І, нарешті, ще більшого скорочення терміну перевірки можна досягти, якщо серед чисел можливих дільників в указаних межах не перевіряти парних дільників, за винятком двійки.

1. Перевірити на простоту два довільних цілих числа розрядністю не менше 5.







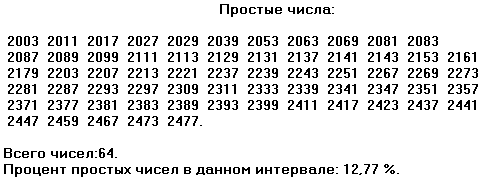


1. Розподілпростих чисел.

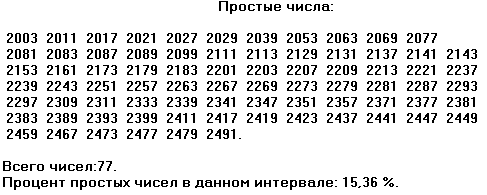
Заданий інтервал виду [x, x+L]. Обрахувати кількість П(x,L) простих чисел в інтервалі і порівняти з величиною L/ln(x). При якихумовахП(x,L)/ L є близьким до 1/ ln(x) при заданих x=2000, L=500, кількістьпростих чисел для ділення 5 – 15, кількість основ 1 – 2?

L/ln(x)=65,781662

* кількістьпростих чисел для ділення15

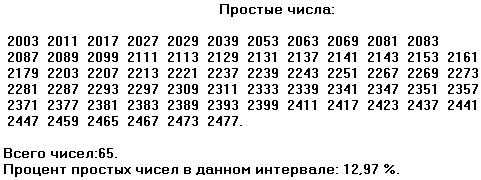


* кількістьпростих чисел для ділення 10

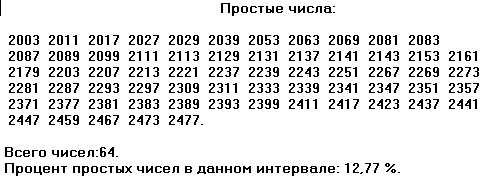


П(x,L)/ L є близьким до 1/ ln(x), коли є більша кількість простих чисел для ділення.

* кількість основ 1



* кількість основ 2



П(x,L)/ L є близьким до 1/ ln(x), коли є менша кількість основ.

* 1. Визначити в інтервалі (1000, 1000+300) усіпростічисла. Нехай *L*(*i*) –різниця між двома сусідніми простими числами. Побудувати гістограму для *L*(*i*). Обрахувати вибірков середнє *L*серед*.* Порівняти з величиною ln(*x*), де *x* – середина інтервалу. Задано: кількість простих чисел для ділення 5 – 20, кількість основ 1 – 3.
  2. Для заданого набору чисел {*k*}оцінити відносну похибку формули для *k* -го простого числа: *p*(*k*)=*k/lnk*, *k*={10,15,20,30,35}
  3. В інтервалі (500, 500+200) побудувати графік відносної кількості натуральних чисел, що проходять «решето Ератосфена», тобто таких, що не діляться на перші *k*простих.Розрахунок зробити для всіх *k ≤*10.
  4. Дляінтервалу (1500, 1500+300):

а) розрахувати точну кількість *Р*0 простих чисел в інтервалі, тобто при перевірці задати тільки тест на подільність. Кількість перших простих чисел для ділення визначається з розрахунку: максимальне число для ділення дорівнює квадратному кореню з максимального значення інтервалу;

б) скласти тест з більшою, ніж у попередньому випадку, кількістю пробних ділень та двома або трьома основами в тесті Ферма. Розрахувати кількість *Р*2 ймовірно простих чисел , які задовільняють цьому тесту. Проаналізувати отримані результати.

4.7. Відомо, що в заданому інтервалі є числа Кармайкла. Визначити їх. Варіанти інтервалів: (1050, 1050+100), (170, 1700+100), (2400+100).

**Висновок:** під час лабораторної роботиявивчив методи генерації простих чисел, що використовуються в системах шифрування з відкритим ключем, та здійснив перевіркучисел на простоту.