УДК 681.3

І. ЯКИМЕНКО
Тернопільський національний економічний університет

ЕФЕКТИВНИЙ АЛГОРИТМ ГЕНЕРУВАННЯ ПРОСТИХ ЧИСЕЛ НА ОСНОВІ ВИКОРИСТАННЯ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ

В даній статті викладені теоретичні основи ефективного алгоритму генерування найбільшого простого числа при застосуванні системи залишкових класів, що дозволяє понизити складність базових обчислювальних процесів та оперативно обчислювати прості числа, які придатні для побудови стійких систем захисту інформаційних потоків з використанням математичного апарату ЕК.

Ключові слова: система залишкових класів, прості числа, алгоритм, сито Еретосфена, тести простоти.

I. IAKYMENKO
Ternopil National Economic University

EFFECTIVE ALGORITHM OF GENERATION OF PRIME NUMBERS BASED ON USING REMAINING CLASSES SYSTEM

This article presents the theoretical background of algorithm for generating the greatest prime number in the application of remaining classes system. The new algorithm allows to reduce complexity of basic computing processes and effectively compute prime number, which are suitable for assembling stable system for protection information flows using the mathematical elliptic curves engine.

Keywords: remaining classes system, prime numbers, algorithm, sieve of Eratosthenes, primarily tests.

Актуальність дослідження

Сучасні комп'ютерні мережі та системи інтенсивно вдосконалюються на основі нових теоретичних положень опрацювання інформаційних потоків та програмно-апаратних засобів реалізації алгоритмів формування, перетворення, ідентифікація та покращення аутентифікації користувачів інформаційних систем.

При цьому, на сучасному етапі розвитку комп'ютерних систем виникає ряд проблем та науково-технічних задач пов'язаних з підвищенням інформаційної стійкості комп'ютерних систем, підвищення швидкодії алгоритмів шифрування/дешифрування а також створення відповідних програмно-апаратних та спецпроцесорних засобів опрацювання інформаційних потоків.

Досвід використання відомих алгоритмів шифрування та розвиток теорії алгоритмів, які широко застосовуються в практиці на основі важко оборотних функцій хешування, факторизації, модулярних та інших операцій вже наблизилися до границь своїх потенційних можливостей і в загальному не можуть бути основою розвитку та вдосконалення засобів захисту інформаційних потоків в сучасних та проектованих комп'ютерних системах.

Наш досвід показує, що на зміну цим методам закономірно прийшли нові алгоритми шифрування на еліптичних кривих, стійкість яких базується на проблемі дискретного логарифма. Якщо виключити вже відомі криптографічно слабкі криві, то стійкість цих систем захисту інформаційних потоків сьогодні оцінюються як експоненційна. Складність атаки на ключ експоненційно пов'язана в цьому випадку з довжиною ключа, тобто зростає швидко і при деякій довжині ключа стає практично нереалізованою. Це означає, що алгоритми шифрування з використання математичного апарату еліптичних кривих при однаковій стійкості мають розмір модуля на порядок менший ніж в традиційних системах. Однією з важливих задач в криптографії еліптичних кривих є генерування модуля криптоперетворення, який повинен задовольняти умовам простоти та розмірності не менше 512 біт.

Аналіз досліджень та огляд літературних джерел

Найбільш розповсюдженим способом знаходження простих чисел є один з найдавніших математичних методів – метод «Сито Еретосфена» [1], згідно якого для знаходження простих чисел необхідно викреслювати з послідовності натуральних чисел числа кратні 2, 3, 5, 7, 11 і т.д. В результаті виконання даної процедури в послідовності залишаються тільки прості числа. Однак для використання даного підходу, затрачається дуже великий обсяг часу.

Інший підхід генерування випадкового простого числа заданого розміру [2] (із заданою кількістю десяткових розрядів κ) полягає в наступному:

Вибирається випадкове натуральне число p між $10k-1$ і $10k+1$.

Далі по черзі перебирають числа p, $p+1$, $p+2$, кожне з яких перевіряється тестом простоти доти, поки якесь число $p+m$ не буде простим. Воно й береться як шукане просте число.

Основні недоліки даного підходу полягає в тому, що великі часові затрати будуть при перевірці чисел на простоту. На сьогоднішній день найбільш поширеними тестами простоти є тест Соловея–Штрассена (та його модифікація Лемана), Рабіна–Міллера [1–3].

Мета роботи

Тому метою даної роботи є розробка ефективного методу генерування багаторозрядних простих чисел, на основі використання системи залишкових класів, який на відмінну від відомих дозволить спростити процедуру ідентифікації та зменшити складність обчислювального процесу.

Система числення залишкових класів

Фундаментальною теоретичною основою СЗК є алгебра і теорія чисел [3], зокрема китайська теорема про залишки [4]. Відомо, що будь–яке ціле додатне число N у десятковій системі числення представляється в СЗК у вигляді набору $(b_1, b_2, b_3, ..., b_n)p_1, p_2, p_3, ..., p_n$ найменших додатних залишків від ділення цього числа на фіксовані цілі додатні попарно взаємно прості числа $p_1, p_2, p_3, ..., p_n$ $(b_i = N \bmod p_i)$, які називаються модулями (n – кількість модулів) [4]. При цьому повинна виконуватись умова $0 \le N \le P-1$, де $P = \prod_{i=1}^{n} p_i$.

Зворотне перетворення із базису Крестенсона у десяткову систему числення ґрунтується на використанні китайської теореми про остачі і є досить складним та громіздким [4]: $N = \left(\sum_{i=1}^{n} b_i B_i \right) \bmod P$, де $B_i = M_i m_i$, $M_i = \frac{P}{p_i}$, m_i шукається з виразу $(M_i m_i) \bmod p_i = 1$, при цьому повинна виконуватись умова $\left(\sum_{i=1}^{n} B_i \right) \bmod P = 1$.

Слід зазначити, що пошук коефіцієнтів $m_i = M_i^{-1} \bmod p_i$ становить значну обчислювальну складність, оскільки для знаходження оберненого елемента потрібно використовувати алгоритм Евкліда із виконанням не більше $5k$ операцій ділення з остачею, де k – кількість цифр в десятковому записі меншого з чисел [5].

Досить перспективними модифікаціями СЗК, які на даний час глибоко досліджуються, є розроблена досконала цілочисельна ($m_i = 1$), напівдосконала ($m_i = \pm 1$), нормалізована та розмежована форми СЗК [6].

Алгоритм ідентифікації простого числа з використанням СЗК

Для генерування простого числа можна скористатися розробленим алгоритмом, який дозволяє ефективно шукати прості числа, основна ідея якого полягає в наступному:

1. Маємо останнє просте число $p_i - \max$.

2. Визначаємо двійкове представлення цього числа n - розрядів.

3. Через розмежовану систему числення залишкових класів та властивість періодичності рекурентним шляхом отримуємо залишок числа p_i по заданому модулю:

$$\begin{cases} c_{i+1} = c_i \cdot 2 (\bmod\ p), c_1 = 1, a_1 = 1 \\ b_{i+1} = (c_{i+1} \cdot a_i + b_i) \bmod\ p, b_1 = 1, i = 1, a_i = 0,1 \end{cases}. \quad (1)$$

Програмним шляхом організовуємо генератор залишків по модулю p_j. В результаті знаходимо зображення цього числа в СЗК до числа простих чисел, які не перевищують $\sqrt{p_i}$ – половина розряду p_i .

4. Додаємо до залишків число 2 по всіх модулях, ця операція припиняється, коли по одному з модулів отримаємо 0. Тоді пропускаємо числа, кратні модулю, по якому залишок дорівнює 0. Операцію повторюємо до тих пір, поки не буде знайдено просте число. Блок схема алгоритму подана рис. 1.

Основними перевагами даного алгоритму ідентифікації простого числа p є використання системи залишкових класів по всіх простих модулях до $\sqrt{p}+1$, якщо один з залишків рівний нулю, то до залишків додаємо 2 по всіх модулях, ця операція припиняється коли по одному з модулів отримаємо 0. Тоді пропускаємо числа кратні модулю, по якому залишок 0 і знаходимо послідовність простих чисел. Це дозволяє значно зменшити складність алгоритму пошуку простих чисел, за рахунок введення циклу D.

Особливості даної структури, яка по ефективності переважає відомі алгоритми завдяки введення блоку (3) швидкого перетворення з двійкової системи числення в систему числення залишкових класів та модуля пошуку залишків в розмежованій системі числення. До переваг даного алгоритму можна віднести й те, що операції виконуються тільки над залишками, а не з великими простими числами. Отже, для генерування p – модуля перетворення груп точок ЕК можна скористатися запропонованим алгоритмом, який дозволяє спростити процедуру знаходження простого числа

Реалізація основних модулів, тобто пошуку простих чисел відбувається в програмному середовищі C++ Buider 6.0. Його основна робота починається з завантаження користувачем головної форми за допомогою меню і надається можливість отримати доступ до основних функцій додатку.

Основні можливості додатку розкриваються лише після того, як відбудеться пошук простих чисел.

Для відбору простих чисел передбачено обмеження, пошук буде відбуватися до вказаного в параметрах числа.

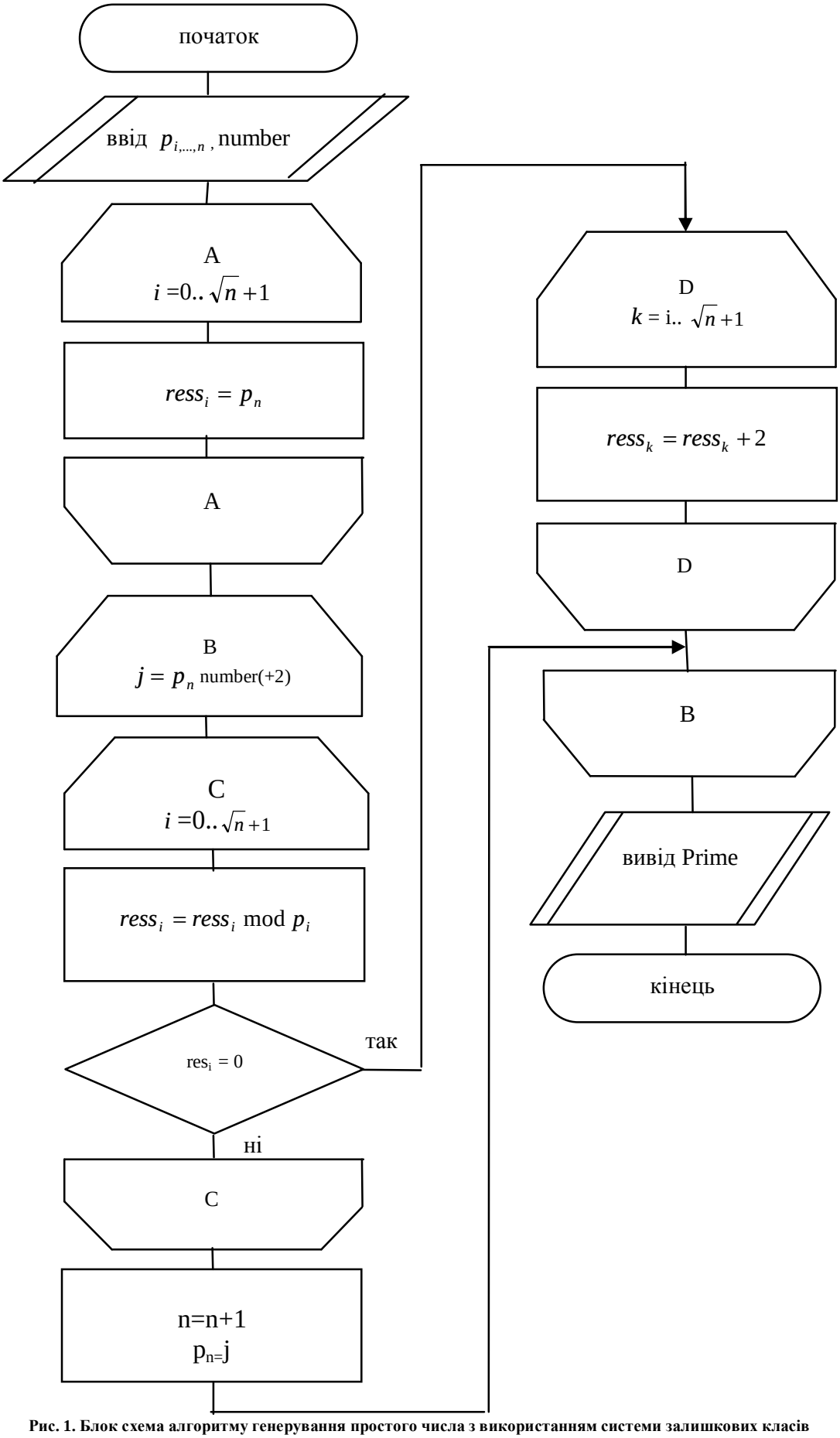

Рис. 1. Блок схема алгоритму генерування простого числа з використанням системи залишкових класів

Основними перевагами даного алгоритму ідентифікації простого числа p є використання системи залишкових класів по всіх простих модулях до $\sqrt{p}+1$, якщо один з залишків рівний нулю, то до залишків додаємо 2 по всіх модулях, ця операція припиняється коли по одному з модулів отримаємо 0. Тоді пропускаємо числа кратні модулю, по якому залишок 0 і знаходимо послідовність простих чисел. Це дозволяє значно зменшити складність алгоритму пошуку простих чисел, за рахунок введення циклу D.

Особливості даної структури, яка по ефективності переважає відомі алгоритми завдяки введення блоку (3) швидкого перетворення з двійкової системи числення в систему числення залишкових класів та модуля пошуку залишків в розмежованій системі числення. До переваг даного алгоритму можна віднести й те, що операції виконуються тільки над залишками, а не з великими простими числами. Отже, для генерування p – модуля перетворення груп точок ЕК можна скористатися запропонованим алгоритмом, який дозволяє спростити процедуру знаходження простого числа

Реалізація основних модулів, тобто пошуку простих чисел відбувається в програмному середовищі C++ Buider 6.0. Його основна робота починається з завантаження користувачем головної форми за допомогою меню і надається можливість отримати доступ до основних функцій додатку.

Основні можливості додатку розкриваються лише після того, як відбудеться пошук простих чисел. Для відбору простих чисел передбачено обмеження, пошук буде відбуватися до вказаного в параметрах числа.

На рисунку 2 показано процес пошуку простих чисел, менших від 1000000. Їх список буде відображений на екрані з вказаним часом початку пошуку та в кінці списку вказаним часом завершення пошуку.

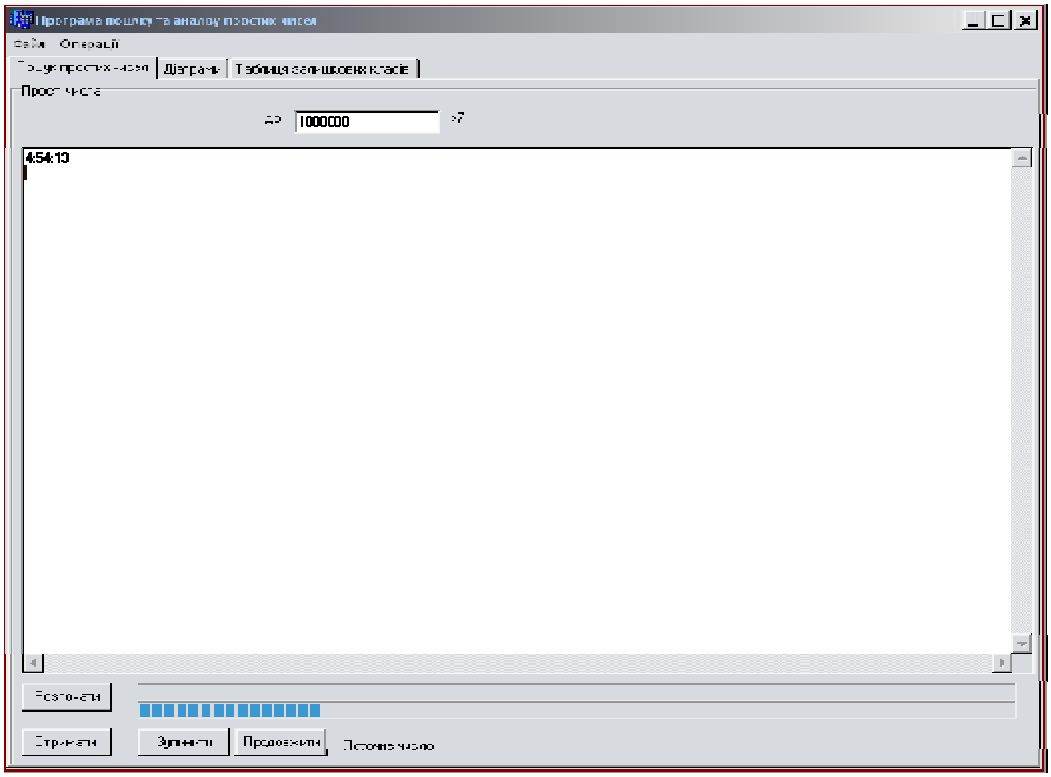

Рис. 2. Процес відбору простих чисел

Також в списку простих чисел будуть відмічені всі прості числа Мерсена та числа Ферма, які представляють особливий інтерес при побудові високопродуктивних спецпроцесорів. Після кожного десяткового представлення через пропуск відображено двійкове представлення чисел (рисунок 3).

Процес пошуку простих чисел відбувається з допомогою створення нового потоку, що дозволяє процесорові розподіляти час між частинами додатку, що в свою чергу забезпечує стабільну роботу, як додатку, так і операційній системі (ОС) в цілому під час обчислень.

Процес відбору простих чисел можна зупинити на певному етапі, та отримати результати пошуку, не очікуючи повного перебору заданого інтервалу.

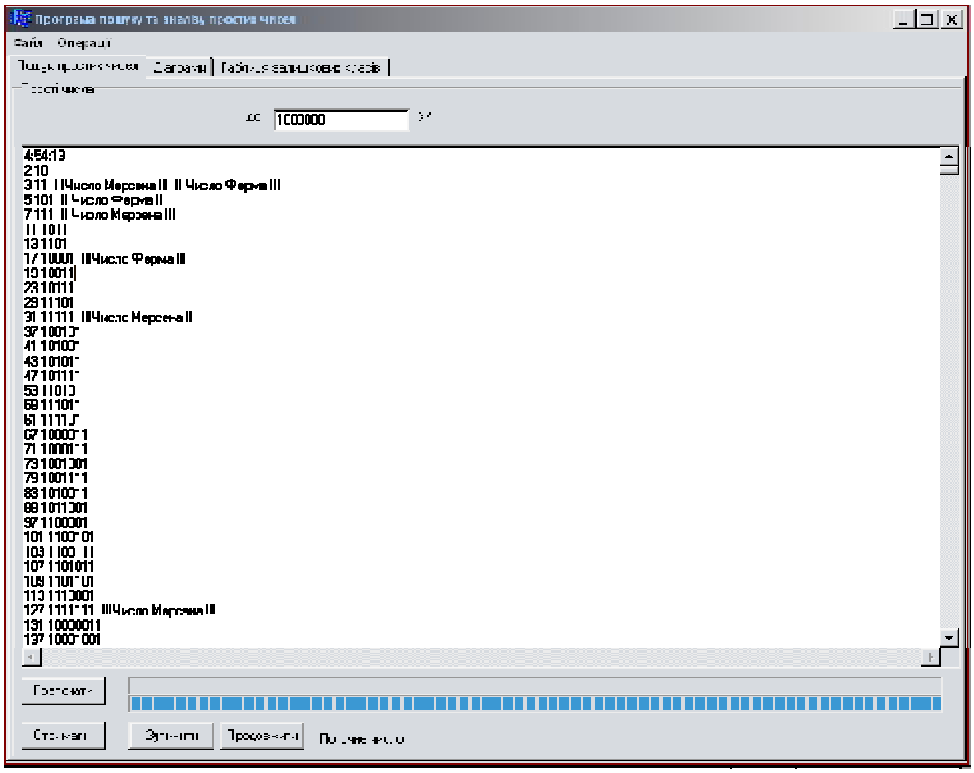

Рис. 3. Результати пошуку простих чисел

Висновки

Викладені теоретичні основи ефективного алгоритму генерування простих чисел, що дозволяє понизити складність базових обчислювальних процесів та оперативно обчислювати прості числа в діапазоні до 2^{256} за 60 с, а в діапазоні 2^{512} за 180 с, які придатні для побудови стійких систем захисту інформаційних потоків з використанням математичного апарату ЕК.

Література

1. Вербіцький О. В. Вступ до криптології / Вербіцький О. В. – Львів, 1998.

2. Ємець В.Ф. Сучасна криптографія. Основні поняття / В.Ф. Ємець, А.О, Мельник, Р.Б. Попович. – Львів, 2003.

3. Шнайер Б. Прикладная криптография. Протоколи, алгоритми, исполнение текстов на языке Си. – М., 2003. 4. www.rsasecurity.com.

4. Николайчук Я.М. Теоретичні основи базисних перетворень СЗК / Я.М. Николайчук, Ю.С. Федорович // Матеріали наукової конференції «Автоматика 2000». – Львів, 2000. – С. 120.

5. Задірака В. Комп'ютерна криптологія : підручник / В. Задірака, О. Олексюк – К., 2002. – 504 с.

6. Якименко І.З. Розмежована система числення залишкових класів та спецпроцеси на її основі. / І.З. Якименко, О.І. Волинський // Поступ в науку : збірник праць Бучацького інституту менеджменту і аудиту. – Бучач, 2009. – № 4. Т. 1. – С. 94–98.

Рецензія/Peer review : 6.1.2016 р. Надрукована/Printed : 11.2.2016 р.
Рецензент: д.т.н., проф. Я.М. Николайчук