УДК 681.32

# МЕТОД ЗНАХОДЖЕННЯ ЗАЛИШКІВ ВЕЛИКО-РОЗРЯДНИХ ЧИСЕЛ МЕРСЕНА В БАЗИСІ РАДЕМАХЕРА

***С.В. Івасьєв, В.І. Пашко***

*Тернопільський національний економічний університет,*
*м. Тернопіль, вул. Львівська, 11, stepan.ivasiev@gmail.com*

**Вступ.** Важливою задачею опрацювання інформаційних потоків у комп'ютерних системах є розробка нових методів та алгоритмів виконання операцій з великорозрядними числами (ВРЧ) [1], які широко використовуються в системах захисту інформаційних потоків. Найбільш відома реалізація алгоритму шифрування RSA, Ель–Гамаля, а також електронного цифрового підпису [1] ґрунтується на алгоритмічній складності задачі факторизації чисел.

Одним з перспективних напрямків при вирішенні задач факторизації ВРЧ є застосування теоретико-числового базису (ТЧБ) Радемахера [1], оскільки в класичній теорії використовується тільки десяткова система числення, яка має обмежені обчислювальні властивості і характеризується експоненційною обчислювальною складністю.

Разом з виникненням в криптографії нових понять і методів розширилося і коло криптографічних додатків теорії чисел. До елементарної та аналітичної теорії чисел все більш широко використовується алгебраїчна теорія чисел і арифметично аналітична геометрія.

Теорема Люка-Лемєра показує що для деякого натурального $n$ значення $2^n–1$ є простим, тоді $n$ також є простим […]. Отже, дана теорема дозволяє суттєво зменшити діапазон пошуку чисел Мерсена, оскільки перебір здіснюється по простим значенням експоненти $n$. На рисунку 1 показано послідовність розподілу простих експонент чисел Мерсена в логарифмічній шкалі.

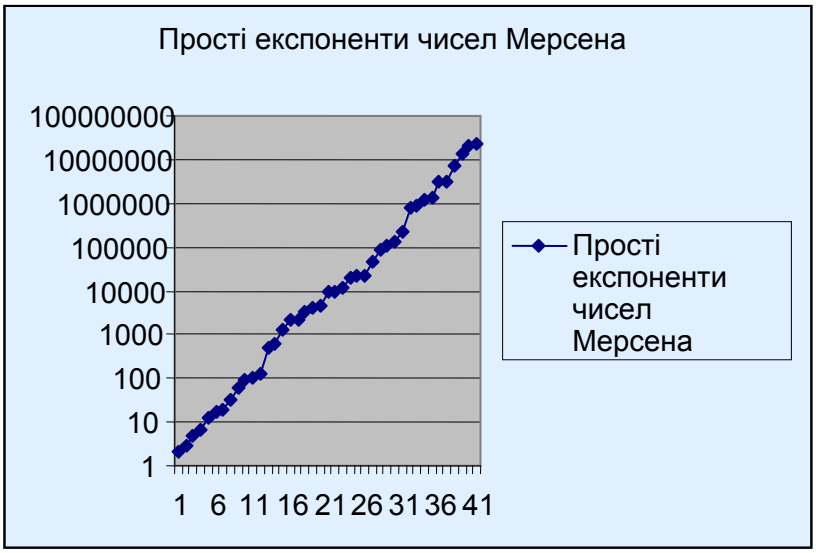


**Рисунок 1 – Розподіл простих експонент чисел**

Аналіз графічних результатів (рис. 1) показує, що розподіл простих експонент в числах Мерсена має певну залежність. З врахуванням апроксимації результатів досліджень, які мають залежність близьку до лінійної, можна оцінити значення наступної експоненти простого числа, деяких похибок можна припустити значення наступної експоненти, що дозволить пришвидшити пошук чисел Мерсена. В той же час слід зазначити, що апроксимація результатів досліджень має залежність близьку до лійної.

Очевидно, що наступні прості числа Мерсена в результаті спостережуваної апроксимації будуть знаходитись в інтервалі 1..2. Однією з важливих операцій при дослідженні чисел Мерсена є факторизація та знаходження залишків по простих модулях.

Класичні алгоритми пошуку залишку базуються на використанні багаторозрядного базису Радемахера, який має певні недоліки та функціональні обмеження. Загальний недолік пошуку залишків є отримання незавжди найменших залишків і також присутня надлишковість порівнянь. Тому є доцільним розробка нового методу, який базується на застосуванні особливостей чисел Мерсена в ТЧБ Радемахера .

Алгоритм пошуку залишку в базисі Радемахера:

- вхід x,P;
- представляємо P в базисі Радемахера наступним чином: P(pn…p0);
- зменшуємо розмір n вектора P на кількість одиниць від Pn до Pi(поки Pi=0 ), який рівний нулю і записуємо в вектор K(Km…K0);
- x=x-n-i;
- додаємо в базисі Радемахера вектор K до P беручи до уваги позицію бітів;
- зменшуємо розмір m вектора K на кількість одиниць від Km до Ki, який рівний нулю і записуємо в вектор K;
- x=x-n-i;
- крок 5 доки x≥0;
- вихід K=res x mod p.

Основними перевагами даного алгоритму є зменшення надлишкового використання пам’яті та кількості порівнянь. Це дозволяє зменшити обчислювальну складність на 1-2 порядки.

**Висновки.** Аналіз існуючих методів та алгоритмів опрацювання великорозрядних чисел показує перспективність їх розвитку, оскільки вимоги до розрядності простих чисел лінійно зростають.

Даний алгоритм вимагає менше обчислювальних ресурсів в порівнянні з існуючими алгоритмами на 1-2 порядки, крім того даний алгоритм придатний для знаходження множника числа Мерсена.

## Літературні джерела

1 Задірака В.К. Комп’ютерна арифметика багаторозрядних чисел: Наукове видання / В. К. Задірака, О. С. Олексюк – К., 2003. – 264 с.

2 Николайчук Я.М. Теорія джерел інформації. – Тернопіль: ТзОВ «Терно–граф», 2010. – 536 с.