**УДК 681.32**

**С. В. ІВАСЬЄВ, І. З. ЯКИМЕНКО, М. М. КАСЯНЧУК**

# ВДОСКОНАЛЕНИЙ АЛГОРИТМ ПОШУКУ СИМВОЛІВ ЯКОБІ

***Тернопільський національний економічний університет***
***46000, вул. Львівська, 11, м. Тернопіль, Україна,***
***E-mail: Stepan.ivasiev@gmail.com***

**Анотація**. В роботі викладено теоретичні основи пошуку символів Якобі, обґрунтовано необхідність та актуальність розробки методів пошуку символів Якобі. Проведений аналіз існуючих методів визначення квадратного лишку за модулем. Досліджено алгоритм пошуку символів Якобі. Запропоновано вдосконалений алгоритм пошуку символів Якобі. Досліджено властивості квадратів в системі залишкових класів. Здійснено оцінку складностей та проведено порівняльний аналіз розробленого та існуючого алгоритмів пошуку символів Якобі.

**Ключові слова:** теоретико-числовий базис, система залишкових класів, символи Якобі, залишки квадратів, багато розрядні числа.

**Аннотация**. В работе изложены теоретические основы поиска символов Якоби, обоснована необходимость и актуальность разработки методов поиска символов Якоби. Проведенный анализ существующих методов определения квадратного остатка по модулю. Исследован алгоритм поиска символов Якоби. Предложено усовершенствованный алгоритм поиска символов Якоби. Исследованы свойства квадратов в системе остаточных классов. Осуществлена оценка сложностей и проведен сравнительный анализ разработанного и существующего алгоритмов поиска символов Якоби.

**Ключевые слова**: теоретико-числовой базис, система остаточных классов, символы Якоби, остатки квадратов, много разрядные числа.

**Abstract**. This paper describes the theoretical foundations of search characters Jacobi, the necessity and urgency of developing methods for finding characters Jacobi. The analysis of existing methods for determining remains square residue. Described algorithm for search Jacobi symbols. An improved search algorithm Jacobi symbols. The properties of squares in the system of residual classes. The estimation of the complexities and the comparative analysis of developed and existing search algorithms Jacobi symbols.

**Keywords**: theoretical and numerical basis, the system of residual classes, symbols Jacobi remains squares, multi-bit number.

## ВСТУП

В задачах асиметричної криптографії, а саме в алгоритмі Шуфа обчислення порядку еліптичної кривої (ЕК), генеруванні параметрів та базових точок ЕК, однією з найбільш трудомісткою операцією є операція знаходження квадратного кореня за модулем (квадратного лишку за модулем) [1]. Багатьма вченими запропоновані різної складності методи вирішення даного класу задач [2].

Проведений аналіз існуючих методів визначення квадратного лишку за модулем говорить про те, що розв'язання даної задачі далеке від досконалості. Тим більше, з інтенсивним розвитком інформаційних технологій зростають вимоги щодо забезпечення необхідного рівня захисту комп'ютерних потоків. В умовах опрацювання багато розрядних чисел перспективу складають алгоритми побудовані на базі системи залишкових класів(СЗК). СЗК дозволяє глибоко розпаралелити обчислення з допомогою використання багато розрядної арифметики. Тому, ці вимоги, в більшості випадках, вирішуються за рахунок збільшення розмірності вхідних параметрів криптоалгоритмів, що призводить опрацювання багаторозрядних чисел. Тому розробка ефективного методу пошуку квадратичного лишку за модулем з використання системи залишкових класів є актуальною задачею у галузі шифрування даних.

## 1. ОГЛЯД МЕТОДІВ ПОШУКУ КВАДРАТИЧНОГО ЛИШКУ ЗА МОДУЛЕМ

Нехай $p$ — просте число, більше 2. Розглянемо відображення

$$F_p \to F_p, \alpha \mapsto \alpha^2,$$

яке зіставляє кожному елементу поля його квадрат. На безлічі ненульових елементів поля F $_p$ це відображення в точності «два-в-один», тобто якщо з ненульового елемента $x$ Î F $_p$ можна витягти квадратний корінь, то таких коренів у нього буде 2 і, крім того, половина елементів з $F_p$* є повними квадратами. Повні квадрати в $F_p$* називаються квадратичними лишками за модулем $p$. Безліч всіх квадратичних лишків по модулю $p$ є підгрупою порядку ($p$ – 1)/2 в мультипликативній групі $F_p$*. Елементи мультипликативної групи $F_p$* з яких не береться квадратний корінь, називаються квадратичними нелишками.

Для виявлення повних квадратів по модулю $p$ вводиться символ Лежандра $\left(\frac{a}{p}\right)$ [1], який вказує на існування квадратичного лишку по модулю $p$. Він дорівнює 0, якщо $a$ ділиться на $p$, 1, якщо $a$ — квадратичний лишок по модулю $p$, і — 1, якщо $a$ — квадратичний нелишок.

Символ Лежандра обчислюється за формулою $\left(\frac{a}{p}\right) = a^{(p-1)/2} (\mathrm{mod}\, p)$ [1]. Слід зазначити, що при збільшенні розрядності основних параметрів, зростає складність обчислень, при виконанні операції модулярного експоненціювання.

Але використання цієї формули пов'язане з обчисленнями великих ступенів і на практиці краще користуватися законом квадратичної взаємності

$$\left(\frac{a}{p}\right) = \left(\frac{p}{q}\right)(-1)^{(p-1)(q-1)/2},$$

або

$$\left(\frac{a}{p}\right) = \begin{cases} -\left(\frac{p}{q}\right), & \text{при } p = q = 3(\mathrm{mod}\ 4) \\ \left(\frac{p}{q}\right), & \text{в інших випадках} \end{cases}.$$

Крім цього, при обчисленні символу Лежандра можна скористатися додатковими формулами [2]:

$$\left(\frac{q}{p}\right) = \left(\frac{q(\mathrm{mod}\, p)}{p}\right);$$

$$\left(\frac{q \cdot r}{p}\right) = \left(\frac{q}{p}\right) \cdot \left(\frac{r}{p}\right);$$

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/s}.$$

Приклад**.** З використанням розкладання на множники обчислимо символ Лежандра.

$$\left(\frac{1}{17}\right) = \left(\frac{3}{17}\right) \cdot \left(\frac{5}{17}\right) = \left(\frac{17}{3}\right) \cdot \left(\frac{17}{5}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right) = (-1) \cdot (-1)^3 = 1.$$

Обчислення квадратного кореня з $a$ за модулем $p$ можна з використанням за допомогою алгоритму Шенкса [3 ].

1. Вибрати довільне $n$, таке що $\left(\frac{n}{p}\right) = -1$.

2. Нехай $e$, $q$ - цілі числа з непарним $q$, що задовольняють співвідношення $p$ — 1 = 2 $^b$ $q$.

3. Покладемо $y = n^q$ (mod $p$), $r = e$, $x = a^{(q-1)/2}$ (mod $p$).

4. Покладемо $b = ax^2 \pmod p$, $x = ax \pmod p$.
5. Поки $b \neq 1 \pmod p$ робити:

Знайти найменше число $m$, таке, що $b^2 = 1 (\mathrm{mod}\ p)$,

Покласти $\tau = y^{2^{y-\tau y}-1} (\mathrm{mod}\ p)$, $y = \tau^2 (\mathrm{mod}\ p)$, $r = m$

Покласти $x = x\tau (\mathrm{mod}\ p)$, $b = by (\mathrm{mod}\ p)$.

6. Вивести $x$.

Якщо $p = 3 \pmod 4$, то для добування квадратного кореня з $a$ можна використовувати формулу [2]

$$x = a^{(p+1)/4} (\mathrm{mod}\ p),$$

яка дає правильну відповідь тому, що

$$x^2 = a^{(p+1)/2} = a^{(p-1)/2} \cdot a = \left(\frac{a}{p}\right) \cdot a = a .$$

Символ Лежандра визначений тільки в разі простого знаменника. Якщо ж знаменник складений, то вводиться символ Якобі [2], узагальнюючий символ Лежандра.

Нехай $n$ — непарне число, більше 2 і

$$n = p_1^{b1} p_2^{b2} \ldots p_k^{bk}.$$

Символ Якобі визначається з використанням математичних основ обчислення символів Лежандра простих дільників числа $n$ наступним чином

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{b1} \left(\frac{a}{p_2}\right)^{b2} \ldots \left(\frac{a}{p_k}\right)^{bk}$$

Символ Якобі можна обчислювати так само, як і символ Лежандра, спираючись на тотожність, виведену із закону квадратичної взаємності:

$$\left(\frac{a}{n}\right) = \left(\frac{2}{n}\right)^b \left(\frac{n(\mathrm{mod}\, a_1)}{a_1}\right) (-1)^{(a_1-1)(n-1)/4},$$

де $a = 2^b a_1$ і $a_1$ непарній. Також при непарному $n$ справедливі наступні співвідношення:

$$\left(\frac{1}{n}\right) = 1;$$

$$\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/s};$$

$$\left(\frac{-1}{n}\right) = (-1)^{(n^2-1)/2}.$$

Використання даних формул пришвидшує алгоритм обчислення символу Якобі і, відповідно, символу Лежандра, як його окремий випадок, без розкладання на множники. Єдине, що потрібно зробити — виділити максимальний ступінь двійки.

## 2. ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ КВАДРАТІВ В СЗК

Усі квадрати цілих чисел можна представити, у вигляді суми непарних чисел (таблиця 1), тобто $\kappa_1 = 1$, $a_1 = 1$, $\kappa_2 = 3$, $a_2 = \kappa_1 + \kappa_2, \ldots$, $\kappa_n = 2n\text{-}1$, $a_n = \sum_{i=1}^{n} k_i$, причому числа $a_n$, $n = 1..\infty$ є квадратами постідовності чисел від 1 до $n$ тобто $a = \sqrt{a_n}$, $a \in Z$.

Таблиця 1

**Суми непарних чисел**

| Непарні числа, $к_n$ | Квадрати, $a_n$ |
|---|---|
| 1 | 1 |
| 3 | 4 |
| 5 | 9 |
| 7 | 16 |
| 9 | 25 |
| 11 | 36 |
| 13 | 49 |
| 15 | 64 |
| 17 | 81 |
| 19 | 100 |
| 21 | 121 |
| 23 | 144 |
| 25 | 169 |
| 27 | 196 |
| 29 | 225 |

Розглянемо залишки квадратів по декількох простих модулях $p_i$, тобто $a_{1_{(p_1,p_2,\ldots,p_n)}} = b_1^1, b_2^1, \ldots, b_n^1$ $a_{2_{(p_1,p_2,\ldots,p_n)}} = b_1^2, b_2^2, \ldots, b_n^2$ , …, $a_{n_{(p_1,p_2,\ldots,p_n)}} = b_1^n, b_2^n, \ldots, b_n^n$ , де $a_i(\mathrm{mod}\, p_i) = b_i^i, 1 \le i \le n$ . В результаті отримуємо значення, які привекдені в таблиці 2.

Таблиця 2

**Залишки квадратів по простих модулях**

| Непарні числа, $к_n$ | Квадрати послідовності цілих чисел, $a_n$ | Залишки по модулю 3, $a_n \bmod 3$ | Залишки по модулю 5, $a_n \bmod 5$ | Залишки по модулю 11, $a_n \bmod 11$ | Залишки по модулю 13, $a_n \bmod 13$ | Залишки по модулю 17, $a_n \bmod 17$ |
|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 3 | 4 | 1 | 4 | 4 | 4 | 4 |
| 5 | 9 | 0 | 4 | 9 | 9 | 9 |
| 7 | 16 | 1 | 1 | 5 | 3 | 16 |
| 9 | 25 | 1 | 0 | 3 | 12 | 8 |
| 11 | 36 | 0 | 1 | 3 | 10 | 2 |
| 13 | 49 | 1 | 4 | 5 | 10 | 15 |
| 15 | 64 | 1 | 4 | 9 | 12 | 13 |
| 17 | 81 | 0 | 1 | 4 | 3 | 13 |
| 19 | 100 | 1 | 0 | 1 | 9 | 15 |
| 21 | 121 | 1 | 1 | 0 | 4 | 2 |
| 23 | 144 | 0 | 4 | 1 | 1 | 8 |
| 25 | 169 | 1 | 4 | 4 | 0 | 16 |
| 27 | 196 | 1 | 1 | 9 | 1 | 9 |
| 29 | 225 | 0 | 0 | 5 | 4 | 4 |

З результатів чисельного експерименту таблиці 2 можна відмітити, що серед залишків по простому модулю 3 відсутній залишок 2, по модулю 5 залишки 2,3 по модулю 11 відповідно 2,6,7,8,10, по 13 немає 2,5,6,7,8, по 17 немає 3,5,6,7,10,11,12,15.

Також, слід зазначити, що система залишків по відповідних модулях утворюють циклічну групу, тобто перебір можна скоротити на половину. В результаті даних міркувань, розроблено алгоритм пошуку символів Якобі, який характеризується меньшою обчислювальною складністю відносно відомих методів і дозволяє ефективно визначати повні квадрати по модулю *p*.

Алгоритм пошуку символа Якобі буде виглядати так:

1. Enter P,m;
2. int I;
3. Int pN=1;
4. Bool is=false;
5. If P==0 return 0; goto 13;
6. If P==1 is=true; goto 12;
7. pN=pN+2;
8. pN=(pN mod m);
9. i++;
10. if (pN ==P) then is=true; goto 12;
11. if (i<m/2) GOTO 7;
12. If (is==false) return -1 else return 1;
13. End.

## 3 ОЦІНКА ТА ПОРІВНЯЛЬНИЙ АНАЛІЗ ЧАСОВОЇ СКЛАДНОСТІ ВІДОМИХ ТА РОЗРОБЛЕНОГО МЕТОДУ ВИЗНАЧЕННЯ СИМВОЛІВ ЯКОБІ

Оскільки в відомих методах пошуку символів Якобі основною трудомісткою операцією є модулярне експоненціювання, то розрахунки показують, що запропонований алгоритм на основі використання системи залишкових класів (основною операцією якого є пошук модуля від числа) дозволяє зменшити складність з $O2(n^3)$, або $O1(n^2 \log n)$ (Монтгомері метод) до $O(n \cdot \log_2 n)$, тобто ефективність зростає в $E2(n) = n$ разів. Графічні залежності даних складностей в логарифмічній шкалі представлені на рис. 1.

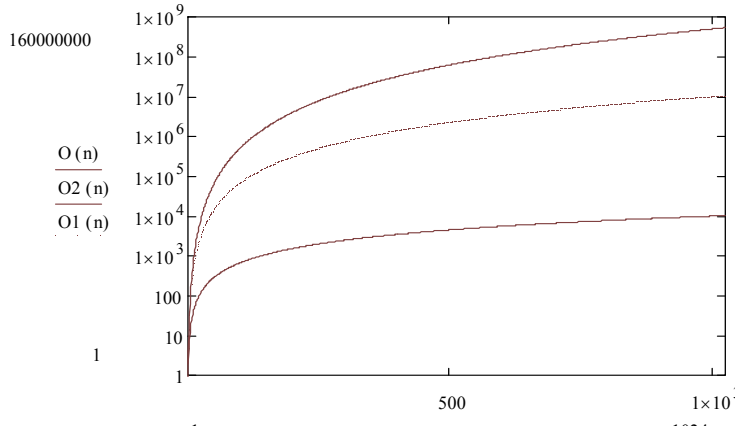


Рис. 1. Часова складність пошуку символів Якобі

Запропонований метод визначеня символів Якобі дозволяє зменшити часову складність за рахунок заміни операції множення додаванням, підвищити швидкодію на 1 порядок.

## ВИСНОВОК

Дослідження показали, що запропонований алгоритм характеризується високою швидкодією та ефективністю для визначення символів Якобі на основі використання системи залишкових класів. Оскільки операція пошуку квадратного кореня за модулем широко застосовується в асиметричній криптографії при генеруванні параметрів та базових точок ЕК, визначення стійкості ЕК методом пошуку їх порядку за допомогою алгоритму Шуфа, то доцільно використовувати розроблений метод в задачах захисту ІП на практиці для вдосконалення систем захисту ІП.

## СПИСОК ЛІТЕРАТУРИ


1. Николайчук, Я. М. Коди поля Галуа : теорія та застосування : монографія / Я. М. Николайчук. — Тернопіль : Терногpаф, 2012. — 576 с.
2. Задірака В. К., Кудін А. М., Людвиченко В. О., Олексюк О. С. Комп'ютерні технології криптографічного захисту інформації на спеціальних цифрових носіях : Навчальний посібник. Київ-Тернопіль: Підручники і посібники, 2007. — 272 с.
3. Якименко І. З. , Касянчук М. М. Теоретичні основи зменшення часової та апаратної складності систем захисту інформаційних потоків на основі еліптичних кривих з використанням теоретико-числового базису Радемахера-Крестенсона // Вісник Національного університету «Львівська політехніка» «Комп'ютерні системи та мережі». — № 694. — 2012. — с. 118—125.
4. Івасьєв С. В. Метод факторизації великорозрядних чисел у базисі Радемахера / С. В. Івасьєв // Вісник Національного університету «Львівська політехніка». — Львів : Вид-во Нац. ун-ту «Львів. політехника», 2012. т. № 745:Комп'ютерні системи та мережі. — С. 85—91.


## REFRENCES


1. Nykolaichuk Y. M., codes Galois fields: theory and application: monograph / Y. M. Nykolaichuk. - Ternopol: Ternohraf, 2012. — 576 p.
2. Zadiraka V. K., Kudin A. M., Lyudvychenko V. A., Oleksyuk A. S. Computer Technology cryptographic protection of information on special digital media: Textbook. Kyiv, Ternopil, textbooks, 2007. — 272 p.
3. Yakimenko I. Z., Kasyanchuk M. M. Theoretical Foundations of reducing the time and complexity of hardware systems to protect information flows based on elliptic curves using theoretical and numerical basis Rademacher-Krestenson // Proceedings of the National University «Lviv Polytechnic» «Computer systems and networks». — № 694 2012. — p. 118—125.
4. Ivasyev S. V. Factorization method multi-bit number numbers in the basis Rademacher / S. V. Ivasyev // Proceedings of the National University «Lviv Polytechnic». — Lviv: Izd Nat. Univ «Lviv. politehnyka» t.№ 2012. 745: Computer systems and networks. — S. 85—91.


Надійшла до редакції 22.06.2015 р.

**ІВАСЬЄВ СТЕПАН ВОЛОДИМИРОВИЧ — аспірант кафедри спеціалізованих комп'ютерних систем, Тернопільського національного економічного університету, м.Тернопіль, Україна.**

**ЯКИМЕНКО ІГОР ЗІНОВІЙОВИЧ — к. т. н., доцент кафедри комп'ютерної інженерії, Тернопільського національного економічного університету, м.Тернопіль, Україна.**

**КАСЯНЧУК МИХАЙЛО МИКОЛАЙОВИЧ — к. ф-м. н., доцент, доцент кафедри комп'ютерної інженерії Тернопільського національного економічного університету, м.Тернопіль, Україна.**