МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

ІВАСЬЄВ СТЕПАН ВОЛОДИМИРОВИЧ

УДК 681.3.06

МЕТОДИ ТА ОБЧИСЛЮВАЛЬНІ ЗАСОБИ РІШЕННЯ ЗАДАЧ ТЕОРІЇ ЧИСЕЛ В БАЗИСАХ РАДЕМАХЕРА - КРЕСТЕНСОНА

05.13.05 – комп'ютерні системи та компоненти

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Тернопіль – 2016

Дисертацією є рукопис.

Робота виконана в Тернопільському національному економічному університеті Міністерства освіти і науки України.

Науковий керівник: доктор технічних наук, професор
Николайчук Ярослав Миколайович,
Тернопільський національний економічний університет, завідувач кафедри спеціалізованих комп'ютерних систем.

Офіційні опоненти: доктор технічних наук, професор
Максимович Володимир Миколайович,
Національний університет «Львівська політехніка», професор кафедри безпеки інформаційних технологій;

кандидат технічних наук, доцент
Білан Степан Миколайович,
Державний економіко-технологічний університет транспорту, професор кафедри телекомунікаційних технологій та автоматики.

Захист відбудеться 2 липня 2016 року о 10^{00} годині на засіданні спеціалізованої вченої ради К 58.082.02 у Тернопільському національному економічному університеті за адресою: 46020, м. Тернопіль, вул. Львівська, 11а (корпус 11, зал засідань вченої ради).

З дисертацією можна ознайомитися у бібліотеці Тернопільського національного економічного університету за адресою: 46020, м. Тернопіль, вул. Бережанська, 4.

Автореферат розісланий 1 червня 2016 р.

Вчений секретар
спеціалізованої вченої ради Яцків В.В

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Важливим напрямком розвитку досліджень у галузі методів та програмно-апаратних засобів опрацювання цифрових даних є вдосконалення алгоритмів, які використовуються в сучасних комп'ютерних системах (КС), та розвиток математичних основ теорії чисел на базі кодових систем різних теоретико-числових базисів (ТЧБ), до яких належать: унітарний, Хаара, Радемахера, Крестенсона, Уолша, Галуа тощо. Вдосконаленням цього класу обчислень на основі названих ТЧБ є створення високопродуктивних компонентів та спецпроцесорів міжбазисних перетворень та рішення задач теорії чисел. Розробка відповідних програмних та апаратних обчислювальних засобів дозволяє підвищити продуктивність, швидкодію, зменшити апаратну та обчислювальну складності методів опрацювання багаторозрядних чисел (БРЧ) при знаходженні набору модулів досконалої та модифікованої досконалої форм системи залишкових класів (СЗК) в різних прикладних задачах обчислювальної математики.

Однією з найбільш складних задач такого класу методів та спецпроцесорів є реалізація алгоритмів опрацювання БРЧ, модульних операцій, модулярного множення та експоненціювання, пошуку квадратичних лишків, пошуку багаторозрядних простих чисел (БПЧ), тестів на простоту тощо.

Успіхи сучасного розвитку мікроелектронної, комп'ютерної техніки та використання потужних багатоядерних суперпроцесорів та кластерів дозволяє ефективно вирішити багато прикладних задач теорії чисел на основі двійкової арифметики ТЧБ Радемахера шляхом створення відповідних алгоритмічних, програмних та мікропроцесорних інструментальних засобів.

Аналіз стану застосування в сучасній комп'ютерній техніці арифметики різних ТЧБ свідчить, що в цілому стан цієї задачі далекий від вирішення. Значний вклад у розвиток теорії методів та високопродуктивних процесорів опрацювання БРЧ на основі ТЧБ Крестенсона внесли відомі українські та зарубіжні вчені Акушський І.Й., Палагін О.В., Брюхович Є.І., Романов С.І., Тарасенко В.П., Николайчук Я.М., Мельник А.О., Червяков В.П., Краснобаєв В.А., B. Omondi, N. Szabo, M. Hosseinzadeh, Lenstra H. W., Lakhani G., L.-L. Yang, L. Hanzo та інші.

В той же час, вирішення наукової задачі розвитку обчислювальних методів та засобів на основі математичних засад теорії чисел знаходиться в стадії становлення та направленості до створення і реалізації високопродуктивних обчислювальних засобів та спецпроцесорів, які б забезпечували необхідну в даний час та в майбутньому швидкодію опрацювання БРЧ в умовах постійного зростання вимог до системних характеристик КС.

Тому розробка підходів, методів, алгоритмів та обчислювальних засобів на основі розвитку алгоритмів та математичних положень теорії чисел у різних ТЧБ є актуальною науковою задачею.

Зв'язок роботи з науковими програмами, планами і темами.

Дисертаційна робота виконувалася у рамках науково-дослідних робіт кафедри спеціалізованих комп'ютерних систем Тернопільського національного економічного університету "Розробка теоретичних засад методів формування та

цифрового опрацювання даних у розподілених спеціалізованих комп'ютерних системах" (Державний реєстраційний номер 0112U008458) та кафедри комп'ютерної інженерії "Опрацювання багаторозрядних чисел в системі залишкових класів" (Державний реєстраційний номер 0115U001607).

Мета і задачі дослідження.

Метою досліджень є зменшення складності, підвищення продуктивності методів та швидкодії алгоритмів, спеціалізованого програмного і апаратного забезпечення у прикладних задачах теорії чисел.

Для досягнення поставленої мети у дисертаційній роботі необхідно розв'язати наступні задачі:

1) провести аналіз:

- характеристик архітектур процесорів опрацювання БРЧ;
- архітектур та характеристик спецпроцесорів кореляційного та спектрального опрацювання чисел у різних ТЧБ;
- методів кодування БПЧ в КС на основі ТЧБ Радемахера та Крестенсона;
- методів пошуку квадратичних лишків, модулярного множення, факторизації БРЧ в задачах теорії чисел;

2) розробити:

- метод компактного кодування масивів БПЧ;
- метод факторизації БРЧ у базисі Радемахера та Крестенсона;
- схемотехнічні рішення генератора квадратів БРЧ у базисі Хаара - Крестенсона, пристрою компактного кодування БПЧ та процесора факторизації БРЧ у базисі Хаара - Крестенсона;
- програмне забезпечення факторизації БРЧ та дослідження задачі факторизації БРЧ для виявлення околу рішення, компактного кодування БПЧ, множення БРЧ;

3) удосконалити:

- метод визначення околу рішення задачі факторизації;
- векторно-модульний алгоритм модулярного множення;
- метод пошуку квадратичних лишків;

Об'єкт дослідження – процеси програмного та апаратного опрацювання багаторозрядних чисел у спеціалізованих комп'ютерних системах з використанням теоретико – числового базису Радемахера – Крестенсона.

Предмет дослідження – методи, алгоритми та засоби зменшення апаратної та часової складностей при опрацюванні багаторозрядних чисел на основі використання теоретико – числового базису Радемахера – Крестенсона.

Методи дослідження. Для дослідження та аналізу методів, алгоритмів і спеціалізованого програмного, апаратного забезпечення у прикладних задачах теорії чисел використані математичні основи теорії чисел, арифметика виконання обчислювальних операцій в ТЧБ Радемахера, Хаара та Крестенсона, теорія інформації, теорія алгоритмів, методи програмованого синтезу та реалізації мікропроцесорних засобів на кристалах.

Наукова новизна отриманих результатів полягає в наступному:

Вперше розроблено:

- метод компактного кодування масивів багаторозрядних простих чисел,

який, на відміну від існуючих, ґрунтується на зберіганні обмеженого числа динамічно кодованих молодших розрядів їх двійкового представлення у базисі Радемахера та інкрементно розрядно-позиційному нарощенні їх більш високих розрядів, що дало можливості зменшити на порядок обсяг необхідної пам'яті;

- метод факторизації багаторозрядних чисел на основі арифметики теоретико-числового базису Радемахера – Крестенсона шляхом представлення цифрових даних у системі залишкових класів, застосування модульної арифметики, виключення операції добування кореня квадратного та здійснення способу розв'язання задач шляхом асоціативного сканування множини розв'язків в околі рішення, що, в порівнянні з відомими методами, дало можливість зменшити розрядності операндів, спростити алгоритм пошуку факторизованих чисел та підвищити швидкодію алгоритму обчислень.

Удосконалено:

- метод визначення околу рішення задачі факторизації шляхом обчислення двійкового логарифму різниці між відомим числом, що факторизується, та добутком, який обчислюється ітераційно, що дало можливість підвищити швидкодію визначення двійкової розрядності числа ітерацій з поліноміальною складністю в порівнянні з існуючими алгоритмами експоненційної складності.

Отримав подальший розвиток*:*

- векторно-модульний метод модулярного множення, який, на відміну від існуючих, реалізований в теоретико-числовому базисі Радемахера – Крестенсона і характеризується меншою кількістю операцій додавання та, відповідно, меншою обчислювальною складністю в порівнянні з існуючими алгоритмами множення;
- метод пошуку квадратичних лишків у кодовій системі базису Крестенсона, який, на відміну від існуючих, характеризуються підвищеною швидкодією та меншою обчислювальною складністю.

Практичне значення одержаних результатів.

1. Розроблено високопродуктивні алгоритми факторизації на основі теореми Ферма, модулярного множення, пошуку квадратичних лишків, компактного кодування БПЧ, перевірки БРЧ на простоту згідно арифметики ТЧБ Хаара – Крестенсона та Радемахера - Крестенсона.
2. Розроблено схемотехнічні рішення пристрою кодування БПЧ, що дало можливість зменшити об'єм використання пам'яті при зберіганні БПЧ.
3. Розроблено схемотехнічні рішення високопродуктивного генератора квадратів БРЧ у ТЧБ Радемахера та Крестенсона, що спрощує реалізацію запропонованого способу факторизації згідно удосконаленого алгоритму Ферма.
4. Розроблена функціональна та структурна схема спецпроцесора рішення задач факторизації у базисі Хаара – Крестенсона на основі запропонованих високопродуктивних методів.

Результати досліджень використані при виконанні науково-дослідних робіт, а також у навчальному процесі на кафедрах комп'ютерної інженерії та спеціалізованих комп'ютерних систем Тернопільського національного економічного університету при викладанні дисциплін «Комп'ютерні системи», «Комп'ютерна криптографія» та «Захист інформації в комп'ютерних системах». Отримані результати впроваджені на ТОВ «Стріла» та ТОВ «Інтеграл» для

опрацювання інформаційних потоків у дистрибутивних та корпоративних комп'ютерних мережах.

Особистий внесок.

У друкованих працях, опублікованих у співавторстві, автору належить: [9,10,14,15,16] - дослідження обчислювальних складностей алгоритмів опрацювання БПЧ та принципів рішення прикладних задач теорії чисел для реалізації спецпроцесорів, [13,17,19] - розроблено метод кодування та зберігання БПЧ, [2,8,11,12] - досліджено та реалізовано алгоритм модульного множення з використанням ТЧБ Рademахера-Крестенсона, [4,18] - розроблено метод локалізації розв'язку задачі факторизації БРЧ, [1,5,6,7,20] - розроблено метод факторизації БРЧ, [3] – розроблено метод визначення квадратичного лишку у СЗК.

Апробація результатів дисертації. Основні результати дисертаційної роботи апробовані на: проблемно-науковій міжгалузевій конференції «Інформаційні проблеми комп'ютерних систем, юриспруденції, енергетики, економіки, моделювання та управління», Бучач, Україна, 2010, 2011, 2014; міжнародній конференції «Досвід проектування і застосування САПР в мікроелектроніці», (CADSM-2011, CADSM-2015), Львів-Поляна, Україна, 2011, 2015; міжнародній молодіжній математичній школі "Питання оптимізації обчислень, (ПОО-XXXVII)", Київ, Україна, 2011, 2014, 2015; міжнародній конференції "Сучасні проблеми радіотехніки, телекомунікації та комп'ютерні науки", (TCSET'2012, TCSET'2014), Львів, Славськ, Україна, 2012, 2014; II Всеукраїнській науково-практичній конференції молодих учених та студентів «Інтелектуальні технології в системному програмуванні», (ІТСП-2013), Хмельницький, Україна, 2013; міжнародній конференції "Захист інформації і безпека інформаційних систем - 2014", Львів, Україна, 2014; міжнародній науково-практичній конференції «Сучасні інформаційні та електронні технології», Одеса, Україна, 2014; IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS–2015), Warsaw, Poland, 2015; V Всеукраїнській школі-семінарі молодих вчених та студентів «Сучасні комп'ютерні інформаційні технології» (ACIT-2015), Тернопіль, Україна, 2015.

Публікації. За матеріалами дисертації опубліковано 20 друкованих праць: 7 статей, з яких 5 у фахових виданнях (1-одноосібна), 13 публікацій - у матеріалах та тезах доповідей конференцій, з яких 3 - у наукових видання, що індексуються наукометричною базою Scopus.

Структура дисертації. Дисертаційна робота складається зі вступу, чотирьох розділів, загальних висновків, списку використаних джерел та додатків. Загальний обсяг дисертації становить 222 сторінки, з них 148 сторінок основного тексту, містить 70 рисунків, 29 таблиць, 14 додатків, список використаних джерел із 172 найменувань.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовано актуальність виконаних досліджень, подано зв’язок дисертаційної роботи з науковими програмами та темами. Сформульовано мету та задачі досліджень, дано характеристику наукової новизни отриманих результатів і практичного значення роботи, наведено відомості про апробацію результатів та їх впровадження.

У **першому розділі** проаналізовано та досліджено методи, апаратні засоби опрацювання БРЧ для задач теорії чисел, визначено їх переваги та недоліки.

Проведена систематизація архітектур універсальних процесорів, що використовуються в персональних комп’ютерах, кластерах та багатоядерних системах, показує широкі можливості паралельного опрацювання інформації, які можна використовувати при обробці БРЧ в прикладних задачах теорії чисел.

Досліджено архітектури, апаратні складності та швидкодії матричних перемножувачів, які використовуються в універсальних процесорах у якості сопроцесорів прискорювачів, які характеризуються низькою швидкодією виконання операцій множення, ділення, піднесення до квадрату та добування квадратного кореня у двійковій арифметиці ТЧБ Радемахера, число розрядів яких при рішенні задач теорії чисел може складати 2^{100}-2^{1024}. Таким чином, застосування двійкової арифметики при розв’язанні задач, що потребують виконання операцій над БРЧ, є обґрунтовано неефективним та недостатньо швидкодіючим.

Викладені схемотехнічні та алгоритмічні рішення реалізації спецпроцесорів кореляційного і спектрального опрацювання даних у різних ТЧБ показують, що спецпроцесори у ТЧБ Радемахера–Крестенсона та Хаара–Крестенсона характеризуються найвищою швидкодією і меншою часовою складністю опрацювання даних на 2 – 3 порядки у порівнянні з іншими.

Проаналізовано методи модулярного множення та експоненціювання у ТЧБ Радемахера – Крестенсона, які характеризуються суттєво більшою швидкодією у порівнянні з двійковою системою числення, що є важливою перевагою його застосування на низових рівнях розподілених КС шляхом використання спеціалізованих процесорів, контролерів та перспективністю використання мультибазисних методів опрацювання багаторозрядних даних у прикладних задачах теорії чисел.

Обґрунтовано необхідність розробки методів, програмних та апаратних засобів компактного кодування БРЧ, модулярного множення, визначення квадратичних лишків, факторизації БРЧ для вирішення задач теорії чисел, підбору системи модулів досконалої і модифікованої досконалої форм СЗК та виконано постановку задачі досліджень.

У другому розділі проведені теоретичні та експериментальні дослідження розроблених методів та критеріїв ефективності опрацювання БРЧ на основі математичного апарату базису Радемахера-Крестенсона.

Розроблено та обґрунтовано доцільність застосування методу знаходження

залишку БРЧ в базисі Радемахера: $P \bmod b$, $P = \sum_{i=0}^{n-1} p_i 2^i$, $b = \sum_{i=0}^{k-1} b_i 2^i$, де $b_i = 0,1$, $p_i = 0,1$ наступною послідовністю кроків. Крок 1. Виділяється k-1 старших розрядів числа P, в результаті чого отримується вектор двійкового представлення $K = (P_{n-1}, P_{n-2}, ..., P_{n-k-1})$. Крок 2. Якщо $K \geq B$, то знаходиться $K \bmod b = K - b = S$ і записується $S = \sum_{i=1}^{k-2} S_i 2^i, S_i = 0,1$, яке у двійковому представленні має вигляд $S = (S_{k-2}, S_{k-3}, ..., S_1, S_0)$. Крок 3. Формується вектор $S_1 = (S^1_{k-2}, S^1_{k-3}, ..., S^1_1, S^1_0, p_{n-k-3})$ шляхом дописування у молодший розряд p_{n-k-3}. Крок 4. Перевіряється нерівність $S_1 > B$. Якщо вона справджується, то шукається значення $S_1 \bmod b = S_1 - b$, в іншому випадку дописується в молодший розряд p_{n-k-4} і отримується $S_2 = (S^2_{k-2}, S^2_{k-3}, ..., S^2_1, S^2_0, p_{n-k-3}, p_{n-k-4})$. Крок 5. Обчислюється значення $S_2 \bmod b$. Дана процедура продовжується доти, поки в молодшому розряді не отримається p_0, тобто вектор $S_n = (S^n_{k-2}, S^n_{k-3}, ..., S^n_1, S^n_0, p_0)$.

Крок 6. Визначається значення $P \bmod b = S_n \bmod b$, для знаходження результуючого залишку в базисі Радемахера.

Розроблено метод векторно-модульного множення n–розрядних чисел $a = \sum_{i=0}^{n-1} a_i \cdot 2^i$ та $b = \sum_{j=0}^{n-1} b_j \cdot 2^j$, де a_i, b_j=0, 1.

Табл.1. Представлення вектор-рядків модульного множення

c_{n-1}		c_i	…	c_1	c_0
a_{n-1}	…	a_j	…	a_1	a_0

Для знаходження результату операції модулярного множення $a \cdot b \bmod p$ будується два вектор-рядки, перший з яких складається з елементів $c_0 = 2^0 b \bmod p$, $c_i = 2 \cdot c_{i-1} \bmod p$, другий - з a_i (табл. 1).

Результат модулярного множення двох n – розрядних чисел визначається згідно формули $a \cdot b \bmod p = \left(\sum_{i=0}^{n-1} a_i \cdot c_i \right) \bmod p$. Розроблений метод характеризується меншою часовою та апаратною складністю порівняно з матрично-модульним в базисі Радемахера – Крестенсона за рахунок зменшення вдвічі кількості суматорів, що визначає перспективи щодо розробки високопродуктивних програмно-апаратних засобів.

Таким чином, в результаті проведених досліджень було встановлено часові складності запропонованого методу і відомих методів (алгоритмів) множення: $O1(n) = n^2$ - стандартний метод множення в базисі Радемахера, $O(n) = n \cdot \log n \cdot \log(\log n)$ - алгоритм Шонхаге-Штрасена, $O3(n) = n^{1,585}$ та $O4(n) = n^{1,465}$ - відповідно алгоритми Карацуби та Тома-Кука, $O2(n) = \begin{cases} 2 \log n, \text{ якщо } n \leq 64 \\ n \log n, \text{ в інших випадках} \end{cases}$ - матрично-модульний алгоритм в ТЧБ Радемахера-Крестенсона, $O5(n) = \log n$ - розроблений векторно-модульний метод.

Розроблений метод реалізовано алгоритмічно і виконано порівняння обчислювальної складності (рис.1) розробленого і відомих алгоритмів.

Чисельний експеримент показує, що використання розробленого векторно-матричного методу, який грунтується на ТЧБ Радемахера - Крестенсона, дозволяє на порядок зменшити часову складність модулярного множення відносно класичного методу і на 50 % - в порівнянні з матрично-модульним алгоритмом в ТЧБ Радемахера-Крестенсона.

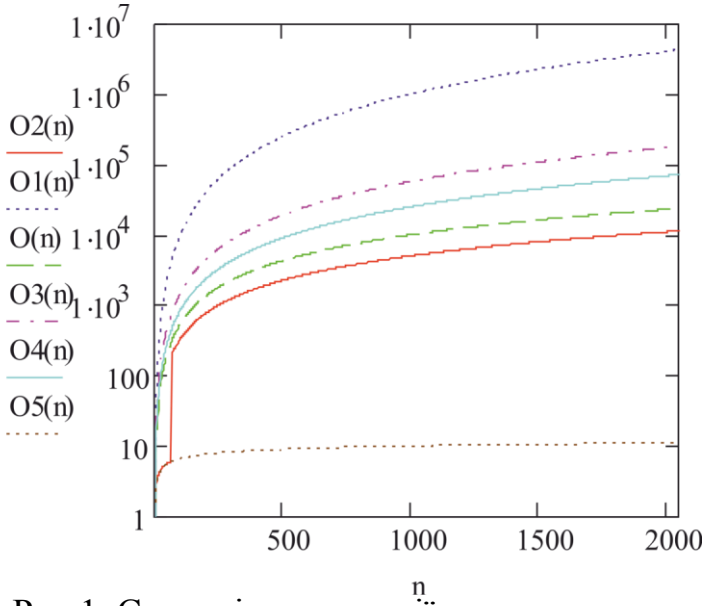

Рис.1. Складність операції модулярного множення відомих та розробленого алгоритмів

Розроблено метод обчислення квадратичних лишків на основі використання СЗК. Представляються залишки квадратів цілих чисел по декількох простих модулях p_j, тобто $a_1(p_1,p_2,...,p_m)=b_1^1,b_2^1,\text{K},b_m^1$, $a_2(p_1,p_2,...,p_m)=b_1^2,b_2^2,\text{K},b_m^2$, $a_n(p_1,p_2,...,p_m)=b_1^n,b_2^n,\text{K},b_m^n$, де $a_i=i^2$, $b_j^i=a_i(mod\ p_j),1\le i\le n,\ 1\le j\le m$, m – кількість модулів. Квадрати цілих чисел доцільно подати у вигляді суми непарних чисел, кількість яких дорівнює даному числу:

$$n^2=\sum_{i=1}^{n}(2i-1). \qquad (1)$$

З врахуванням співвідношення (1) шукані залишки отримуємо за допомогою рекурентної формули:

$$b_j^i=\left(b_j^{i-1}+z_i^j\right)mod\ p_j, \qquad (2)$$

де $z_j^i=z_i\ mod\ p_j, zi=2i-1$.

Відповідні результати по модулях 3, 5, 7 представлені в табл. 2 та відображають циклічні властивості квадратичних лишків по простих модулях. Ці властивості дозволяють скоротити наполовину процес ітераційного перебору в реалізованому алгоритмі визначення квадратичності. З табл. 2 видно, що кількість квадратичних лишків

Табл.2. Пошук квадратичних лишків

N	z_i	a_n	p_1=3		p_2=5		p_3=7	
			z_1^i	b_1^i	z_2^i	b_2^i	z_3^i	b_3^i
1	1	1	1	1	1	1	1	1
2	3	4	0	1	3	4	3	4
3	5	9	2	0	0	4	5	2
4	7	16	1	1	2	1	0	2
5	9	25	0	1	4	0	2	4
6	11	36	2	0	1	1	4	1
7	13	49	1	1	3	4	6	0

для кожного модуля становить $(p_j+1)/2$ (включаючи 0). Це випливає з рівності $n^2 \bmod p_j = (-n^2) \bmod p_j = (p_j-n)^2 \bmod p_j$. Особливістю квадратичних лишків є також властивість циклічності, яка використана для більш ефективного обчислення згідно (2).

Відомо, що в методах пошуку символів Якобі основною трудомісткою операцією є модулярне експоненціювання. Аналіз показав, що розроблений алгоритм на основі запропонованого методу з використанням СЗК (основною операцією якого є пошук залишку 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 (рис.2).

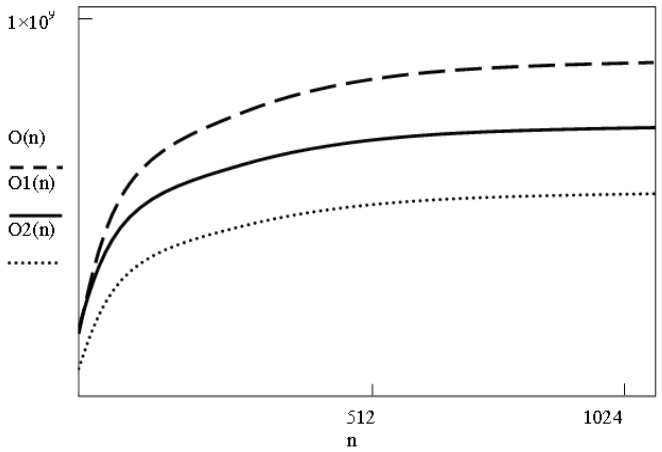

Рис.2. Порівняльна характеристика обчислювальної складності визначення квадратичних лишків

Результати чисельного експерименту свідчать про те, що розроблений метод характеризується меншою часовою складністю в порівнянні з відомими (зокрема, знаходження символів Якобі та Лежандра) і дозволяє ефективно визначати повні квадрати по модулю *P*.

Вперше розроблено метод компактного кодування великих за об'ємом масивів БПЧ, для зберігання яких проводиться аналіз 15 бітів, тобто від 0 до 15 розряду.

Зміна в старших розрядах на +1 контролюється бітом синхронізації, який також зберігається і вказує порядковий номер простого числа, в якому додається 1 (рис. 3). З рис. 3 видно, що розроблений метод дозволяє в декілька порядків збільшити швидкодію доступу та збереження кодів БПЧ, оскільки для запису 1024 – бітного числа використовуються лише 15-бітне закінчення та біт синхронізації. Для збереження послідовності БРЧ до 1024 для кожного простого числа зазначеної розрядності необхідно 128 байт, а при використанні розробленого методу - лише 2 байти.

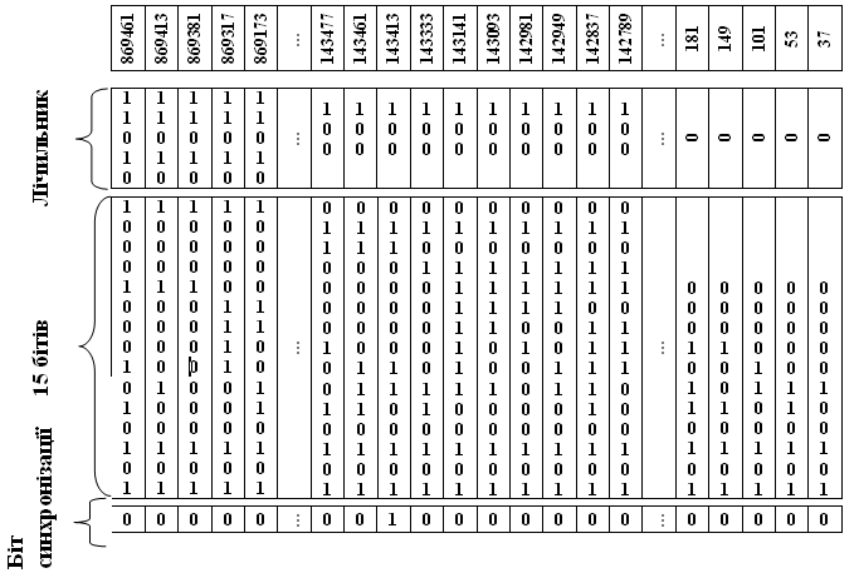

Рис.3. Схема розбиття числа на групи розрядів.

Таким чином, використання розроблених методів дозволяє зменшити часові складності існуючих алгоритмів на 1–2 порядки при опрацюванні БРЧ в

прикладних задачах обчислювальної математики та теорії чисел.

У третьому розділі розроблені методи факторизації з використанням СЗК базису Крестенсона на основі визначення околу рішення задачі шляхом обчислення двійкового логарифму різниці між відомим числом, що факторизується, та добутком, який обчислюється ітераційно.

Зокрема, розроблено метод, що базується на теоремі Ферма, в основі якого лежать наступні дії: добувається $\sqrt{P_0}$ і округлюється до більшого цілого $\sqrt{P_0} \Rightarrow \tilde{P}_c$, $\tilde{P}_c$ підноситься до квадрату тільки один раз і отримується $F_1 - P_0 = \Delta_0$, далі обчислюється число:

$$S_k = k(2\tilde{P}_c + k) + \Delta_0. \qquad (3)$$

Значення $\sqrt{S_k} = \overset{0}{\Delta}$ перевіряється на існування цілого кореня для єдиного знайденого k з рівняння (3), в результаті цього можна отримати шукані P_1 і P_2 згідно виразу $P_1 = \overset{0}{\Delta} - P^* c + k$, $P_2 = \overset{0}{\Delta} 2P^* c + k$.

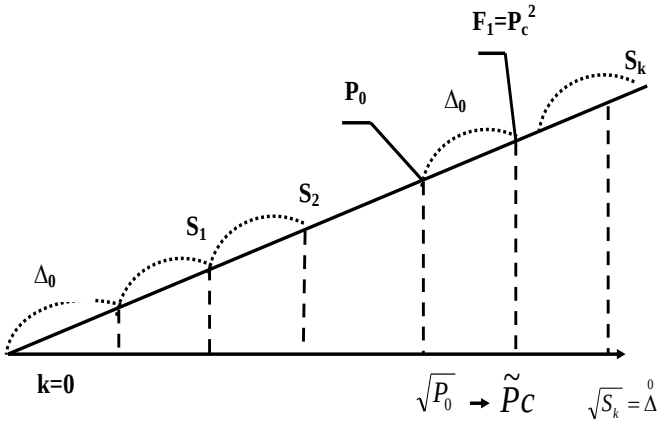

Рис.4. Схема факторизації БРЧ згідно розробленого алгоритму.

Оскільки k – багаторозрядне число, то метод, в якому відсутні операції піднесення $\tilde{P}c + k$ до квадрату, буде мати меншу обчислювальну складність. Розрядності чисел, що використовуються в методі, менші, ніж в алгоритмі Ферма (рис. 4.) На основі розробленого методу спроектовано та реалізовано схему спецпроцесора для факторизації.

Для відомих (тестових) БРЧ RSA отримаємо результати досліджень змінної k (рис. 5), що ілюструють різницю двійкових логарифмів добутків для шуканого розв'язку, та числа, що факторизується.

Метод реалізується шляхом визначення двійкового логарифму різниці пропонованих множників та їх добутку для порівняння з числом, що факторизується, причому число k змінюється ітераційно та порозрядно логарифмічно зростає. На кожній ітерації методу обчислюється пропонований добуток та логарифм різниці розрядностей між числом,

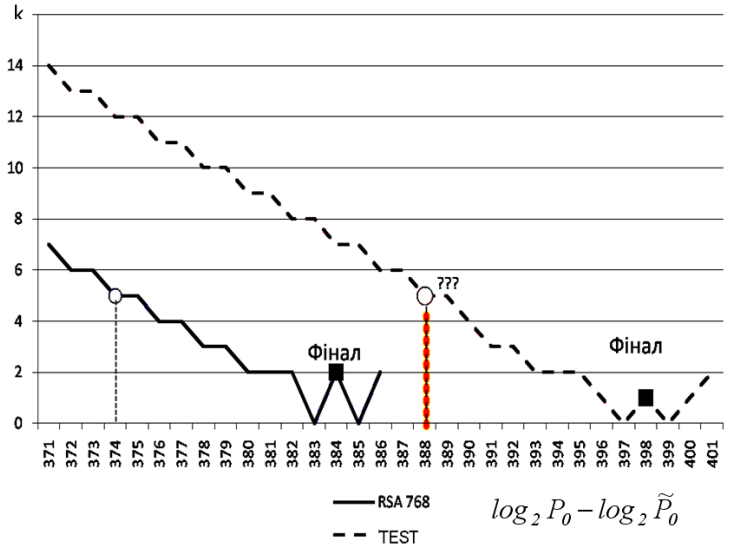

Рис.5. Деталізована – модель пошуку розрядності k=2^i для тестових відомих RSA

що факторизується, для кожного з k. Ітераційний процес продовжується, поки пропонований добуток для заданого k не буде дорівнювати 0 або ж не стане від'ємним.

Запропонований метод дозволяє виявити розрядності множників в процесі дослідження числа, що факторизується, та розрядність числа k – кількості кроків до наступного цілого квадрату як єдиного розв'язку задачі факторизації. Це дозволяє проводити перебір Ферма - подібними методами в розрядності розв'язку.

В результаті дослідження процесу збіжності залишкової функції P_i*, яка визначається згідно співвідношення $P_i^* = P_0 \, mod(P* \pm 2i)$, де $i=1,...,n-1$, $P^* = \left|\sqrt{P_0}\right|$. Слід відмітити, що в результаті перетворень значення кількості змін пилкоподібної залишкової функції наближається до зони розв'язку задачі факторизації при умові: $\lim\limits_{i \to n} P_i^* \to 0$.

Вперше розроблено метод факторизації БРЧ на основі арифметики ТЧБ Радемахера – Крестенсона шляхом представлення цифрових даних у СЗК.

Згідно Ферма, проводиться пошук пар натуральних чисел, що задовільняють рівність $P_0 = A^2 – B^2$, на основі виразу:

$$\Delta_n = \sqrt{n^2 - P_0}\,, \qquad (4)$$

де $n = \left[\sqrt{P_0}\right] + k$, k=1, 2, 3, … . При цьому кількість ітерацій k дорівнюватиме тому значенню, для якого параметр Δ_n буде цілим числом. Звідси можна знайти шуканий розклад на множники:

$$P_0 = (n - \Delta_n)(n + \Delta_n). \qquad (5)$$

Табл.3. Ключ факторизації по модулях 3, 5

k	N	z_i	$(\Delta_n)^2$	p_1=3			p_2=5			Y_n
				z_1^i	Δ_n^1	y_n^1	z_2^i	Δ_n^2	y_n^2	
1	62	123	33	0	0	1	3	3	0	0
2	63	125	158	2	2	0	0	3	0	0
3	64	127	285	1	0	1	2	0	1	1
4	65	129	414	0	0	1	4	4	1	0
5	66	131	545	2	2	0	1	0	1	0
6	67	133	678	1	0	1	3	3	0	0
7	68	135	813	0	0	1	0	3	0	1
8	69	137	950	2	2	0	2	0	1	0
9	70	139	1089	1	0	1	4	4	1	1

Основна ідея розробленого методу ґрунтується на пошуку квадратичних лишків параметру Δ_n за формулою (4) при k=1. При цьому кожна наступна ітерація, яка виконується згідно властивості (1) та виразу $L_k = \sqrt{(\Delta_0)^2 + (2n-1)}$, продовжується доти, поки параметр L_k не буде цілим числом.

Слід взяти до уваги властивість, що квадрат числа по будь-якому простому модулю є квадратичним лишком по цьому ж модулю. Відповідно, знайшовши залишки даного числа за простим модулем p_j, можна отримати для нього одне із значень часткового ключа факторизації y_n^j, яке дорівнює 0 або 1. При цьому значенню 1 відповідає випадок, коли $\Delta_n^j = (\Delta_n)^2 \; mod \; p_j = (\Delta_{n-1}^j + z_j^i) mod \; p_j$ є квадратичним лишком по p_j і тоді Δ_n може бути цілим числом. Значення ключа факторизації для числа n визначається наступним чином: $Y_n = y_n^1 \wedge y_n^2 \wedge ... \wedge y_n^m$ (табл. 3). Вектор $Y(Y_1, Y_2, …, Y_n)$, в якому Y_i=0 або 1, утворює загальний ключ

факторизації. В даному прикладі Y(001000101)(див. табл. 3). Це означає, що на дев'ятій ітерації можливий випадок, коли Δ_n буде цілим числом, що і підтверджується обчисленням: $\sqrt{1089} = 33$.

Слід відмітити, що частковий ключ факторизації y_n^j володіє властивістю циклічності, період якої дорівнює модулю p_j. Тому перевагою запропонованого методу є те, що при розрахунках немає необхідності визначати всі поточні значення $(\Delta_n)^2$. При цьому число $(\Delta_n)^2$, корінь квадратний з якого може бути цілим числом (Y_n=1), отримуємо згідно формули обчислення суми арифметичної прогресії, яку утворює послідовність $(\Delta_n)^2 = (z_{i\ min} + k)(k-1) + (\Delta_n)^2_{min}$.

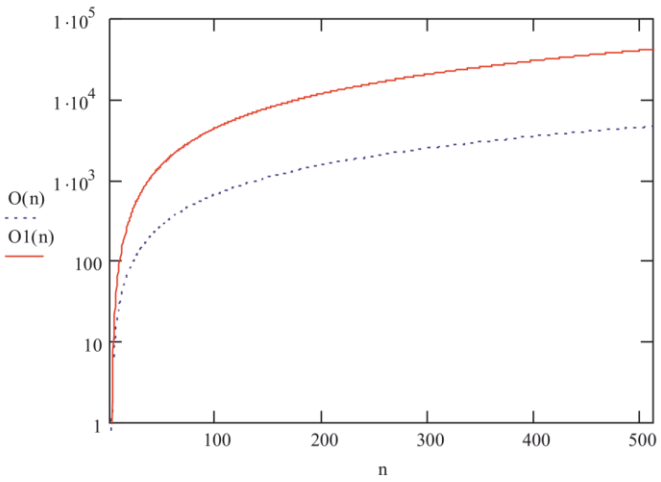

Рис.6. Порівняльна характеристика розробленого методу та методу факторизації Ферма

Крім того, можна використати іншу формулу, для класичного алгоритму Ферма:

$$(\Delta_n)^2 = (n_{min} + k - 1)^2 - P_0. \quad (6)$$

Запропонований підхід при достатньо великому модулю m, який є добутком значної кількості простих модулів, дозволяє уникнути операції перевірки кореня квадратного, а вектор Y з ознаками однозначно вкаже на розв'язок рівності (4). Ефективність використання запропонованого методу факторизації $O(n) = (n \cdot log_2 n)$ в порівнянні з методом Ферма $O1(n) = (n \cdot log_2^2 n)$ представлена на рис. 6.

Таким чином, розроблений метод факторизації з використанням СЗК дозволяє змінити зону розрядностей обчислювальних ресурсів на декілька порядків нижче по шкалі квадратів та замінити операцію знаходження кореня квадратного, на якій базується обчислювальна складність алгоритму Ферма, на операцію порівняння згенерованого ключа факторизації, що формується на основі ознак квадратичності.

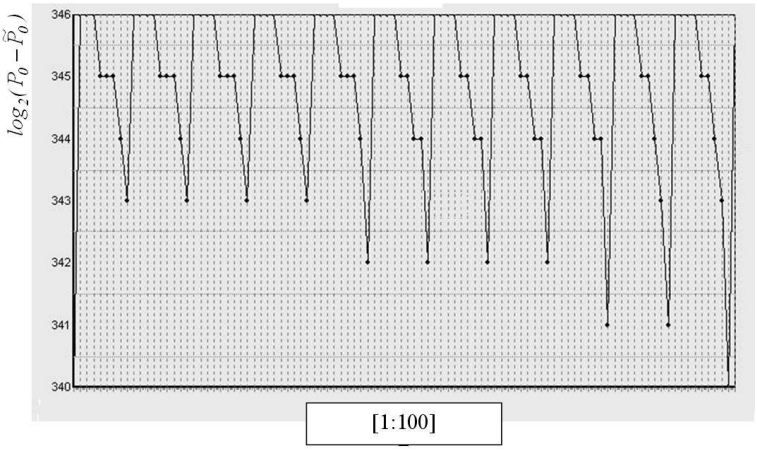

Рис.7. Моделі фракталів в околі рішень RSA 210 -696 Біт

У результаті реалізації запропонованого методу звуження околу рішення задачі для єдиного k отримуються моделі – фрактали (рис. 7), які відображають поведінку стрибків розрядностей в

залежності від значення *k*, що змінюється лінійно, тобто додаванням 1 до молодшого розряду.

Проведені дослідження показують, що зображення моделей фракталів в околі рішення задачі факторизації мають чітку структуру та дозволяють, з допомогою маніпуляцій старших розрядів множників, виявити деяку послідовність старших розрядів розв'язку. Встановлені верхні розряди розв'язків задачі факторизації призводять до зменшення необхідної кількості ітерацій для Ферма-подібних алгоритмів факторизації на декілька порядків.

У четвертому розділі представлено розроблені програмні та апаратні засоби опрацювання та факторизації БРЧ на основі описаних вище методів.

Розроблене програмне забезпечення комп'ютерного моделювання та рішення задач теорії чисел на основі застосування спеціалізованої бібліотеки А. Ленстра, об'єктно – орієнтованої мови С++. Реалізовані програмні модулі для виконання: факторизації, генерування ключа факторизації згідно модуля БРЧ, дослідження процесу факторизації, кодування простих чисел з однаковим закінченням, знаходження залишку БРЧ, реалізації елементарних операцій над БРЧ, перевірки n – розрядних чисел на простоту. Реалізація програмних засобів підтверджує ефективність розроблених методів на основі встановлених часових характеристик, що співпадають з теоретичними розрахунками часових складностей.

Структурна схема розробленого пристрою піднесення до квадрату за модулем представлена на рис. 8. Перед початком кожного циклу роботи квадратора всі Д-тригери модульних лічильників пристрою мікрокомандою скидаються в «0», крім нульового тригера, який встановлюється в стан «1». При поступанні кожного імпульсу унітарного коду числа на вхідній шині 1 у модульних лічильниках 2 накопичуються коди залишків числа імпульсів у СЗК базису Хаара-Крестенсона, що поступають на входи логічних модулів рандомізації 3. На виходах останніх формується код квадрату числа вхідних імпульсів у ТЧБ Хаара-Крестенсона, який поступає на шину пристрою 4.

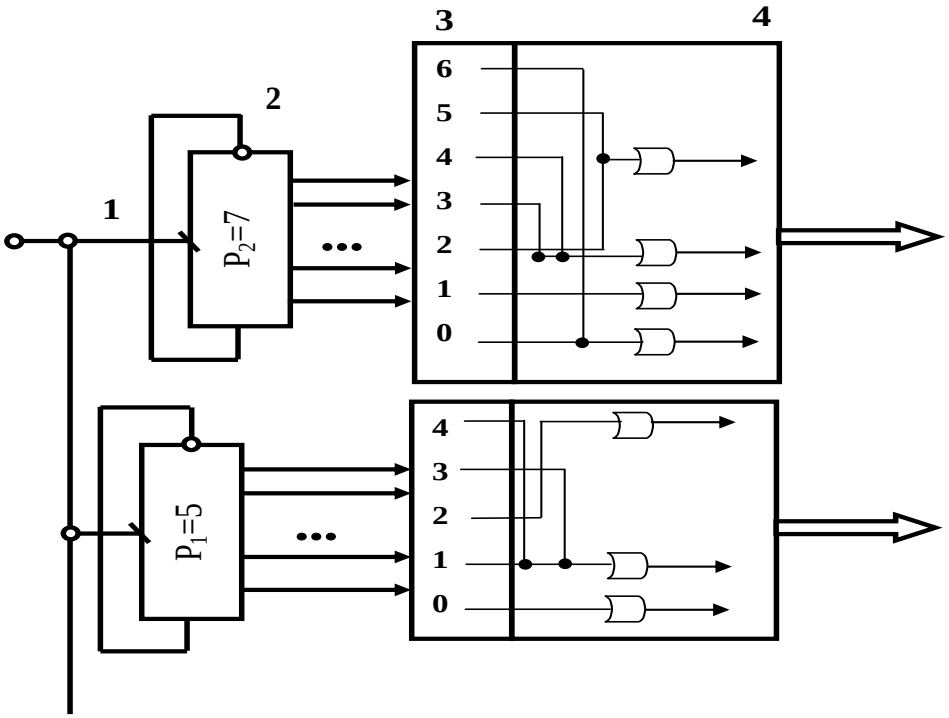

Рис.8. Структурна схема квадратора в системі взаємно простих модулів 5 і 7

Швидкодія операції піднесення чисел до квадрату у базисі Хаара-Крестенсона не залежить від числа модулів та їх розрядності. В запропонованому пристрої ця операція виконується за 3 мікротакти.

На основі розробленого методу компактного кодування БПЧ запропоновано структурну схему пристрою зберігання та генерування БПЧ (рис. 9).

В структурі пристрою функціональні модулі виконують наступні операції: БІ – блок ініціалізації, оснащений інтерфейсною шиною 1, реалізує зв'язок з зовнішнім пристроєм і виконує стартові функції: записує в ПЗП стартовий код з 15 біт молодших розрядів БПЧ, а в суматор - багаторозрядний стартовий код старших розрядів БПЧ і запускає генератор імпульсів ГІ.

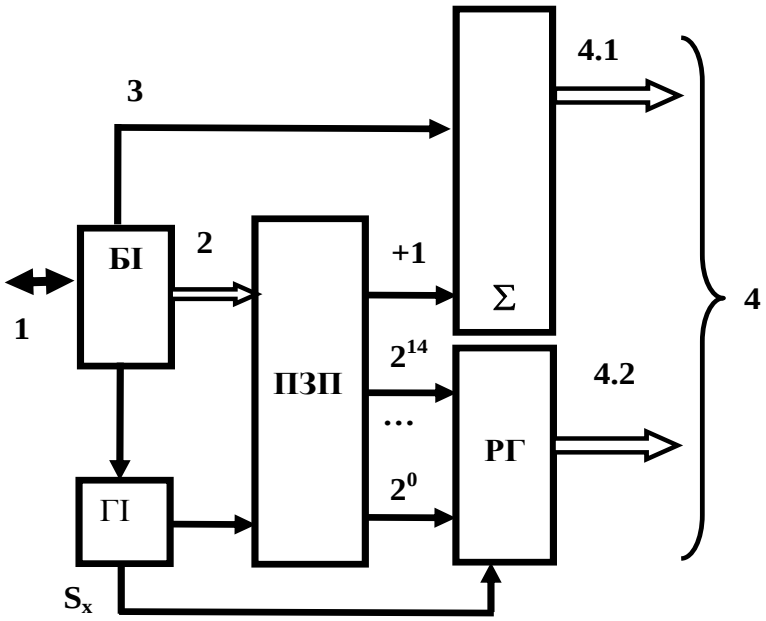

Рис.9. Структурна схема пристрою компактного кодування та генерування БПЧ

В процесі генерування імпульсів відбувається інкрементне генерування адресів ПЗП, що забезпечує генерування кодів молодших розрядів БПЧ. У момент появи біта синхронізації на виході ПЗП відбувається нарощення кодів суматора шляхом додавання 1. Перший вихід генератора інкрементно зміщує адресацію ПЗП, а другий вихід реалізує запис інформації в регістр та запис стартового коду суматора. На шині 4 формується послідовність кодів БПЧ.

В залежності від розрядності стартового коду розрядність генерованих БПЧ може довільно зростати. У результаті досягається зменшення об’єму кодів для зберігання БПЧ відповідно в межах 32 розрядів у два рази, для 256 розрядів - у 16 разів, а при 1024 розрядах - в 64 рази.

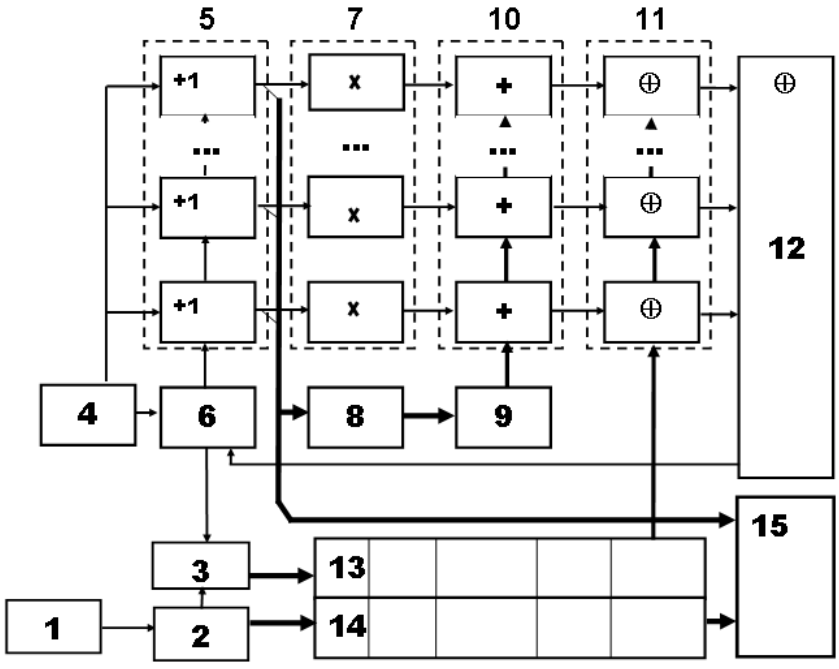

Рис.10. Функціональна схема спецпроцесора факторизації в СЗК

Розроблено функціональну структуру високопродуктивного спецпроцесора факторизації БРЧ у СЗК базису Крестенсона (рис. 10). Даний спецпроцесор призначений для

виконання операцій над двійковими БРЧ $n > 2^{10} - 2^{32}$ і реалізований на регістрах кристалів флеш-пам’яті, яка характеризується високою частотою зчитування порядку 1-2 ГГц та достатнім об’ємом пам’яті порядку 128-256 Гбайт.

Процес факторизації ініціюється блоком 4, який записує стартовий код числа ітерацій в блок 5 та виконує запуск тактового генератора 6. Під дією тактових сигналів останнього здійснюється інкрементне формування та запис зростаючих кодів СЗК у стекову асоціативну пам'ять 13, 14, а також покрокове кодування числа ітерацій у блоці 5 та їх реєстрація у блоці 15. При цьому синхронно у блоці 7 виконується піднесення числа ітерацій до квадрату, а в блоці 8 відбувається перемноження числа ітерацій на постійний код $2P_c$. В блоці 9 отримані результати додаються з кодом Δ_0. Отримана сума додається до квадратів чисел, які формуються у блоці 10. В блоці 11 відбувається порівняння отриманої суми блоку 10 з усіма кодами асоціативної пам’яті 13. У випадку співпадіння одного з кодів, що визначається блоком 12, його вихідний сигнал зупиняє тактовий генератор 6. При цьому на виході 15 реєструється код числа ітерацій та кореня квадратного асоціативної пам’яті 14, що є завершенням процесу факторизації.

Введення виконання операції факторизації БРЧ на основі представлення чисел у СЗК дозволяє в $k \cdot log_2 n$ разів підвищити ефективність спецпроцесора шляхом виконання модульних операцій за 2 - 4 мікротакти. Останні не містять наскрізних переносів і їх швидкодія не залежить від розрядності чисел, які факторизуються.

Експериментальний зразок високопродуктивного спецпроцесора факторизації БРЧ реалізовано на платі AlteraCyclone і передано ТОВ «Стріла» та ТОВ «Інтеграл» в якості компоненти процесу шифрування та дешифрування інформаційних потоків дистрибутивних та корпоративних комп’ютерних мереж.

У додатках наведено лістинг програмних модулів для виконання процесу факторизації розробленими методами, визначення квадратичності лишку, кодування та зберігання простих БРЧ та реалізації схем основних компонентів спеціалізованого процесора факторизації БРЧ. Подані документи про використання результатів дисертаційної роботи.

ВИСНОВКИ

У дисертаційній роботі розв’язано науково-практичну задачу розробки методів та обчислювальних засобів рішення задач теорії чисел у базисах Радемахера - Крестенсона:

1. Проаналізовані і досліджені архітектури спецпроцесорів та методи опрацювання багаторозрядних чисел для задач теорії чисел, способи кодування даних в комп’ютерних системах на основі різних теоретико-числових базисів та існуючі алгоритми факторизації. Обґрунтовано перспективи застосування різних теоретико - числових базисів при розв’язанні задач теорії чисел та виконана постановка завдання досліджень.

2. Отримано аналітичні вирази характеристик складності формування й опрацювання багаторозрядних чисел в задачах теорії чисел, перевірки на

простоту, модулярного множення, визначення квадратичних лишків, які склали теоретичну основу спрощення часових характеристик компонентів методу факторизації та зменшення часової складності.

3. Розроблено метод компактного кодування масивів багаторозрядних простих чисел шляхом зберігання молодших двійкових розрядів та інкрементного нарощення кодів старших розрядів, який призводить до зменшення об'єму необхідної пам'яті на один-два порядки при зростанні розрядності генерованих простих чисел.

4. Розроблено метод факторизації багаторозрядних чисел шляхом вдосконалення та спрощення алгоритму Ферма та виконання модульних обчислювальних операцій у базисі Радемахера-Крестенсона, що дозволило, у порівнянні з відомими методами, зменшити обчислювальну складність з $n \cdot log_2^2 n$ до $n \cdot log_2 n$.

5. Розроблено метод визначення околу рішення задачі факторизації для багаторозрядних чисел врахуванням симетричності екстремумів залишкової функції, графічної ідентифікації моделей фракталів та матричного представлення добутків багаторозрядних чисел у базисі Радемахера, що дозволило підвищити швидкодію алгоритму більш, ніж в два рази.

6. Розроблено високопродуктивні методи визначення квадратичних лишків та векторно - модульного множення багаторозрядних чисел у базисі Радемахера - Крестенсона, які, порівняно з відомими, забезпечують підвищення швидкодії обчислень на один – два порядки.

7. Розроблено функціональні та структурні рішення пристроїв компактного кодування багаторозрядних простих чисел, квадратора та спецпроцесора факторизації багаторозрядних чисел у базисі Радемахера та Хаара - Крестенсона, які, в порівнянні з існуючими, забезпечують зменшення об'єму кодів пам'яті в 4-16 разів при розрядностях 32-128 та підвищують швидкодію квадратора та спецпроцесора факторизації на 2-3 порядки.

8. Розроблено програмне забезпечення комп'ютерного моделювання та рішення задач теорії чисел в базисі Радемахера - Крестенсона на основі застосування спеціалізованої бібліотеки А. Ленстра, об'єктно – орієнтованої мови С++, засобів VHDL для проектування на ПЛІС, що підтверджують збігання з теоретичними розрахунками.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Стаття у закордонному журналі

1. Николайчук Я.М. Метод факторизации многоразрядных чисел на основе свойств квадратичности вычетов в системе остаточных классов / Я. Н. Николайчук, С.В. Ивасьев, И.З. Якименко, М.Н. Касянчук // Вестник Брестского государственного технического университета. – 2015. – № 5(95): Физика, математика, информатика. – С. 42–45.

Статті у спеціалізованих фахових виданнях

2. Івасьєв С.В. Метод факторизації велико-розрядних чисел в базисі Радемахера / С.В. Івасьєв // Вісник Національного університету “Львівська політехніка”, Комп’ютерні системи та мережі. – Львів. – 2012. – №745. – С. 118–126.
3. Николайчук Я. М. Ефективний метод модулярного множення в теоретико-числовому базисі Радемахера–Крестенсона / Я.М. Николайчук, М.М. Касянчук, І.З. Якименко, С.В. Івасьєв // Вісник Національного університету «Львівська політехніка». Комп’ютерні системи та мережі. – 2014. – № 806. – С. 195-199.
4. Івасьєв С.В. Вдосконалений алгоритм пошуку символів Якобі / С.В. Івасьєв, І.З. Якименко, М.М. Касянчук // Методи та системи оптико-електронної і цифрової обробки зображень та сигналів. – 2015. – Том 29, № 1 (2015). – С. 45-50.
5. Івасьєв С.В. Збіжність екстремумів залишкової функції в околі розв’язку задачі факторизації / С.В. Івасьєв, Я.М. Николайчук, І.З. Якименко, І.Р. Колісник // Вісник Хмельницького національного університету. Технічні науки. – 2015. – №4. – С.157 – 164.
6. Timoshenko L.M. Factorization algorithms for cryptographic analisis of asymmetric crypto systems/ L.M. Timoshenko, K.V. Verbik, Ya.M. Nikolaichuk, S.V. Ivasiev // Informatics and Mathematical Methods in simulation. – 2014. – vol 4. - №4. – P. 342 -348.

Статті та друковані праці конференцій

7. Тимошенко Л.М. Удосконалення алгоритму факторизації для криптографічних систем захисту інформації / Л.М. Тимошенко, С.В. Івасьєв, К.В. Вербик // Сучасна спеціальна техніка. – 2014. –№ 3(38). – С 56-59.
8. Kozaczko D. Vector Module Exponential in the Remaining Classes System / D. Kozaczko, S. Ivasiev, I.Yakymenko, M. Kasianchuk / Proceedings of the 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS–2015) – Warsaw, Poland. – V.1. – September, 2015. – P.161–163. (індексована наукометричною базою Scopus).
9. Kasjanchuk M. Fundamental theoretical and algorithmic principles of the appli-ed tasks decision of theory of numbers and construction of the high-performance spe-cial processors on their basis / M. Kasjanchuk, I. Yakymenko, S. Ivasiev, Ya. Nykolaychuk / XI International Conference “The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM-2011)”, 23-25 February, 2011, Polyana-Svalyava (Zakarpattya), Ukraine. – P.168-169. (індексована наукометричною базою Scopus).
10. Ivasiev S. Fundamental Backgrounds of the Discrete Logarithms Theory in the Rademacher-Krestensons Basis / Stepan Ivasiev, Mykhajlo Kasyanchuk, Ihor Pazdriy, Rostyslav Trembach, Ihor Yakymenko / Proceedings of the XI-th International conference “Modern Problems of Radio Engineering,

Telecommunications and Computer Science" (TCSET-2012). – Lviv-Slavsk. – P.93. (індексована наукометричною базою Scopus).

11. Kasianchuk M. Efficient methods for modular multiplication through the use of Rademacher- Krestenson TNB / M. Kasianchuk, I. Yakymenko, S. Ivasiev, Ya.Nykolaychuk / Proceedingsofthe XI–th International Conference "Modern Problems of RadioEngineering, Telecommunications and ComputerScience" (TCSET–2014).–L'viv–Slavske.– 2014. – P.93-94.
12. Касянчук М.М. Векторно-модульний метод множення багаторозрядних чисел в базисі Рademахера-Крестенсона / М.М. Касянчук, І.З. Якименко, Я.М.Николайчук, С.В. Івасьєв / Матеріали Міжнародної конференції "Захист інформації і безпека інформаційних систем - 2014", Львів, 2014. – С. 53-54.
13. Івасьєв С.В. Метод організації компактної бібліотеки простих чисел великої розрядності / С.В. Івасьєв // Збірник матеріалів міжнародної наукової координаційної наради «Інформаційні проблеми комп'ютерних систем, юриспруденції, енергетики, економіки, моделювання та управління» (ICSM). – Тернопіль, 2014 р. – С. 86-89.
14. Касянчук М.М. Теоретичні основи аналітики та алгоритми оптимізації обчислень простих чисел. / М.М. Касянчук, І.З. Якименко, О.І. Волинський, С.В. Івасьєв // Проблемно-наукова міжгалузева конференція «Інформаційні проблеми комп'ютерних систем, юриспруденції, енергетики, економіки, моделювання та управління. – Бучач, – 2010. - С.33-36.
15. Івасьєв С.В. Метод знаходження залишків велико-розрядних чисел в базисі Рademахера / С.В. Івасьєв, О.І.Волинський // Поступ в науку : збірник наукових праць Бучацького інституту менеджменту і аудиту. – 2011. – Т1.- №7.–С.88-91.
16. Касянчук М.М. Теорія та оптимізація алгоритмів опрацювання великорозрядних чисел у базисі Крестенсона /М.М. Касянчук, І.З.Якименко, С.В. Івасьєв // Праці міжнародної молодіжної математичної школи "Питання оптимізації обчислень (ПОО-XXXVII)". – К.: Інститут кібернетики імені В.М. Глушкова НАН України, 2011. – С. 67-68.
17. Якименко І.З. Метод зберігання простих великорозрядних чисел у базисі Рademахера / І.З. Якименко, М.М. Касянчук, С.В. Івасьєв// Праці міжнародної молодіжної математичної школи "Питання оптимізації обчислень (ПОО-XXXVII)". – К.: Інститут кібернетики імені В.М. Глушкова НАН України, 2013. – С. 142-144.
18. Николайчук Я.М. Фундаментальні засади теорії факторизації багаторозрядних чисел на основі фракталів зображень в околі рішення / Я.М.Николайчук, С.В.Івасьєв // Збірник матеріалів міжнародної наукової координаційної наради «Інформаційні проблеми комп'ютерних систем, юриспруденції, енергетики, економіки, моделювання та управління» (ICSM). – Тернопіль, 2014 р. – С. 116-120.
19. Николайчук Я.М. Метод збереження простих великорозрядних чисел у базисі Рademахера / Я.М. Николайчук, І.З. Якименко, М.М. Касянчук, С.В. Івасьєв // Праці міжнародної молодіжної математичної школи "Питання оптимізації обчислень (ПОО-XXXVII)" Київ: Інститут кібернетики імені В.М. Глушкова НАН України, 2015. – С. 159 – 161.

20. Николайчук Я.М. Метод факторизації багаторозрядних чисел та дослідження в околі розв'язання задач / Я.М. Николайчук, С.В. Івасьєв // Матеріали XIV Міжнародного наукового семінару “Сучасні проблеми інформатики в управлінні, економіці та освіті”. Київ-Шацьк, 2015. – С.83-88.

АНОТАЦІЇ

Івасьєв С.В. Методи та обчислювальні засоби рішення задач теорії чисел у базисах Радемахера - Крестенсона. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05− комп’ютерні системи та компоненти. − Тернопільський національний економічний університет, Тернопіль, 2016.

В дисертаційній роботі на основі розроблених методів обчислень у базисах Радемахера-Крестенсона та алгоритмів факторизації багаторозрядних чисел, компактного кодування багаторозрядних простих чисел, знаходження залишків багаторозрядних чисел, модулярного множення, визначення квадратичності лишку числа за модулем, визначення околу рішення задачі факторизації отримані аналітичні вирази характеристик складностей, які, порівняно з існуючими, характеризуються меншою часовою складністю, розширеними функціональними можливостями, в тому числі щодо зменшення на порядок об’єму необхідної пам’яті при збереженні багаторозрядних простих чисел.

Реалізовано на базі С++ основні компоненти, що відповідають теоретично розрахованим параметрам і підтверджують правильність та результативність запропонованого наукового підходу з вдосконалення методів і алгоритмів опрацювання багаторозрядних та багаторозрядних простих чисел для прикладних задач теорії чисел.

Розроблено схемотехнічні рішення генератора квадратів БРЧ у базисі Крестенсона, процесора факторизації багаторозрядних чисел у базисі Хаара – Крестенсона та пристрою кодування багаторозрядних простих чисел.

Ключові слова: часова складність, теоретико-числовий базис Радемахера-Крестенсона, факторизація, модулярне множення, квадратичний лишок.

Ивасьев С.В. Методы и вычислительные средства решения задач теории чисел в базисах Радемахера - Крестенсона. - Рукопись.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.05- компьютерные системы и компоненты. - Тернопольский национальный экономический университет, Тернополь, 2016.

В диссертационной работе представлены теоретические обоснования и новое решение научной задачи разработки и усовершенствования методов повышения производительности и уменьшения временной сложности программной и аппаратной реализации алгоритмов факторизации многоразрядных чисел, проверки на простоту, компактного кодирования простых чисел, вычисления остатков многоразрядных чисел, модулярного умножения, определения квадратичности остатка числа по модулю в теоретико-числовом базисе

Радемахера-Крестенсона для прикладных задач теории чисел.

Впервые предложены методы компактного кодирования массивов многоразрядных простых чисел, которые базируются на хранении ограниченного числа динамически кодированных младших разрядов их двоичного представления в базисе Радемахера и инкрементном разрядно-позиционном наращивании их более высоких разрядов, что позволило уменьшить на порядок объем требуемой памяти, а также факторизации многоразрядных чисел на основе арифметики теоретико-числового базиса Радемахера-Крестенсона путем представления цифровых данных в системе остаточных классов, что позволило уменьшить разрядности операндов, упростить алгоритм поиска факторизированних чисел и повысить быстродействие алгоритма вычислений.

Усовершенствован метод определения окрестности решения задачи факторизации путем вычисления двоичного логарифма разницы между известным числом и факторизируемим произведением, которое исчисляется итерационно, что дает возможность ускорить определение двоичной разрядности числа итераций с полиноминальной сложностью в сравнении с существующими методами экспоненциальной сложности.

Получили дальнейшее развитие методы векторно-модульного модулярного умножения в теоретико-числовом базисе Радемахера-Крестенсона, поиск квадратичных вычетов в кодовой системе базиса Крестенсона, которые характеризуются повышенным быстродействием и меньшей вычислительной сложностью

Реализовано на базе С ++ основные компоненты, которые соответствуют теоретически рассчитанным параметрам и подтверждают правильность и результативность предложенного научного подхода по совершенствованию методов и алгоритмов обработки многоразрядных чисел и многоразрядных простых чисел для прикладных задач теории чисел.

Разработано схемотехнические решения генератора квадратов многоразрядных чисел в базисе Крестенсона и процессора факторизации многоразрядных чисел в базисе Хаара-Крестенсона.

Ключевые слова: временная сложность, теоретико-числовой базис Радемахера - Крестенсона, факторизация, модулярное умножение, квадратичный вычет.

Ivasiev S.V. Methods and Computational Tools for Solving the Problems in Theory of Numbers for Rademacher’s and Krestenson’s Basis. – Manuscript.

The thesis for the degree of candidate of technical sciences, specialty 05.13.05- Computer Systems and Components. - Ternopil National Economic University, Ternopil, 2016.

The analytical expressions for characteristics of complexity, which are characterized by a lower temporal complexity in comparison with the existing, enhanced functional capabilities and reduce the amount of required memory procedure while maintaining big numbers have been obtained in this thesis on the basis of the developed methods of calculations in the Rademacher’s and Krestenson’s Basis and big

numbers factorization algorithm, big prime numbers compact coding, finding residues of big numbers, modular multiplication, determining quadratic residue of a number by module, method of determining the vicinity for solving the problems of factorization for the computer system.

The main components that meet the theoretically calculated parameters and confirm the correctness and effectiveness of the proposed scientific approach to improve methods and algorithms for processing big and big prime numbers for applied tasks in the theory of numbers has been implemented on the basis in C ++.

Circuit engineering solutions for generator of squares big numbers in the Krestenson's Basis and the processor for factorization of big numbers in Haar-Krestenson's Basis.

Key words: temporal complexity, Rademacher's and Krestenson's theoretical and numeral bases, factorization, modular multiplication, quadratic residue.

Підписано до друку 25.05.2016 р.
Формат 60х84/16. Гарнітура Times.
Папір друк. Друк офсетний.
Умов. друк. арк. 0,9. Обл.-вид. арк. 0,9.
Наклад 100 прим. Зам. № 05/16/3-5

Віддруковано у видавничому центрі "Вектор"
46018, м. Тернопіль, вул. Львівська, 12,
Тел. 8 (0352) 40-08-12

Свідоцтво про внесення суб'єкта видавничої справи
до державного реєстру видавців, виготівників
і розповсюджувачів видавничої продукції
серія ТР № 46 від 07 березня 2013р.
ФО Осадца Ю.В.