З рис. 13 видно, що ємнісні сенсори сили мають лінійну залежність ємності від сили дотику та дають змогу вимірювати відносний рівень сили з певною роздільною здатністю. Тому для реалізації інтерфейсу користувача з використанням сили дотику можна використати резистивні сенсори сили фірм Interlink та IEE з вимірюванням опору та класичні ємнісні сенсори сили.

Висновки. Показано наявні на ринку сенсори сили та проведено аналіз їх лінійності та роздільної здатності. Запропоновано схеми вимірювання сили на базі програмованої системи на кристалі (ПСнК) фірми Cypress. Наведено числові результати досліджень сенсорів провідних фірм виробників (IEE, Interlink, Click Touch).

1. Apple website. http://www.apple.com/iphone/, 2010. 2. Cypress website. http://www.cypress.com/capsense/. 2010. 3. Analog Devices website. http://www.analog.com, 2010. 4. Introducing to mTouch Capacitive Touch Sensing. Microchip website. http://techtrain.microchip.com, 2010. 5. PE website. http://www.pe-icdesign.de, 2010. 6. QMatrix Technology White Paper, Quantum & Atmel, Quantum http://data.qprox.com, 2010. 7. Omron website, http://www.omron.co.jp, 2010. 8. Touch Panel System Using MC34940/MC33794 E-Field Sensors, Frescale Semiconductor, www.freescale.com, 2010. 9. Synaptics website, http://www.synaptics.com/technology, 2010. 10. Interlink Electronics, Sensor Technologies, http://www.interlinkelec.com, 2010. 11. IEE, A Sense for Innovation, http://www.iee.lu, 2010. 12. ClickTouch, http://www.clicktouch.be, 2010.

УДК 681.31

М.М. Касянчук, Я.М. Николайчук, І.З. Якименко
Інститут проблемно-орієнтованих комп'ютерних систем КД ЦІЗІТ НАН України

ТЕОРІЯ АЛГОРИТМІВ ПЕРЕТВОРЕНЬ КИТАЙСЬКОЇ ТЕОРЕМИ ПРО ЗАЛИШКИ В МАТРИЧНО–РОЗМЕЖОВАНОМУ БАЗИСІ РАДЕМАХЕРА–КРЕСТЕНСОНА

Описано принципово новий метод виконання перетворень при застосуванні Китайської теореми про залишки та пошуку оберненого елемента, уникаючи громіздких операцій ділення з остачею, факторизації та піднесення до степеня багаторозрядних чисел. Здійснено порівняльний аналіз обчислювальних складностей класичного та запропонованого алгоритмів.

The paper describes crucially new method due to performance of transformation under the implementation of Chinese reminder theorem and inverse elements finding, without the bulky operations of division with remainder, factorization and exponentiation of multibit numbers. The comparative analisys of computational complexity of classical and the proposed algorithms was performed.

Вступ. Перетворення Китайської теореми про залишки (КТЗ) [1] є фундаментальною основою вирішення широкого класу задач теорії чисел, а також прикладних задач інженерії та інформатики.

Незважаючи на свою простоту та древню історію, КТЗ продовжує представляти себе у новому світлі і відкривати нові перспективи свого застосування, особливо у математиці, інформатиці (машинна арифметика) [2], криптографії [3] тощо. Побудова непозиційної системи

числення в обчислювальних системах (системи залишкових класів) для виконання операцій з великими числами [4], дискретне перетворення Фур'є, генерування таємних ключів в асиметричних криптосистемах [5], зв'язок з класичною поліноміальною інтерполяційною теорією, багатовимірні обчислення, можливість зведення вивчення кільця лишків за модулем m (де m – довільне ціле число) до вивчення кільця лишків за модулем p^s (p – просте число), дослідження алгебраїчних кілець, можливість арифметичної самокорекції кодів та розпаралелення обчислень, визначення послідовності великого числа зразків ДНК – ось далеко не повний перелік сучасного застосування КТЗ.

Аналіз публікацій і окреслення проблеми. КТЗ є одним з найдавнішим, але важливим обчислювальним алгоритмом. Ще в першому столітті нашої ери китайський математик Сунь–Цзи придумав загадку, якою було покладено початок модулярній арифметиці: знайти число, яке при діленні на 3 дасть в остачі 2, на 5 – 3, на 7 – 2. Крім того, він показав у частковому випадку еквівалентність розв'язку системи модулярних рівнянь і розв'язку одного модулярного рівняння.

Протягом майже двох тисяч років КТЗ постійно вдосконалювалася та розвивалася. Зокрема, в XIII столітті інший китайський математик Цань Цзю–шао розв'язав наведену вище задачу. У XVIII столітті німецький математик Л.Ейлер навів загальне формулювання та доведення КТЗ, а К.–Ф. Гаусс істотно розвинув його у своїх знаменитих „Арифметичних дослідженнях".

І, нарешті, в середині XX століття чеські учені М. Валах та А. Свобода запропонували використати древню китайську ідею на новому технічному рівні, створивши перші модулярні електронно–обчислювальні машини „Епос" та „Епос–2". Їх ідеї підтримали радянські та українські вчені Ф. Лукін, І. Акушський, Д. Юдіцький, Є. Адріанов, В. Амербаєв, Я. Николайчук та інші.

Слід зазначити, що сьогодні існує декілька еквівалентних формулювань КТЗ. Найпоширеніше з них таке [6]: якщо натуральні числа $p_1, p_2, \ldots, p_k$ попарно взаємно прості, то для будь-яких цілих $r_1, r_2, \ldots, r_k$, таких що $0 \le r_i < p_i$, існує число N, яке при діленні на p_i дає залишок r_i при всіх i=1, 2, ..., k; більше того, якщо існує два такі числа N_1 та N_2, то $N_1 \bmod P = N_2 \bmod P$, де $P = \prod_{i=1}^{k} p_i$.

Цю теорему можна можна подати у вигляді системи порівнянь [7]:

$$\begin{cases} N \bmod p_1 = r_1 \\ N \bmod p_2 = r_2 \\ \ldots\ldots\ldots\ldots\ldots \\ N \bmod p_i = r_i \\ \ldots\ldots\ldots\ldots\ldots \\ N \bmod p_k = r_k. \end{cases} \qquad (1)$$

Шукане число обчислюється за формулою:

$$N = \left(\sum_{i=1}^{k} M_i m_i r_i \right) \bmod P, \qquad (2)$$

де $M_i = \frac{P}{p_i} = p_1 p_2 \ldots p_{i-1} p_{i+1} \ldots p_k$, $m_i = M_i^{-1} \bmod p_i$.

Зазначимо, що сьогодні відомі три способи пошуку оберненого елемента m_i:

1) перевірка шляхом послідовної підстановки чисел натурального ряду у формулу, поки не буде виконуватись умова $M_i m_i \bmod p_i = 1$;

2) використовуючи функцію Ейлера, можна знайти $m_i = M_i^{-1} \bmod p_i = M_i^{\varphi(p_i)-1} \bmod p_i$ [4];

3) за допомогою розширеного алгоритму Евкліда [6].

Однак кожен з цих способів характеризується значною обчислювальною складністю при виконанні ділень з остачею, піднесення до степеня, знаходженні функції Ейлера (факторизації p_i). Причому всі ці операції повинні виконуватися над дуже великими числами, що приводить до переповнення розрядної сітки сучасних потужних обчислювальних засобів.

Професор Я.М. Николайчуком запропонував досконалу форму системи залишкових класів, у якій підбір модулів такий, що $M_i \bmod p_i = 1, m_i = 1$ [8]. У циклі робіт [9–11] було розвинуто цю теорію та розроблено її модифікований варіант, коли $M_i \bmod p_i = \pm 1, m_i = \pm 1$, тобто відповідний підбір модулів дає змогу уникнути процедури знаходження оберненого елемента. Недолік цього методу полягає в тому, що не завжди є можливість вибору відповідної системи модулів.

Мета роботи. Метою роботи є розроблення принципово нового методу перетворень при використанні КТЗ та пошуку оберненого елемента з меншою обчислювальною складністю, уникаючи громіздких операцій ділення з остачею, факторизації та піднесення до степеня багаторозрядних чисел.

Теоретичні основи алгоритмів перетворення КТЗ в базисі Радемахера–Крестенсона. Для спрощення розглянемо два взаємно прості модулі $p_1 < p_2$. Нехай потрібно знайти число N, яке при діленні на p_1 дає залишок r_1, а при діленні на p_2 – залишок r_2 [6], що еквівалентно такій системі порівнянь [1]:

$$\begin{cases} N \bmod p_1 = r_1 \\ N \bmod p_2 = r_2. \end{cases} \tag{3}$$

Відповідно до (2), розв'язок (3) можна подати у вигляді:

$$N = \left(r_1 p_2 \left(p_2^{-1} \bmod p_1\right) + r_2 p_1 \left(p_1^{-1} \bmod p_2\right)\right) \bmod p_1 p_2. \tag{4}$$

Для знаходження $p_2^{-1} \bmod p_1$ подамо p_2 у двійковій формі: $p_2 = a_{n-1}2^{n-1} + a_i \cdot 2^i + \ldots + a_1 \cdot 2^1 + a_0 \cdot 2^0$, де $a_i = 0,1$ і сформуємо табл. 1.

Таблиця 1

Знаходження залишків степенів двійки

2^{n-1}	2^{n-2}	…	2^i	…	2	1
a_{n-1}	a_{n-2}	…	a_i	…	a_1	a_0
$p_{2\,n-1}$	$p_{2\,n-2}$	…	$p_{2\,i}$	…	$p_{2\,1}$	$p_{2\,0}$

Щоб знайти елемент p_{2i}, необхідно попередній елемент p_{2i-1} домножити на 2 (дописати в кінці 0 у двійковому записі) і порівняти з модулем p_1. Остаточна формула для p_{2i} матиме такий вигляд:

$$p_{2i} = \begin{cases} 2 \cdot p_{2\,i-1}, & 2 \cdot p_{2\,i-1} < p_1; \\ 2 \cdot p_{2\,i-1} - p_1, & 2 \cdot p_{2\,i-1} \geq p_1. \end{cases} \tag{5}$$

Отже, уникнувши громіздкої операції ділення, знаходимо залишок $p_3 = p_2 \bmod p_1$. Він дорівнюватиме сумі тих p_{2i}, для яких відповідні $a_i = 1$. Тоді $p_2^{-1} \bmod p_1 = p_3^{-1} \bmod p_1$.

Для знаходження оберненого елемента знову ж шукаємо залишок $p_1 \bmod p_3 = p_{10}$. Оскільки $p_{10} \neq 0$, то далі виконується така послідовність кроків: $(p_1+1) \bmod p_3 = (p_{10}+1) \bmod p_3 = p_{11}$; $(2p_1+1) \bmod p_3 = (p_{11}+p_1) \bmod p_3 = p_{12}$; …. ; $(i \cdot p_1+1) \bmod p_3 = (p_{1i-1}+p_1) \bmod p_3 = p_{1i}$; … . Описану послідовність продовжуємо доти, поки p_{1i} не дорівнюватиме нулю. Зазначимо, що процедура знаходження p_{1i} аналогічна визначенню залишку p_3.

Обернений елемент $p_2^{-1} \bmod p_1$ дорівнюватиме результату ділення $(i \cdot p_1+1)$ на p_3. Для уникнення цієї громіздкої операції потрібно описаним вище методом знайти залишки

$b_i=(i\cdot p_1+1) \bmod p_3\cdot q_i^s$, де q_i пробігає послідовність простих чисел, $p_3\cdot q_i^s <(i\cdot p_1+1)$, s=1, 2, … , причому *s* збільшується на 1, коли $b_i=0$. Шукане обернене число p_2^{-1} дорівнюватиме добутку тих q_i^s, для яких відповідні $b_i=0$. Аналогічним алгоритмом шукається $p_1^{-1} \bmod p_2$.

Наступним кроком є обчислення добутків трьох множників за модулем P у кожному доданку (4). Операцію множення пропонуємо виконати матричним методом, що істотно зменшує обчислювальну складність.

Розглянемо два числа $x=x_{n-1}2^{n-1}+\ldots+x_i2^i+\ldots+x_12+x_0$ та $y=y_{n-1}2^{n-1}+\ldots+y_j2^j+\ldots+y_12+y_0$, де x_i, y_j=0, 1, n–розрядність модуля P. Для знаходження результату їх множення за модулем P побудуємо матрицю, наведену в табл. 2, де $c_{ij}=2^{i+j} \bmod P$.

Таблиця 2

Матриця для множення двох n–розрядних двійкових чисел

	b_{n-1}	…	b_j	…	b_1	b_0
a_{n-1}	$c_{n-1\ n-1}$	…	$c_{n-1\ j}$	…	$c_{n-1\ 1}$	$c_{n-1\ 0}$
…	…	…	…	…	…	…
a_i	$c_{i\ n-1}$	…	c_{ij}	…	c_{i1}	c_{i0}
…	…	…	…	…	…	…
a_1	$c_{1\ n-1}$	…	c_{1j}	…	c_{11}	c_{10}
a_0	$c_{0\ n-1}$	…	c_{0j}	…	c_{01}	c_{00}

Добуток чисел *x* та·*y* отримуємо за формулою:

$$x \cdot y = \left(\sum_{m,k=1}^{n-1} c_{mk} \right) \bmod P, \qquad (6)$$

де x_m, y_k=1, тобто c_{mk} знаходиться на перетині стовпця та рядка, для яких відповідні x_i та y_j дорівнюють 1.

Останнім кроком знаходження шуканого числа N є визначення суми двох чисел за модулем P.

Застосування запропонованих алгоритмів. Розглянемо приклад. Нехай потрібно знайти число N, яке при діленні на p_1=43 дає остачу r_1=10, а при діленні на p_2=209 – остачу r_2 =100 (P=209·43=8987).

Знайдемо p_3=209 mod 43 матричним методом, представленим у табл. 3.

Таблиця 3

Знаходження залишку за модулем

2^i	128	64	32	16	8	4	2	1
209	1	1	0	1	0	0	0	1
$2^i mod$ 43	42	21	32	16	8	4	2	1

Отже, p_3=(42+21+16+1) mod 43=37. Далі знаходимо $p_3^{-1} \bmod 43 = 37^{-1} \bmod 43$. Шукаємо 43 mod 37=6, додаємо 1 і послідовно додаємо 6, поки в результаті додавання за mod 37 не буде 0. Подамо це у вигляді табл. 4.

Таблиця 4

Пошук оберненого елемента за модулем

i	0	1	2	3	4	5	6
p_{1i}	6	7	13	19	25	31	0

Звідси число K_1=6·43+1, яке націло ділиться на 37. Добуток 6·43 знайдемо також матричним методом, представленим у табл. 5, записавши обидва множники у двійковій формі: $6=(110)_2$; $43=(101011)_2$.

Таблиця 5

Множення двох n–розрядних двійкових чисел

	0	0	0	1	1	0
1	1024	512	256	128	64	32
0	512	256	128	64	32	16
1	256	128	64	32	16	8
0	128	64	32	16	8	4
1	64	32	16	8	4	2
1	32	16	8	4	2	1

Отже, K_1=6·43+1=(128+64+32+16+8+4+4+2)+1=259. Діленням можна знайти, що $p_3^{-1} \bmod p_1$ = 37^{-1}mod 43=259:37=7. Матричним методом це представлено в табл. 6 (не перевіряючи парного простого числа 2).

Таблиця 6

Пошук оберненого елемента 37^{-1}mod 43

2^i	256	128	64	32	16	8	4	2	1	
259	1	0	0	0	0	0	0	1	1	
2^imod 3·37	34	17	64	32	16	8	4	2	1	(34+2+1)mod 111=37
2^imod 5·37	71	128	64	32	16	8	4	2	1	(71+2+1)mod 185=74
2^imod 7·37	256	128	64	32	16	8	4	2	1	(256+2+1)mod 259=0

Звідси видно, що $p_3^{-1} \bmod p_1$ =37^{-1}mod 43=7. Далі шукаємо $p_1^{-1} \bmod p_2$ =43^{-1}mod 209. Вище було знайдено, що 209 mod 43=37. Будуємо табл. 7.

Таблиця 7

Пошук оберненого елемента 43^{-1}mod 209
в розмежованому базисі

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
p_{2i}	37	38	32	26	20	14	8	2	39	33	27	21	15	9	3	40	34	28	22
i	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	
p_{2i}	16	10	4	41	35	29	23	17	11	5	42	36	30	24	18	12	6	0	

Тоді K_2=36·209+1=7525 і $p_1^{-1} \bmod p_2$ =43^{-1}mod 209=7525:43=175. Матричним методом отримуємо аналогічний результат, представлений у табл. 8.

Таблиця 8

Пошук оберненого елемента 43^{-1}*mod* 209
матричним методом

2^i	4096	2048	1024	512	256	128	64	32	16	8	4	2	1	
7525	1	1	1	0	1	0	1	1	0	0	1	0	1	
2^imod 3·43	97	113	121	125	127	128	64	32	16	8	4	2	1	(97+113+121+ +127+64+32+ +4+1) mod 129=45
2^imod 5·43	11	113	164	82	41	128	64	32	16	8	4	2	1	(11+113+164 +41+64+32+ +4+1)mod 215=0
2^imod 5^2·43	871	973	1024	512	256	128	64	32	16	8	4	2	1	(871+973+1024+ +256+64+32+4+ +1)mod 1075=0

Продовження табл. 8

$2^i \bmod 5^3 \cdot 43$	4096	2048	1024	512	256	128	64	32	16	8	4	2	1	(4096+2048+1024+ +256+64+32+4+ +1)mod 5375=2150
$2^i \bmod 5^2 \cdot 7 \cdot 43$	4096	2048	1024	512	256	128	64	32	16	8	4	2	1	(4096+2048+1024+ +256+64+32+4+ +1)mod 7525=0

Отже, $p_1^{-1} \bmod p_2 = 43^{-1} \bmod 209 = 5^2 \cdot 7 = 175$. Звідси видно, що шукане число: N=(209·7·10+ +43·175·100) mod 8987=3235.

Оцінка та порівняльний аналіз обчислювальних складностей відомих та запропонованих алгоритмів. При перетвореннях згідно з КТЗ використовуються такі основні модульні операції: знаходження оберненого елемента; знаходження залишків; операції множення та додавання.

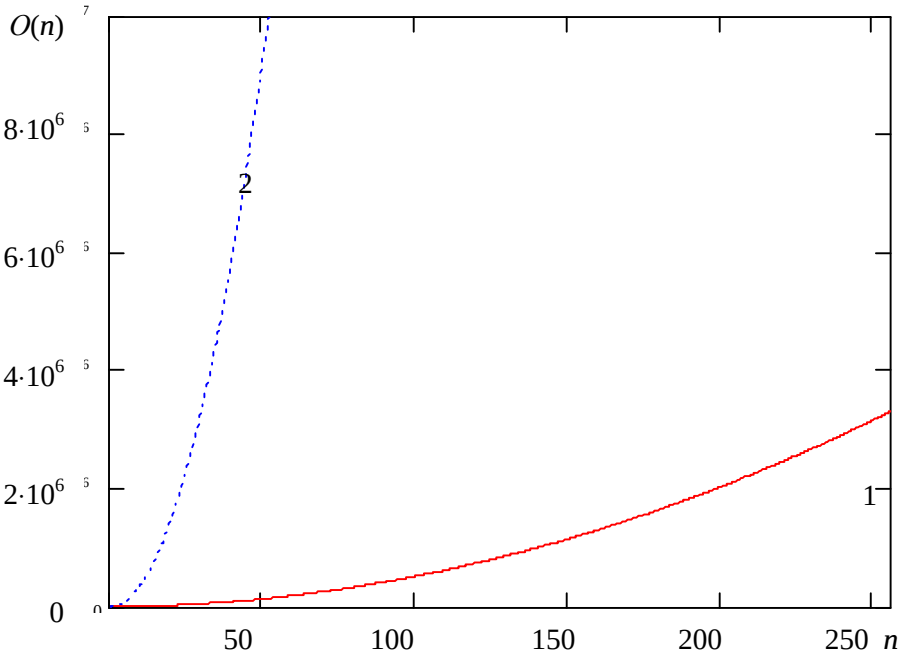
Тому при визначенні обчислювальних складностей відомого та запропонованого алгоритмів, які дозволяють виконувати перетворення КТЗ, потрібно враховувати складності вищезазначених операцій, наведені у табл. 9.

Таблиця 9

Обчислювальні складності основних операцій КТЗ

№ з/п	Основні операції	Обчислювальна складність операцій у запропонованому алгоритмі	Обчислювальна складність операцій у класичному алгоритмі
1.	Пошук оберненого елемента	$O\left(\frac{n^2 \cdot k}{2} \cdot\right)$	$O1(17{,}5k \cdot ((n+1)^2 + n^2 + n)$
2.	Пошук залишків	$O\left(\log_2 n/2\right)$	$O1((n+1)^2 + n)$
3.		$O\left(\log_2 k \cdot (2 \cdot \log_2{}^2 n + n\right)$	$O1(k \cdot (2n^2 + n))$

де k – кількість взаємно простих модулів.



Графіки залежності обчислювальних складностей від розрядності чисел n запропонованим методом (1) та класичним (2)

Враховуючи табличні дані, алгоритмічна складність Китайської теореми про залишки з використанням запропонованого методу становить $O\left(\left(\log_2 k\cdot(2\cdot\log_2{}^2 n+n\right)+\frac{n^2\cdot k}{2}+\left(\log_2 n/2\right)\right)$, а з використанням класичного алгоритму – $O1(37k\cdot n^2+53{,}5k\cdot n+17{,}5k+n^2+3n+1))$.

На рисунку показано графіки залежності обчислювальних складностей від розрядності чисел *n*. З рисунка видно, що використання запропонованого алгоритму, який грунтується на використанні теоретико-числового базису Крестенсона, дає змогу істотно зменшити обчислювальну складність КТЗ відносно класичного.

Висновки. У роботі викладено теоретичні основи алгоритмів перетворення КТЗ в базисі Радемахера–Крестенсона. Основними перевагами запропонованих теоретичних положень та алгоритмів є зменшення обчислювальної складності, що відкриває нові перспективи високопродуктивного опрацювання великорозрядних чисел в задачах захисту інформаційних потоків в комп'ютерних системах та знаходження мультистепеневої функції за заданим модулем.

1. Бухштаб А.А. Теория чисел. – М.: Просвещение, 1966. – 384 с. 2. Акушский И.Я., Юдицкий Д.И. "Машинная арифметика в остаточных классах". – М: Сов.радио, 1968. – 440 с. 3. Задірака В., Олексюк О. Комп'ютерна криптологія: Підручник.– К.:2002. – 504 с. 4. Задірака В.К., Олексюк О.С. Комп'ютерна арифметика багаторозрядних чисел: Наукове видання. – К.: 2003. – 264 с. 5. Фергюсон Н., Шнайер Б. Практическая криптография: Пер. с англ. – М.: – Вильямс, 2005. – 424 с. 6. Вербіцький О.В. Вступ до криптології. – Львів:ВНТЛ, 1998.–.248 с. 7. Бородін О.І. Теорія чисел. – К.: Вища школа, 1970. – 275 с.8. Николайчук Я.М. Теорія джерел інформації. – Тернопіль: ТзОВ „Терно–граф", 2010. – 536 с. 9. Касянчук М.М. Теорія та математичні закономірності досконалої форми системи залишкових класів // Праці Міжнародного симпозіуму „Питання оптимізації обчислень (ПОО–XXXV)". Т.1. – Київ–Кацивелі.– 2009.– С. 306–310. 10. Касянчук М.М. Теорія перетворення досконалої форми системи залишкових класів базису Крестенсона // Матеріали проблемно–наукової міжгалузевої конференції „Інформаційні проблеми комп'ютерних систем, юриспруденції, економіки та моделювання (ПНМК–2009)". – Тернопіль-Бучач. – 2009. – С.133–137. 11. Kasyanchuk M. Conception of theoretical bases of the accomplished form of Krestenson's transformation and its practical application // Proceedings of the 4–th International Conference "Advanced Computer Systems and Network: Design and Application" (ACSN–2009).–L'viv.– 2009. – P.299–301.