Секція 3
КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

УДК 681.32

Стефурак Н.А. [1], *Шкіра Ю.Р.* [2], *Івасьєв С.В.*[2], *Будзанівська Н.М.* [3]
[1]*Галицький коледж ім. В. Чорновола*
[2]*Тернопільський національний економічний університет*
[3]*Теребовлянський НВК*

АЛГОРИТМИ ЗНАХОДЖЕННЯ КОРЕНЯ КВАДРАТНОГО

Вступ. При реалізації алгоритмів опрацювання багаторозрядних простих чисел в задачах теорії чисел та криптографічних перетворень виникає ряд трудомістких операцій. Однією з таких операцій є знаходження цілого кореня квадратного, зокрема для алгоритмів факторизації [1], що побудовані на методі Ферма. Дослідження алгоритмів знаходження цілого кореня квадратного дозволяє оцінити обчислювальну складність операції та приводить до необхідності розробки нових алгоритмів обчислення цілої частини кореня квадратного з врахуванням різних теоретико числових базисів.

Метою роботи є дослідження алгоритмів обчислення кореня квадратного з багаторозрядних чисел та розробка алгоритму знаходження кореня квадратного.

1. Корінь квадратний

Квадратний корінь з числа a, - це таке число, квадрат якого дорівнює a, Тобто рішення рівняння щодо змінної x. $\sqrt{a} = x; x^2 = a.$

Квадратним коренем називають також функцію $\sqrt{x}$ змінної x, яка кожному $x \geq 0$ ставить у відповідність арифметичне значення кореня (рисунок 1) [2].

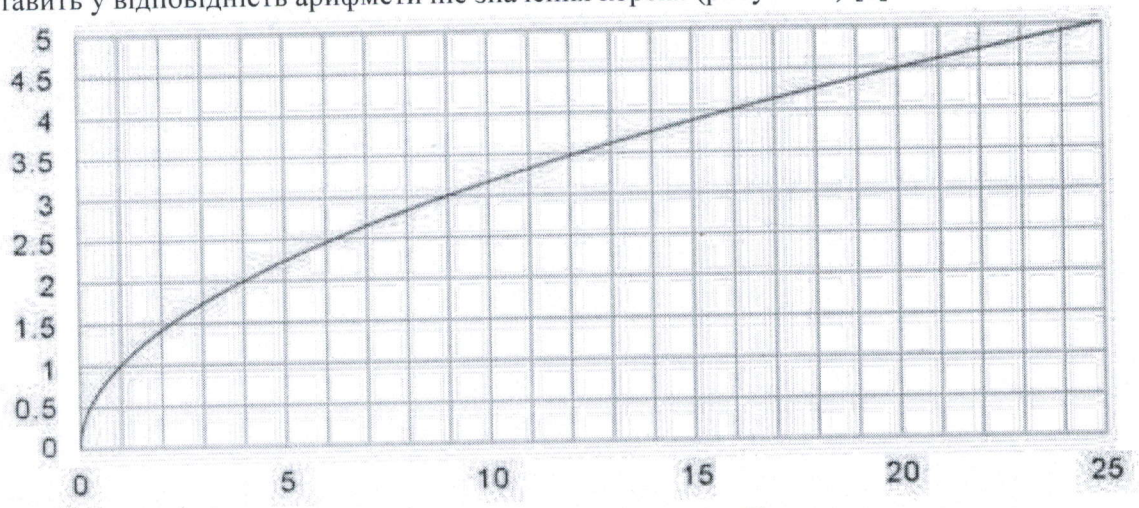

Рисунок 1 - Графік функції $\sqrt{x}$

2. Методи обчислення кореня квадратного

В ході даного дослідження мною було виявлено кілька алгоритмів добування квадратного кореня [2]:

1. Арифметичний.

2. Груба оцінка.
3. Стовпчиком.
4. Вавилонський спосіб.
5. Метод Герона.
6. Метод Ньютона.
7. Десятковий.

Наведемо приклади деяких з них. Арифметичний спосіб:

$1 = 1^2$;
$1 + 3 = 2^2$;
$1 + 3 + 5 = 3^2$.

Тобто, дізнатися цілу частину квадратного кореня числа можна, віднімаючи з нього всі непарні числа по порядку, поки залишок не стане менше наступного від'ємника числа або дорівнює нулю, і порахувавши кількість виконаних дій. Наприклад, так:

$9 - 1 = 8$;
$8 - 3 = 5$;
$5 - 5 = 0$.

Виконано 3 дії, квадратний корінь числа 9 дорівнює 3. Недоліком такого способу є те, що якщо корінь який отримують не є цілим числом, то можна дізнатися тільки його цілу частину, але не точніше. У той же час такий спосіб цілком доступний для примітивних обчислень, для нескладних задач пошуку квадратного кореня.

Вавилонський спосіб наближеного обчислення квадратних коренів можна ілюструвати на наступному прикладі.

Обчислимо $\sqrt{2}$, тобто знайдемо за допомогою методу наближених обчислень додатній корінь рівняння $x^2=2$. Це рівняння рівносильне наступному:

$$x = \frac{2}{x} \qquad (1)$$

Припустимо, що ми маємо деякий наближене значення x_0 числа рівне 1.

Згідно (1), $x_0 = 1$ треба порівняти з числом $\frac{2}{x_0}$, тобто з $\frac{2}{1}$; якщо x_0 і $\frac{2}{x_0}$ збігаються, то x_0 - точне значення числа $\sqrt{2}$ рівне 1. Так як 1 не дорівнює $\frac{2}{1}$, то одне з чисел менше, а інше більше, ніж $\sqrt{2}$, тобто лежить між 1 і $\frac{2}{1}$.

Можна припустити, що середнє арифметичне цих чисел $x_1 = \frac{1}{2}(x_0 + \frac{2}{x_0})$ є найкращим наближенням числа $\sqrt{2}$, ніж вихідне наближення x_0, тобто $x_1 = \frac{1}{2}(x_0 + \frac{2}{x_0}) = \frac{1}{2}(1 + \frac{2}{1}) = \frac{3}{2} = 1{,}5$. Це наближення x_1 можна поліпшити таким же

способом, тобто взяти середнє арифметичне чисел $x_1 и \frac{2}{x_1}$ і так далі.

$$x_2 = \frac{1}{2}(x_1 + \frac{2}{x_1}) = \frac{1}{2}(\frac{3}{2} + \frac{2}{3/2}) = \frac{17}{12} = 1{,}416666667 \ .$$

$$x_3 = \frac{1}{2}(x_2 + \frac{2}{x_2}) = \frac{1}{2}(\frac{17}{12} + \frac{2}{17/12}) = \frac{577}{400} = 1{,}4142115686 \ ..$$

$$x_4 = \frac{1}{2}(x_3 + \frac{2}{x_3}) = \frac{1}{2}(\frac{577}{408} + \frac{2}{577/408}) = \frac{665857}{470832} = 1{,}414213562 \ .$$

$$x_5 = \frac{1}{2}(x_5 + \frac{2}{x_5}) = \frac{1}{2}(\frac{665857}{470832} + \frac{2}{665857/470832}) = 1{,}4175213562 \ .$$

Як бачимо, вже п'яте наближення не відрізняється (при обчисленнях з дев'ятьма знаками після коми) від четвертого. Природно прийняти, що приблизно дорівнює 1,414213562.

Проведемо обчислення, для визначення точності способу:

$$x_n - \sqrt{2} = \frac{1}{2}(x_{n-1} + \frac{2}{x_{n-1}}) - -\sqrt{2} = 1/(2x_{n-1})(x_{n-1} - 2)^2. \qquad (2)$$

Рівність (2) дає можливість висловити помилку наближення x_n (тобто число $\left|x_n - \sqrt{2}\right|$) через помилку попереднього наближення x_n-1:

$$x_1 - \sqrt{2} = 1/(2x_0)(x_0 - 2)^2 = 0{,}500 \text{ або } 50\ \%.$$
$$x_2 - \sqrt{2} = 1/(2x_1)(x_1 - 2)^2 = 0{,}833 \text{ або } 8{,}3\ \%.$$
$$x_3 - \sqrt{2} = 1/(2x_2)(x_2 - 2)^2 = 0{,}012 \text{ або } 1{,}2\ \%.$$

Формула, за допомогою якої обчислювалися послідовні наближення числа по вавилонському способу, може бути записана наступним чином:

$$x_n = f(x_n\text{-}1). \qquad (3)$$

В даному випадку в якості опції $f(x)$ береться функція

$$f(x) = 1/2\ (x + 2 / x). \qquad (4)$$

Легко бачити також, що рівняння (1), яке наближено вирішувалося цим способом, переписується з допомогою функції (4) у вигляді:

$$f(x) = x. \qquad (5)$$

Такий спосіб наближеного обчислення квадратних коренів називається методом ітерацій. Ітерація (з латинської iteratio - повторення) - результат повторного застосування будь-якої математичної операції. [3]

До обчислення квадратних коренів зводяться багато геометричних задач. Наприклад, теорема Піфагора: квадрат довжини гіпотенузи прямокутного трикутника дорівнює сумі квадратів довжин катетів цього трикутника. Довести її можна з допомогою наступного креслення (рисунок. 2).

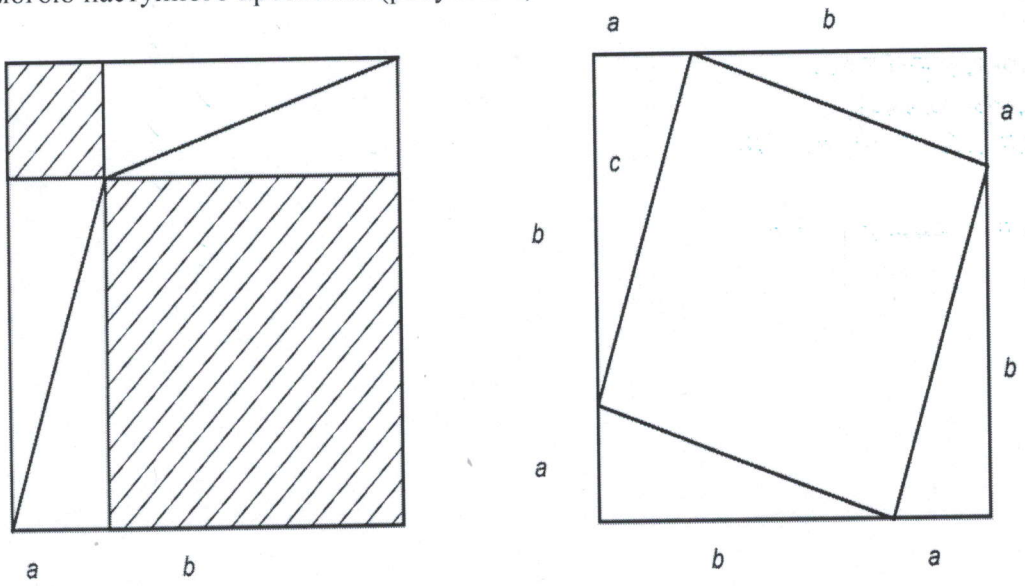

Рисунок 2 - Геометричне доведення теореми Піфагора

Бачимо, що площі заштрихованих фігур в обох квадратах рівні, але в одному випадку площа дорівнює $a^2 + b^2$ а в іншому c^2[4]. Значить $a^2 + b^2 = c^2$.

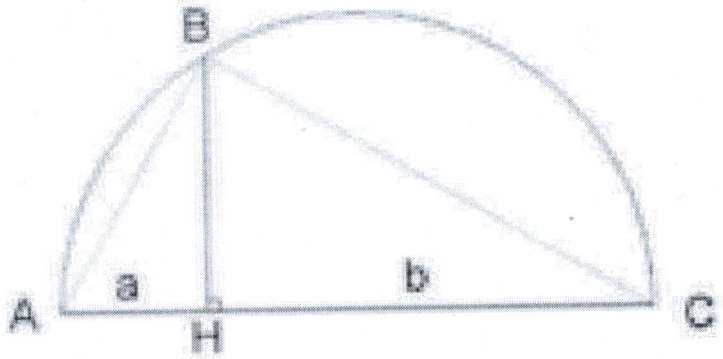

Рисунок 3 - Обчислення квадратного кореня методом геометричних побудов

$$|BH| = \sqrt{|AH| \cdot |HC|}.$$

Особливо, якщо $|AH| = 1, a|HC| = x, mo|BH| = \sqrt{x}$.

При вирішенні математичних задач далеко не завжди буває потрібно знати абсолютно точну відповідь, досить знайти його наближене значення з прийнятною точністю. Багато алгоритми обчислення квадратних коренів з позитивного дійсного числа S вимагають деякого початкового значення. Якщо початкове значення занадто далеко від справжнього значення кореня, обчислення сповільнюються. Тому корисно мати грубу оцінку, яка може бути дуже неточна, але легко обчислюється.

Якщо S ≥ 1, нехай D буде числом цифр S зліва від десяткової коми. Якщо S <1, нехай D буде числом нулів, що йдуть підряд, праворуч від десяткової коми, взяте зі знаком мінус. Тоді груба оцінка виглядає так: Якщо D непарній, D = 2n + 1, тоді використовуємо $\sqrt{S} \approx 2 \cdot 10^n$.

Якщо D парне, D = 2n + 2, тоді використовуємо $\sqrt{S} \approx 6 \cdot 10^n$. Два і шість використовуються тому, що $\sqrt{\sqrt{1 \cdot 10}} = \sqrt[4]{10} \approx 2 и \sqrt{\sqrt{10 \cdot 100}} = \sqrt[4]{1000} \approx 6.$ Ми вирішили дізнатися яка похибка результату при обчисленні таким способом. Розглянемо число 49. Провівши обчислення таким способом, ми отримуємо відповідь рівний шести.

Можна зробити висновок, що чим більше число, тим більше результат відрізняється від істинного значення кореня.

Також обчислити корінь квадратний можна використавши метод обчислення стовпчиком. Цей спосіб дозволяє знайти наближене значення кореня з будь-якого дійсного числа з будь-якою наперед заданою точністю. До недоліків методу можна віднести збільшується складність обчислення зі збільшенням кількості знайдених цифр.

Для ручного вилучення кореня застосовується запис, схожа на поділ стовпчиком. Виписується число, корінь якого шукаємо. Праворуч від нього будемо поступово отримувати цифри шуканого кореня. Нехай витягується корінь з цілого числа N. Для початку подумки або мітками розіб'ємо число N на групи по дві цифри зліва і праворуч від десяткового дробу. При необхідності, групи доповнюються нулями - ціла частина доповнюється зліва, десяткова справа. Так 31234.567 можна уявити, як 03 12 34. 56 70. На відміну від ділення знесення виробляється такими групами по 2 цифри.

1. Запишемо число N на листку.

2. Знайдемо a, квадрат якого менше групи старших розрядів числа N (старша група - найлівіша не дорівнює нулю), а квадрат a + 1 більше групи старших розрядів числа. Записати знайдене a праворуч від N (це чергова цифра шуканого кореня). (На першому кроці прикладу $a^2 = 2^2 = 2 * 2 = 4 <6$, а $(a + 1)^2 = 3^2 = 3 * 3 = 9> 6$).

3. Записати квадрат a під старшою групою розрядів. Провести віднімання з старшої групи розрядів N виписаного квадрата числа a і записати результат віднімання під ними.

4. Зліва від цього результату віднімання провести вертикальну риску і зліва від межі записати число, що дорівнює вже знайденим цифрам результату (ми їх виписуємо праворуч від N) помножене на 20. Назвемо це число b. (На першому кроці прикладу це число просто є b = 2 * 20 = 40, на другому b = 26 * 20 = 520).

5. Провести знесення наступної групи цифр, тобто дописати наступні дві цифри числа N праворуч від результату віднімання. число утворене "Склеєними" результатом вирахування і дописати двома цифрами назвемо c. (На першому кроці прикладу це число просто є c = 296, на другому c = 2096). Якщо зноситься перша група після десяткового дробу числа N, то потрібно поставити крапку праворуч від вже знайдених цифр шуканого кореня.

6. Тепер потрібно знайти таке a, що (b + a) * a менше або дорівнює c, але (b+(A+1)) * (a + 1) більше, ніж c. Записати знайдене a праворуч від N, як чергову цифру шуканого кореня. Цілком можливо, що a виявиться рівним нулю. Це нічого не міняє - записуємо 0 праворуч від вже знайдених цифр кореня. (На першому кроці прикладу це число 6, тому що (40 + 6) * 6 = 46 * 6 = 276 <296, але (40 + 7) * 7 = 47 * 7 =

329> 296) Якщо число знайдених цифр вже задовольняє шуканої точності припиняємо процес обчислення.

7. Записати число (b + a) * a під c. Провести віднімання стовпчиком числа (B+a)*a з c і записати результат віднімання під ними. Перейти до кроку 4. [7]

Метод Герона, був відомий ще в Стародавній Греції і приписується Герону Олександрійському. Наприклад: нехай треба знайти корінь з 720. Так як 720 не має раціонального кореня, то візьмемо корінь з дуже малої похибкою в такий спосіб. Так як найближчий до 720 квадрат є 729, і воно має коренем 27, то розділимо 720 на 27. Виходить $26\frac{2}{3}+27=53\frac{2}{3}$.

Розділимо результат на 2, отримаємо $26\frac{5}{6}$. Це і є результат. якщо звести це число в квадрат, отримаємо $720\frac{1}{36}$ Похибка становить 1/36 одиниці. Але при бажанні похибка може бути і меншою. Для зменшення величини похибки процедуру слід виконати ще й ще раз з знову отриманої величиною. У нашому випадку з числом $720\frac{1}{36}$ [3].

Другий метод Герона для знаходження наближеного значення квадратного кореня числа x полягає в тому, що число x представляють у вигляді суми a^2+b, де a^2 найближчий до числа x точний квадрат натурального числа a і використовують формулу $\sqrt{a^2+b}\approx a+\frac{b}{2a}$. [3]. Обчислимо за допомогою формули корінь квадратний, наприклад з числа 28 $\sqrt{28}=\sqrt{5^2+3}\approx 5+\frac{3}{2\cdot 5}\approx 5{,}3$. Піднімемо до квадрату отриманий результат. Похибка становить 0,09. Методи Герона мають самий маленький коефіцієнт похибки.

Висновки. Досліджені та проаналізовані алгоритми обчислення кореня квадратного з багаторозрядних чисел потребують значних обчислювальних ресурсів. Розробка ефективного алгоритму обчислення кореня квадратно з багаторозряних чисел дозволить збільшити швидкодію багатьох алгоритмів крипто аналізу та зокрема задач факторизації побудованих на основі теореми Ферма.

Перелік використаних джерел.

1. Тимошенко Л.М. Алгоритми факторизащї для криптоаналізу асиметричних криптосистем //Тимошенко Л.М., К.В. Вербик, Николайчук Я.М., Івасьєв С.В. / Інформатика та математичні методи в моделюванні. – Одеса 2014.- № 4(4). – С. 342-349

2. Задірака В.К. Комп'ютерна криптологія: Підручник /В.К. Задірака, О.С. Олексюк // – Київ: – 504 с.

3. Майоров С.А. Принципы организации цифровых машин / С.А. Майоров, Г.И. Новиков// – Л.: Машиностроение, –1974. – 306 с.

4. Касянчук М.М. Теорія та оптимізація алгоритмів опрацювання великорозрядних чисел у базисі Крестенсона / Касянчук М.М., Якименко І.З. Івасьєв, С.В.// Праці міжнародної молодіжної математичної школи "Питання оптимізації обчислень (ПОО-XXXVII)" Київ: Інститут кібернетики імені В.М. Глушкова НАН України, 2011. С. 67-68.