Національний університет «Чернігівський колегіум» імені Т. Г. Шевченка

Природничо-математичний факультет

Кафедра математики та економіки

Кваліфікаційна робота

освітнього ступеня «магістр»

на тему

«Ланцюгові дроби в математиці та навколишньому світі»

Виконала:

Студентка 2 курсу, 62 групи

спеціальності 111 Математика

Борисенко Катерина Сергіївна

Науковий керівник:

кандидат педагогічних наук,

доцент Нак Марина Миколаївна

Чернігів – 2019 р.

Роботу подано до розгляду «____»_____ 2019 року.

Студент(ка) _____ _____
(підпис) (прізвище і ініціали)

Науковий керівник _____ _____
(підпис) (прізвище і ініціали)

Рецензент _____ _____
(підпис) (прізвище і ініціали)

Кваліфікаційна робота розглянута на засіданні кафедри

_____
(назва кафедри)

протокол №____ від «_____»_____2019 року.

Студент(ка) допускається до захисту даної роботи в екзаменаційній комісії.

Завідувач кафедри _____ _____
(підпис) (прізвище і ініціали)

Зміст

ВСТУП

Вже понад 2000 років математики займаються ланцюговими дробами. Зрозуміло, що цей величезний відрізок часу могла витримати, не загинувши, лише така теорія, яка має фундаментальне значення в математиці. Дійсно, ланцюгові дроби є одним з найголовніших апаратів математики, який відіграв в її розвитку надзвичайно велику роль.

Нині в теоретичному плані неперервні дроби грають важливу роль, оскільки дозволяють посилити і розвинути результати класичної математики на випадок багатьох аргументів, причому сам апарат ланцюгових дробів часто підказує формулювання такого роду узагальнень, зокрема, в теорії чисел.

Застосування ланцюгових дробів саме в теорії чисел помітне в: узагальненні основних алгоритмів (Ейлера, Остроградського, Евкліда), знаходженні розв’язку класичної задачі про алгебраїчні ірраціональності вищих степенів, знаходженні розв’язків деяких діофантових рівнянь та їх систем. Також неперервні дроби дають велику перевагу в точності при наближеному знаходженні квадратних коренів, обчисленні логарифмів чисел.

Теорія ланцюгових дробів пов'язана з теорією наближень дійсних чисел раціональними, з теорією динамічних систем, а також з багатьма іншими розділами математики.

Теорія матричних гіллястих ланцюгових дробів дозволяє розв'язати наступні завдання: добування квадратного кореня, кореня третього та четвертого степеня і кореня будь-якого раціонального числа за допомогою матриць, розв'язування рівнянь за допомогою матриць другого порядку, розв’язування рівнянь вищих степенів за допомогою матриць.

Також, окрім застосувань ланцюгових дробів у математиці, вони широко використовуються у навколишньому світі. Проблема складання календаря тісно пов'язана з ланцюговими дробами. Вперше порядок у відліку часу спробував навести в I ст. до н.е. римський імператор Юлій Цезар, адже до цього календар був не досить точний. За юліанським календарем до XVI століття накопичилася помилка, яка складала близько 10 діб. В результаті чого була проведена наступна

реформа календаря римським папою Григорієм XIII, ім'ям якого і називається діюча календарна система. Розв'язуванням цієї задачі займалося багато математиків, серед яких був і Омар Хайям. У 1864 році російським астрономом Йоганном Медлером була запропонована ще одна поправка до юліанського календаря, яка була основана на знаходженні вже четвертого відповідного дробу до запису тривалості астрономічного року у вигляді ланцюгового дробу [23, с.129].

Ланцюгові дроби вперше були згадані в роботах грецьких математиків. Можливо, що при знаходженні наближення до числа $\sqrt{3}$ Архімед (212 рік до н.е.) користувався методом, який є доволі близьким до розкладу цього числа в ланцюговий дріб. За весь цей час ланцюгові дроби з'являлися в різних працях, але вперше вони зустрічаються в такому вигляді, в якому відомі нам зараз, в роботі «Алгебра» італійського математика Рафаеля Бомбеллі, яка вийшла у 1572 році. Крокуючи в історії далі, можна відмітити Лео Фробеніуса та Анрі Паде, які використовували підхідні дроби ланцюгових дробів для наближення аналітичних функцій в кінці 19 століття. Близькими до нашого часу також є дослідження аналітичних питань ланцюгових дробів, яке проходило у 60-х роках XX-го століття в Марийському педагогічному інституті.

З огляду на все це тема моєї дипломної роботи є досить актуальною.

Метою роботи є: розглянути властивості неперервних ланцюгових дробів та їх підхідних дробів, супроводжуючи їх застосуванням у математиці та навколишньому середовищі.

Об'єкт дослідження: теорія ланцюгових дроби.

Предмет дослідження: застосування ланцюгових дробів та їх властивості.

Завдання даної магістерської роботи:

1) розглянути ланцюгові дроби в ході їх історичного розвитку;
2) розкрити їх основні поняття, властивості ланцюгових дробів, алгоритми запису скінченних та нескінченних ланцюгових дробів;
3) розглянути застосування ланцюгових дробів в математиці, а саме: у застосуванні до розв'язування рівнянь, представлення числа π за

допомогою ланцюгового дробу, у геометричній теорії ланцюгових дробів;

4) розкрити суть та розглянути застосування ланцюгових дробів в навколишньому світі.

Робота складається зі вступу, двох розділів, висновку, списку використаних джерел та додатків.

У І розділі розглядається етапи розвитку ланцюгових дробів, основні поняття скінченних та нескінченних ланцюгових дробів, їх підхідних дробів та властивостей, наведено алгоритм запису раціональних чисел у вигляді скінченних ланцюгових дробів та алгоритм запису ірраціональних чисел у вигляді нескінченних ланцюгових дробів.

У ІІ розділі розглядається геометрична теорія ланцюгових дробів, наближення дійсного числа підхідними дробами, розв'язування рівнянь, а саме: діофантові рівняння виду $ax + by = c$ і рівняння Пелля. Також розглядається застосування ланцюгових дробів в навколишньому середовищі: астрономії, мистецтві, криптографії.

Апробація: результати магістерської роботи розглядались та доповідались на двох конференціях: Регіональній науково-практичній конференції студентів, аспірантів і молодих учених «Крок у науку: дослідження у галузі природничо-математичних дисциплін та методик їх навчань» з темою «Ланцюгові дроби в астрономії» 28 листопада 2018 року та на Всеукраїнській науково-практичній конференції студентів, аспірантів і молодих учених «Крок у науку: дослідження у галузі природничо-математичних дисциплін та методик їх навчання» з темою «Ланцюгові дроби в криптографії» 27 листопада 2019 року.

Розділ І. ТЕОРІЯ ЛАНЦЮГОВИХ ДРОБІВ

1.1. Історія ланцюгових дробів

За деякими джерелами ланцюгові дроби вже розглядали та застосовували математики Стародавньої Греції. Наприклад, алгоритм Евкліда (III ст. до н.е.) дуже тісно пов'язаний із ланцюговими дробами. Він дає можливість представити будь-яке раціональне число у вигляді ланцюгового дробу [20].

Китайський астроном Цзу Чун-Чжі (V ст. н. е.) довів, що число π знаходиться між числами 3,1415926 і 3,1415927, він вказав за раціональне наближення до π величину $\frac{355}{133}$.

Серед математиків середньовіччя ближче за всіх підійшов до поняття ланцюгового дробу Омар Хаям. Він поклав ці дроби в основу своєї ідеї про реформу календаря. Тривалість всього року за його наближеннями становила $365\ \frac{8}{33}$ та мала похибку усього 19 секунд за рік.

Алгоритм утворення ланцюгових дробів також був знайдений в Індії, про що свідчить праця «Вінець системи» індійського математика Бхаскара II.

Але вперше ланцюгові дроби були введені в 1572 році італійським математиком Бомбеллі. Вони описуються в статті, написаній саме в той час, коли в Італії та Франції вперше з'явилися алгебраїчні поняття та позначення. Знаходячи квадратні корені з чисел Бомбеллі прийшов до ланцюгових дробів.

Далі у часі використання ланцюгового дробу, причому знову за допомогою знаходження квадратних коренів, належить італійському математику Катальді. Він запропонував новий частинний випадок формули $\sqrt{a^2+b} = a + \frac{b}{2a+\frac{b}{2a+\cdots}}$ у вигляді: $\sqrt{18} = 4 + \frac{2}{8+\frac{2}{8+\frac{2}{8}}}$. Він ввів повторне застосування дробової риски у записі ланцюгового дробу в 1613 році, тобто вже сучасний запис ланцюгового дробу. Окрім всього цього Катальді помітив, що значення ланцюгового дробу завжди знаходиться поміж сусідніх підхідних дробів [21].

У середині XVII століття англійський математик Джон Валліс розклав трансцендентне число $\frac{4}{\pi}$ у нескінченний добуток $\frac{4}{\pi} = \frac{3\cdot3}{2\cdot4}\cdot\frac{5\cdot5}{4\cdot6}\cdot\frac{7\cdot7}{6\cdot8}\cdot\frac{9\cdot9}{8\cdot10}\dots$, а лорд Броукнер, перший президент Королівського товариства, близько 1659 року опублікував розклад цього числа у ланцюговий дріб без доведення :

$$\frac{4}{\pi} = 1 + \cfrac{1}{2 + \cfrac{9}{2 + \cfrac{25}{2 + \cdots}}}$$

Наступним кроком у розвитку ланцюгових дробів зробив Християн Гюйгенс. Він побудував модель сонячної системи за допомогою зубчастих коліс. Розрахунки показали, що відношення числа зубців $\frac{m}{n} \approx \frac{77708431}{2640858}$ двох будь-яких коліс повинно бути рівним відношенню часу обернення двох планет навколо Сонця. Таке відношення виражається досить точно у вигляді (нескоротного) дробу з великими чисельниками та знаменниками. А виготовлення таких коліс дуже складне. Тоді Гюйгенс знайшов серед дробів з меншим чисельником та знаменником підхідний дріб до числа $\frac{77708431}{2640858}$. Він розв'язав таку задачу за допомогою розкладання звичайного дробу в ланцюговий і тому обмежився розглядом правильних ланцюгових дробів. Завдяки чому був знайдений ланцюговий дріб $\frac{73}{51}$, апроксимуючий дріб з великим чисельником та знаменником, та який має похибку в десятитисячну частку від одиниці. Гюйгенс звернув увагу на те, що не можна знайти звичайний дріб з меншим чисельником та знаменником, ніж підхідний, який був би ближче до значення ланцюгового дробу. А також, що підхідні дроби можуть бути то більші, то менші від значення ланцюгового дробу.

Дев'ятнадцяте століття стало часом дуже сильного розвитку аналітичної теорії ланцюгових дробів. Методи неперервних дробів застосовувались при вивченні спеціальних функцій, для знаходження конкретних чисельних результатів. В області теорії розкладу та збіжності неперервних дробів, елементами яких є лінійні функції комплексної змінної, працювали такі

математики: П’єр Лаплас, Лежандр, Якобі, Ейзенштейн, Бернахрд Ріман, Фробеніус, Анрі Пуанкаре. Ці дослідження надали великий вплив на подальший розвиток математики. Наприклад, у працях Анрі Пуанкаре та Томас Стілтєс, в яких розклад в неперервні дроби застосовувався у зв’язку з розбіжними рядами, уперше з’явились асимптотичні розклади. Також відомо, що методи, які були відкриті Лео Фробеніусом і Анрі Паде у кінці 19 століття для наближення аналітичних функцій підхідними неперервними дробами під назвою апроксимацій Паде, стали головним обчислювальним засобом в задачах статистичної механіки, швидко поширюючись на інші розділи теоретичної фізики [23].

Тобто, можемо дійти до висновку, що ланцюговими дробами займалися час від часу, і першим, хто врешті-решт систематизував всі існуючі знання про ланцюгові дроби і виклав повну їх теорію, наскільки це було можливо зробити в ту епоху, був Леонард Ейлер. У його працях розглядались питання про використання ланцюгових дробів для розв’язування диференціальних рівнянь, алгоритм знаходження підхідних дробів, представлення ірраціональних чисел у вигляді ланцюгових дробів, застосував їх до розкладу функцій, дав важливе їх узагальнення. Праці Ейлера були продовжені згодом Софроновим Михаїлом (1729-1760), академіком Висковатим Василем Івановичем (1779-1819), Бернуллі Даніелем (1700-1782) та ін. Більшість важливих результатів належать французькому математику Жозефу Лагранжу, який знайшов метод наближеного розв’язку диференціальних рівнянь за допомогою ланцюгових дробів [22].

Варто зауважити, що сам термін «ланцюговий дріб» з’явився лише у XVIII столітті, а до цього математики користувались лише поняттям «нескінченний дріб».

Ланцюгові дроби мають ряд унікальних властивостей, що забезпечують їм широке використання в прикладній та теоретичній математиці. Саме цим і пояснюється підвищений інтерес математиків до даної теорії протягом кількох століть. У сучасному світі ланцюгові дроби знаходять все більше застосування в

обчислювальній техніці, оскільки вони дозволяють будувати ефективні алгоритми для знаходження розв'язку ряду завдань на ЕОМ.

1.2. Правильні скінченні ланцюгові дроби

1.2.1. Розклад раціонального числа в правильний ланцюговий дріб

Нехай позначимо за α будь-яке число, а буквою q_0 – найбільше ціле число, яке при цьому не є більшим за α. При нецілому α будемо мати:

$$\alpha = q_0 + \frac{1}{\alpha_1};\ \alpha_1 > 1.$$

Точно так само при нецілих $\alpha_1, \dots, \alpha_n$ маємо :

$$\alpha_1 = q_1 + \frac{1}{\alpha_2};\ \alpha_2 > 1;$$

$$\dots\dots\dots\dots..$$

$$\alpha_{n-1} = q_{n-1} + \frac{1}{\alpha_n};\ \alpha_n > 1,$$

$$\alpha_n = q_n + \frac{1}{\alpha_{n+1}};\alpha_{n+1} > 1$$

і так далі [11, с. 15].

Якщо число α раціональне, тоді для деякого натурального n матимемо $\alpha_{n+1} = 0$, отже, записи, згадані вище, обірвуться. А якщо дане число ірраціональне, то запис буде продовжуватись нескінченно. З першого випадку матимемо розклад α в ланцюговий дріб:

$$\alpha = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\dots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}}$$

А у другому випадку з ірраціональним α:

$$\alpha = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\dots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n + \dots}}}}}$$

Означення: Вираз вигляду

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ldots + \cfrac{1}{q_s + \cdots}}}}$$

де числа $q_0, q_1, \ldots -$ цілі $-$називають елементарним ланцюговим, або елементарним неперервним, дробом. [16, с.100]

Числа $q_0, q_1, \ldots$ називають елементами даного ланцюгового дробу, а правильні дроби $\frac{1}{q_1}, \frac{1}{q_2} \ldots -$називаються першою, другою ланкою і т.д., ланкою ланцюгового дробу відповідно. Число ланок може бути як скінченним, так і нескінченним.

Теорема 1: Кожне раціональне число можна подати у вигляді деякого скінченного раціонального дробу.

Доведення. Нехай $z -$ довільно вибране раціональне число і $z = \frac{a}{b}$, де a і $b -$цілі числа, причому $b \geq 1$.

Застосувавши до цих чисел алгоритм Евкліда, дістанемо рівності:

$$\begin{cases} a = bq_0 + r_1, \\ b = r_1 q_1 + r_2, \\ r_1 = r_2 q_2 + r_3, \\ \cdots \\ r_{n-2} = r_{n-1} q_{n-1} + r_n, \\ r_{n-1} = r_n q_n \end{cases}$$

де $q_1, q_{2,\ldots} q_{n-1}$ називаються неповними послідовними частками, яким відповідають остачі $r_2, r_3, \ldots, r_n$ за теоремою про ділення з остачею $b > r_2 > > r_3 > \cdots > r_n > 0$, а q_n відповідає остача 0 [16, с. 100].

З отриманої системи рівностей внаслідок застосування алгоритму (виділення цілої частини дробу та обернення дробової частини) отримаємо рівносильну систему:

$$\begin{cases} \frac{a}{b} = q_0 + \frac{r_1}{b}, \\ \frac{b}{r_1} = q_1 + \frac{r_2}{r_1}, \\ \cdots \\ \frac{r_{n-2}}{r_{n-1}} = q_{n-1} + \frac{r_n}{r_{n-1}}, \\ \frac{r_{n-1}}{r_n} = q_n \end{cases}$$

звідки

$$\frac{a}{b} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ldots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}}$$

Такий вираз називається скінченим ланцюговим дробом. При цьому слід пам'ятати, що $q_0 \in Z, q_1 \ldots q_n \in N$.

Можемо бачити, що процес розкладу в ланцюговий дріб раціонального числа $\frac{a}{b}$ є послідновним виділенням цілої частини й обернення дробової частини, а також є скінченним, оскільки сам алгоритм Евкліда послідовного ділення a на b є скінченним.

Для зручності запису ланцюговий дріб можна позначати і так:

$$\frac{a}{b} = [q_0; q_1, q_2, \ldots, q_n].$$

Такий запис називають зображенням раціонального числа $\frac{a}{b}$ скінченним ланцюговим дробом або розкладом числа $\frac{a}{b}$ у скінченний ланцюговий дріб. У цьому записі ціле число відділяється крапкою з комою, а інші числа – комами.

Теорема 2: Існує один і тільки один скінченний ланцюговий дріб, який рівний раціональному числу.

Доведення: Справді, якщо

$$\frac{a}{b} = [q_0; q_1, q_2, \ldots, q_n], \quad (1)$$

$$\frac{a}{b} = [q_0'; q_1', q_2', \ldots, q_n'], \quad (2)$$

то

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ldots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}} = q_0' + \cfrac{1}{q_1' + \cfrac{1}{q_2' + \cfrac{1}{\ldots + \cfrac{1}{q_{s-1}' + \cfrac{1}{q_s'}}}}} \quad (3)$$

Не втрачаючи загальності міркувань, вважатимемо, що $s \geq n$. Оскільки дроби

$$\cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ldots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}} \text{ і } \cfrac{1}{q_1' + \cfrac{1}{q_2' + \cfrac{1}{\ldots + \cfrac{1}{q_{s-1}' + \cfrac{1}{q_s'}}}}}$$

менші від 1, то кожне з чисел q_0 і q_0' дорівнює цілій частині числа $\frac{a}{b}$ і тому маємо $q_0 = q_0'$. Віднявши почастинно від рівності (3) рівність $q_0 = q_0'$, дістанемо

$$\cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ldots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}} = \cfrac{1}{q_1' + \cfrac{1}{q_2' + \cfrac{1}{\ldots + \cfrac{1}{q_{s-1}' + \cfrac{1}{q_s'}}}}} \quad (4)$$

Дроби, що стоять у лівій і правій частинах рівності (4), мають однакові чисельники: кожен з чисельників дорівнює 1. Тому знаменники цих дробів також рівні між собою, тобто:

$$q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ldots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}} = q_1' + \cfrac{1}{q_2' + \cfrac{1}{\ldots + \cfrac{1}{q_{s-1}' + \cfrac{1}{q_s'}}}}.$$

Міркуваннями, аналогічними викладеним вище, доведемо, що $q_1 = q_1'$, $q_2 = q_2'$ і т.д..

Через n кроків ми прийдемо до рівності:

$$q_n = q'_n + \cfrac{1}{q'_{n+1} + \cfrac{1}{\ldots + \cfrac{1}{q'_{s-1} + \cfrac{1}{q'_s}}}},$$

де $s > n$. Звідси випливає, що $s = n$ і, отже $q_n = q_n$, бо при $s > n$ ціле число q_n мало б дорівнювати дробовому числу

$$q'_n + \cfrac{1}{q'_{n+1} + \cfrac{1}{\ldots + \cfrac{1}{q'_{s-1} + \cfrac{1}{q'_s}}}}$$

чого не може бути.

Отже, ми довели, що в зображеннях (1) і (2) $n = s$ і $q_0 = q'_0$, $q_1 = q'_1$, $q_2 = q'_2 \ldots q_n = q'_n$, тобто ці зображення нічим не відрізняються одне від одного. Теорему доведено [16, с. 102].

Вище згадані теореми встановлюють взаємо-однозначні відповідності між раціональними числами і скінченими ланцюговими дробами.

Приклад 1. Розкласти задане число в ланцюговий дріб

$$\frac{53}{37}$$

Спочатку запишемо його у вигляді суми цілої частини та дробової (остачі):

$$\frac{53}{37} = 1 + \frac{16}{37}.$$

Остачу можемо записати у вигляді дробу:

$$\frac{1}{\frac{37}{16}},$$

причому знаменник цього дробу більше одиниці. Тепер аналогічні дії зробимо з числом 37/16:

$$\frac{37}{16} = 2 + \frac{1}{\frac{16}{5}}$$

і оскільки маємо

$$\frac{16}{5} = 3 + \frac{1}{5},$$

то

$$\frac{53}{37} = 1 + \frac{16}{37} = 1 + \frac{1}{37/16} = 1 + \frac{1}{2 + \frac{1}{\frac{16}{5}}} = 1 + \frac{1}{2 + \frac{1}{3 + \frac{1}{5}}} = (1; 2,3,5).$$

Приклад 2. За даним скінченим неперервним дробом знайти відповідний йому звичайний дріб:

$$\frac{a}{b} = (2; 1,1,2,1,2)$$

$$\frac{a}{b} = 2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{3 + \frac{1}{1 + \frac{1}{2}}}}} = 2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{3 + \frac{2}{3}}}} = 2 + \frac{1}{1 + \frac{1}{1 + \frac{3}{11}}} =$$

$$= 2 + \frac{1}{1 + \frac{11}{14}} = 2 + \frac{14}{25} = \frac{64}{25}.$$

Отримали, у результаті всіх перетворень, дріб $\frac{64}{25}$.

1.2.2. Підхідні дроби

Обриваючи ланцюговий дріб, можна отримати раціональні наближення до даного числа, які називаються підхідними дробами (нумерація відповідних дробів починається з нуля).

Нехай $[q_0; q_1, \dots, q_n]$ (5) це деякий даний ланцюговий дріб. Значенням цього ланцюгового дробу буде деякий звичайний дріб $\frac{R}{S}$. Отже, ланцюговий дріб (5) зображується звичайним дробом. Проте таке зображення не є єдиним, бо якщо $\frac{R}{S} = [q_0; q_1, \dots, q_k]$, то й $\frac{Rl}{Sl} = [q_0; q_1, \dots, q_n]$, де $l -$ це будь-яке ціле число відмінне від нуля.

Канонічним зображенням нуль-членного ланцюгового дробу $[q_0] = q_0$ будемо вважати дріб $\frac{q_0}{1}$. Припустимо тепер, що канонічне зображення визначене

для кожного ланцюгового дробу, у якого число ланок менше ніж n. І тепер визначимо його для $n-$членного ланцюгового дробу [16, с. 104] .

Розглянемо $n-$членний ланцюговий дріб $[q_0; q_1, \dots, q_n]$. З означення ланцюгового дробу випливає співвідношення:

$$[q_0; q_1, \dots, q_n] = q_0 + \frac{1}{[q_1, \dots, q_n]}$$

Дріб $[q_1, \dots, q_n] - (n-1)-$членний, а отже, для нього канонічне зображення уже визначене за припущенням. Нехай цим зображенням буде звичайний дріб $\frac{P'}{Q'}$, тоді:

$$[q_0; q_1, \dots, q_n] = q_0 + \frac{Q'}{P'} = \frac{q_0 P' + Q'}{P'}.$$

Останній дріб $\frac{q_0 P' + Q'}{P'}$ вважатимемо канонічним зображенням ланцюгового дробу $[q_0; q_1, \dots, q_n]$. Таким чином, канонічне зображення тепер однозначно визначене для будь-якого скінченного ланцюгового дробу. Це канонічне зображення дробу будемо позначати символом $\frac{P}{Q}$. Тоді для чисельників та знаменників канонічних зображень $\frac{P}{Q}$ та $\frac{P'}{Q'}$ двох ланцюгових дробів $[q_0; q_1, \dots, q_n]$ та $[q_1, \dots, q_n]$ будемо мати співвідношення

$P = q_0 P' + Q', \quad Q = P'.$ (6)

Ланцюговий дріб $[q_0; q_1, \dots, q_s]$ (7)

де $0 \le s \le n$, будемо називати відрізком ланцюгового дробу $[q_0; q_1, \dots, q_n]$.

Означення 1: Канонічне зображення відрізка (7) називають $s-$м підхідним дробом або підхідним дробом порядку s ланцюгового дробу (5).

Ланцюговий дріб (8) має $n+1$ підхідних дробів:

$\frac{P_0}{Q_0}, \frac{P_1}{Q_1}, \dots, \frac{P_n}{Q_n}.$ (8)

За формулами $P_1 = q_0 q_1 + 1$, $Q_1 = q_1$, отже, $\frac{P_1}{Q_1} = \frac{q_0 q_1 + 1}{q_1}$, $P_2 = q_0(q_1 q_2 + 1) + q_2 = q_2(q_0 q_1 + 1) + q_0 = q_2 P_1 + P_0$, $Q_2 = q_1 q_2 + 1 = q_2 Q_1 + Q_0$ (9)

і

$$\frac{P_2}{Q_2} = \frac{q_2 P_1 + P_0}{q_2 Q_1 + Q_0}$$

Теорема 1(правило утворення підхідних дробів): Для будь-якого $s \geq 2$

$$P_s = q_s P_{s-1} + P_{s-2}, \qquad Q_s = q_s Q_{s-1} + Q_{s-2}. \qquad (10)$$

Доведення: При $s = 2$, як показують співвідношення (9), формули (10) правильні. Припустимо, що вони правильні для $s = m - 1 (m > 2)$, і доведемо, що тоді вони правильні й для $s = m$. Розглянемо відрізок

$$[q_1; q_2, \dots, q_m] \qquad (2 < m \leq n) \qquad (11)$$

ланцюгового дробу $[q_0; q_1, \dots, q_n]$. Підхідний дріб порядку r дробу (11) позначатимемо символом $\frac{P'_r}{Q'_r}$.

За формулами (6)

$$P_m = q_0 P'_{m-1} + Q'_{m-1} \text{ і } Q_m = P'_{m-1} \qquad (12)$$

Але оскільки за припущенням формули (10) правильні для $s = m - 1$, то, застосувавши їх до дробу $[q_1; q_2, \dots, q_m]$, дістанемо:

$$P'_{m-1} = q_m P'_{m-2} + P'_{m-3}, \qquad Q'_{m-1} = q_m Q'_{m-2} + Q'_{m-3} \qquad (13)$$

(тут стоїть q_m, а не q_{m-1}, оскільки дріб починається з q_1, а не з q_0).

Зі співвідношень (12), (13) і за формулами (6):

$$P_m = q_0(q_m P'_{m-2} + P'_{m-3}) + (q_m Q'_{m-2} + Q'_{m-3}) =$$
$$= q_m(q_0 P'_{m-2} + Q'_{m-2}) = q_m P_{m-1} + P_{m-2}.$$
$$Q_m = q_m P'_{m-2} + P'_{m-3} = q_m Q_{m-1} + Q_{m-2},$$

тобто $P_m = q_m P_{m-1} + P_{m-2}$ і $Q_m = q_m Q_{m-1} + Q_{m-2}$.

Теорему доведено.

Послідовне обчислення чисельників P_n і знаменників Q_n підхідних дробів за допомогою формули (10) зручно записувати за схемою:

	q_0	q_1	…	q_{n-1}	q_n
P_s	$P_0 = q_0$	$P_1 = q_0q_1 + 1$	…	$P_{n-1} = q_{n-1}P_{n-2} + P_{n-3}$	$P_n = q_nP_{n-1} + P_{n-2}$
Q_s	$Q_0 = 1$	$Q_1 = q_1$	…	$Q_{n-1} = q_{n-1}Q_{n-2} + Q_{n-3}$	$Q_n = q_nQ_{n-1} + Q_{n-2}$

Щоб обчислити $P_s(s = 2,3,\dots,n)$ за цією схемою, потрібно число q_s, що стоїть над P_s, помножити на число P_{s-1}, яке передує P_s, і до одержаного добутку додати число P_{s-2}, що передує числу P_{s-1}. За аналогічним правилом обчислюється також і Q_s.

Приклад 1: Знайти підхідні дроби ланцюгового дробу:

$$[-2; 2; 1; 3; 1; 1; 4; 3].$$

q_s	-2	2	1	3	1	1	4	3
P_s	-2	-3	-5	-18	-23	-41	-187	-602
Q_s	1	2	3	11	14	25	114	367

$$(S = 0,1,2,\dots,8).$$

Останній підхідний дріб рівний величині усього ланцюгового дробу.

Розглянемо деякі властивості підхідних дробів.

Теорема 2: При $s = 1,2,\dots,n$ справджується співвідношення

$$P_sQ_{s-1} - P_{s-1}Q_s = (-1)^{s-1} \qquad (14)$$

Доведення: При $s = 1$ рівність (14) справедлива:

$P_1 = q_0q_1 + 1, Q_0 = 1, P_0 = q_0, Q_1 = q_1$, тому $P_1Q_0 - P_0Q_1 = 1$.

Нехай рівність (14) правильна при деякому $s = m$ $(1 \le m \le n-1)$, і доведемо, що тоді вона правильна й при тоді $s = m + 1$. Це справді так:

$$P_{m+1}Q_m - P_mQ_{m+1} = (P_mq_{m+1} + P_{m-1})Q_m - P_m(Q_mq_{m+1} + Q_{m-1}) =$$
$$= -(P_mQ_{m-1} - P_{m-1}Q_m) = -(-1)^{m-1} = (-1)^m$$

тобто

$$P_{m+1}Q_m - P_mQ_{m+1} = (-1)^m.$$

Отже, за принципом математичної індукції рівність (14) правильна при будь-якому $s = 1,2,\dots,n.$ З даної теореми випливає справедливість такого твердження.

Наслідок: Кожен підхідний дріб – нескоротній.

Доведення: Дріб $\frac{P_0}{Q_0}$ нескоротній, оскільки $Q_0 = 1$. Нескоротний також і кожен з дробів $\frac{P_s}{Q_s}$ $(s = 1,2,\dots,n)$. Справді, припустимо, що деякий з дробів $\frac{P_m}{Q_m}$ скоротний, тобто $(P_0, Q_0) = d > 1$ $(1 \le m \le n)$. Тоді ліва частина рівності

$$P_m Q_{m-1} - P_{m-1} Q_m = (-1)^{m-1}$$

ділитиметься на число d, а тому і права її частина $(-1)^{m-1}$ також має ділитися на d, що неможливо. Отже, наше припущення невірне. Твердження доведено.

Таким чином, розклад раціональних чисел в ланцюговий дріб дозволяє здійснювати скорочення дробів. Справді, якщо звичайний дріб $\frac{P}{Q}$ розкласти у ланцюговий дріб, то останній підхідний дріб $\frac{P_n}{Q_n}$ цього ланцюгового дробу буде нескоротним дробом і дорівнюватиме $\frac{P_n}{Q_n}$ [16, с. 107].

Приклад 2: Скоротити дріб $\frac{2329}{9911}$.

Знаходячи цей дріб у вигляді скінченного ланцюгового дробу, отримаємо:

$$\frac{2329}{9911} = [0; 4,3,1,10,1,2].$$

Знаходимо підхідні дроби:

	0	4	3	1	10	1	2
P_s	0	1	3	4	43	47	137
Q_s	1	4	13	17	183	200	583

$\frac{2329}{9911} = \frac{137}{583}$, де $\frac{137}{583}$ – вже нескоротній дріб.

Теорема 3 : При $s \ge 2$ справджується співвідношення:

$$P_s Q_{s-2} - P_{s-2} Q_s = (-1)^s q_s. \qquad (15)$$

Доведення: Замінюючи в лівій частині (15) P_s і Q_s по формулам $P_s = = q_s P_{s-1} + P_{s-2}$, $Q_s = q_s Q_{s-1} + Q_{s-2}$ та застосовуючи теорему 2, отримаємо:

$$P_s Q_{s-2} - P_{s-2} Q_s = (P_{s-1} q_{s.} + P_{s-2}) Q_{s-2} - P_{s-2}(Q_{s-1} q_s + Q_{s-2}) =$$

$$= q_s (P_{s-1} Q_{s-2} - P_{s-2} Q_{s-1}).$$

Оскільки за теоремою $P_{s-1} Q_{s-2} - P_{s-2} Q_{s-1} = (-1)^{s-2}$, то

$$P_s Q_{s-2} - P_{s-2} Q_s = (-1)^n a_{n.}$$

Теорему доведено.

Теорема 4: Парні підхідні дроби утворюють зростаючу, а непарні підхідні дроби – спадаючу послідовність.

Доведення: Поділимо обидві частини співвідношення (16) на $Q_s \cdot Q_{s-2}$. Тоді будемо мати:

$$\frac{P_s}{Q_s} - \frac{P_{s-2}}{Q_{s-2}} = \frac{(-1)^s q_s}{Q_s Q_{s-2}},$$

Звідси випливає, що при s парному маємо

$$\frac{P_s}{Q_s} > \frac{P_{s-2}}{Q_{s-2}},$$

а при s непарному маємо

$$\frac{P_n}{Q_n} < \frac{P_{n-2}}{Q_{n-2}}.$$

Теорему доведено.

Два підхідних дроби $\frac{P_{s-1}}{Q_{s-1}}$ і $\frac{P_s}{Q_s}$, у яких номер відрізняється на одиницю, називатимемо сусідніми.

Теорема 5: З двох підхідних дробів $\frac{P_{s-1}}{Q_{s-1}}$ і $\frac{P_s}{Q_s}$ даного ланцюгового дробу парний дріб завжди менше від непарного.

Доведення: Поділімо частини співвідношення (14) на $Q_s \cdot Q_{s-2}$. Тоді матимемо:

$$\frac{P_s}{Q_s} - \frac{P_{s-1}}{Q_{s-1}} = \frac{(-1)^{s-1}}{Q_s Q_{s-1}}$$

При парному s справджується нерівність

$$\frac{P_n}{Q_n} < \frac{P_{n-1}}{Q_{n-1}},$$

а при непарному s

$$\frac{P_s}{Q_s} > \frac{P_{s-1}}{Q_{s-1}}$$

Отже, з двох сусідніх дробів $\frac{P_{s-1}}{Q_{s-1}}$ і $\frac{P_s}{Q_s}$ парний завжди менший від непарного.

Теорему доведено [7, с. 66].

З цієї теореми випливає справедливість наступного твердження.

Наслідок: Кожен парний підхідний дріб даного ланцюгового дробу менший від будь-якого підхідного непарного порядку цього ланцюгового дробу.

Справді, якщо хоча б один парний дріб $\frac{P_{2m}}{Q_{2m}}$ був не менший від деякого підхідного дробу $\frac{P_{2k+1}}{Q_{2k+1}}$ непарного порядку, то згідно з теоремою 4 останній підхідний парний дріб також був би більший від останнього підхідного дробу непарного порядку, що суперечить умові теореми 5.

В теорії ланцюгових дробів існують не тільки скінченні, а й нескінченні дроби, які утворюються з ірраціональних чисел. Надалі будемо розглядати нескінченні ланцюгові дроби у представленні ірраціональних чисел та їх збіжності.

1.3. Нескінченні ланцюгові дроби

1.3.1. Представлення ірраціональних чисел нескінченними ланцюговими дробами

Для ірраціонального числа розклад в ланцюговий дріб повинен бути нескінченним, оскільки скінченний ланцюговий дріб дорівнює раціональному числу [10, с. 39].

Вираз

$$q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \cdots}}, (q_i \in Z, i = 1, \dots; q_2, \dots > 0) \qquad (1)$$

який виникає при такому процесі, називається правильним нескінченним ланцюговим дробом або дробом нескінченної довжини. Позначається він $(q_1, q_2, \dots)$, а числа $q_1, q_2, \dots -$ її елементами або неповними частками.

Розклад ірраціонального числа α може бути тільки в єдиному вигляді, тому що процес виділення цілої частини – однозначний.

Розглянемо розкладання ірраціонального числа в ланцюговий дріб. Нехай $\alpha = \sqrt{11}$. Виділимо з нього цілу частину $\left|\sqrt{11}\right| = 3$, а дробову частину $\sqrt{11} - 3$, яка менша за 1, представимо у вигляді $\frac{1}{\alpha_2}$, де $\alpha_2 = \frac{1}{\sqrt{11}-3} > 1$.

Повторюючи виділення цілої частини та обернення дробової, ми одержимо:

$$\alpha = \alpha_1 = \sqrt{11} = 3 + \frac{1}{\alpha_2}, \alpha_2 > 1;$$

$$\alpha_2 = \frac{1}{\sqrt{11} - 3} = \frac{\sqrt{11} + 3}{2} = 3 + \frac{1}{\alpha_3}, \alpha_3 > 1;$$

$$\alpha_3 = \frac{2}{\sqrt{11} - 3} = \frac{2(\sqrt{11} + 3)}{2} = 6 + \frac{1}{\alpha_4}, \alpha_4 > 1.$$

Якщо зупинитися на цьому кроці, то матимемо:

$$\alpha = 3 + \cfrac{1}{3 + \cfrac{1}{6 + \cfrac{1}{\alpha_4}}}$$

З іншого боку, з формули для α_3 бачимо, що $\sqrt{11} = 3 + \frac{1}{\alpha_4}$, тому $\alpha_3 = \alpha_4$, внаслідок чого, починаючи з даного моменту, неповні частки стануть повторюватися.

Нескінченний неперервний дріб, який має певну послідовність неповних часток, починаючи з деякого номера періодично повторюється, називається періодичним неперервним дробом.

Якщо періодичне повторення починається з першого номеру, то ланцюговий дріб називається чисто періодичним, в іншому ж випадку – змішано періодичним.

Чисто періодичний дріб $(q_1', \dots, q_e', q_1', \dots, q_e', \dots)$ записується у вигляді $\left((q_1', \dots, q_e')\right)$, а змішано періодичний $(q_1, \dots, q_k, q_1', \dots, q_e', q_1', \dots, q_e', \dots)$ – у вигляді $\left(q_1, \dots, q_k, (q_1', \dots, q_e')\right)$.

Тоді, $\sqrt{11}$ розкладається в змішано періодичний дріб (3,3,6,3,6,….) або (3,(3,6)).

У загальному випадку розкладання дійсного ірраціонального числа α таке ж, як і у вище наведеному прикладі. Зупиняючись в процесі виділення цілої частини після $k-$го кроку, матимемо:

$$\begin{cases} \alpha = \alpha_1 = q_1 + \frac{1}{\alpha_2}, q_1 = [\alpha_1], \alpha_2 > 1; \\ \alpha_2 = q_2 + \frac{1}{\alpha_3}, q_2 = [\alpha_2], \alpha_3 > 1; \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ \alpha_k = q_k + \frac{1}{\alpha_{k+1}}, q_k = [\alpha_k], \alpha_{k+1} > 1; \end{cases} \qquad (2)$$

З цього слідує:

$$\alpha = \cfrac{1}{q_2 + \cfrac{1}{\dots \\ \dots \\ + \cfrac{1}{q_k + \cfrac{1}{\alpha_{k+1}}}}}$$

α_k числа називаються залишковими числами $k-$розкладання [2].

Для нескінченного ланцюгового дробу (1) можна побудувати нескінченну послідовність скінченних дробів $\gamma_1 = q_1, \gamma_2 = (q_1, q_2), \dots, \gamma_k = (q_1, \dots, q_k), \dots$, які називаються підхідними дробами. Закон їх утворення такий же, як і для підхідних дробів скінченних неперервних дробів, тому що цей закон залежить тільки від неповних часток $q_1, \dots, q_k$, і зовсім не залежить від того, чи є q_k останнім елементом або за ним слідує ще один q_{k+1}. Тому для них зберігаються також властивості, які виводяться із закону утворення чисельників і знаменників підхідних дробів:

1) $\gamma_k = \frac{P_k}{Q_k} = \frac{q_k P_{k-1} + P_{k-2}}{q_k Q_{k-1} + Q_{k-2}}$,

причому $P_k = q_k P_{k-1} + P_{k-2};\ Q_k = q_k Q_{k-1} + Q_{k-2}$.

2) $P_kQ_{k-1} - P_{k-1}Q_k = (-1)^k$, звідки випиває нескоротність підхідних дробів $\gamma_k = \frac{P_k}{Q_k}$

3) $\gamma_k - \gamma_{k-1} = \frac{(-1)^k}{Q_kQ_{k-1}}$

Тепер порівняємо підхідний дріб γ_{k+1} та частину розкладання α до залишкового члена α_{k+1}:

$$\gamma_{k+1} = \cfrac{1}{q_2 + \cfrac{1}{\ddots + \cfrac{1}{q_k + \cfrac{1}{q_{k+1}}}}}$$

та

$$\alpha = \cfrac{1}{q_2 + \cfrac{1}{\ddots + \cfrac{1}{q_k + \cfrac{1}{q_{k+1}}}}}$$

Бачимо, що обчислення γ_{k+1} по γ_k проводиться в такий же спосіб, як і обчислення α по γ_k. Відмінність полягає лише в тому, що в першому випадку γ_k заміняється на $q_k + \frac{1}{q_{k+1}}$, а в другому q_k на $q_k + \frac{1}{q_{k+1}}$. Тому завдяки формулі $\gamma_{k+1} = \frac{q_{k+1}P_k + P_{k-1}}{q_{k+1}Q_k + Q_{k-1}}$ можемо зробити висновок про справедливість співвідношення

$$\alpha = \frac{q_{k+1}P_k + P_{k-1}}{q_{k+1}Q_k + Q_{k-1}} \qquad (3)$$

Завдяки цій формулі можна довести наступну теорему щодо розташування підхідних дробів у розкладі $\alpha \in R$.

Теорема 1: Дійсне число α завжди знаходиться між двома сусідніми підхідними дробами свого розкладу. Причому воно ближче до наступного, ніж до попереднього підхідного дробу.

Доведення: З формули (3) випливає:

$$\alpha \cdot \alpha_{k+1} \cdot Q_k + \alpha \cdot Q_{k-1} = \alpha_{k+1} \cdot P_k + P_{k-1}$$

$$\alpha_{k+1} \cdot (\alpha \cdot Q_k - P_k) = P_{k-1} - \alpha \cdot Q_{k-1}$$

$$\alpha_{k+1} \cdot Q_k \cdot \left(\alpha - \frac{P_k}{Q_k}\right) = Q_{k-1} \cdot \left(\frac{P_{k-1}}{Q_{k-1}} - \alpha\right)$$

$$\alpha_{k+1} \cdot Q_k \cdot (\alpha - \gamma_k) = Q_{k-1} \cdot (\gamma_{k-1} - \alpha)$$

Але $\alpha_{k+1} > 1$, $Q_k > Q_{k-1}$, і тому $\alpha_{k+1} \cdot Q_k > Q_{k-1} > 0$.

З цього слідує:

1) $(\alpha - \gamma_k)$ та $(\gamma_{k-1} - \alpha)$ мають однаковий знак, а це означає, що α перебуває між γ_{k-1} та γ_k ,
2) $|\alpha - \gamma_k| < |\gamma_{k-1} - \alpha|$, тобто це означає, що α ближче до γ_k.

Теорему доведено.

1.3.2. Збіжність нескінченних ланцюгових дробів

Означення 1: Нескінченній дріб $q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \cdots}}$ називається збіжним, якщо існує границя його підхідних дробів, тобто $\lim\limits_{n\to\infty} \frac{P_n}{Q_n}$.

Означення 2: Величиною нескінченного збіжного ланцюгового дробу називається границя його підхідних дробів, тобто таке число α, що $\alpha = \lim\limits_{n\to\infty} \frac{P_n}{Q_n}$.

Скінченні та нескінченні ланцюгові дроби об'єднують спільним поняттям ланцюгових дробів, розуміючи під цим вираз виду $[q_0; q_1, ...]$, де послідовність цілих чисел $q_0, q_1 \geq 1, q_2 \geq 1 ...$ може бути скінченною або нескінченною, причому у випадку скінченної послідовності останній член буде $q_n > 1$ [4, с. 95].

Властивості підхідних дробів, їх чисельників та знаменників, скінченних підхідних ланцюгових дробів справедливі і для нескінченних. Дійсно, як би не було велике число n, підхідні дроби $\frac{P_0}{Q_0}, \frac{P_1}{Q_1}, \ldots, \frac{P_n}{Q_n}$ до нескінченного дробу $[q_0; q_1, \ldots]$ є також підхідними дробами до скінченного дробу $[q_0; q_1, \ldots, q_n, q_{n+1}]$, так що всі властивості скінченних підхідних дробів є вірними і для всіх n.

Теорема 1: Якщо $q_0, q_1, \ldots$ - елементи ланцюгового дробу $q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \cdots}}$, то послідовність чисел P_n та Q_n, визначена рекурентними умовами:

$$\text{при } n \geq 2 \begin{cases} P_n = P_{n-1} q_n + P_{n-2} \\ Q_n = Q_{n-1} q_n + Q_{n-2} \end{cases} \qquad (1)$$

та початковими умовами:

$$P_0 = q_0, Q_0 = 1, P_1 = q_0 q_1 + 1, Q_1 = q_1, \qquad (2)$$

має властивість, що при всіх n співвідношення $\frac{P_n}{Q_n}$ рівне $n-$ му підхідному дробу $[q_0; \ldots, q_n]$.

Теорема 2: При збільшенні номера n знаменники Q_n нескінченного ланцюгового дробу, починаючи з $n = 1$, монотонно, необмежено зростають.

Теорема 3: При збільшенні n чисельники P_n додаткового нескінченного ланцюгового дробу монотонно, необмежено зростають.

Теорема 4: Модулі відстаней між сусідніми підхідними дробами монотонно зменшуються зі збільшенням номера та наближаються до нуля.

Доведення: До цього було доведено для скінченних дробів, що

$$\left| \frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n} \right| = \left| \frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}} \right|$$

і згідно з теоремою 2 $Q_n \to \infty$, то

$$\left| \frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n} \right| = \frac{1}{Q_{n+1} Q_n} \to 0.$$

Теорема 5: Будь-який нескінченний ланцюговий дріб збігається.

Доведення: Нехай даний ланцюговий дріб $[q_0; q_1, \ldots]$, де всі q_n −цілі числа та $q_n \geq 1$ при всіх $n = 1,2,3 \ldots$. Підхідні дроби з парними та непарними номерами є лівими та правими кінцями системи вкладених один в один інтервалів. Згідно з теоремою 4 маємо: $\left| \frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n} \right| \to 0$, так що довжини інтервалів : $\left(\frac{P_0}{Q_0}, \frac{P_1}{Q_1} \right), \left(\frac{P_2}{Q_2}, \frac{P_3}{Q_3} \right), \ldots$ наближаються до нуля при збільшенні n.

Згідно з відомою теоремою математичного аналіза ліві та праві кінці такої системи вкладених один в один інтервалів, довжини яких наближаються до нуля,

мають спільну границю, яка являє собою деяке дійсне число α, таке, що $\alpha = \lim\limits_{n\to\infty} \frac{P_n}{Q_n}$.

Розглянувши представлення скінченних та нескінченних ланцюгових дробів можемо перейти до розгляду їх застосування, оскільки вони знайшли своє місце не тільки в математиці, а й в інших науках та сферах діяльності людини.

РОЗДІЛ ІІ. ЗАСТОСУВАННЯ ЛАНЦЮГОВИХ ДРОБІВ

2.1. Ланцюгові дроби в математиці

2.1.1. Застосування ланцюгових дробів до розв'язування рівнянь

2.1.1.1. Діофантові рівняння виду $ax + by = c$

У класичному розумінні, діофантові рівняння – це поліноміальні рівняння з цілими раціональними коефіцієнтами, змінні в яких можуть набувати лише цілі значення, або системи алгебраїчних рівнянь з цілими коефіцієнтами, які містять число невідомих, яке перевищує число рівнянь.

Так вони названі на честь давньогрецького математика Діофанта Александрійського. Діофантові рівняння також можуть називати невизначеними. Найважливішим твором Діофанта є «Арифметика», який містив 13 книг. Але до нашого часу збереглись тільки 6 перших книг. В них зібрано 189 задач на знаходження цілих додатніх розв'язків невизначених рівнянь, до яких підібрані ілюстрації та методи розв'язування [19, с. 152].

Хоча на перший погляд їх розв'язування може здатися дуже складним, але існують методи, які дозволяють розв'язувати такі рівняння навіть учню середньої школи. Отже, розв'язати діофантове рівняння означає:

1) з'ясувати, чи має дане рівняння розв'язок в цілих числах;
2) якщо ми дізналися, що дане рівняння має розв'язок в цілих числах, то треба далі з'ясувати скінченна чи нескінченна множина його розв'язків;
3) останній крок – знайти всі цілі розв'язки цього рівняння.

Діофантові рівняння не входять в програму шкільного курсу математики, але можуть зустрічатися в завданнях математичних олімпіад (для учнів та студентів) різних рівнів.

Розв'язування діофантового рівняння $ax + by = c$, де $a,\ b, c$ –цілі коефіцієнти, зводиться до наступного алгоритму:

1) для початку потрібно представити дріб $\frac{a}{b}$ у вигляді скінченного ланцюгового дробу та записати його;

2) скласти таблицю для знаходження значень чисельника та знаменника відповідних дробів $\frac{P_k}{Q_k}$ для отриманого ланцюгового дробу, де останній відповідний дріб $\frac{P_n}{Q_n} = \frac{a}{b}$.

	q_0	q_1	q_2	…	q_n
P_i	q_0	$q_0q_1 + 1$	$(q_0q_1 + 1)q_2 + q_0$	…	a
Q_i	1	q_0	q_2q_1	…	b

Загальний розв'язок в цілих числах невизначеного рівняння $ax + by = c$, де $(a, b) = 1$, можна записати:

$$\begin{cases} x = (-1)^{n-1}cQ_{n-1} + bt, \\ y = (-1)^n cP_{n-1} - at, \end{cases} t \in \mathbb{Z}.$$

Розглянемо приклад за даним алгоритмом.

Приклад 1: Розв'яжіть в цілих числах методом ланцюгових дробів рівняння $38x + 117y = 209$.

Розв'язання:

$$38x + 117y = 209,$$

$$(38{,}117) = 1,$$

Розкладемо дріб $\frac{38}{117}$ у ланцюговий дріб, одержимо:

$$\frac{12}{31} = [0; 3{,}12{,}1{,}2]$$

Складемо таблицю:

n		0	1	2	3	4
q_n		0	3	12	1	2
P_n	1	0	1	12	13	38
Q_n	0	1	3	37	40	117

$$P_{n-1} = P_3 = 13$$

$$Q_{n-1} = Q_3 = 40$$

Тоді загальний розв'язок буде:

$$\begin{cases} -x = (-1)^3 \cdot 209 \cdot 40 + 117t, \\ y = (-1)^4 \cdot 209 \cdot 12 - 38t, \end{cases} t \in \mathbb{Z}$$

$$\begin{cases} x = -8360 + 117t, \\ y = 2717 - 38t, \end{cases} t \in \mathbb{Z}$$

$71 \cdot 117 = 8307$, тоді приймаючи $t = 71$, одержимо: $\begin{cases} x = -53 + 117l, \\ y = 19 - 38l, \end{cases} l \in \mathbb{Z}.$

Відповідь: : $\begin{cases} x = -53 + 117l, \\ y = 19 - 38l, \end{cases} l \in \mathbb{Z}.$

2.1.1.2. Рівняння Пелля

Рівняння Пелля – це клас невизначених рівнянь другого порядку. Вони пов'язані з багатьма задачами з теорії чисел. Отже, що ж таке рівняння Пелля? Це рівняння виду $x^2 - my^2 = 1$, де $m -$ це ціле додатнє число, яке не є точним квадратом (якщо $m^2, m \in N$, то рівняння зводиться до $(x - my)(x + my) = 1$ і не має цілих розв′язків). Розв'язування таких рівнянь – задача непроста, хоч і виконується різними методами елементарної математики.

Зробимо два зауваження: по-перше, при будь-якому m рівняння має принаймні два розв'язки : $x = \pm 1, y = 0$. Ці розв'язки назвемо тривіальними. По-друге, обмежимося знаходженням тільки невід'ємних розв'язків (тобто це розв'язки з невід'ємними x та y), оскільки, якщо змінити знак у x або y, то ліва частина рівняння не зміниться.

Рівняння Пелля, як прийнято їх зараз називати, були знайдені вже в працях математиків Давньої Греції та Індії. В творах індійського математика XII століття Бхаскарі було запропоновано загальний спосіб розв'язування таких рівнянь («Циклічний метод»). Але в ті часи це не поставало питання: чи завжди даний метод веде до розв'язку. В загальному вигляді вище згадану задачу сформулював лише в середині XVII століття математик П'єр Ферма. Наступними у часі знайшли спосіб розв'язування даного рівняння англійські математики Джон Валліс та лорд Броункер, який був відмінний від циклічного. Але й вони не довели, що цей метод завжди може призводити до успіху. Лише вже

наприкінці XVIII століття математик Лагранж довів гіпотезу, яку сформулював П'єр Ферма. Леонард Ейлер випадково приписав авторство цих рівнянь Джону Пеллю. Саме завдяки цій помилці рівняння отримали ім'я математика, який навіть не мав до них відношення.

Отже, як же розв'язати таке рівняння? Першим методом, який спадає на думку, це метод перебору. Тобто, можемо підставляти по черзі числа $x = 1,2, \ldots$ у формулу $y = \sqrt{\frac{x^2-1}{D}}$ до тих пір, поки вираз під коренем не виявиться повним квадратом. Але це не дуже перспективний метод, оскільки розв'язки можуть бути настільки великі, що навіть на самій потужній ЕОМ можна й не добратися звичайним перебором [6, с. 3].

Виявляється, розв'язати рівняння Пелля можна за допомогою неперервних дробів. Розглянемо цей метод (без доведення).

Теорема 1: Нехай $(x, y) -$ додатний розв'язок рівняння Пелля. Тоді $\frac{x}{y} -$ це підхідний дріб $\sqrt{m}$. Тоді всі розв'язки даного рівняння можуть бути знайдені за формулою

$$x + y\sqrt{m} = (x_0 + y_0\sqrt{m})^k,$$

де $k - 1,2, \ldots$, а $(x_0, y_0) -$ розв'язок з найменшим значенням y. Для знаходження найменшого розв'язку треба розкласти число $\sqrt{m}$ в ланцюговий дріб. Якщо $\sqrt{m} = [q_0; \overline{q_1, \ldots, q_n, 2q_0}]$ і $\frac{P_n}{Q_n}$ є підхідним дробом числа $\sqrt{m}$ з номером n, то ${P_n}^2 - m{Q_n}^2 = (-1)^{n-1}$, також якщо $n -$ непарне (довжина періоду парна), то $P_n = x_0$, $Q_n = y_0$ і буде найменшим розв'язком рівняння Пелля. Якщо період непарний ($n -$ парне), то будемо шукати найменший розв'язок за наступною формулою: $x_0 + y_0\sqrt{m} = (P_n + Q_n\sqrt{m})^2$.

Приклад 1: Розв'язати рівняння $x^2 - 5y^2 = 1$ в натуральних числах.

Скористаємось фактом, що $\sqrt{5} = [2; \overline{4,4,4, \ldots}]$. Тоді $\frac{P_n}{Q_n} = [2,4] = \frac{9}{4}$, а $x_0 = 9, y_0 = 4$. Тоді $x + y\sqrt{5} = (9 + 4\sqrt{5})^k, k = 1,2, \ldots$.

Приклад 2. Розв'язати рівняння $x^2 - 7y^2 = 1$.

Розкладемо $\sqrt{7}$ в ланцюговий дріб і отримаємо, що $\sqrt{7} = [2; \overline{1,1,1,4}]$ і

$$\frac{P_n}{Q_n} = 2 + \frac{1}{1 + \dfrac{1}{1 + \dfrac{1}{1+4}}} = \frac{8}{3}.$$

Довжина періоду парна, тому найменший розв'язок рівняння буде $x_0 = 8$, $y_0 = 3$, а розв'язок отримаємо за формулою (в натуральних числах) $x + y\sqrt{7} = (8 + 3\sqrt{7})^k$, де $k = 1,2, \dots$.

При $k = 2$ будемо мати $x = 127, y = 48$.

2.1.2. Число π

Що ж таке число π? Існує стаття, в якій згадується число π, яка називається «Про фонтануючу силу китів». В ній описується задача з практики китоловів. Нехай ви помітили фонтан кита та захотіли визначити, чи варто вирушати на охоту, або ж м'ясо, яке ви отримаєте потім, не варте цього. Насамперед треба дізнатись яка залежність між фонтануючою силою та об'ємом кита. Тому в статті була наведена формула для об'єма кита: $V = \pi r^2 l$, де $r -$ це оцінка половини ширини кита, а $l -$ оцінка його довжини (кит вважається циліндричним). Але тільки важко було пояснити китоловам, що ж таке це число π. В статті було таке пояснення: «…де число π – це константа, яка для гренландських китів рівна 3». Для китів інших порід треба брати інше значення, судячи з усього.

Про наближення числа π знали ще в давнину. Наприклад, є досить точне наближення, яке пов'язують з Архімедом, але воно було відоме ще до нього: $\pi \approx \frac{22}{7} = 3\frac{1}{7}$. І це як раз є початком ланцюгового дробу, в який можемо розкласти число π. Цей дріб нескінченний, тому, беручи довші початкові частини цього дробу, можна отримувати більш точні наближення.

Зауважимо, що чисельник дробу $\frac{22}{7}$ – двозначне число, знаменник – однозначне, а точність наближення цього дробу – три десяткові знака *а)* (рис.1).

Шість правильних десяткових знаків зможемо отримати, якщо обірвемо даний ланцюговий дріб далі *в)* (рис.1).

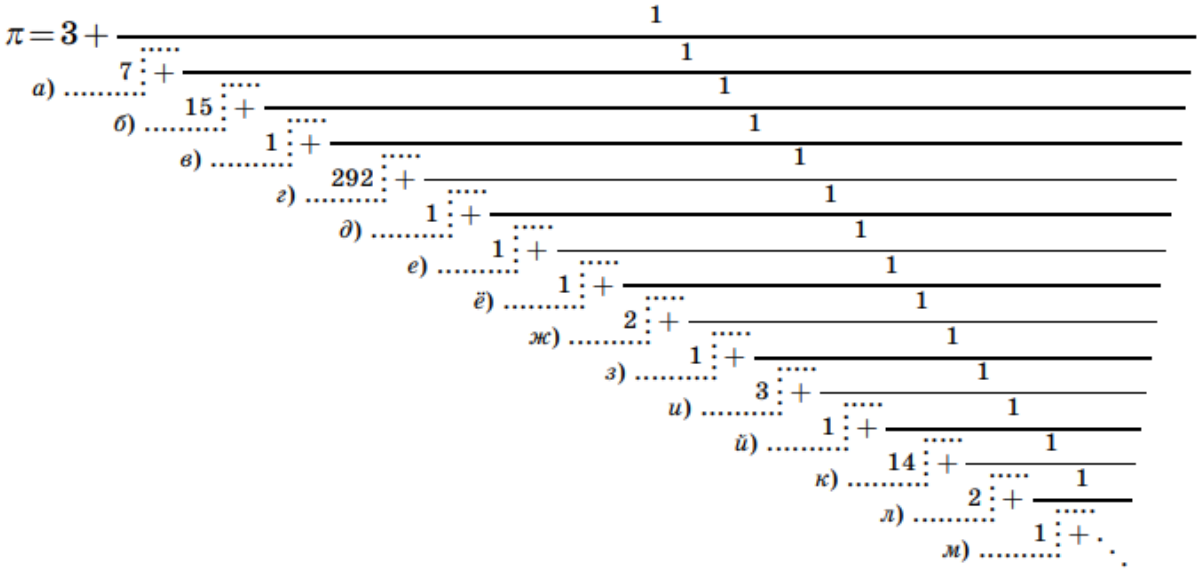


Рис.1

Нове наближення – це відношення двох тризначних чисел. Існує правило, яке допоможе запам’ятати цей дріб: треба написати велике число 113355, розбити його на два тризначних числа та розділити більше на менше. Отримаємо:

$$\pi \approx 3 + \frac{1}{7 + \frac{1}{16}} = \frac{255}{113}.$$

Але є більш прості наближення цього числа, наприклад, відношення довжини кола до його діаметра.

Нам відомо, що число $\pi = 3{,}141\,592\ldots$. Отже, можемо записати його у вигляді нерівності $3{,}141 < \pi < 3{,}142$.

Далі запишемо дроби лівої та правої частини вищезгаданої нерівності у вигляді ланцюгових дробів:

$$3{,}141 = 3 + \frac{1}{\frac{1000}{141}} = 3 + \frac{1}{7 + \frac{1}{\frac{141}{13}}} = 3 + \frac{1}{7 + \frac{1}{10 + \frac{1}{\frac{13}{11}}}} =$$

$$= 3 + \frac{1}{7 + \frac{1}{10 + \frac{1}{1 + \frac{1}{\frac{11}{2}}}}} = 3 + \frac{1}{7 + \frac{1}{10 + \frac{1}{1 + \frac{1}{5 + \frac{1}{2}}}}}$$

$$3{,}142 = 3 + \frac{1}{\frac{1000}{142}} = 3 + \frac{1}{7 + \frac{1}{\frac{142}{13}}} = 3 + \frac{1}{7 + \frac{1}{10 + \frac{1}{\frac{13}{12}}}} = 3 + \frac{1}{7 + \frac{1}{10 + \frac{1}{1 + \frac{1}{12}}}}$$

Бачимо, що існує спільна частина цих розкладів, яка дає наближення для числа: $\pi \approx 3\frac{1}{7} = \frac{22}{7}$. Дане наближення є точним до трьох знаків після десяткової коми і похибка менша, ніж $\frac{1}{500}$.

Якщо взяти для числа π наближення такі:

$$3{,}141591 < \pi < 3{,}141592$$

то за таким же методом отримаємо:

$$\pi \approx 3 + \frac{1}{7 + \frac{1}{15}} = \frac{333}{106}.$$

Дане наближення має чотири правильні цифри після десяткової коми і похибку меншу, ніж $\frac{1}{10000}$.

Можемо взяти ще більш точне наближення:

$$3{,}141592653 < \pi < 3{,}141592654.$$

Знову ж за таким же методом отримаємо ланцюговий дріб:

$$\pi \approx 3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{1 + \cdots}}} = \frac{355}{113}.$$

Таке наближення має похибку, яка не перевищує $\frac{1}{1000000}$. Воно було відкрите ще у давні часи римським філософом Андріаном Мецієм [8, с. 3].

2.1.3. Геометрична теорія ланцюгових дробів. Алгоритм «витягування носів»

В основі геометрії чисел по Мінковскому знаходиться звичайний шкільний зошит у клітинку – площа, на якій намальована координатна сітка. Розглянемо будь-яку пряму $y = ax$; наприклад нехай це буде $a = \frac{10}{7}$. Якщо наше a −це раціональне число, то на цій прямій будуть ще цілі точки, крім початку координат. У даному випадку пряма буде виглядати наступним чином:
виявляється, побудова ланцюгового дробу числа a пов'язане зі знаходженням цілих точок, які знаходяться близько з даною прямою.

А саме, існує геометричний алгоритм «витягування носів», який дозволяє будувати цілі точки, які знаходяться максимально близько до прямої, одну за одною та в той самий час отримувати ланцюговий дріб.

Отже, розглянемо цей алгоритм.

Нехай існують одиничні вектори (рис.2): $\overrightarrow{e_1}$ і $\overrightarrow{e_2}$. Між ними знаходиться наша пряма. Далі, до вектора $\overrightarrow{e_1}$ будемо додавати вектор $\overrightarrow{e_2}$ до тих пір, поки не перескочимо через пряму. Тобто, треба знайти найбільше натуральне число a_0, таке, щоб кінець вектора $\overrightarrow{e_3} = \overrightarrow{e_1} + a_0\overrightarrow{e_2}$ знаходився все ще нижче за пряму. В даному випадку $a_0 = 1$.

Далі продовжуємо. Щоб отримати вектор $\overrightarrow{e_4}$, додамо до $\overrightarrow{e_2}$ вектор $\overrightarrow{e_3}$ (який вже є), помножений на коефіцієнт a_1. Цей коефіцієнт обираємо так, щоби не перескочити через пряму, тобто так, щоби вектор $\overrightarrow{e_4}$ залишався вище прямої, а якщо до нього додати $\overrightarrow{e_3}$, то ми перейдемо через пряму. З цього випливає, що $a_1 = 2$. Отримаємо вектори все більш довші, тому алгоритм і назвали «витягування носів».

Далі, $\overrightarrow{e_5} = \overrightarrow{e_3} + a_2\overrightarrow{e_4}$. Якщо візьмемо $a_2 = 3$, то попадемо як раз на пряму.

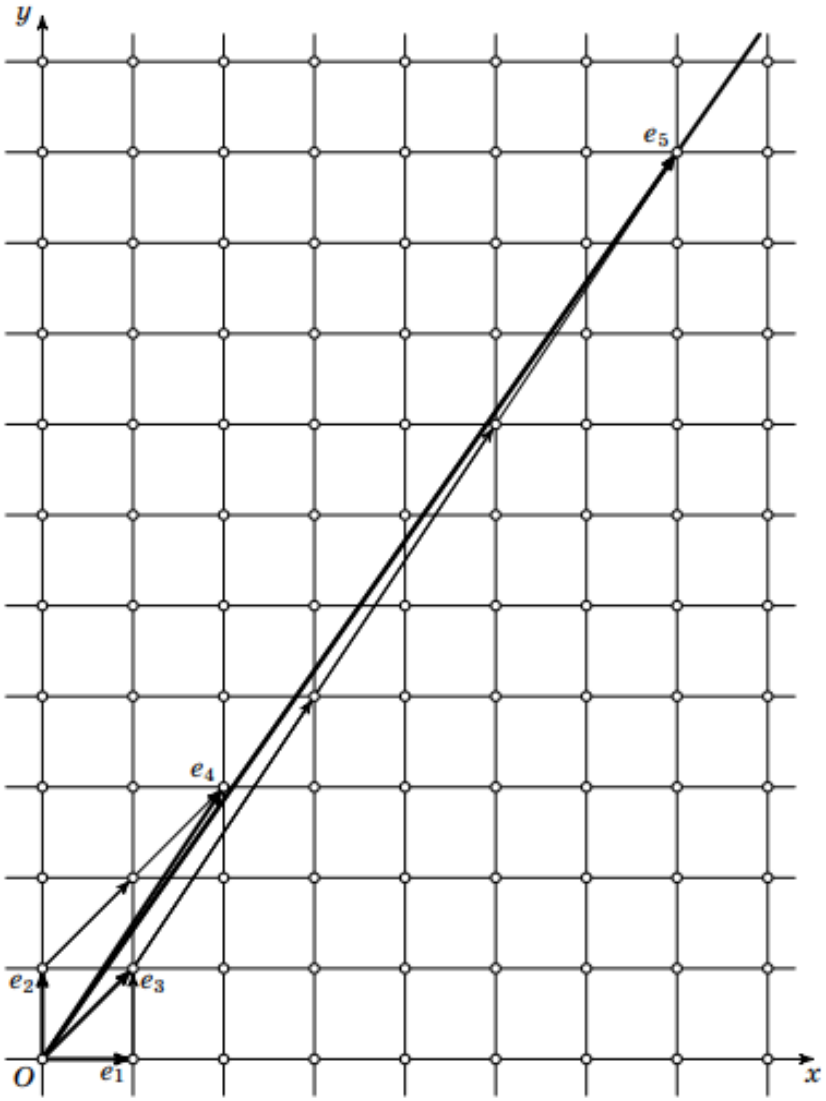


Рис.2

Отже, $a_0 = 1, a_1 = 2, a_2 = 3$,

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = 1 + \frac{1}{2 + \frac{1}{3}} = \frac{10}{7}.$$

Можна довести, що даний алгоритм завжди дає цілі числа a_0, a_1,… , які і будемо отримувати при розкладі a в ланцюговий дріб. Точки, які ми отримуємо, відразу дають і елементи ланцюгового дробу.

Доведення цього факту нескладне. Головне – що, пряма, яка має рівняння $y = Ax$, в будь-якій системі координат задається так же рівнянням $x = \frac{1}{A}y$ в системі координат, де переставили між собою осі абсцис та ординат. А пряма з рівнянням $y = Ax$ в системі з базисними векторами e (на осі x) та f (на осі y) при $A = a + B$ задається рівнянням $z = Bw$ в системі з базисними векторами

$e + af$ (на осі w) та f (на осі z). Ланцюговий дріб отримуємо при послідовному застосуванні (по черзі) цих двох фактів.

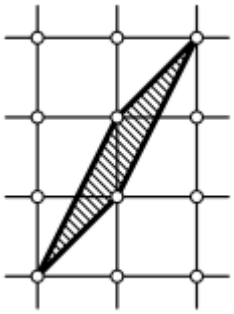


Рис.3

Розглянемо дві леми (без доведень), які є основою геометрії чисел.

Лема 1. Розглянемо на площі з координатною сіткою «пустий» паралелограм (рис.3) з вершинами у вузлах сітки, тобто такий, що ні всередині, ні на його границях немає інших вузлів сітки. Площа такого паралелограма дорівнює 1.

Лема 2. (формула площі паралелограма)

Розглянемо паралелограм (рис.4), який натягнутий на вектори з координатами (a, b) і (c, d) (ці числа не обов'язково мають бути цілі). Будемо вважати, що його площа має додатній знак, якщо оберт від першого вектора до другого йде в ту ж сторону, що і оберт від осі Ox до Oy, і від'ємний знак в протилежному випадку. Тоді

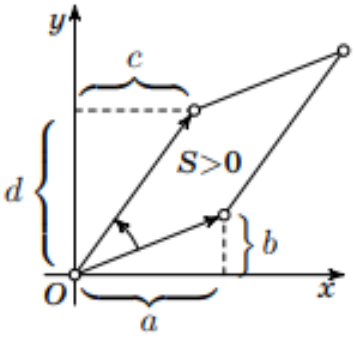


Рис.4

$$S = \begin{vmatrix} a & b \\ c & d \end{vmatrix}$$

(число $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$ називається визначником матриці $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$).

Тепер повернемося до алгоритму. Вектори $\overrightarrow{e_1}$ і $\overrightarrow{e_2}$ визначають одиничний квадрат, а тому відповідний визначник рівний одиниці. Візьмемо вектор $\overrightarrow{e_3}$. Від $\overrightarrow{e_2}$ до $\overrightarrow{e_3}$ оберт у від'ємну сторону, всередині та на сторонах паралелограма, натягнутого на ці вектори, немає цілих точок, тому цей визначник рівний -1. Якщо продовжувати далі, то бачимо, що побудова кожен раз має такий алгоритм: існує паралелограм (натягнутий на вектори $\overrightarrow{e_{k-1}}$ та $\overrightarrow{e_k}$), до однієї його сторони ($\overrightarrow{e_{k-1}}$) додаємо іншу декілька разів, далі замінюємо першу сторону на отриману суму ($\overrightarrow{e_{k+1}} = \overrightarrow{e_{k-1}} + a_{k-2}\overrightarrow{e_k}$) і міняємо сторони місцями. При цьому величина площі не змінюється, а змінюється тільки знак.

Нехай $(q_k, p_k) -$ це координати вектора $\overrightarrow{e_k}$; причому q_k та $p_k -$ це цілі числа. Площа S_k паралелограма, який натягнутий на вектори $\overrightarrow{e_k}$ та $\overrightarrow{e_{k+1}}$, рівний $\begin{vmatrix} q_k & p_k \\ q_{k+1} & p_{k+1} \end{vmatrix}$ [8, с. 5].

2.2. Ланцюгові дроби в навколишньому світі

2.2.1. Ланцюгові дроби в фізиці та астрономії

У фізиці ланцюгові дроби вперше з'явились в астрономічних дослідженнях. При описі сумірності частот різних періодичних рухів, наприклад кеплеровських рухів планет, астрономам довелось дізнатися раціональні наближення до цих ірраціональних чисел. При цьому важливе значення мало, наскільки можливо наблизити ірраціональне число раціональним дробом з не дуже великим знаменником. Досить близьке наближення називається резонансом і може привести до поганої реакції однієї планети рухами іншої.

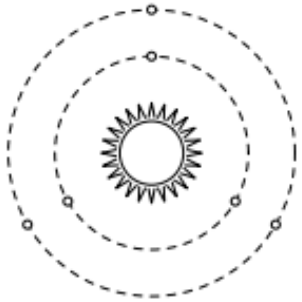


Рис.5

Розглянемо наступну модель (рис.5). Нехай дві планети обертаються навколо «Сонця» по концентричних колах в одну сторону. Якщо відношення періодів їх обертання навколо «Сонця» з великою точністю рівне раціональному числу, нехай це буде $\frac{10}{7}$, то ці дві планети знаходитимуться на маленькій відстані (настільки мінімальній, наскільки це можливо), одна від одної поблизу трьох фіксованих точок. На маленькій відстані, як це відомо, найбільша гравітація, тому над орбітами цих двох планет будуть відбуватися сильні деформації лише в трьох напрямках. Планети при цьому будуть неначе «зіштовхувати» одна одну з орбіт.

Інша річ, якщо відношення періодів обертання планет з великою вірогідністю – раціональне число з більшим знаменником. Воно довільне, тому нехай буде $\frac{151}{700}$. Тоді «точок великої гравітації» 549, і взаємний вплив («стикання») планет більш «розмазаний».

Саме тому астрономи дуже рано (цим цікавились ще Ньютон та Кеплер) задалися таким питанням, які ж практичні величини цих, як кажуть, неповних частот (елементів) ланцюгового дробу, тобто якщо маємо

$$\alpha = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\dots}}},$$

тоді наскільки великі числа $q_0, q_1, \dots$, якщо число α – звичайне випадкове число. Якщо будь-яке число, наприклад q_2, завелике (нехай це буде мільйон), то наближення $\alpha \approx q_0 + \frac{1}{q_1}$ (яке ми отримаємо, якщо обірвемо дріб перед q_2) буде дуже точним. Тому питання постає в тому, чи збільшуються ці коефіцієнти та з якою швидкістю, мають вони реальне астрономічне значення для долі всього Всесвіту, для долі Сонячної системи, нашої цивілізації.

Перше важливе математичне дослідження цього питання належало астроному Гуго Гільдену, який опублікував його в доповідях Паризької академії наук у 1888 році (H. Gylden. Quelques remarques relativement ´ a la repr ` esentation des nombres ´ irrationels par des fraction continues // C. R. Acad. Sci. Paris. V. 107. 1888. P. 1584—1587.). Хоча астрономи й досліджували відношення частот різних планет, більших та менших, та знали коефіцієнти q_i цих відношень. Не дуже багато, але деякі знали. А Гільден навів таблиці, з яких можна дізнатися, наскільки великі числа q_i.

Теорема, яка дала астрономам остаточку відповідь на це питання називається теоремою Кузьміна (хоча, можливо, була доведена шведським математиком Андерс Віманом, який опублікував її у 1900 році, а сам Кузьмін довів її лише у 1928 році).

Найважливіше відкриття для даної теореми зробив Карл Гаусс. Хоча він не тільки не доводив, але й не формулював цю теорему, він знайшов відповідь – тобто, вказав на вірогідність того, що якесь з чисел q_i рівне 1,2,3… . Ці вірогідності дає нам формула Гаусса. Але як саме він знайшов цю формулу та який самі він надавав сенс їй, - невідомо.

Ймовірність визначається наступним чином: треба обрати числа $q_0, q_1, ..., q_n$ (які є цілими додатними числами), потім подивитися скільки серед них, нехай, одиниць, поділити їх на n та наблизити n до нескінченності. Виявляється, що границя існує і рівна одному й тому ж числу при майже всіх q. Це число саме й називається вірогідністю p_1 появи одиниці.

Теорема Кузьміна каже, що вірогідність появи деякого числа k задається формулою:

$$p_k = \frac{1}{\ln 2} \ln\left(1 + \frac{1}{k(k+2)}\right)$$

($\frac{1}{\ln 2}$ – не залежить від числа k нормуючий коефіцієнт; він потрібен для того, щоби сума всіх ймовірностей була рівна 1).

Якщо ж k – велике число, тоді

$$\frac{1}{k(k+2)} \approx \frac{1}{k^2}$$

це маленьке число, а натуральний логарифм суми одиниці та маленького числа приблизно рівний цьому маленькому числу. Тому, чим більше k, тим ймовірність p_k зменшується як $\frac{1}{k^2 \ln 2}$ – обернено пропорційного квадрату k, і коли число k велике, тоді ймовірність маленька. Найбільша ймовірність має одиниця: якщо $k = 1$, тоді

$$\frac{1}{k(k+2)} = \frac{1}{3},\ \ln\left(1 + \frac{1}{3}\right) \approx \frac{1}{3},\ p_1 \approx \frac{1}{3 \ln 2} \approx 0{,}48.$$

Бачимо, що одиниць дуже багато: майже половина [8, с. 12].

2.2.2. Ланцюгові дроби в криптографії

У сучасному світі ланцюгові дроби знайшли місце і в такій сфері як криптографія.

Нехай $\frac{a}{b}$ –раціональне число, в якому знаменник додатній (a, b –цілі числа). Застосуємо до цих чисел алгоритм Евкліда, який зазвичай використовують для знаходження НСД (a, b):

$$a = bq_0 + r_1, \frac{a}{b} = q_0 + \frac{1}{\frac{b}{r_1}},$$

$$b = r_1 q_1 + r_2, \frac{b}{r_1} = q_0 + \frac{1}{\frac{r_1}{r_2}},$$

…

$$r_{n-2} = r_{n-1}q_{n-1} + r_n, \qquad \frac{r_{n-2}}{r_{n-1}} = q_{n-1} + \frac{1}{\frac{r_{n-1}}{r_n}},$$

$$r_{n-1} = r_n q_n, \frac{r_{n-1}}{r_n} = q_n.$$

Тоді

$$\frac{a}{b} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ldots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}}$$

Числа $q_0, q_1, \ldots$ називаються неповними частками послідовних поділів у алгоритмі Евкліда, а останній вираз, який ми отримали, - ланцюговим дробом, який можна позначати $\frac{a}{b} = [q_0; \ldots, q_n]$.

Дроби $\delta_1 = q_0, \delta_2 = q_0 + \frac{1}{q_1}, \ldots$ називаються підхідними. Для таких дробів $\delta_s = \frac{P_s}{Q_s}, s = 2,3, \ldots, n$ справджується формула:

$$\frac{P_s}{Q_s} = \frac{q_s P_{s-1} + P_{s-2}}{q_s Q_{s-1} + Q_{s-2}}, P_0 = 1, Q_0 = 0, P_0 = q_1, Q_1 = 1.$$

Ланцюгові дроби можна також ефективно використовувати при розв'язання конгруенцій $ax \equiv b(\mathrm{mod}\, m)$, за умови, що a, b, m –цілі, НСД$(a, m) = 1$, розв'язок $ax \equiv b(\mathrm{mod} m)$ – єдиний і подається у вигляді:

$$x \equiv (-1)^{n-1} P_{n-1} b(\mathrm{mod}\, m),$$

де $\frac{m}{a} = [q_0, \ldots, q_n], \delta_{n-1} = \frac{P_{n-1}}{Q_{n-1}}$ [12, с. 1].

.Існує запропонована у 1977 році система RSA, яка є однією з найпопулярніших криптосистем з відкритим ключем. Відкритий ключ – ключ

шифрування – може бути у вільному доступі без втрати стійкості шифру і лише ключ дешифрування (таємний ключ) має триматися у секреті [2, с. 150]. Генерування ключів (відкритого та таємного) в даній системі здійснюється за наступним алгоритмом:

1) обираються два досить великі прості числа p та q, обчислюють їх добуток $n = p \cdot q$. Для числа n далі треба обчислити функцію Ейлера $\varphi(n) = \varphi(p) \cdot \varphi(q) = (p-1)(q-1) = n - p - q - 1$;
2) випадково обирають ціле число e, яке має бути взаємно простим з $\varphi(n)$ та не перевищувати його;
3) для елемента e за алгоритмом Евкліда знаходять елемент d, обернений до e за $\mathrm{mod}\ \varphi(n)$, тобто такий, що $d < \varphi(n)$ і

$$e \cdot d \equiv 1\big(\mathrm{mod}\ \varphi(n)\big).$$

Вище описані дії визначають відкритий ключ e, n і таємний ключ d.

Число n називають модулем, а e і $d-$ відкритою й секретною експонентами відповідно. Пари чисел (e, n) є відкритою частиною ключа, а $(e, d) -$ секретною [4].

Цей таємний ключ, як розв'язок конгруенції $e \cdot d \equiv 1\big(\mathrm{mod}\ \varphi(n)\big)$, можна шукати за формулою $x \equiv (-1)^{n-1} P_{n-1} b(\mathrm{mod}\ m)$, де $\frac{\varphi(n)}{e} = [q_0, \dots, q_k]$, тобто з використанням скінченних ланцюгових дробів.

Розглянемо приклади.

Приклад 1: Проведіть процедуру генерування ключів шифру RSA, якщо $p = 5, q = 7, e = 11$.

1. Відомо, що $p = 5, q = 7$.
2. Обчислюємо функцію Ейлера для $n = p \cdot q = 5 \cdot 7 = 35$;

$$\varphi(p) \cdot \varphi(q) = (p-1)(q-1) = 24.$$

3. З умови маємо елемент $e = 11$. Перевіряємо, що виконуються умови $e \le \varphi(n)$ і $\mathrm{НСД}\big(e, \varphi(n)\big) = 1$.
4. Знаходимо елемент d, обернений до елемента e за модулем $\varphi(n)$, тобто, $11 \cdot\ d \equiv 1(\mathrm{mod}\ 24)$.

Для цього скористаємось алгоритмом Евкліда:

$$24 = 11 \cdot 2 + 2;$$

$$11 = 2 \cdot 5 + 1;$$

$$2 = 1 \cdot 2 + 0.$$

Отже, $1 = 11 \cdot 11 - 24 \cdot 5$; звідки $d = 11$.

Отримали відкритий ключ: $n = 35, e = 11$ та таємний ключ $d = 11$ [2, с. 152].

Приклад 2: Нехай $p = 41, q = 53, e = 1297$. Знайдемо таємний ключ d.

Спочатку переконаємось, що $\text{НСД}\big(e, \varphi(n)\big) = (1297,2080) = 1$ й одночасно знайдемо ланцюговий дріб $\frac{2080}{1297}$. Застосувавши алгоритм Евкліда до 1297 та 2080, знайдемо такий ланцюговий дріб:

$$\frac{2080}{1297} = [1,1,1,1,1,10,4,1,4].$$

Для знаходження таємного ключа розв'яжемо конгруенцію:

$$1297 \cdot d \equiv 1(2080).$$

Розв'язок даної конгруенції можна знайти за формулою

$$x \equiv (-1)^{n-1} P_{n-1} b (\text{mod}\, m).$$

Для цього треба скласти таблицю підхідних дробів, застосувавши при цьому рекурентну формулу $\frac{P_s}{Q_s} = \frac{q_s P_{s-1} + P_{s-2}}{q_s Q_{s-1} + Q_{s-2}}$, $P_0 = 1,\ Q_0 = 0, P_0 = q_1, Q_1 = 1$:

Чисельники підхідних дробів

q_s		1	1	1	1	1	10	4	1
P_s	1	1	2	3	5	8	85	348	433

Тоді за формулою $x \equiv (-1)^{n-1} P_{n-1} b (\text{mod}\, m)$ будемо мати:

$$d \equiv (-1)^8 433 (\text{mod}\ 2080) \equiv 433 (\text{mod}\ 2080).$$

Отже, таємний ключ $d = 433$ [12, с. 3].

Розглянутий приклад є досить ілюстративним, тому що реально в криптосистемі RSA використовують дуже великі прості числа.

Приклад 3: Маємо $(n = 400271, e = 117353) -$ відкриті ключи криптосистеми RSA. За допомогою атаки Вінера визначте закриту експоненту d і значення функції Ейлера, та факторизуйте модуль криптосистеми.

Отже, у криптосистемі RSA закрита експонента $d < \frac{1}{3}\sqrt[4]{n}$, то за відкритим ключем (n, e) можна визначити d, провівши атаку Вінера за наступною схемою:

1) розкласти число $\frac{e}{n}$ у ланцюговий дріб;
2) знайти всі відхідні дроби $\frac{P_i}{Q_i}$ для ланцюгового дробу;
3) з отриманих підхідних дробів знайти послідовним випробуванням той, для якого вираз $eQ_i - 1$ буде ділитися без остачі на P_i. Тоді $Q_i = d$ – закрита експонента (таємний ключ) криптосистеми, а $P_i = k -$ це таке ціле число, для якого $(e, d) - k\ \varphi(n) = 1$, $\varphi(n) -$ значення функції Ейлера.

Отже розкладемо дріб $\frac{e}{n}$ у ланцюговий:

$$\frac{e}{n} = \frac{117353}{400271} = \frac{1}{\frac{400271}{117353}} = \frac{1}{3 + \frac{48212}{117353}} = \frac{1}{3 + \frac{1}{2 + \frac{20929}{48212}}} = \cdots =$$

$$= \cfrac{1}{3 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{3 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{11 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \frac{1}{2}}}}}}}}}}}}}.$$

$$\frac{e}{n} = \frac{117353}{400271} = \left[0; \frac{1}{3}, \frac{1}{2}, \frac{1}{2}, \frac{1}{3}, \frac{1}{3}, \frac{1}{2}, \frac{1}{2}, \frac{1}{11}, \frac{1}{1}, \frac{1}{1}, \frac{1}{1}, \frac{1}{4}, \frac{1}{2}\right].$$

Далі послідовно будемо знаходити підхідні дроби:

i	-1	0	1	2	3	4	5	6	7	8	9	10	11	12	13
b_i			1	1	1	1	1	1	1	1	1	1	1	1	1
a_i		0	3	2	2	3	3	2	2	11	1	1	1	4	2
P_i	1	0	1	2	5	…									
Q_i	0	1	3	7	17	…									

$$\frac{P_1}{Q_1} = \frac{1}{3}; \frac{P_2}{Q_2} = \frac{2}{7}; \frac{P_3}{Q_3} = \frac{5}{17} \dots$$

Для третього підхідного дробу різниця буде

$$e \cdot Q_3 - 1 = 117353 \cdot 17 - 1 = 1995000$$

ділиться націло на $P_3 = 5$.

$d = Q_3 = 17 -$ таємний ключ. Підставивши у рівняння $(e, d) - k\,\varphi(n) = 1$ значення e, k і d зможемо обчислити значення функції Ейлера $\varphi(n) = 399000$. Щоби знайти числа p, q, на які розкладається модуль криптосистеми, нам залишається лише розв'язати систему рівнянь:

$$\begin{cases} n = pq, \\ \varphi(n) = (p-1)(q-1) \end{cases} \Rightarrow \begin{cases} pq = 400271, \\ (p-1)(q-1) = 399000 \end{cases} \Rightarrow \begin{cases} p = 701, \\ q = 571. \end{cases}$$

У додатках наведено приклади програм, які демонструють реалізацію алгоритмів для допомоги генерування ключів (знаходження списку простих чисел, виборка двох будь-яких чисел з цього списку, знаходження їх добутку та знаходження числа e, що воно не більше за $\varphi(n)$).

2.2.3. Юліанський та Григоріанський календарі

З астрономії нам відомо, що один календарний рік має $365{,}24219\ldots$ так звані «середні доби». У повсякденному житті таке відношення року досить складне та незручне, тому була необхідність спростити число, хоча й менш точним через це. При цьому з року в рік накопичується похибка, тому, щоб її компенсувати, до одного року додають один день. Такий рік ми називаєм високосним [17, с. 32].

Спочатку представимо число (справжнє) року у вигляді підхідного дробу

$$365{,}24219\ldots = [365; 4,7,1,3,5, \ldots].$$

Перший підхідний дріб $365\frac{1}{4}$ відповідає юліанському стилю, в якому кожен четвертий рік є високосним. В середньовіччі від такого року відмовились, оскільки через це виникає помилка: 11 хвилин 14 секунд в рік.

Третій підхідний дріб $[365; 4,7,1, \dots] = 365\frac{8}{33}$ покладений в основу персидського календаря, який у 1079 році запропонував відомий математик, астроном та поет Омар Хайям. Такий календар має похибку в рік на 19 секунд. В ньому всі роки розбиті на 33-річні цикли, всередині кожного цикла сім разів вважається високосним кожен четвертий рік, а на восьмий раз – п'ятий.

На четвертому наближенні $[365; 4,7,1,3, \dots] = 365\frac{31}{128}$ заснований календар, який запропонував астроном Йоганн Медлер у 1864 році. Але він не був прийнятий за невідомих причин, хоча в рік давав похибку лише в одну секунду.

Наразі ми живемо по григоріанському стилю, яке основане на наближенні $365\frac{97}{400}$. Даний календар має похибку в рік приблизно на 27 секунд.

Голландський вчений Христиан Гюйгенс у 1862 році побудував один з перших механічних планетаріїв. Застосувавши теорію ланцюгових дробів при проектуванні зубчастих коліс, що забезпечило дуже високу точність при взаємному русі моделей планет [18, с.129].

Чому затемнення повторюються через кожні 18 років?

Ще задовго до нашої ери вавилоняни спостерігали за небом та помітили, що ряд затемнень – сонячних та місячних – повторюються кожні 18 років і 10 днів. Цей період назвали «саросом». Користуючись їм, древні люди передбачали, коли саме прийдуть затемнення, але вони не знали, чим саме обумовлена така правильна періодичність і чому виконується саме така тривалість. Обгрунтування періодичності затемнень було знайдено пізніше, за результатами дуже ретельного вивчення руху Місяця.

Чому дорівнює час обернення Місяця по орбіті? Відповідь на це питання може бути різним, в залежності від того, в який момент рахувати обернення Місяця

навколо Землі завершеним. Усього астрономи розрізняють п’ять місячних народжень, але нас будуть цікавити тільки два з них:

1. Перше називається «синодичним», тобто проміжок часу, за який Місяць обертається по своїй орбіті повний оберт, якщо слідкувати за цим з Сонця. Це – період часу, який знаходиться між двома однаковими фазами Місяця (наприклад, від нового місяця до нового). Він дорівнює $29,65306$ днів.
2. Другий місяць називається «драконячим», тобто це проміжок часу, за завершенням якого Місяць повертається до того «вузла» своєї орбіти (вузол – це перетин орбіти Місяця з площиною орбітою Землі). Він дорівнює $27,2123$ днів.

Затемнення виникають тільки в ці моменти, коли сам Місяць в фазі повного місяця або нового місяця знаходиться в стані одного зі своїх вузлів: тоді його центр знаходиться на одній прямій з центрами Землі та Сонця. Очевидно, що якщо затемнення було сьогодні, то воно повинне знову бути через такий проміжок часу, яке містить ціле число синодичних та драконячих місяців: тоді повторюються умови, за яких відбуваються затемнення.

Як знайти такі проміжки часу? Для цього потрібно розв’язати рівняння

$$29,5306x = 27,2123y,$$

де x та y – цілі числа. Перепишемо рівняння у вигляді пропорції

$$\frac{x}{y} = \frac{272123}{295306},$$

з якої можемо прийти до найменших точних розв’язків, в яких маємо, що $x = 272\,123$, а $y = 295\,306$. Отримали великий, в десятки тисячоліть, проміжок часу, який практично даремний. Древнім астрономам доводилось задовольнятись наближеним розв’язком. Найбільш зручний засіб для того, щоби відшукати наближення в таких випадках дають нам саме ланцюгові дроби. Розгорнемо дріб $\frac{295306}{272123}$ в неперервний. А саме: виключивши ціле число, та маємо

$$\frac{295306}{272123} = 1\frac{23\,183}{272\,123}.$$

В останньому дробі поділимо чисельник та знаменник на чисельник:

$$\frac{295306}{272123} = 1 + \frac{1}{11\frac{17110}{23183}}.$$

Чисельник та знаменник дроба $\frac{17110}{23183}$ ділимо на чисельник і так будемо робити й надалі. Отримаємо:

$$\frac{295306}{272123} = 1 + \cfrac{1}{11 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{4 + \cfrac{1}{17 + \cfrac{1}{1 + \frac{1}{7}}}}}}}}}.$$

З цього дробу, якщо взяти перші його наближення та відкинувши всі інші, отримаємо наступні послідовні наближення:

$$\frac{12}{11}, \frac{13}{12}, \frac{38}{35}, \frac{51}{47}, \frac{242}{223}, \frac{1019}{939} \text{ і так далі.}$$

П’ятий дріб в цьому ряді дає вже достатню точність. Якщо ми зупинимося на ній, тобто якщо прийняти $x = 223$, а $y = 242$, то проміжок повтору затемнень буде рівний 223 синодичним місяцям, або 242 драконячим. Це становить 6585 діб, тобто 18 років 11,3 діб.

Саме таке походження сароса. Знаючи це (тобто звідки він пішов) ми можемо знати, наскільки точно за його допомогою можна передбачити затемнення. Також бачимо, що, рахуючи сарос рівним 18 рокам та 10 добам, відкидають 0,3 діб. Це може сказатися на тому, що затемнення, які розраховані за таким скороченим проміжком, може наступити в інший час дня, ніж в попередній раз (приблизно пізніше на 8 годин), і тільки при застосуванні проміжку, який рівний потрійному точному саросу, затемнення будуть повторюватись майже в той самий момент дня. Крім того, сарос не враховує зміни відстані Місяця від Землі та Землі від Сонця, зміни, які мають також свій період. Від цих відстаней залежить, чи буде сонячне затемнення повним чи ні.

Тому сарос дає нам можливість передбачити лише те, що в конкретний день затемнення повинно статися: але чи буде воно повним, а також чи буде можливе спостерігання за цим затемненням в тих місцях, як і в попередній раз, сказати напевно неможливо.

Може бути навіть так, що незначне окреме затемнення Сонця через 18 років зменшує свою фазу до нуля, тобто воно не спостерігається зовсім. Та навпаки, стають помітними невеликі окремі затемнення Сонця, які раніше не помічались.

В наші дні астрономи вже не використовують сарос. Примхливі рухи земного супутника вивчені настільки добре, що затемнення розраховуються наперед з точністю до секунди [14, с. 95].

2.2.4. Золотий перетин

Чи можливо красу передати за допомогою формул та рівнянь? Чи існує у світі один єдиний стандарт всього прекрасного? Можливо виміряти гармонію за допомогою циркуля та лінійки? Математика дає на всі ці питання одну відповідь - золотий перетин. Це ключ до розуміння секретів досконалості в природі та мистецтві. На початку 16 століття в Італії навіть вийшла книга, в якій це число мало назву «божественна пропорція». Саме дотримання «божественної пропорції» допомагає митцям досягати естетичного ідеалу. Найстаріші відомості про золотий перетин відносяться до часів античної культури.

Перше чітке формулювання дав приблизно в 300 році до н.е. Евклід. «Початки» складаються з 13 книг. В шостій починається історія золотого перетину: «Поділити пряму лінію в крайньому та середньому відношення означає поділити її на два таких відрізка, щоб відношення всієї лінії до великого відрізку була рівна відношенню великого відрізка до меншого» Або, якщо більш коротко, «Ціле відноситься до більшої частини, як більша частина до меншої». Перший англійський переклад робіт Евкліда був зроблений у 1570 році Генрі Біллінгелі, який потім став лорд-мером Лондона.

Зобразити це число майже неможливо, і не тому, що воно дуже велике, - воно трошки більше за одиницю, – а тому, що воно складається з нескінченного ряда

чисел, які ніколи не утворюють повторювальну групу. В професійній математичній літературі золотий перетин позначають грецькою літерою т «тау» - від грецького слова «томе», що переводиться як «перетин». Але на початку 20 століття американський математик Марк Барр запропонував позначати золотий перетин літерою $Ф$ – по першій літері великого давньогрецького скульптора Фідія, оскільки митці вважають, що саме він найпершим застосовував золотий перетин. Крайнє та середнє відношення згодом стало саме тим числом, яке зараз називається «золотий перетин».

Порахуємо ж значення числа $Ф$:

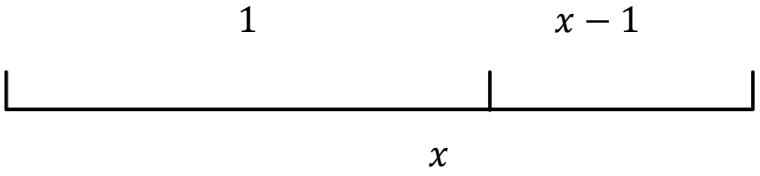


Рис. 6

Поділимо відрізок на дві частини (рис.6), тоді він буде поділений у крайньому та середньому відношення, інакше кажучи, у «золотому» відношення, якщо $\frac{x}{1} = \frac{1}{x-1}$. Якщо дроби рівні, то рівні і відповідні відношення по правилу «хрест навхрест»: $\frac{a}{b} = \frac{c}{d} \leftrightarrow a \cdot d = b \cdot c$. З цього випливає квадратне рівняння:

$$x(x-1) = 1 \cdot 1 \rightarrow x^2 - x = 1;$$

яке дорівнює рівнянню $x^2 - x - 1 = 0$. (1)

Таке рівняння має два розв’язки, але нас цікавить лише невід’ємний:

$$x = \frac{1+\sqrt{5}}{2} \approx 1{,}618.$$

Так як рівняння (1) є відношенням між довжинами частин відрізка, то воно не залежить від довжини самого відрізка. Інакше кажучи, значення золотого перетину не залежить від початкової довжини.

Оскільки вираз містить квадратний корінь, число $Ф$ буде ірраціональним числом. Це означає, що ми не можемо записати його у вигляді кінцевого десяткового числа. Більш того, нескінченний рядок десяткових знаків не містить

періодично повторюваних груп цифр. Число Φ, таким чином, є неперіодичним десятковим числом, яке неможливо обчислити до кінця. Крім того обчислення числа Φ в більшій степені не має сенсу, тому що воно більш важливе в геометричному вигляді, а не в числовому. Досить буде лише сказати, що $\Phi = 1{,}618033988749894$, тому що п'ятнадцять знаків після коми достатньо для будь-яких можливих розрахунків.

Можемо взяти калькулятор та зробити декілька простих розрахунків, взявши при цьому наближення до числа Φ з точністю до п'яти десяткових знаків: $\Phi = 1{,}61803$.

Більш точне значення Φ з 99 знаками після коми зображено на рис. 7:

1,61803398874989484820458683436563811772030917980576286213544
86227052604628189024497072072041893911374847540880753868917521
26633862223536931793180060766726354433389086595939582905638322
26613199282902678806752087668925017116962070322210432162695486
26262963136144381497587012203408058879544547492461856953648644
49241044320771344947049565846788509874339442212544877066478091
58846074998871240076521705751797883416625624940758906970400028
12104276217711177780531531714101170466659914669798731761356006
70874807101317952368942752194843530567830022878569978297783478
45878228911097625003026961561700250464338243776486102838312683
30372429267526311653392473167111211588186385133162038400522216
57912866752946549068113171599343235973494985090409476213222981
01726107059611645629909816290555208524790352406020172799747175
34277759277862561943208275051312181562855122248093947123414517
02237358057727861600868838295230459264787801788992199027077690
38953219681986151437803149974110692608867429622675756052317277
7520353613936.

Рис. 7

Розглянемо декілька способів знаходження числа Φ. Допустимо, що нам потрібно знайти значення виразу, який складається з нескінченних коренів:

$$\sqrt{1+\sqrt{1+\sqrt{1+\cdots}}}$$

Позначимо шукану величину за x. Тоді отримаємо: $x = \sqrt{1+\sqrt{1+\sqrt{1+\cdots}}}$

Тепер піднесемо до квадрату обидві частини рівняння:

$$x^2 = 1 + \sqrt{1 + \sqrt{1 + \cdots}}$$

Важливо пам’ятати, що оскільки вираз правої частини нашого рівняння прямує до нескінченності, то воно рівне нашому початковому x. Тому ми отримаємо квадратне рівняння: $x^2 = 1 + x$, яке є рівнянням, що описує золотий перетин!

Тепер розглянемо інший нескінченний вираз, але тепер з дробами:

$$1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cdots}}}}$$

Такий вираз відомий нам вже як ланцюговий дріб. Як і в попередньому випадку, прирівняємо все до x:

$$x = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cdots}}}}$$

Але, оскільки ланцюговий дріб прямує до нескінченності, знаменник другого доданка правій частині рівний x. І ми отримуємо вираз $x = 1 + \frac{1}{x}$.

Помножимо обидві частини на x і буде: $x^2 = 1 + x$, а це знову рівняння, яке описує золотий перетин. Оскільки ланцюговий дріб, який відповідає золотому перетину, складається лише з одиниць, він дуже повільно сходиться. В такому відношенні золотий перетин «складніше» виразити в вигляді ланцюгового дробу, ніж будь-яке інше ірраціональне число [9, с. 9].

Привабливість золотого перетину в першу чергу заснована на тому факті, що воно має неймовірну властивість з’являтися там, де його ніяк не чекаєш. В наш час багато людей має велику кількість карток: кредитні, візитні та інші. Ми користуємося ними щодня, не помічаючи, що більшість карток мають однаковий розмір та форму. І це все пояснюється золотим перетином.

Нехай уявимо прямокутник, одна сторона якого у 1,618 разів довше за другу. Прямокутник з таким відношенням сторін називають «золотим». На перший погляд він може здатися звичайним.

Але проведемо експеримент з двома кредитними картками (рис.8). Покладемо одну з них горизонтально, а іншу – вертикально так, щоби їх нижні сторони знаходились на одній лінії:

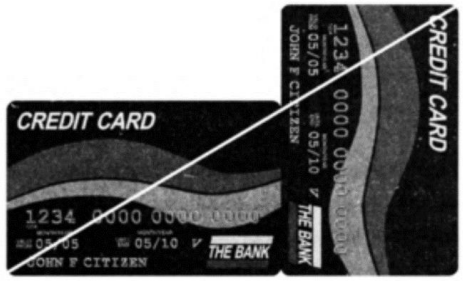


Рис.8

Якщо в горизонтальній карті ми проведемо діагональну лінію та продовжимо її, то побачимо, що вона пройде через правий верхній кут вертикальної картки – приємна несподіванка. Зробивши такий експеримент з двома книгами однакового розміру, а саме з підручниками або книгами кишенькового формату, ми отримаємо, можна на це розраховувати, такий же результат.

Тобто, якщо помістити два прямокутника поряд (один горизонтально, а другий вертикально), потім провести через вершини A та B лінію і, якщо ця лінія проходить точно через вершину C, то маємо точно два «золотих» прямокутника (рис.9).

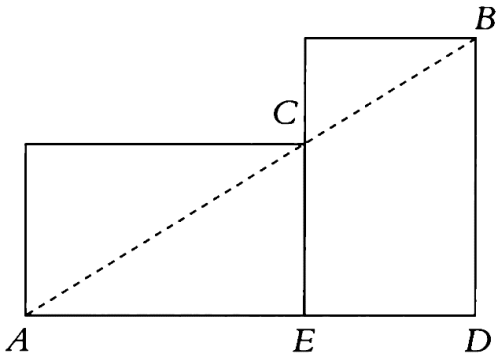


Рис. 9

Ця властивість характерна для двох «золотих» прямокутників однакового розміру.

Пояснити цей факт можна наступним чином: за теоремою Фалеса, якщо дві паралельні прямі перетинають дві сторони трикутника, то вони відтинають пропорціональні відрізки. На (рис.9) ми бачимо, що AB проходитиме через C, коли $\frac{AD}{DB} = \frac{AE}{EC}$ [13, с.10].

Як же побудувати золотий прямокутник? Почнемо з квадрата $ABCD$ (рис.10), чиї сторони будуть шириною «золотого» прямокутника. Точка M −середина сторони AB. Проведемо дугу окружності з центром в точці M та радіусом MC. Ця дуга перетинається з продовженням відрізка AB. Позначимо цей перетин точкою E. Тоді довжина відрізка AE буде довжиною шуканого «золотого» прямокутника. Проведемо перпендикуляр з точки E, який перетинає продовження відрізка DC в точці F. Таким чином, ми побудували «золотий» прямокутник $AEFD$.

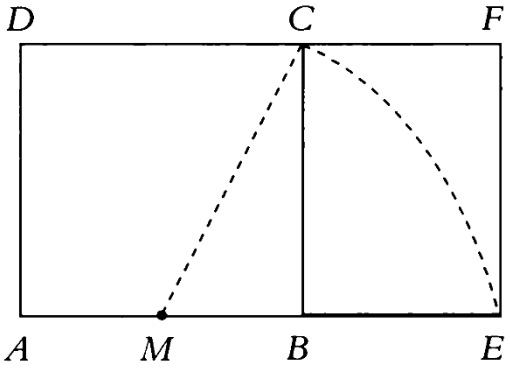


Рис. 10

Щоби перевірити «золотий» перетин, відшукаємо довжини сторін знайденого прямокутника. Нехай $AB = AD = 1$, тоді

$$AE = AM + ME = \frac{1}{2} + ME.$$

Так як ME рівна довжині гіпотенузи прямокутного трикутника MBC, за теоремою Піфагора маємо:

$$ME^2 = MC^2 = MB^2 + BC^2 = \left(\frac{1}{2}\right)^2 + 1^2 = \frac{1}{4} + 1 = \frac{5}{4}.$$

Звідси $ME = \sqrt{\frac{5}{4}} = \frac{\sqrt{5}}{2}$. І з цього слідує , що $AE = \frac{1}{2} + \frac{\sqrt{5}}{2} = \frac{1+\sqrt{5}}{2} = Ф$.

Це значить, що сторони прямокутника $AEFD$ рівні 1 та $Ф$. Тобто наш прямокутник дійсно є «золотим» [13, с. 56].

Золотий перетин можливо зустріти не тільки в природних явищах, але і в різних творах мистецтва. Наприклад, на (рис.11) ми бачимо Леонардо «Тайна вечеря»: відношення сторін картини приблизно рівне золотому перетину: прямокутники визначають як розміри картини, так і положення Христа та Його учнів. Також можна помітити, що стіни та вікна на задньому плані слідують правилу золотого перетину.

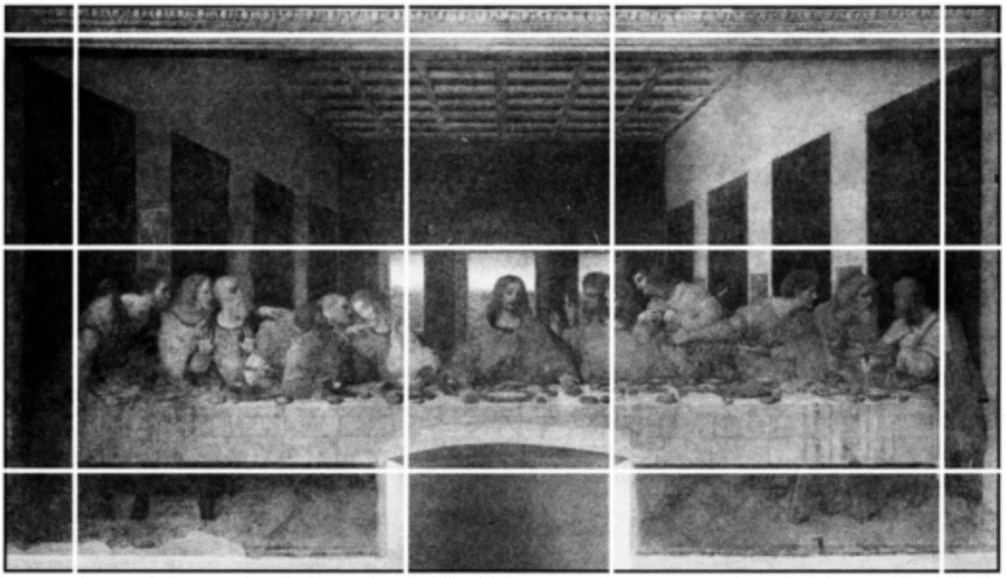


Рис. 11

Леонардо робив лише ілюстрації до роботи «Про божественну пропорцію», але сам Пачолі згадував про його важливий внесок до науки. Леонардо застосовував наукові знання про пропорції людського тіла до теорій Пачолі та Вітрувія про красу.

На композиції «Вітрувіанська людина» (рис.12) чоловіча фігура, яка вписана в круг та квадрат, розташована в центрі Всесвіту. Вітрувій вивів пропорції людської фігури з простих спостережень: він вважав, що зріст людини рівний розмаху рук, і якщо чоловік, який лежить на спині, розведе руки та ноги по сторонам, то його фігура буде вписана в окружність. Леонардо знайшов геніальний розв'язок, яке основане на тому, що квадрат та круг мають різні центри. Геніталії людини знаходяться в центрі квадрата, а пупок – в центрі кола. Ідеальні пропорції людського тіла на такому малюнку відповідають відношенню між стороною квадрата та радіусом круга: золотому перетину. Завдяки золотому перетину геометрія об'єднала красу та мистецтво.

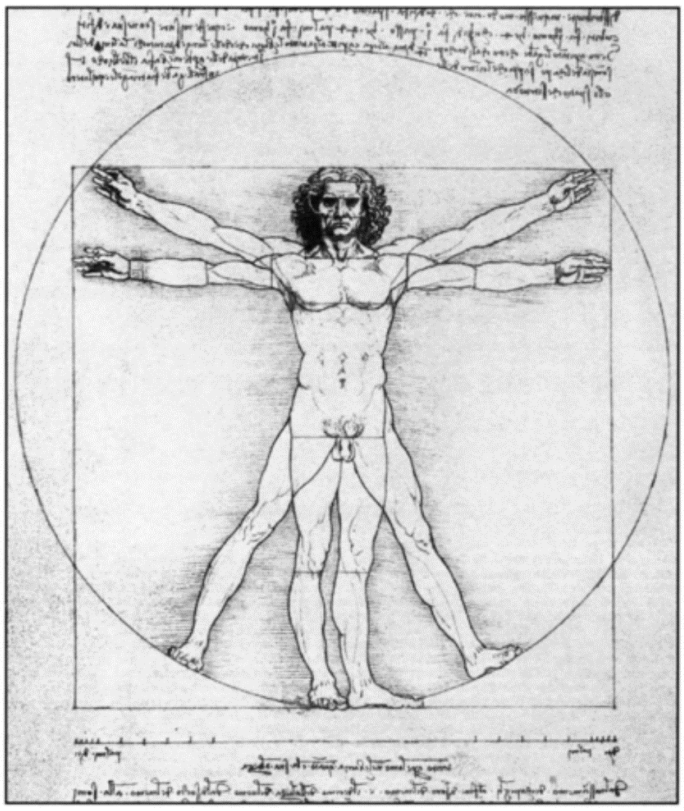


Рис. 12

Як не згадати про Мону Лізу, портер якої (рис. 13) також побудований на золотому перетині. Дослідження показали, що її обличчя і в цілому, і в деталях обрамлено елегантною послідовністю «золотих» прямокутників різних розмірів [13, с.11].

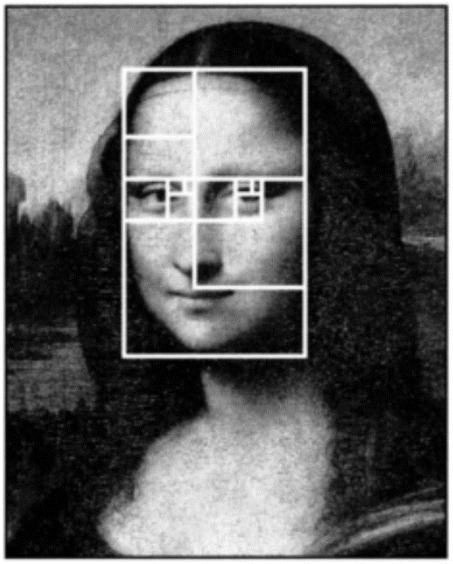


Рис. 13

Зв’язок золотого перетину з красою – питання не тільки людського сприйняття. Нібито сама природа виділила Φ важливу роль. Візьмемо вже відомий нам «золотий» прямокутник і впишемо в нього квадрат, сторони якого рівні ширині прямокутника. Отримаємо новий «золотий» прямокутник. Можна повторити таку процедуру декілька разів (рис. 14).

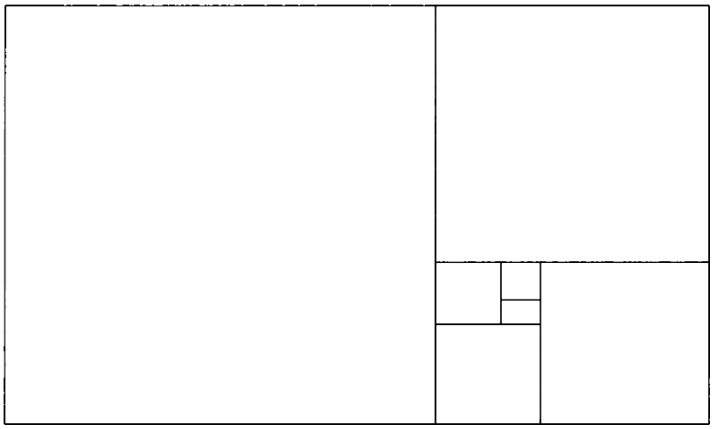


Рис. 14

Тепер в кожному з квадратів проведемо дугу, як показано на (рис. 15). Радіус кожної дуги рівний стороні відповідного квадрата. Тепер отримаємо наступний рисунок:

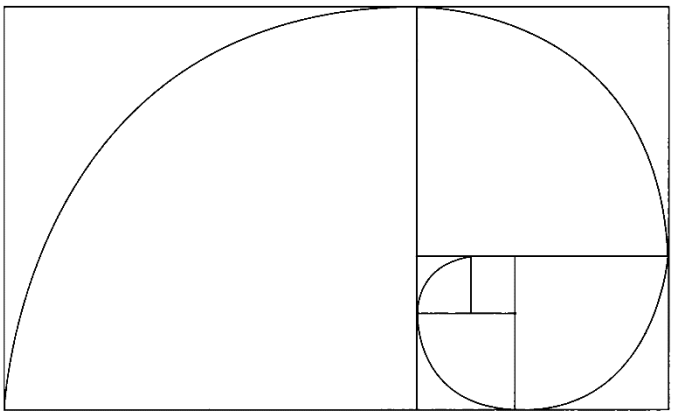


Рис. 15

Спіраль є такою кривою лінією, форма якої не змінюється при зміні розміру. Якщо провести пряму лінію від центра спіралі, до будь-якої іншої, кути перетинів з кривою завжди будуть однаковими [13, с. 14].

Властивості спіралі привабили не тільки вчених, а й митців. На (рис.16) зображена робота Мауріца Корнеліуса Ешера. Ешер часто малював спіраль, як це можна побачити на гравюрі 1953 року, під назвою «Спіраль».

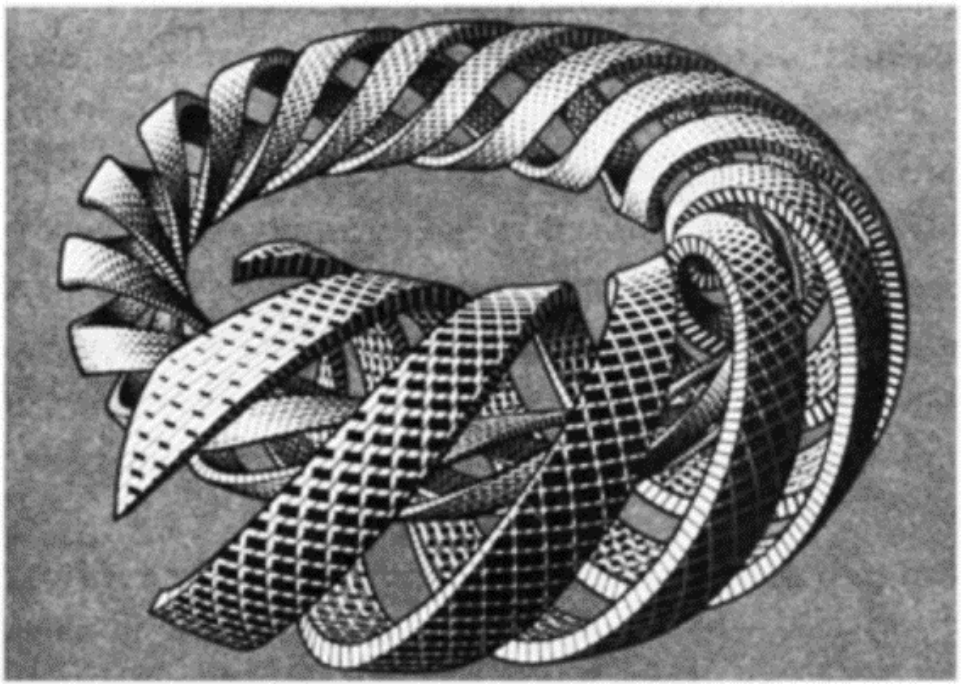
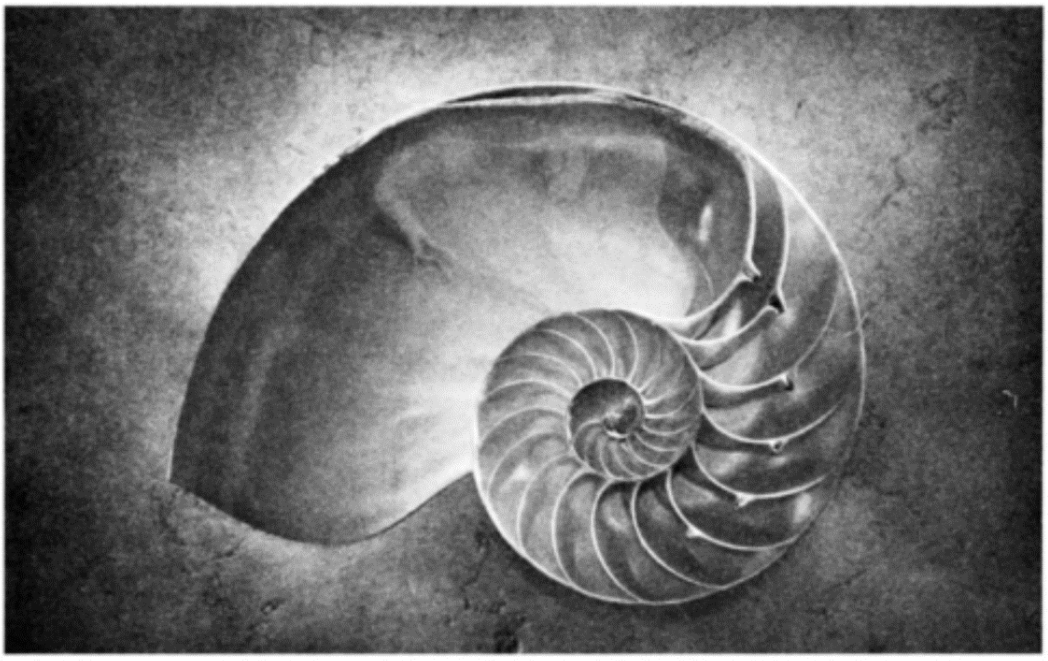


Рис. 16

Також спіраль часто зустрічається в фізичному світі: від раковини наутілуса (рис.17) (раковина збільшується з додаванням внутрішніх камер, кожна з яких більша за попередню, але форма раковини залишається незмінною):

Рис. 17



До рукавів галактик (рис.18):

Рис.18

І навіть в спіралі пелюстків королеви квітів (рис.19).

На прикладі королеви квітів розглянемо світ рослин. Наявність тут золотого перетину потребує введення чисел Фібоначчі. Це послідовність чисел, яка починається з двох одиниць, а кожне наступне число рівне сумі двох попередніх:

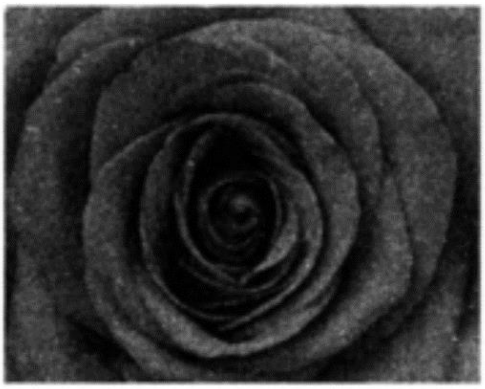


Рис. 19

1,1,2,3,5,8,13,21,34,55,89,144,233,377,610 ....

Частка від ділення будь-якого числа послідовності на попереднє йому число наближається до Φ, даючи все більш точне значення для кожного наступного числа послідовності: $\frac{1}{1} = 1$; $\frac{2}{1} = 2$; $\frac{3}{2} = 1{,}5$; $\frac{5}{3} = 1{,}666$ ...; $\frac{8}{5} = 1{,}6$; $\frac{13}{8} = 1{,}625$;…; $\Phi = 1{,}6180339887$ ... . Частка сорокового числа послідовності співпадає з «золотим» числом з точністю до чотирнадцятого десяткового знака [13, с. 16].

Розглянемо ще одну квітку (рис. 20), яка зовнішньо сильно відрізняється від троянди, - соняшник:

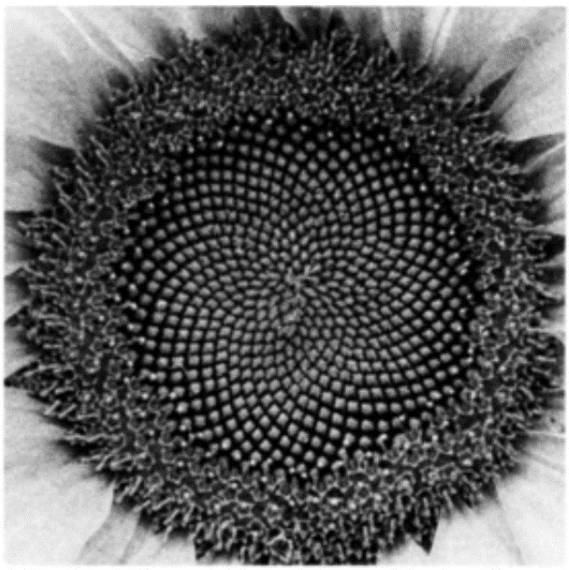


Рис. 20

Перше, що ми бачимо, - насіння розташовані по спіралям двох видів: за годинниковою стрілкою та проти. Якщо ми порахуємо спіралі за годинниковою

стрілкою та проти, то отримаємо два прості числа: 21 та 34. В структурі квітки з’явились два числа, які йдуть один за одним в послідовності Фібоначчі.

Протягом багатьох років людина в своєму мистецтві вчилася у природи, намагаючись осягнути закони її гармонії, її красу. Вона жила в духовній єдності з гармонією природи. Нас оточують золоті пропорції, вони з’являються на самих різних рівнях – від атомних сполучень до будови людського тіла. В цьому – ключ до гармонії систем. Можна прийти до висновку, що вираз Піфагора: «Числа правлять світом» дійсно істинний.

ВИСНОВКИ

Розвиток та широке запровадження сучасних інформаційних технологій помітно підвищили вразливість інформації, яка знаходиться в інформаційно-телекомунікаційних системах. Використання засобів обчислювальної техніки з програмним забезпеченням для обробки інформації може бути однією з найважливіших причин такої вразливості, оскільки таке масове використання обчислювальної техніки дозволяє легко копіювати, видаляти або просто контролювати, одним словом, отриману інформацію. Такі дії отримали назву «інформаційна війна». І саме завдяки цьому захист інформації відіграє важливу роль в даний час для різних корпорацій, закладів та загалом для звичайних людей, які користуються ПК. Надійно захистити свою інформацію користувач може за допомогою криптографічних методів, до яких можна віднести перетворення інформації за допомогою шифрування. Під час передачі власної інформації по відкритим електронним каналам зв'язку взагалі неможливо обійтись без криптографії (це розділ прикладної математики, який вивчає моделі, алгоритми, програмні та апаратні засоби перетворення інформації для приховування її змісту).

І саме в цій дуже важливій для сьогодення сфері ланцюгові дроби знайшли для себе застосування. Існує криптографічна система RSA, яка базується на теорії чисел і в якій використовуються ланцюгові дроби. Таку систему майже неможливо зламати, що гарантує її велику надійність в шифруванні інформації.

Також ланцюгові дроби застосовуються, звичайно, не тільки в сфері криптографії, вони дуже популярні в астрономії (особливо у пошуках проміжків часу, за який відбуваються затемнення), раніше вони використовувались у складанні календарів.

В математиці їх можна зустріти при добуванні числа з квадратного кореня, знаходження розв'язків рівняння Пелля або діофантових рівнянь, в узагальненні алгоритму Ейлера.

Як можна помітити, ланцюгові дроби мають надзвичайно широке застосування в самих різних сферах як математики, так і життя, навколишнього

світу. Їх актуальність розглянута та доведена, вони знаходять своє використання ще з давніх часів, а залучення до такого розділу прикладної математики, як криптографія, подає надію, що ланцюгові дроби будуть актуальні ще дуже довгий час.

В ході магістерської роботи були виконані такі поставлені на початку завдання:

1) розглянуто історичний розвиток ланцюгових дробів від давнини до сьогодення;
2) розглянуто побудову ланцюгового дробу та основні їх поняття: скінченні та нескінченні ланцюгові дроби, їх підхідні дроби;
3) досліджено наближення дійсного числа раціональними дробами;
4) розкрита суть застосування ланцюгових дробів до розв’язування різних рівнянь: рівняння Пелля, діофантових рівнянь;
5) досліджене застосування ланцюгових дробів в навколишньому світі.

В процесі роботи дійшли до таких висновків:

1) ланцюгові дроби знайшли для себе застосування не тільки в математичній сфері, але й у навколишньому світі, вони зустрічаються в золотому перетині, в складанні календарів, навіть використовувались для розрахунків затемнень;
2) теорія неперервних дробів поширюється також на функції та на розв’язування рівнянь;
3) ланцюгові дроби почали застосовуватися в такій важливій для сьогодення сфері як криптографія, що доводить їх актуальність, причому ще з давніх часів.

Список використаних джерел:

1. А.Я. Хинчин. Цепные дроби, изд.3. – М.: Физмагтиз., 1961. –112с.
2. Акуленко І. А., Красношлик Н. О., Лещенко Ю. Ю. / Основи криптології. Матерілаи міжпредметного курсу за вибором (математика та інформатика) для учнів 9-х класів із поглибленим вивченням математики, 10-х класів, які вивчають математику (інформатику) на профільному рівні : навч.-метод. пос. для учнів і вчителів / І. А. Акуленко, Н. О. Красношлик, Ю. Ю. Лещенко – Черкаси, 2016. – 224 с.
3. Башмакова И.Г. Диофант и диофантовы уравнения. - М.: Наука, 1972. - 68 с.
4. Безущак О.О., Ганюшкін О.Г. Елементи теорії чисел: Навчальний посібник. – К.: Видавничо–поліграфічний центр "Київський університет", 2003. – 203 с.
5. Бескин Н.М. Бесконечные цепные дроби // Квант. – 1970. – №8. – С.1017.
6. Бугаенко В. О. Уравнения Пелля (Серия: «Библиотека «Математическое просвещение»»). М.: МЦНМО, 2001. – 32с.
7. Бухштаб А. А. Теория чисел / Бухштаб А. А. – М. : Книга по требованию, 2012. – 386 с.
8. В. И. Арнольд. Цепные дроби.– М.: МЦНМО, 2000.–Т.14. – 40 с.
9. Васютинский Н.А. Золотая пропорция. – М. : Мол. гвардия, 1990. – 238 с.
10. Гладковский. С. Н. Анализ условно-периодических цепных дробей, ч. 1. – Незлобная, 2009. – 138 с.
11. И. М. Виноградов, «Основы теории чисел», УМН, 1938, № 4, 336–338
12. М.М.Стасюк, Р.М.Тацій, О.Ю.Пазен Скінченні ланцюгові дроби та їх застосування в криптографії // Збірник наукових праць за матеріалами дистанційної всеукраїнської наукової конференції «Математика у технічному університеті XXI сторіччя», 2017. – 26 с.
13. Мир математики: в 40 т. Т. 1: Фернанд Корбалан. Золотое сечение. Математический язык красота. / Пе. С англ. – М.: Де Агостин, 2014. –

160с.

14. Перельман Я.И. Занимательная астрономия (издание седьмое), М., ГТТИ, 1954. – 212 с.
15. Пошук молодих. Випуск 15: Збірник матеріалів Всеукраїнскьої студентської науково-практичної конференції («Технології компетентнісно-орієнтованого навчання природничо-математичних дисциплін»), (Херсон, 14015 квітня 2016р) / Укладач: В. Д. Шарко. – Херсон: ПП Вишемирський В.С. – 2016. – 172 с.
16. С.Т. Завало, В.Н. Костарчук, Б.И. Хацет. Алгебра і теорія чисел: В 2-х ч. – К.:Вища школа, 1976. – 384 с.
17. Устинов А.В. Цепные дроби вокруг нас. – Квант, 2 (2010), 32-33.
18. Энциклопедический словарь юного математика / Сост. Э-68 А. П. Савин. – М.: Педагогика, 1989. – 353 с.: ил.
19. http://enpuir.npu.edu.ua/bitstream/123456789/15453/1/Prats′ovytyy_Vasylenko_Lysenko.pdf
20. http://www.tmnlib.ru/jirbis/files/upload/books/VKR/2017/TOBOLSK/ENF/Kudin%20I.M..pdf
21. https://pandia.ru/text/78/002/10803.php
22. https://uk.wikipedia.org/wiki/RSA
23. https://vuzlit.ru/849958/istoriya_tsepnyh_drobey

Додаток А

Тут наводиться приклад алгоритму на мові програмування Python 3, за допомогою якого на екран можна вивести список простих чисел до якогось заданого числа включно. Даний алгоритм можна застосувати для генерування ключів в системі RSA, тобто для першого пункту знаходження великих простих чисел. Після запуску алгоритму з'явиться рядок, в який треба ввести довільне число l.

```
l = int(input('l:'))
# создаем пустой список для хранения простых чисел
lst = []
# в k будем хранить количество делителей
k = 0
# пробегаем все числа от 2 до N
for i in range(2, l+1):
    # пробегаем все числа от 2 до текущего
    for j in range(2, i):
        # ищем количество делителей
        if i % j == 0:
            k = k + 1
    # если делителей нет, добавляем число в список
    if k == 0:
        lst.append(i)
    else:
        k = 0
# выводим на экран список
print (lst)
```

Такий ми можемо отримати результат, коли введемо, наприклад, число 112:

```
l:112
[2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109]
```

Додаток Б

Тут наведено приклади алгоритмів, які можуть допомогти при наступних пунктів алгоритму генерування ключів, а саме:

1. Алгоритм для виборки будь-яких двох чисел з отриманого раніше списку простих чисел:

```
import random
from random import sample
random.sample(lst,2)
```

```
[97, 43]
```

2. Знаходження числа n (тобто знаходження добутку двох простих чисел):

```
n=97*43
print(n)
```

```
4171
```

Та знаходження числа φ:

```
phi=(97-1)*(43-1)
print(phi)
```

```
4032
```

3. Обирається довільне число e, таке, щоб воно не перевищувало число φ:

```
import random
e = random.randint(2, phi)

print("Random number between 2 and phi is % s" % (e))
```

```
Random number between 2 and phi is 2775
```

Додаток В

У літературі [2] наводиться приклад програми для генерування ключів на мові Python для шифру RSA:

```
import random
def GenerateKeyRSA(p,q):
    n=p*q
    phi=(p-1)*(q-1)
    nsd=0
    while (nsd!=1):
        e=random.randint(2,phi)
        (nsd,d,v)=ExtEucl(e,phi)
    d=(d+phi)%phi
    print ('Public key (n,e) = '), (n,e)
    print ('Private key (n,d) = '), (n,d)
    return e,d,n
```