



Донбаська державна машинобудівна академія

«МАТЕМАТИКА У ТЕХНІЧНОМУ УНІВЕРСИТЕТІ XXI СТОРІЧЧЯ»

**ДИСТАНЦІЙНА ВСЕУКРАЇНСЬКА
НАУКОВА КОНФЕРЕНЦІЯ**

**15-16 травня 2017 р.
Краматорськ, Україна**



**Міністерство освіти і науки України
Донбаська державна машинобудівна академія
Вінницький національний технічний університет
Дніпродзержинський державний технічний університет
Криворізький металургійний факультет
Національної металургійної академії України,
Приазовський державний технічний університет
Інститут хімічних технологій Східноукраїнського
національного університету ім. В. Даля
Черкаський державний технологічний університет**



**ДИСТАНЦІЙНА ВСЕУКРАЇНСЬКА НАУКОВА КОНФЕРЕНЦІЯ
«МАТЕМАТИКА У ТЕХНІЧНОМУ УНІВЕРСИТЕТІ
XXI СТОРІЧЧЯ»**

**15-16 травня 2017 р.
Краматорськ, Україна**

УДК 51(06)+378.147(06)+004(06)+51(091)
МЗ4

Збірник наукових праць за матеріалами дистанційної всеукраїнської наукової конференції «Математика у технічному університеті ХХІ сторіччя», 15 – 16 травня, 2017 р., Донбаська державна машинобудівна академія, м. Краматорськ. – Краматорськ : ДДМА, 2017. – 350 с.

Затверджено до публікації згідно з рішенням вченої ради Донбаської державної машинобудівної академії (протокол № 9 від 25.05.17)

Програмний комітет:

Акуленко І. А., доктор педагогічних наук, професор, Черкаський національний університет ім. Б. Хмельницького, м. Черкаси
Бевз В. Г., доктор педагогічних наук, професор, Національний педагогічний університет ім. М. П. Драгоманова, м. Київ
Власенко К. В., доктор педагогічних наук, професор, Донбаська державна машинобудівна академія, м. Краматорськ
Гайдей В. О., кандидат фізико-математичних наук, доцент, Національний технічний університет України «КПІ», м. Київ
Ключко В. І., доктор педагогічних наук, професор, Вінницький національний технічний університет, м. Вінниця
Крилова Т. В., доктор педагогічних наук, професор, Дніпровський державний технічний університет, м. Дніпро
Кульчицька Н. В., кандидат педагогічних наук, доцент, Прикарпатський національний університет ім. В. Стефаника, м. Івано-Франківськ
Лиходесва Г. В., кандидат педагогічних наук, доцент, Бердянський державний педагогічний університет, м. Бердянськ
Лов'янова І. В., доктор педагогічних наук, професор, ДВНЗ «Криворізький державний педагогічний університет», м. Кривий Ріг
Матяш О. І., доктор педагогічних наук, професор, Вінницький державний педагогічний університет ім. М. Коцюбинського, м. Вінниця
Михалевич В. М., доктор технічних наук, професор, Вінницький національний технічний університет, м. Вінниця
Моторіна В. Г., доктор педагогічних наук, професор, Харківський національний педагогічний університет ім. Г.С. Сковороди, м. Харків
Новіков О. О., кандидат фізико-математичних наук, доцент, ДВНЗ «Донбаський державний педагогічний університет», м. Слов'янськ
Петрук В. А., доктор педагогічних наук, професор, Вінницький національний технічний університет, м. Вінниця
Семенець С. П., доктор педагогічних наук, професор, Житомирський державний університет ім. І. Франка, м. Житомир
Семеріков С. О., доктор педагогічних наук, професор, ДВНЗ «Криворізький національний університет», м. Кривий Ріг
Скворцова С. О., доктор педагогічних наук, професор, ДЗ «Південноукраїнський національний педагогічний університет імені К.Д. Ушинського», м. Одеса
Тарасенкова Н. А., доктор педагогічних наук, професор, Черкаський національний університет ім. Б. Хмельницького, м. Черкаси
Тімошин А. С., кандидат фізико-математичних наук, доцент, Інститут хімічних технологій Східноукраїнського національного університету ім. В. Даля, м. Рубіжне
Триус Ю. В., доктор педагогічних наук, професор, Черкаський державний технологічний університет, м. Черкаси
Хом'юк І. В., доктор педагогічних наук, професор, Вінницький національний технічний університет, м. Вінниця
Холькін О. М., доктор фізико-математичних наук, професор, ДВНЗ «Приазовський державний технічний університет», м. Маріуполь
Чашечникова О. С., доктор педагогічних наук, професор, Сумський державний педагогічний університет ім. А.С. Макаренка, м. Суми
Швець В. О., кандидат педагогічних наук, професор, Національний педагогічний університет ім. М.П. Драгоманова, м. Київ
Щерба А. І., кандидат фізико-математичних наук, доцент, Черкаський державний технологічний університет, м. Черкаси

УДК 51(06)+378.147(06)+004(06)+51(091)
МЗ4

© Автори
© ДДМА, 2017

Зміст

Пленарні виступи	12
<i>Власенко К. В., Сітак І. В.</i>	
Розробка комп'ютерно-орієнтованих засобів навчання диференціальних рівнянь бакалаврів з інформаційних технологій.....	12
<i>Кондратов С. А., Черный А. А., Савяк Р. П.</i>	
Бутстреп-модель для определения высвобождения лекарственных препаратов в человеческом организме.....	15
<i>Лов'янова І. В., Потапова О. М.</i>	
Використання системи комп'ютерної математики Maxima у процесі математичної підготовки майбутніх інженерів.....	17
<i>Михалевич В. М., Добранюк Ю. В., Крупський Я. В.</i>	
Фрагменти електронних освітніх ресурсів з функції двох змінних в середовищі СКМ Maple	20
<i>Семенець С. П.</i>	
Особливості змісту навчання математики в технічному університеті.....	23
<i>Стасяк М. М., Тацій Р. М., Пазен О. Ю.</i>	
Скінчені ланцюгові дроби та їх застосування в криптографії.....	26
<i>Тарасенкова Н. А., Коломієць О. М.</i>	
Реалізація особистісного підходу як основа компетентнісного навчання аналітичної геометрії у ВНЗ.....	29
Секція 1. Історія математики	31
<i>Белых Н. В.</i>	
Математика в жизни и исследованиях Альберта Эйнштейна.....	31
<i>Бірюкова Т. В., Олар О. І., Микитюк О. Ю.</i>	
Деякі історичні аспекти становлення біометрії	34
<i>Власенко К. В., Тертишна А. К.</i>	
Історія розвитку поняття «Інтеграл»	37
<i>Карпенко Л. М., Челпан В. М.</i>	
М. В. Остроградський – гордість української нації.....	40
<i>Мельник Н. В., Буликан А. В., Сусь Б. А.</i>	
Остроградський – наш вітчизняний вчений	43
<i>Паламарчук В. О., Карлаш (Панченко) Ю. Д.</i>	
Історія застосування визначеного інтеграла у економіці.....	46
<i>Паламарчук В. О., Савченко Г. Б.</i>	
Історичний шлях теорії ймовірностей	49

УДК 512.8
СКІНЧЕНІ ЛАНЦЮГОВІ ДРОБИ ТА ЇХ ЗАСТОСУВАННЯ В
КРИПТОГРАФІЇ

М.М. Стасюк, Р.М. Тацій, О.Ю. Пазен

Львівський державний університет безпеки життєдіяльності, Львів
e-mail: marta_stasiuk@yahoo.com

Ланцюгові дроби мають різноманітні застосування у фізиці, астрономії, геометрії, теорії чисел, криптографії.

Нехай $\frac{a}{b}$ – раціональне число з додатним знаменником, тобто a, b – цілі числа. Застосуємо до чисел a і b алгоритм Евкліда, який найчастіше використовують для знаходження НСД (a, b) . Маємо:

$$\begin{aligned} a &= bq_1 + r_2, & \frac{a}{b} &= q_1 + \frac{1}{\frac{b}{r_2}}, \\ b &= r_2q_2 + r_3, & \frac{b}{r_2} &= q_2 + \frac{1}{\frac{r_2}{r_3}}, \\ r_{n-2} &= r_{n-1}q_{n-1} + r_n, & \frac{r_{n-2}}{r_{n-1}} &= q_{n-1} + \frac{1}{\frac{r_{n-1}}{r_n}}, \\ r_{n-1} &= r_nq_n, & \frac{r_{n-1}}{r_n} &= q_n. \end{aligned} \tag{1}$$

Тоді

$$\frac{a}{b} = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \dots + \frac{1}{q_n}}} \tag{2}$$

Числа q_1, q_2, \dots, q_n називаються неповними частками послідовних поділів у алгоритмі Евкліда, а вираз (2) – ланцюговим дробом і позначається

$$\frac{a}{b} = [q_1, q_2, \dots, q_n] \quad (3)$$

Дроби $\delta_1 = q_1, \delta_2 = q_1 + \frac{1}{q_2}, \delta_3 = q_1 + \frac{1}{q_2 + \frac{1}{q_3}}, \dots$ називаються підхідними дробами. Для підхідних дробів $\delta_s = \frac{P_s}{Q_s}, s = 2, 3, \dots, n$, справджується рекурентна формула [1]

$$\frac{P_s}{Q_s} = \frac{q_s P_{s-1} + P_{s-2}}{q_s Q_{s-1} + Q_{s-2}}, \quad P_0 = 1, \quad Q_0 = 0, \quad P_1 = q_1, \quad Q_1 = 1. \quad (4)$$

Ланцюгові дроби можна ефективно використовувати при розв'язанні конгруенцій

$$ax \equiv b \pmod{m}. \quad (5)$$

За умови, що a, b, m – цілі, $\text{НСД}(a, m) = 1$, розв'язок (5) – єдиний і подається у вигляді [1]

$$x \equiv (-1)^{n-1} P_{n-1} b \pmod{m}, \quad (6)$$

де $\frac{m}{a} = [q_1, q_2, \dots, q_n]$, а $\delta_{n-1} = \frac{P_{n-1}}{Q_{n-1}}$.

Запропонована в 1977 році система RSA є однією з найпопулярніших криптосистем з відкритим ключем. Генерування ключів (відкритого і таємного) в цій системі здійснюється [2] наступним чином: а) вибирають два досить великі прості числа p і q та обчислюють їх добуток $n = p \cdot q$. Для числа n обчислюють функцію Ейлера $\varphi(n) = \varphi(p) \cdot \varphi(q) = (p-1)(q-1)$; б) випадковим чином вибирають елемент $e \in Z_{\varphi(n)}^*$, який не перевищує $\varphi(n)$ і взаємно простий з $\varphi(n)$; в) знаходять інверсію елемента e за $\text{mod } \varphi(n)$, тобто розв'язують конгруенцію

$$e \cdot d \equiv 1 \pmod{\varphi(n)}, \quad (7)$$

яка через сформульовані вимоги, має єдиний розв'язок.

Описані дії визначають відкритий ключ $e, n = p \cdot q$ і таємний ключ d .

Таємний ключ d , як розв'язок конгруенції (7), можна шукати за формулою (6), де $\frac{\varphi(n)}{e} = [q_1, q_2, \dots, q_k]$, тобто використовуючи скінчені ланцюгові дроби.

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

Переконаємось, що НСД $(e, \varphi(n)) = (1297, 2080) = 1$ й одночасно знайдемо ланцюговий дріб $\frac{2080}{1297}$. Застосувавши алгоритм Евкліда до чисел 2080 і 1297 , прийдемо до такого ланцюгового дроби

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

Для знаходження таємного ключа d розв'яжемо конгруенцію

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

Розв'язок цієї конгруенції знайдемо за формулою (6). Для цього складемо таблицю чисельників підхідних дроби, використовуючи рекурентну формулу (4):

Таблиця 1

Чисельники підхідних дроби

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

Тоді за формулою (6) маємо:

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

Отже таємний ключ $d = 433$. Зауважимо, що приклад – ілюстративний, бо реально в криптосистемі *RSA* використовують дуже великі прості числа.

Література

1. И. М. Виноградов Основы теории чисел/ И. М. Виноградов. – Москва.:Наука, 1965. –172с.
2. Вербіцький О.В. Вступ до криптології / О.В.Вербіцький. –Львів.: ВНТЛ, 1998. –246с.