Актуальні питання у сучасній науці
№ 5(47) 2026
ISSN 2786-6300 Print

УДК 378.147:511.48:004.056

https://doi.org/10.52058/2786-6300-2026-5(47)-3169-3187

Матурін Юрій Петрович кандидат фізико-математичних наук, доцент, Дрогобицький державний педагогічний університет імені Івана Франка, м. Дрогобич, https://orcid.org/0000-0002-0544-1329

Хаць Руслан Васильович кандидат фізико-математичних наук, доцент, Дрогобицький державний педагогічний університет імені Івана Франка, м. Дрогобич, https://orcid.org/0000-0001-9905-5447

Комарницька Леся Іванівна кандидат фізико-математичних наук, доцент, Дрогобицький державний педагогічний університет імені Івана Франка, м. Дрогобич, https://orcid.org/0009-0001-0907-1038

Р-АДИЧНІ ЧИСЛА В КОМП'ЮТЕРНИХ НАУКАХ

Анотація. У статті розроблено, теоретично обґрунтовано та концептуалізовано інноваційну дидактичну модель вивчення теорії р-адичних чисел, орієнтовану на здобувачів другого (магістерського) рівня вищої освіти, які навчаються за освітньо-професійною програмою «Середня освіта (Математика, інформатика)». Актуальність дослідження зумовлена наявністю істотного концептуального розриву між традиційним дедуктивним викладанням абстрактної вищої алгебри та реальними потребами сучасної комп'ютерної інженерії. Традиційне введення р-адичних чисел, що ґрунтується на аксіоматичному формалізмі, теоремі Островського, метричних просторах і поповненні поля раціональних чисел Q за допомогою фундаментальних послідовностей Коші, створює для студентів значні труднощі. Математична інтуїція, сформована в межах архімедової природи поля дійсних чисел R, вступає у суперечність із неархімедовою метрикою, у якій послідовність p^n при n, що прямує до нескінченності, наближається до нуля. За відсутності наочних фізичних аналогій р-адичний аналіз часто сприймається як ізольована абстрактна конструкція, відірвана від практичного змісту.

Для подолання цієї методичної проблеми запропоновано змінити організацію навчального процесу, відмовившись від класичного низхідного підходу на користь стратегії висхідного проєктування. У межах цієї стратегії навчання розпочинається не з математичних аксіом, а з постановки інтуїтивно зрозумілої проблеми з галузі комп'ютерних наук, розв'язання якої логічно приводить до побудови апарату р-адичних чисел. Органічним доповненням

ISSN 2786-6300 Print

виступає принцип подвійного подання, за яким кожному абстрактному теоретико-числовому поняттю відповідає його алгоритмічний або структурний відповідник в інформатиці. Для введення кільця цілих p-адичних чисел Zp, зокрема Z_2, використано тригерну задачу, пов'язану з парадоксом машинного подання чисел. Студентам пропонується уявний експеримент: абстрагуватися від обмежень 32- або 64-бітного формату та припустити, що бітовий рядок необмежено продовжується вліво. Саме такий перехід від скінченного регістра до нескінченного породжує кільце Z_2, а ультраметрична нерівність $|x + y|_p \leq \max(|x|_p, |y|_p)$ набуває прозорого інформатичного тлумачення через кількість нулів у молодших розрядах.

Перший дидактичний кейс присвячено алгебраїчній природі доповняльного коду. На відміну від традиційного трактування як технічного правила, алгоритм подання від'ємних чисел інтерпретується як природна скінченна проєкція нескінченного 2-адичного цілого числа. Аналіз 2-адичного додавання послідовності нескінченних одиниць до одиниці дає змогу встановити тотожність $-1 = \ldots1111111_2$ у кільці Z_2. На цій основі правило доповняльного коду виводиться як строгий наслідок співвідношення $A + {\sim}A = -1$, звідки випливає $-A = {\sim}A + 1$. Обмеженість машинного слова, наприклад 32-бітного типу int, пояснюється через фактор-кільце $Z_2 / 2^{32}Z_2$, а знакове переповнення постає як закономірний наслідок модульної редукції, а не як випадкова програмна аномалія.

Другий етап методики орієнтований на виявлення прикладного потенціалу p-адичного аналізу у сфері потокової криптографії. Магістрантам пропонується задача побудови швидкого генератора псевдовипадкових чисел, який не використовує обчислювально витратних операцій і максимально спирається на апаратні можливості процесора. Для цього вводиться поняття T-функцій як відображень вигляду $f: Z_2 \to Z_2$, у яких значення кожного біта результату залежить лише від молодших або рівнозначних бітів аргументу. Показано, що цій умові відповідають базові логічні та арифметичні операції процесора. Кульмінаційним моментом є встановлення еквівалентності між інформатичним означенням T-функції та математичним поняттям 1-ліпшицевого відображення у 2-адичній метриці. На прикладі нелінійної функції оновлення стану $x_{n+1} = x_n + (x_n^2 \text{ OR } 5) \bmod 2^{64}$ продемонстровано, що апарат p-адичного диференціювання дає змогу аналітично довести її ергодичність без повного перебору 2^{64} станів.

Запропонована методика ґрунтується на засадах педагогічного конструктивізму й передбачає перетворення лекційної аудиторії на інтерактивну STEM-лабораторію. Опанування p-адичної математики здійснюється не лише через теоретичний аналіз, а й через самостійне комп'ютерне моделювання засобами Python або SageMath. Лабораторний практикум охоплює три рівні: побудову алгоритмів перетворення раціональних чисел у p-адичний ряд і осмислення леми

Гензеля як ітераційного алгоритму; візуалізацію 2-адичних чисел і T-функцій на нескінченних бінарних деревах; дослідження рядів Тейлора для p-адичної експоненти та логарифма, що дає змогу емпірично виявити специфіку збіжності в просторі Q_p. Упровадження розробленої моделі забезпечує переорієнтацію математичної підготовки магістрантів від ізольованого аксіоматичного формалізму до міждисциплінарного інженерного бачення, сприяє подоланню відчуження від абстрактної алгебри та формує готовність до розроблення й викладання сучасних STEM-курсів.

Ключові слова: p-адичні числа, 2-адичні цілі числа, неархімедова метрика, ультраметрика, комп'ютерна арифметика, доповняльний код, T-функції, потокові шифри, генератор псевдовипадкових чисел (PRNG), прикладна криптографія, математична освіта, магістерська підготовка, висхідне проєктування, принцип подвійного подання, STEM-освіта.

Yuriy Maturin Candidate of Sciences in Physics and Mathematics, Docent, Drohobych Ivan Franko State Pedagogical University, Drohobych, https://orcid.org/0000-0002-0544-1329

Ruslan Khats' Candidate of Sciences in Physics and Mathematics, Docent, Drohobych Ivan Franko State Pedagogical University, Drohobych, https://orcid.org/0000-0001-9905-5447

Lesia I. Komarnytska Candidate of Sciences in Physics and Mathematics, Docent, Drohobych Ivan Franko State Pedagogical University, Drohobych, https://orcid.org/0009-0001-0907-1038

P-ADIC NUMBERS IN COMPUTER SCIENCE

Abstract. The paper develops, theoretically substantiates, and conceptualizes an innovative didactic model for studying the theory of p-adic numbers, designed for students pursuing the second (master's) level of higher education within the educational and professional program "Secondary Education (Mathematics, Computer Science)." The relevance of the study is determined by the existence of a substantial conceptual gap between the traditional deductive teaching of abstract higher algebra and the actual needs of modern computer engineering. The traditional introduction of p-adic numbers, grounded in axiomatic formalism, Ostrowski's theorem, metric spaces, and the completion of the field of rational numbers Q by means of fundamental Cauchy sequences, creates significant cognitive difficulties for students. Mathematical intuition formed within the framework of the Archimedean nature of the field of real numbers R comes into conflict with the non-Archimedean metric, in which the

sequence p^n, as n tends to infinity, approaches zero. In the absence of clear physical analogues, p-adic analysis is often perceived as an isolated abstract construction detached from practical meaning.

To overcome this methodological difficulty, the study proposes a reorganization of the learning process by replacing the classical top-down approach with a bottom-up design strategy. Within this framework, instruction begins not with mathematical axioms but with the formulation of an intuitively comprehensible problem from computer science, the solution of which logically leads to the construction of the apparatus of p-adic numbers. An organic complement to this approach is the principle of dual representation, according to which every abstract number-theoretic concept is paired with its algorithmic or structural counterpart in computer science. To introduce the ring of p-adic integers Z_p, and in particular Z_2, the authors employ a trigger problem connected with the paradox of machine representation of numbers. Students are invited to perform a thought experiment: to abstract away from the limitations of the 32-bit or 64-bit format and assume that a bit string extends indefinitely to the left. It is precisely this transition from a finite register to an infinite one that gives rise to the ring Z_2, while the ultrametric inequality $|x + y|_p \leq \max(|x|_p, |y|_p)$ acquires a transparent computer-science interpretation through the number of trailing zeros in the least significant positions.

The first didactic case is devoted to the algebraic nature of two's complement representation. In contrast to the traditional view of this procedure as a purely technical rule, the representation of negative integers is interpreted as a natural finite projection of an infinite 2-adic integer. An analysis of the 2-adic addition of an infinite sequence of ones and the unit element makes it possible to establish the identity $-1 = \ldots 1111111_2$ in the ring Z_2. On this basis, the rule of two's complement is derived as a strict consequence of the relation $A + {\sim}A = -1$, from which $-A = {\sim}A + 1$ follows. The boundedness of a machine word, for example a 32-bit int type, is explained through the quotient ring $Z_2 / 2^{32}Z_2$, while signed overflow is interpreted not as an accidental programming anomaly but as a natural consequence of modular reduction.

The second stage of the methodology is aimed at revealing the applied potential of p-adic analysis in stream cryptography. Students are given the task of designing a fast pseudorandom number generator that avoids computationally expensive operations and relies as fully as possible on the hardware capabilities of the processor. For this purpose, T-functions are introduced as mappings of the form $f: Z_2 \to Z_2$, in which the value of each output bit depends only on the less significant or equally significant bits of the input. It is shown that this condition is satisfied by the basic logical and arithmetic operations of the processor. The culminating point of this stage is the establishment of the equivalence between the computer-science definition of a T-function and the mathematical notion of a 1-Lipschitz mapping in the 2-adic metric. Using the nonlinear state update function $x_{n+1} = x_n + (x_n^2 \text{ OR } 5) \bmod 2^{64}$ as an example,

ISSN 2786-6300 Print

the article demonstrates that the apparatus of p-adic differentiation makes it possible to prove its ergodicity analytically, without exhaustive traversal of all 2^{64} states.

The proposed methodology is grounded in the principles of pedagogical constructivism and presupposes the transformation of the lecture classroom into an interactive STEM laboratory. Mastery of p-adic mathematics is achieved not only through theoretical analysis but also through independent computer modeling using Python or SageMath. The laboratory practicum includes three levels: the construction of algorithms for converting rational numbers into p-adic expansions and understanding Hensel's lemma as an iterative algorithm; the visualization of 2-adic numbers and T-functions on infinite binary trees; and the investigation of Taylor series for the p-adic exponential and logarithm, which makes it possible to identify empirically the specific character of convergence in the space Q_p. The implementation of the proposed model reorients the mathematical preparation of master's students from isolated axiomatic formalism toward an interdisciplinary engineering perspective, contributes to overcoming alienation from abstract algebra, and forms readiness for the development and teaching of contemporary STEM courses.

Keywords: p-adic numbers, 2-adic integers, non-Archimedean metric, ultrametric, computer arithmetic, two's complement representation, T-functions, stream ciphers, pseudorandom number generator (PRNG), applied cryptography, mathematics education, master's level training, bottom-up design, principle of dual representation, STEM education.

Постановка проблеми. Сучасна модернізація вітчизняної природничо-математичної освіти об'єктивно потребує системного подолання глибокої методичної прірви, що історично сформувалася між фундаментальними, високоабстрактними теоретичними засадами вищої математики та їхньою безпосередньою прикладною реалізацією у сфері новітніх інформаційних технологій.

Особливої гостроти ця проблема набуває у процесі фахової підготовки здобувачів другого (магістерського) рівня вищої освіти, які навчаються за освітньо-професійною програмою «Середня освіта (Математика, інформатика)» і готуються до комплексної професійної діяльності в галузі викладання.

У традиційній освітній практиці опанування фундаментальних алгебраїчних структур і теоретико-числових понять нерідко супроводжується для студентів суттєвими дидактичними труднощами. Зокрема, під час розгляду можливих поповнень поля раціональних чисел Q основна увага традиційно зосереджується виключно на архімедовій метриці, що приводить до побудови поля дійсних чисел R.

Водночас альтернативне поповнення за неархімедовою метрикою, відповідно до теореми Островського, яке приводить до виникнення поля p-

ISSN 2786-6300 Print

адичних чисел Q_p та кільця цілих p-адичних чисел Z_p, у більшості випадків або залишається поза межами навчальних програм, або подається ізольовано − як своєрідний екзотичний і надмірно абстрактний математичний конструкт, позбавлений очевидного фізичного чи прикладного змісту.

Водночас у комп'ютерній складовій підготовки магістрантів спостерігається своєрідна дзеркальна ситуація. Базові засади комп'ютерної архітектури, зокрема машинна арифметика фіксованої розрядності, доповняльний код як спосіб подання від'ємних чисел, циклічне переповнення типів даних, а також ключові принципи сучасної кібербезпеки, пов'язані з проєктуванням потокових шифрів і генераторів псевдовипадкових послідовностей на основі нелінійних булевих функцій, викладаються переважно як сукупність прагматичних інженерних прийомів або алгоритмічних інструкцій, орієнтованих на механічне засвоєння. При цьому, як правило, не акцентується, що математичною моделлю ідеального мікропроцесора є саме кільце 2-адичних цілих чисел Z_2, а значна частина алгоритмів потокового шифрування ґрунтується на положеннях p-адичної ергодичної теорії.

Наслідком такої дезінтеграції навчального змісту стає формування у свідомості магістрантів стійкого когнітивного дисонансу: вища алгебра й теорія чисел починають сприйматися як «чиста наука заради науки», тоді як програмування − як «ремесло, позбавлене математичного підґрунтя». За таких умов майбутні вчителі не усвідомлюють внутрішньої синергії між цими дисциплінами, що істотно обмежує їхню здатність формувати в учнів цілісний науковий світогляд і проєктувати сучасні міждисциплінарні STEM-курси.

Отже, постає об'єктивна суперечність між надзвичайно високим евристичним і прикладним потенціалом теорії p-адичних чисел у галузі комп'ютерних наук, з одного боку, та відсутністю цілісної, науково обґрунтованої методичної системи їх вивчення у межах професійної підготовки майбутніх учителів математики та інформатики − з іншого. Необхідність подолання цієї суперечності шляхом розроблення інноваційних дидактичних підходів, що забезпечують інтеграцію абстрактної математики й комп'ютерної інженерії, становить актуальну науково-педагогічну проблему, розв'язанню якої присвячено це дослідження.

Аналіз останніх досліджень і публікацій.

Сучасний етап розвитку математичної науки та комп'ютерної інженерії засвідчує стале зростання інтересу до p-адичних чисел не лише як до об'єкта абстрактної теорії чисел, а й як до ефективного інструмента моделювання обчислювальних і криптографічних процесів. Класичні засади p-адичного аналізу ґрунтовно викладено у працях Н. Кобліца та Ф. Гувеа [1, 2]. Саме ці дослідження створили фундамент для подальшого переосмислення p-адичних структур у прикладному контексті.

Подальший розвиток проблематики відбувся у сфері комп'ютерних наук і криптографії. Зокрема, робота О. Клімова та А. Шаміра [3] стала важливим етапом у виявленні криптографічного потенціалу Т-функцій. Цей напрям було суттєво поглиблено у наступних публікаціях інших дослідників, де р-адична ергодична теорія постає вже як розвинений інструментарій прикладної алгебраїчної динаміки, релевантний для аналізу дискретних обчислювальних систем і криптографічних алгоритмів.

Водночас у працях, присвячених алгоритмічним засадам комп'ютерної арифметики, наголошується на фундаментальному значенні побітових операцій, модульної арифметики, машинної розрядності та ефективних обчислювальних процедур для сучасних цифрових систем. У цьому контексті особливу вагу має робота Д. Кнута [4]. Для розуміння сучасних криптографічних технік важливими є також дослідження Дж. Каца та І. Лінделла [5], де висвітлено архітектуру сучасної криптографії, роль генераторів псевдовипадкових чисел і вимоги до криптографічної стійкості алгоритмів. У сукупності ці праці підтверджують, що між р-адичним аналізом, машинною арифметикою та потоковою криптографією існує глибокий концептуальний зв'язок.

Разом із тим аналіз наукових джерел дає підстави стверджувати, що наявні дослідження переважно зосереджені або на власне математичній природі р-адичних чисел [1, 2], або на їх прикладних криптографічних і алгоритмічних аспектах [3–5]. Натомість питання дидактичної адаптації цього теоретичного апарату до потреб магістерської підготовки майбутніх учителів математики та інформатики розроблено недостатньо. Зокрема, у сучасній науково-методичній літературі фактично відсутні цілісні моделі навчання, які б поєднували в межах єдиної методичної системи класичну теорію р-адичних чисел, машинну арифметику доповняльного коду, Т-функції та програмне моделювання. Саме ця обставина зумовлює необхідність розроблення інноваційного дидактичного підходу, що забезпечував би органічну інтеграцію абстрактної алгебри, комп'ютерної інженерії та прикладної криптографії у процесі фахової підготовки магістрантів.

Мета статті. Метою статті є розроблення, теоретичне обґрунтування та концептуалізація інноваційної дидактичної моделі вивчення теорії р-адичних чисел для здобувачів другого (магістерського) рівня вищої освіти, які навчаються за освітньо-професійною програмою «Середня освіта (Математика, інформатика)». Дослідження безпосередньо спрямоване на подолання глибокого епістемологічного розриву між традиційним аксіоматично-дедуктивним викладанням абстрактної вищої алгебри та реальними прикладними потребами сучасної комп'ютерної інженерії. Для досягнення цієї мети пропонується впровадження методологічної стратегії висхідного проєктування у поєднанні з дидактичним принципом «подвійного подання», який дає змогу розглядати

кожне математичне поняття в нерозривному зв'язку з його інформатичним алгоритмічним відповідником.

Зокрема, стаття має на меті демістифікувати машинну арифметику шляхом строгого обґрунтування того, що комп'ютерний доповняльний код для подання від'ємних чисел є природною скінченною проєкцією нескінченного 2-адичного цілого числа у фактор-кільці Z_2 / $2^{32}Z_2$. Крім того, важливим завданням дослідження є розкриття прикладного потенціалу p-адичного аналізу у сфері сучасної кібербезпеки через вивчення T-функцій як 1-ліпшицевих відображень, що становлять теоретичну основу для проєктування швидких і криптографічно стійких генераторів псевдовипадкових послідовностей. Невід'ємним складником поставленої мети є також перетворення суто теоретичного курсу на інтерактивну дослідницьку лабораторію, у межах якої магістранти здійснюють самостійне програмне моделювання p-адичних алгебраїчних структур засобами мови Python або системи SageMath.

У підсумку практична реалізація запропонованої методики покликана сформувати у майбутніх викладачів високий рівень міждисциплінарної фахової компетентності, забезпечивши їх надійним концептуальним інструментарієм для розроблення та впровадження інноваційних STEM-курсів у закладах освіти.

Виклад основного матеріалу.

1. Від класичного дедуктивного формалізму до алгоритмічного конструктивізму.

Традиційна парадигма та її обмеження. Історично склалося так, що введення p-адичних чисел у курсах вищої алгебри та теорії чисел здебільшого здійснюється в межах дедуктивного, формально-аксіоматичного підходу, успадкованого від класичної університетської математичної освіти. Такий спосіб побудови навчального матеріалу, як правило, розпочинається з формального означення p-адичного нормування на полі раціональних чисел Q. Далі вводиться відповідна неархімедова метрика, після чого на завершальному етапі здійснюється абстрактна топологічна операція поповнення простору за допомогою фундаментальних послідовностей Коші.

Означення p-адичних чисел може бути сформульоване наступним чином:

Q_p — це метричне поповнення поля раціональних чисел Q відносно p-адичної норми, елементи поповнення називаються p-адичними числами, арифметичні дії над ними вводяться природнім чином.

Попри бездоганність цього підходу з погляду математичної строгості, у дидактичному аспекті він породжує для здобувачів вищої освіти значні труднощі. Основна причина полягає в тому, що математична інтуїція студентів упродовж тривалого часу формується переважно в межах класичного математичного аналізу та геометрії, а отже, міцно пов'язується з архімедовою

природою [6] поля дійсних чисел R. Відповідно до архімедового принципу, багаторазове додавання одиниці неминуче приводить до необмеженого зростання величини, що цілком узгоджується з повсякденним фізичним досвідом вимірювання довжин, мас чи інших величин.

Натомість неархімедова метрика вимагає прийняття контрінтуїтивного положення: послідовність степенів простого числа p, коли показник необмежено зростає, не віддаляється від нуля, а прямує до нього. Іншими словами, що більше число ділиться на основу p, то меншим воно стає в сенсі цієї нової метрики. Для магістрантів такий епістемологічний розрив перетворюється на істотний пізнавальний бар'єр. Через відсутність звичних просторових образів і неможливість прямої візуалізації в межах звичного тривимірного простору топологічні конструкції p-адичного аналізу нерідко сприймаються студентами як штучні й відірвані від реальності побудови, позбавлені очевидного практичного чи інженерного змісту.

Стратегія висхідного проєктування. Усвідомлюючи наявність цих фундаментальних дидактичних труднощів, ми пропонуємо принципово змінити вектор викладання й архітектуру навчального процесу. Замість руху від абстрактних топологічних тверджень до поодиноких числових прикладів, що відповідає класичному низхідному підходу, у дослідженні застосовується методична стратегія висхідного проєктування.

Сутність цієї стратегії полягає в тому, що навчальний процес розгортається не від математичних аксіом, а від конкретної, інтуїтивно зрозумілої та професійно значущої проблеми у сфері комп'ютерної інженерії. Лише після її аналізу відбувається послідовне вибудовування математичного апарату, здатного забезпечити її розв'язання. За такого підходу неархімедова метрика, ультраметричні простори та p-адичні числа постають не як апріорно задані теоретичні конструкції, а як природний, логічно вмотивований і концептуально необхідний результат розв'язання фундаментальної інформатичної проблеми. Унаслідок цього магістранти самі доходять висновку про потребу розширення звичного математичного інструментарію.

Принцип «подвійного подання» в міждисциплінарному контексті. Органічним методологічним доповненням стратегії висхідного проєктування є дидактичний принцип «подвійного подання». Відповідно до нього кожне абстрактне алгебраїчне або теоретико-числове поняття має отримувати свій «цифровий двійник», тобто чіткий структурний, алгоритмічний або програмний відповідник у сфері комп'ютерних наук. Це дає можливість магістрантам, які навчаються за освітньо-професійною програмою «Середня освіта (Математика, інформатика)», аналізувати один і той самий об'єкт одночасно в перспективі двох наукових дисциплін. Наприклад, математичний об'єкт може розглядатися як елемент фактор-кільця і водночас як стан бітового регістра мікропроцесора.

ISSN 2786-6300 Print

Такий підхід забезпечує синтез знань і сприяє формуванню цілісного наукового світогляду майбутнього педагога.

Тригерна задача: парадокс машинного подання чисел. Практична реалізація запропонованої методики розпочинається з постановки тригерної задачі, що спирається на добре відомий студентам матеріал з архітектури обчислювальних систем. Вихідною точкою виступає концептуальний парадокс машинного подання цілих чисел.

Студентам відомо, що сучасна комп'ютерна пам'ять і арифметико-логічні пристрої центрального процесора оперують даними у формі бітових рядків, тобто дискретних послідовностей нулів і одиниць, жорстко обмежених апаратною розрядністю системи. У стандартній архітектурі використовуються машинні слова й регістри фіксованої довжини, наприклад 8, 16, 32 або 64 біти. Будь-яка арифметична операція, результат якої перевищує цю розрядність, неминуче супроводжується відкиданням старших бітів. В інформатиці це явище визначається як переповнення, а з математичного погляду є точною реалізацією арифметики за модулем степеня числа 2, наприклад за модулем 2 у 32 степені для стандартного цілого типу даних.

На цьому етапі викладач свідомо створює ситуацію контрольованого пізнавального напруження, ставлячи перед магістрантами евристичне запитання: яким чином можна математично строго, аналітично точно й внутрішньо несуперечливо описати арифметику ідеального мікропроцесора, якби фізичні обмеження на кількість розрядів було усунуто? Інакше кажучи, що станеться з математичною структурою обчислень, якщо дозволити машинному слову нескінченно продовжуватися вліво, у бік старших розрядів?

Від апаратного регістра до нескінченності: конструювання кільця Z_p. Саме цей експеримент, що передбачає поступове абстрагування від скінченного фізичного машинного слова до нескінченного ідеального математичного регістра, є найбільш природним, психологічно прийнятним та алгоритмічно інтуїтивним шляхом до введення поняття кільця цілих p-адичних чисел Z_p. Для інформатики найбільш релевантним є випадок, коли p дорівнює 2, що безпосередньо приводить до кільця 2-адичних цілих чисел Z_2.

У процесі моделювання такої ситуації студенти самостійно усвідомлюють, що звичайне натуральне число завжди має скінченний двійковий запис, або, що рівнозначно, нескінченну кількість нулів ліворуч від старшого значущого біта. Натомість допущення нескінченної кількості значущих, тобто ненульових, цифр ліворуч концептуально породжує нову числову множину. При цьому, перенесення розряду під час додавання таких нескінченних бітових послідовностей алгоритмічно відбувається так само, як і в класичній арифметиці під час додавання у стовпчик, однак сам процес поширюється вліво без межі. Унаслідок цього p-адичні числа постають у свідомості здобувача не як ізольований об'єкт

ISSN 2786-6300 Print

із теореми Островського, а як природне алгебраїчне узагальнення повсякденної комп'ютерної арифметики на гіпотетичний випадок пам'яті необмеженого обсягу.

Алгоритмічна та інформаційна природа ультраметрики. Завершальним етапом цього методичного блоку є перехід від інтуїтивного алгоритмічного розуміння до строгих топологічних властивостей відповідної множини. Насамперед це стосується дидактичного пояснення сильної нерівності трикутника, тобто ультраметричної нерівності, згідно з якою p-адична норма суми двох чисел не перевищує максимуму p-адичних норм доданків.

У традиційному дедуктивному курсі математичного аналізу ця властивість часто виглядає надто абстрактною і майже не має інтуїтивних аналогів у геометрії Евкліда. Однак у запропонованому інформатичному форматі вона набуває прозорого алгоритмічного змісту. Здобувачам пояснюється, що p-адична абсолютна величина, або p-адична норма числа, безпосередньо пов'язана з кількістю нулів, якими закінчується його запис у p-ічній системі числення. Інакше кажучи, йдеться про позицію першого ненульового молодшого розряду, якщо розглядати запис справа наліво. Що більше нулів міститься наприкінці такого запису, тобто що на вищий степінь основи p ділиться число без остачі, то ближчим воно є до нуля в p-адичному топологічному сенсі, а його норма є меншою.

Логічний наслідок цього стає очевидним для майбутнього фахівця з програмування: коли процесор виконує порозрядне додавання двох p-адичних або звичайних двійкових чисел, кількість нулів наприкінці суми, а отже і p-адична норма результату, жорстко визначається структурою самих доданків. Кількість нульових молодших розрядів у результаті за жодних умов не може бути меншою, ніж мінімальна кількість нульових молодших розрядів серед доданків. Саме це і становить алгоритмічний зміст ультраметричної нерівності.

Подібна алгоритмічна візуалізація істотно послаблює когнітивний бар'єр, пов'язаний зі сприйняттям ультраметрики. Більше того, вона дає змогу дидактично продуктивно перетворити складну абстрактну топологію неархімедових метричних просторів на наочний і добре знайомий фахівцям з інформатики процес обробки структур даних, зокрема маніпуляцій із префіксними деревами або n-арними деревами цифрового пошуку.

За такого підходу топологічна відстань між числами осмислюється не як абстрактна геометрична величина, а як глибина збігу їхніх молодших розрядів у пам'яті комп'ютера.

Саме це методичне досягнення закладає міцне концептуальне підґрунтя для подальшого вивчення застосувань p-адичного аналізу в теорії потокових шифрів, проєктуванні сучасних генераторів псевдовипадкових чисел і розробленні стійких протоколів кібербезпеки.

ISSN 2786-6300 Print

2. 2-адичні числа та машинна арифметика.

Криза механічного запам'ятовування у викладанні інформатики. Одним із фундаментальних і концептуально найважливіших етапів реалізації запропонованої методики є глибоке переосмислення внутрішнього машинного подання від'ємних цілих чисел у пам'яті сучасних обчислювальних систем. Аналіз актуального стану викладання дисциплін комп'ютерного циклу засвідчує наявність суттєвої методичної проблеми: у традиційних курсах інформатики та архітектури комп'ютерів поняття доповняльного коду, або two's complement, здебільшого подається здобувачам освіти як суто прагматичний інженерний прийом. Як правило, викладання обмежується формулюванням механічного правила: для того щоб отримати бітове подання від'ємного числа, потрібно інвертувати всі біти його додатного модуля, а потім додати до результату одиницю.

Наслідком такого редукціоністського підходу є те, що магістранти змушені засвоювати цей алгоритм як догму. Вони розуміють, як саме він працює на рівні операцій із даними, і навіть усвідомлюють його апаратну доцільність, оскільки використання доповняльного коду уможливлює реалізацію віднімання через додавання без побудови окремого процесорного блоку для цієї операції. Проте фундаментальна математична природа відповідного явища залишається для них незрозумілою. У результаті доповняльний код сприймається як своєрідна інтелектуальна «чорна скринька», відірвана від строгих закономірностей вищої алгебри.

Зміна парадигми: від інженерного прийому до нескінченних* p*-адичних рядів. Запропонована методика передбачає принципово інший, алгебраїчно строгий підхід до інтерпретації цієї проблеми. Комп'ютерний доповняльний код розглядається не як штучний винахід інженерної практики, а як природна скінченна проєкція нескінченного 2-адичного цілого числа. На цьому етапі магістрантам демонструється канонічний розклад довільного цілого числа x у 2-адичний ряд, що є базовою формою подання елементів кільця Z_2:

$$x = a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + a_3 \cdot 2^3 + \ldots + a_k \cdot 2^k + \ldots ,$$

де всі коефіцієнти a_i належать множині {0; 1}.

Дидактична цінність такого запису полягає в тому, що він зовні нагадує звичне подання числа у двійковій системі числення, добре знайоме студентам. Водночас викладач акцентує принципово важливу обставину: на відміну від класичної арифметики дійсних чисел R, де нескінченна сума додатних степенів двійки є розбіжною, у 2-адичній метриці цей ряд виявляється збіжним. Це пояснюється тим, що зі зростанням індексу k значення 2^k у 2-адичному сенсі стає все ближчим до нуля. Таким чином, кожне 2-адичне ціле число може бути інтерпретоване як нескінченний двійковий рядок, що необмежено продовжується вліво: …$a_3a_2a_1a_0$.

ISSN 2786-6300 Print

Пізнавальний прорив: аналіз природи від'ємної одиниці. Справжній дидактичний перелом у сприйнятті теми відбувається під час аналізу алгебраїчної природи числа −1. Викладач навмисно ініціює проблемну дискусію, звертаючи увагу студентів на парадоксальну обставину: у полі дійних чисел R не існує жодної нескінченної суми, що складається лише з додатних доданків і водночас дорівнює від'ємному числу.

Для подолання цього стереотипу студентам пропонується практичний експеримент − виконати 2-адичне додавання у стовпчик нескінченного рядка одиниць до звичайної математичної одиниці: $\ldots1111111_2 + 1_2$. Виконуючи цю операцію справа наліво, магістранти бачать, що додавання одиниці до наймолодшого розряду породжує нуль у результаті та перенос одиниці до наступного розряду. У кожному наступному розряді повторюється та сама ситуація: сума двох одиниць знову дає нуль і новий перенос. Таким чином, студенти безпосередньо спостерігають феномен нескінченного хвильового перенесення розряду вліво. Наслідком цього процесу є послідовне перетворення всіх бітів нескінченного рядка на нулі: $\ldots1111111_2 + 1_2 = \ldots0000000_2 = 0$. Саме цей момент є дуже важливим. Спираючись винятково на логіку арифметичних дій, магістранти самостійно приходять до фундаментального висновку: якщо сума послідовності $\ldots1111111_2$ і числа 1 дорівнює нулю, то ця послідовність є додатковим оберненим елементом до одиниці. Отже, у строгому алгебраїчному сенсі кільця Z_2 виконується тотожність: $-1 = \ldots1111111_2$.

Узагальнення алгоритму: алгебраїчна природа інверсії. Після усвідомлення цього факту викладач пропонує магістрантам самостійно вивести відоме інженерне правило побудови доповняльного коду вже не як емпіричний алгоритм, а як строгий математичний наслідок. Нехай A − довільне число. Якщо здійснити над ним побітову логічну інверсію, тобто операцію NOT, то буде отримано число, яке позначимо через ~A. Очевидно, що сума числа та його повної інверсії дає нескінченний рядок одиниць, оскільки в кожному розряді поєднуються 0 і 1: $A + \sim A = \ldots1111111_2$. Оскільки нескінченний рядок одиниць у 2-адичній арифметиці дорівнює −1, то одержуємо співвідношення $A + \sim A = -1$. Звідси безпосередньо випливає, що $-A = \sim A + 1$.

Таким чином, магістранти наочно переконуються, що правило «інвертуй і додай одиницю» не є випадковим технічним прийомом мікроелектроніки, а становить прямий і логічно неминучий наслідок алгебраїчної структури кільця 2-адичних цілих чисел.

Фактор-кільця та строге обґрунтування машинної розрядності. Завершальний етап цього дидактичного кейсу пов'язаний із переходом від нескінченних ідеальних математичних структур до реальної комп'ютерної архітектури. Фізична обчислювальна машина не може оперувати нескінченними бітовими послідовностями, оскільки довжина будь-якого регістра є скінченною.

Тому 32-бітне машинне слово, яке в мовах програмування високого рівня, зокрема C, C++, Java або C#, репрезентується типом int, у межах запропонованої методики математично строго розглядається як елемент фактор-кільця $Z_2 / 2^{32}Z_2$.

Для студента ця алгебраїчна конструкція означає таке. Ідеал $2^{32}Z_2$ складається з усіх нескінченних 2-адичних чисел, які закінчуються щонайменше тридцятьма двома нулями. Перехід до фактор-кільця є математично еквівалентним ігноруванню всіх розрядів числа, починаючи з тридцять третього і далі вліво. Саме така побудова є точною математичною моделлю того, як фізично працює центральний процесор під час відкидання старших бітів.

Більше того, явище знакового переповнення, або integer overflow, яке в традиційній практиці програмування часто розглядається як помилка, аномалія або непередбачувана поведінка системи, у межах цієї дидактичної моделі дістає цілком строге математичне пояснення. Додавання одиниці до максимально можливого додатного числа призводить до переходу через межу розрядності, що в алгебраїчному сенсі є звичайною модульною редукцією 2-адичного числа за ідеалом $2^{32}Z_2$. Отже, процесор не помиляється − він точно виконує операції в межах відповідного фактор-кільця.

Завдяки такому інтегративному підходу доповняльний код перестає бути для магістранта незрозумілим технічним прийомом. Він постає як витончена й концептуально прозора алгоритмічна реалізація вищої арифметики. Студент, який проходить цей шлях, уже не обмежується роллю виконавця технічних операцій, а набуває якостей інженера-математика, здатного бачити глибоку алгебраїчну закономірність у базових механізмах машинних обчислень. Такий дидактичний досвід істотно підвищує рівень його фахової компетентності та посилює мотивацію до вивчення абстрактних математичних дисциплін.

3. p-адична динаміка та криптографія (T-функції як 1-ліпшицеві відображення).

Кібербезпека як простір прикладного застосування вищої алгебри. Другий концептуальний етап запропонованої методики повністю спрямований на виявлення прикладного потенціалу p-адичних чисел у галузі сучасної кібербезпеки та криптографії. У традиційних курсах захисту інформації провідне місце, як правило, відводиться асиметричній криптографії, зокрема системам типу RSA та криптографії на еліптичних кривих. Водночас для багатьох високошвидкісних застосувань, таких як шифрування відеопотоків у режимі реального часу, захист каналів зв'язку поколінь 5G і 6G або забезпечення безпеки пристроїв Інтернету речей з обмеженими обчислювальними ресурсами, асиметричні алгоритми виявляються надто повільними.

За таких умов вирішального значення набувають симетричні потокові шифри, функціональним ядром яких є криптографічно стійкі генератори псевдовипадкових чисел.

Саме в цьому контексті перед магістрантами формулюється фундаментальна інженерно-математична проблема: яким чином побудувати надзвичайно швидкий генератор псевдовипадкових послідовностей, здатний максимально ефективно використовувати апаратний паралелізм сучасних суперскалярних багатоядерних процесорів. Ключова вимога полягає у відмові від обчислювально витратних операцій, зокрема повільного апаратного ділення, множення великих чисел, а також від використання нелінійних таблиць підстановки, які спричиняють затримки через промахи в кеш-пам'яті процесора.

Концепція* T-*функцій та їхня апаратна природа. Для розв'язання цієї проблеми вводиться поняття T-функцій, розроблене у роботах О. Клімова та А. Шаміра. T-функція визначається як спеціальне алгебраїчне відображення вигляду $f: Z_2 \to Z_2$, яке задовольняє принципову умову: значення і-того біта результату залежить лише від значень бітів аргументу з індексами від 0 до і включно.

Аналізуючи цю умову в контексті апаратної архітектури комп'ютера, магістранти доходять важливого висновку: їй відповідають усі базові побітові логічні операції процесора, зокрема AND, OR, XOR, NOT, а також стандартні операції машинного додавання, віднімання і множення. Причина полягає в тому, що під час звичайного додавання у стовпчик перенесення розряду поширюється лише справа наліво, тобто від молодших бітів до старших, тоді як старші біти не можуть змінювати значення молодших. Унаслідок цього T-функції постають як природна алгебраїчна мова функціонування самого мікропроцесора.

Топологічний зміст* T-*функцій у світлі* p-*адичного аналізу. Наступний етап становить кульмінацію абстрактного осмислення теми, оскільки саме тут магістрантам розкривається глибокий зв'язок між бітовою архітектурою комп'ютера та неархімедовою топологією. Спираючись на фундаментальні результати p-адичної ергодичної теорії, пов'язані насамперед з іменем В. Анашина, викладач доводить твердження, яке має принципове значення: інформатичне означення T-функції є повністю еквівалентним математичному поняттю 1-ліпшицевого відображення відносно 2-адичної метрики. Це співвідношення виражається нерівністю: $|f(x) - f(y)|_2 \leq |x - y|_2$.

Студенти інтерпретують її зміст таким чином: якщо два цілі числа x та y збігаються у своїх молодших k розрядах, то їхні образи f(x) та f(y) також гарантовано збігатимуться у тих самих молодших k розрядах. Інакше кажучи, зміна старших бітів аргументу не може впливати на молодші біти результату. Це і є точним математичним описом відсутності зворотного інформаційного впливу в роботі процесора.

Таким чином, неархімедова топологія виявляється не абстрактною побудовою, а природним апаратом для опису інформаційних потоків у цифрових системах.

ISSN 2786-6300 Print

Доведення ергодичності: аналітичний підхід замість повного перебору. Практичне значення цієї теорії розкривається під час вивчення умов ергодичності. Ергодичність на Z_2 означає, що функція породжує єдиний цикл максимально можливої довжини. Для 64-бітного регістра такий цикл охоплює 2^{64} станів, тобто понад 18 квінтильйонів можливих комбінацій. Якщо намагатися перевірити проходження всіх цих станів методом прямого перебору, навіть найпотужнішим обчислювальним системам знадобився б надзвичайно тривалий час. Натомість магістрантам пропонується розглянути конкретну криптографічну функцію оновлення стану регістра:

$$x_{n+1} = x_n + (x_n^2 \text{ OR } 5) \bmod 2^{64}.$$

Із застосуванням апарату p-адичного диференціювання, зокрема відповідних теорем Анашина, студенти отримують можливість аналітично довести ергодичність цієї нелінійної функції. Для цього вони обчислюють p-адичну похідну та досліджують її властивості за модулем 2 і 4. У результаті виявляється, що функція здійснює повну перестановку всіх 2^{64} можливих станів без колізій і пропусків. Таке доведення стає для студентів переконливим прикладом переваги аналітичного мислення над грубою обчислювальною силою.

Саме на цьому етапі у здобувачів формується глибоке розуміння того, яким чином неперервна, нескінченновимірна p-адична математика стає надійним теоретичним підґрунтям для створення високошвидкісних і криптографічно стійких алгоритмів потокового шифрування.

У результаті p-адичний аналіз постає не як віддалений розділ абстрактної теорії чисел, а як дієвий інструмент сучасної комп'ютерної інженерії та кібербезпеки.

4. Програмна реалізація як інтерактивна дослідницька лабораторія.

Конструктивізм та експериментальна математика. Високий рівень абстракції p-адичного аналізу потребує спеціально організованих підходів до закріплення навчального матеріалу. Саме тому невід'ємною й органічною складовою розробленої методичної системи виступає комп'ютерне моделювання. В основу цього етапу покладено принципи педагогічного конструктивізму, згідно з якими математичне поняття найефективніше засвоюється тоді, коли магістрант самостійно «конструює» його у віртуальному середовищі. У такому форматі традиційна лекційна аудиторія трансформується у високотехнологічну дослідницьку STEM-лабораторію. Здобувачам пропонується самостійно спроєктувати й реалізувати архітектуру класів для повноцінної роботи з p-адичними числами, використовуючи об'єктно-орієнтовані можливості мови програмування Python або спеціалізовані алгебраїчні модулі системи комп'ютерної алгебри SageMath.

Навчальні лабораторні завдання та рівні складності. Лабораторний практикум охоплює три взаємопов'язані рівні складності.

Арифметика та лема Гензеля як алгоритм. Перше завдання передбачає створення алгоритму перетворення звичайних раціональних чисел x, що належать полю Q, у їхній канонічний p-адичний ряд. У ході виконання цього завдання студенти усвідомлюють, що знаменита лема Гензеля є не лише абстрактною теоремою про існування кореня многочлена в кільці Z_p, а й потужним ітераційним алгоритмом, який можна розглядати як точний p-адичний аналог методу Ньютона. Реалізуючи цей алгоритм програмно, магістранти покроково, розряд за розрядом, знаходять коефіцієнти p-адичного розкладу й бачать, як з кожною ітерацією наближений результат стає дедалі точнішим у сенсі неархімедової метрики. У межах цього ж завдання студенти самостійно програмують процедуру знаходження мультиплікативного оберненого елемента в кільці Z_p і мають можливість зіставити логіку та ефективність цього процесу з класичним розширеним алгоритмом Евкліда.

Візуалізація топології через дерева. Друге завдання спрямоване на розвиток просторово-топологічного мислення. Оскільки 2-адичні цілі числа Z_2 можуть бути геометрично інтерпретовані як границя, тобто множина всіх нескінченних шляхів, повного нескінченного бінарного дерева, магістрантам пропонується створити програмну візуалізацію 2-адичних T-функцій у вигляді спрямованих графів на таких деревах. У цьому випадку невидима абстрактна топологія набуває на екрані комп'ютера наочного образу: студенти спостерігають, як 1-ліпшицева функція впорядковано відображає одні гілки дерева в інші, не порушуючи їхньої внутрішньої структури. Такий візуальний досвід істотно послаблює дискомфорт, який зазвичай супроводжує сприйняття топології нульвимірних просторів.

Парадокси* p-*адичного математичного аналізу. Третє, найбільш складне завдання пов'язане з дослідженням швидкості збіжності нескінченних рядів Тейлора для фундаментальних аналітичних функцій, зокрема p-адичної експоненти $\exp_p(x)$ та p-адичного логарифма $\log_p(x)$. Саме на цьому етапі студенти стикаються з одним із найбільш незвичних для класичного мислення фактів: завдяки властивостям ультраметрики для збіжності числового ряду в просторі Q_p достатньо, щоб його загальний член прямував до нуля. Отже, необхідна умова

Коші в цьому контексті водночас стає і достатньою. Магістранти програмують обчислення таких рядів і емпірично досліджують їхні радіуси збіжності, які суттєво відрізняються від відповідних характеристик у класичному дійсному аналізі. Зокрема, вони переконуються, що p-адична експонента збігається лише на досить вузькому околі нуля.

Підсумкове значення програмної реалізації. У результаті цей практично орієнтований етап навчання докорінно змінює характер сприйняття теорії чисел, перетворюючи її з абстрактної й формально складної дисципліни на захопливу

сферу експериментального комп'ютерного дослідження. Завдяки програмній реалізації складних алгебраїчних структур майбутні вчителі математики та інформатики долають бар'єр відчуження від предмета. Вони набувають цінного досвіду інтеграції чистої математичної теорії з сучасним програмуванням, що безпосередньо формує їхню готовність до розроблення та викладання авторських міждисциплінарних STEM-курсів у закладах освіти.

Висновки. Проведене дослідження засвідчило, що інтеграція теорії p-адичних чисел із комп'ютерною арифметикою, потоковою криптографією та програмним моделюванням є методично продуктивною у процесі підготовки магістрів за предметною спеціальністю А4.04 «Середня освіта (Математика)». Запропонована дидактична модель, що поєднує стратегію висхідного проєктування з принципом подвійного подання, сприяє подоланню відчуження від абстрактної алгебри, посиленню міждисциплінарних зв'язків і формуванню готовності магістрантів до розроблення та викладання сучасних STEM-курсів.

Література:

1. Koblitz, N. (1984). p-adic Numbers, p-adic Analysis, and Zeta-Functions (2nd ed.). Springer-Verlag. https://doi.org/10.1007/978-1-4612-1112-9

2. Gouvêa, F.Q. (2020). p-adic Numbers: An Introduction (3rd ed.). Springer. https://doi.org/10.1007/978-3-030-47295-5

3. Klimov, A., & Shamir, A. (2004). Cryptographic applications of T-functions. In Selected Areas in Cryptography: 10th Annual International Workshop, SAC 2003 (Vol. 3006, pp. 248–261). Springer. https://doi.org/10.1007/978-3-540-24654-1_18

4. Knuth, D.E. (2014). The Art of Computer Programming, Volume 2: Seminumerical Algorithms (3rd ed.). Addison-Wesley Professional.

5. Katz, J., & Lindell, Y. (2020). Introduction to Modern Cryptography (3rd ed.). CRC Press. https://doi.org/10.1201/9781351133036

6. Хаць Р.В., Комарницька Л.І., Матурін Ю.П. Аксіоматичний та конструктивний підходи до побудови теорій числових множин. *Перспективи та інновації науки (Серія "Педагогіка")*, 2(60), 2026, 1572-1585. https://doi.org/10.52058/2786-4952-2026-2(60)-1572-1585

References

1. Koblitz, N. (1984). p-adic Numbers, p-adic Analysis, and Zeta-Functions (2nd ed.). Springer-Verlag. https://doi.org/10.1007/978-1-4612-1112-9

2. Gouvêa, F.Q. (2020). p-adic Numbers: An Introduction (3rd ed.). Springer. https://doi.org/10.1007/978-3-030-47295-5

3. Klimov, A., & Shamir, A. (2004). Cryptographic applications of T-functions. In Selected Areas in Cryptography: 10th Annual International Workshop, SAC 2003 (Vol. 3006, pp. 248–261). Springer. https://doi.org/10.1007/978-3-540-24654-1_18

4. Knuth, D.E. (2014). The Art of Computer Programming, Volume 2: Seminumerical Algorithms (3rd ed.). Addison-Wesley Professional.

5. Katz, J., & Lindell, Y. (2020). Introduction to Modern Cryptography (3rd ed.). CRC Press. https://doi.org/10.1201/9781351133036

6. Khats, R.V., Komarnytska, L.I., & Maturin, Yu.P. (2026). Aksiomatychnyi ta konstruktyvnyi pidkhody do pobudovy teorii chyslovykh mnozhyn. *Perspektyvy ta innovatsii nauky (Seriia "Pedahohika"*), 2(60), 1572-1585 [in Ukrainian]. https://doi.org/10.52058/2786-4952-2026-2(60)-1572-1585

Дата першого надходження статті до видання: 27.04.2026
Дата прийняття статті до друку після рецензування: 11.05.2026