• the lack of a balance between the ever-increasing amount of training information and the reduction of the number of hours for the study of topics, ie, the lack of time to study, which impedes the implementation of the link integrative component of training.

• There are few cognitive students, due to the lack of visible relationships between the learning process and future professional activities, which reduces the motivation for learning and the use of mathematical methods and models.

Originality. *For the first time, the definition of the concept of «mathematical competence of economists» is formulated, its definition is formulated, its structure is described. The factors influencing the formation of mathematical competence of future economists and the group of professionally important qualities of specialists are highlighted.*

Conclusion. *Considering and analyzing the problem of forming the mathematical competence of future economists in a higher educational institution, it should be noted that a modern economist must possess modern economic and mathematical methods, be able to use them to simulate real economic situations, because it allows him to master the theoretical issues of the modern economy, contributes to the increase level of qualification and general professional culture of a specialist. Prospects for further development of the problem under investigation are: to identify qualitative differences in the content content of plans and programs for the formation of professional and mathematical competence of economists, depending on their specialization; development of students' culture in the process of mastering economic and mathematical competences; improvement of mathematical competence of specialists of economic activity in the system of professional development.*

Keywords: *mathematical competence, future economists, mathematical competence of economists.*

Одержано редакцією 11.10.2017 р.
Прийнято до публікації 04.12.2017 р.

УДК 372.851

АКУЛЕНКО Ірина Анатоліївна,
доктор педагогічних наук, професор
кафедри алгебри і математичного аналізу
Черкаського національного університету
імені Богдана Хмельницького
e-mail: akulenkoira@ukr.net
ЛЕЩЕНКО Юрій Юрійович,
кандидат фізико-математичних наук,
доцент кафедри алгебри і математичного
аналізу Черкаського національного
університету імені Богдана Хмельницького
e-mail: ylesch@gmail.com

НАВЧАННЯ ДОВЕДЕНЬ МАТЕМАТИЧНИХ ТВЕРДЖЕНЬ У КУРСІ ЗА ВИБОРОМ «ОСНОВИ КРИПТОЛОГІЇ»

У статті розкрито особливості навчання доведень математичних тверджень учнів, які вивчають математику поглиблено, на прикладі опанування ними змісту курсу за вибором «Основи криптології».

Ключові слова: *доведення математичних тверджень, навчання математики на поглибленому рівні, курс за вибором.*

Постановка проблеми. Оволодіння учнями мистецтвом доведення, аргументації та спростування є одним із найважливіших навчальних результатів на рівні загальної

середньої освіти. Потужний потенціал у цьому контексті має навчання математики, зокрема у контексті навчання доведень математичних тверджень. Процес навчання доведень математичних фактів є довготривалим, займає весь термін вивчення систематичних курсів алгебри й геометрії та вимагає провадження логічної пропедевтики у початковій школі й у 5-6 класах.

На різних етапах шкільної математичної освіти реалізуються різні етапи навчання доведень. У початковій школі формується початковий суб'єктний досвід щодо верифікації певних тверджень (перевірка, переважно дослідним шляхом, індуктивні міркування на основі повної й неповної індукції). У 5-6 класах реалізується пропедевтичний етап щодо навчання учнів евристичних прийомів, опанування окремих логічних умінь та вдосконалення загальних і спеціальних розумових прийомів (порівняння, аналогія, аналіз, синтез, абстрагування, конкретизація, підведення об'єктів під поняття, вибір ознак понять, що відповідають даним умови, розгортання умови, виведення наслідків із належності об'єкта до обсягу поняття тощо), формування ціннісного ставлення до необхідності не лише дослідної перевірки правильності певного твердження з опорою на попередньо сформований суб'єктний досвід, а й до провадження доказових міркувань з опорою на інтуїтивні неусвідомлювані вміння застосовувати логічні операції й закони у створенні суджень і умовиводів. У 7-8 класах учні демонструють спроможність будувати ланцюжки умовиводів, ґрунтовані на законах логіки, і усвідомлювати цей процес, однак налаштовані школярі цього вікового періоду переважно на запам'ятовування представленого їм доведення (з опорою на виділення його головної ідеї, виокремлення кроків у доведенні), ніж до самостійного його створення, «винайдення». Старший шкільний вік (за характеристикою психологів (П. Блонський [7], Р. Немов, В. Давидов, Ж. Піаже, Р. Солсо, Д. Халперн [14])) – це вік, коли в школярів формуються операційні структури доведень, і вони усвідомлено послуговуються ними у самостійному пошуку й конструюванні доведень. П. Блонський зауважував [7, с. 102], що розвиток вміння доводити припадає головним чином на старші класи, а вдосконалення цього вміння проходить дві стадії: 1) у підлітковому віці учень швидше запам'ятовує доведення, ніж самостійно користується ним, і ще менше він його створює; 2) в юнацькому ж віці вже помітно актуалізується критичне ставлення до запропонованих доведень і прагнення до провадження власних. Відтак, проблема навчання школярів доведень математичних тверджень є актуальною як для основної, так і для старшої школи, у навчанні як алгебри, так і геометрії.

Особливого значення вона набуває для учнів, які вивчають математику на профільному чи поглибленому рівнях. Оскільки, якщо в курсі математики, що вивчається на рівні стандарту, мова йде швидше про доказові міркування, аніж про доведення в строгому розумінні цього слова, доведення ж математичних тверджень у курсі алгебри чи геометрії, що вивчається на профільному чи поглибленому рівнях, передбачають підвищення рівня логічної строгості в їхньому провадженні. Одним із вагомих результатів навчання математики на цих рівнях передбачена спроможність учнів не лише відтворювати запропоновані (вчителем чи підручником) доведення математичних фактів, а й конструювати власні чи спростовувати запропоновані доведення, ґрунтуючись на методах наукового пізнання і прийомах евристичного й логічного мислення.

Аналіз досліджень та публікацій. Загальні методичні аспекти навчання доведень математичних тверджень розглядали в своїх роботах В. Брадіс, Є. Ляпін, М. Бескін, М. Метельський, Я. Грудьонов, З. Слєпкань, С. Семенець, Н. Тарасенкова, Л. Фрідман та інші. Загальні питання методики навчання доведень дедуктивним методом досліджено науковцями російської (Г. Глейзер, В. Гусєв, В. Далінгер, Г. Дорофеєв, Ю. Колягін, О. Лященко, Г. Саранцев, І. Смірнова, А. Столяр, І. Шаригін, та ін.) та вітчизняної

методичної шкіл. Проблематика навчання доведень математичних тверджень розроблялася українськими науковцями в таких напрямах: методика конструювання й навчання доведень тверджень курсу алгебри (Г. Бевз, В. Бевз), методика конструювання й навчання доведень тверджень курсу геометрії основної і старшої школи (М. Бурда, Н. Тарасенкова [13]), психолого-педагогічні основи навчання учнів доведень (З. Слєпкань [11]), застосування евристик у процесі пошуку способу доведення математичних фактів (О. Скафа [10]), формування й розвиток логічних умінь у навчанні учнів, які вивчають математику поглиблено (Н. Тарасенкова, І. Акуленко [1]), розвиток умінь старшокласників доводити математичні твердження у процесі вивчення алгебри і початків аналізу (Н. Кугай [7]), навчання доведень у курсі стереометрії, що вивчається на поглибленому рівні (С. Яценко [16]), формування вмінь учнів доводити математичні твердження під час вивчення функціональної змістової лінії на поглибленому рівні (В. Кірман [6]), вивчення елементів математичної логіки і теоретичних основ доведень у поглибленому курсі математики (Ю. Лещенко [2]) та ін. Сучасні наукові розвідки додатково зосереджуються на перевагах і застереженнях щодо застосуванні ІКТ у навчанні доведень, зокрема на основі комп'ютерного експерименту (М. Жалдак, С. Семеріков, Т. Ширікова [15] та ін.).

Попри широкий спектр педагогічних, психологічних, методичних досліджень проблема навчання учнів, які вивчають математику поглиблено, способам доведень і способам пошуку доведень математичних тверджень (за результатами анкетування учнів, учителів і студентів) залишається актуальною у шкільній практиці. Вчителю необхідно дидактично виважено поєднати ступінь логічної строгості й доступність для учнів власне способу доведення, евристичну й логічну складові процесу пошуку доведення, скоригувати рівень вимог щодо доведень математичних тверджень зі здібностями й рівнем пізнавального інтересу школярів. Проводити таку роботу необхідно як на уроках математики, так і в позаурочній роботі, наприклад, залучаючи зміст курсів за вибором.

Мета статті – розкрити особливості навчання доведень математичних тверджень у курсі за вибором «Основи криптології» (для учнів, які вивчають математику поглиблено).

Виклад основного матеріалу. Курс за вибором «Основи криптології» [3] скерований, зокрема на цілісне й систематизоване засвоєння учнями змісту окремих математичних понять і фактів, що мають широке застосування в теорії захисту інформації, розширення математичного світогляду учнів, підвищення їхнього інтересу до математики та її прикладних аспектів, удосконалення способів математичної діяльності. Його теоретичну основу складають елементи теорії захисту інформації, теорії подільності й теорії конгруенцій в кільці цілих чисел (програмовий матеріал 8-го класу з поглибленим вивченням математики), теорії ймовірностей і комбінаторики (програмовий матеріал 9-го класу з поглибленим вивченням математики), основи алгоритмізації та програмування (курс інформатики 8-9 клас). Тому він призначений для учнів 9-х класів із поглибленим вивченням математики або для учнів 10-х класів, які вивчають математику (інформатику) на профільному рівні.

Особливе значення у вивченні курсу мають шифри Цезаря, Віженера, шифр з автоключем, асиметричні шифри, оскільки їхнє вивчення ґрунтоване на базових поняттях теорії чисел та вміннях виконувати дії додавання і множення в кільці лишків за модулем, застосовуючи властивості конгруенцій за модулем, з якими школярі знайомилися на уроках алгебри у 8 класі [8].

Базовим відношенням виступає відношення конгруентності. Базові поняття – конгруенція, числа, конгруентні за модулем, просте (складене) число, найбільший спільний дільник (НСД), найменше спільне кратне (НСК), взаємно прості числа,

канонічний розклад натурального числа. Базові математичні факти – теорема про ділення з остачею, ознаки конгруентності чисел за модулем, властивості подільності цілих чисел, властивості конгруенцій, що зберігають модуль, властивості НСД і НСК двох натуральних чисел, властивості простих чисел, мала теорема Ферма й наслідок з неї, теорема, що обґрунтовує алгоритм Евкліда. Базові способи діяльності – алгоритм Евкліда, застосування властивостей конгруенцій для виконання їх елементарних перетворень, встановлення факту взаємної простоти двох натуральних чисел, алгоритм знаходженн НСД двох натуральних чисел.

Нові поняття – повна і зведена системи лишків за даним модулем, лінійна конгруенція з одним невідомим, розв'язок лінійної конгруенції з одним невідомим, рівносильні конгруенції з одним невідомим, елементарні перетворення конгруенцій, число, обернене до даного за модулем (обернений клас лишків за модулем), лінійне представлення НСД двох натуральних чисел, система конгруенцій, розв'язок системи конгруенцій, функція Ейлера, мультиплікативна функція, конгруенція другого степеня, квадратичні лишки і нелишки за простим модулем, арифметичний квадратний корінь за модулем. Нові математичні факти – необхідна й достатня умова взаємної простоти двох чисел, властивість мультиплікативності функції Ейлера, формула для знаходження функції Ейлера для довільного натурального числа і такого, що є степенем простого числа, теорема Ейлера, теорема про кількість розв'язків конгруенції $x^2 \equiv k(\mathrm{mod}\, p)$, де k – квадратичний лишок за простим модулем p, $НСД(k;p) \equiv 1$, $p > 2$, теорема про кількість квадратичних лишків і нелишків у зведеній системі лишків, критерій Ейлера для квадратичних лишків і нелишків, Китайська теорема про остачі. Нові способи діяльності – знаходження оберненого класу лишків за модулем, розв'язування лінійних конгруенцій (метод спроб, штучний метод, метод оберненого класу лишків), розв'язування систем лінійних конгруенцій з двома змінними, встановлення наявності розв'язків та розв'язування найпростіших конгруенції другого степеня виділенням повного квадрата, зведення квадратної конгруенції $ax^2 + bx + c \equiv 0(\mathrm{mod}\, m)$, де $НСД(a;m) \equiv 1$ до двочленної, розв'язування конгруенцій другого степеня за складеним модулем на основі Китайської теореми про остачі, знаходження арифметичного квадратного кореня із числа за простим і складеним модулем.

Вищеперелічені нові математичні факти пропонуємо доводити на рівні логічної строгості, доступному для учнів цієї вікової категорії, тобто здійснюючи змістові доведення. Навчальним результатом виступатиме оволодіння школярами способами міркувань відповідно до аналітичного, синтетичного, аналітико-синтетичного методів доведення, методу від супротивного, повної індукції і конструктивного способу доведення математичних фактів. Більш детально зупинимося на твердженнях, які доводяться конструктивним способом.

Як відомо, у математиці конструктивне доведення – це метод доведення, що підтверджує існування певного математичного об'єкта шляхом конструювання способу відтворення даного об'єкта. Він протиставляється неконструктивному доведенню (також відомому як теорема доведення існування, або «чиста» теорема існування), яке доводить існування певного об'єкта без наведення прикладів. Говорячи про конструктивний спосіб доведення ми будемо говорити скоріше про конструктивний спосіб пошуку доведення, коли допоміжні конструкції дозволяють спочатку навести спосіб відтворення певного об'єкта, а потім побудувати низку умовиводів, що доводять математичне твердження щодо властивостей математичного об'єкта. Наприклад, такі допоміжні конструкції автори підручника [8] використовують у доведенні зліченності множини раціональних, цілих чисел (таблиці, у які записані нескінченні послідовності цих чисел), алгоритму Евкліда (низка рівностей, у вигляді яких записується теорема про ділення з

остачею) тощо. Зауважимо, що навчання побудови й використання таких допоміжних конструкцій у доведенні алгебраїчних фактів виявляється більш утрудненим порівняно з геометричними фактами, відтак, потребує від учителя більшої уваги. Глибинні причини цього факту, який підтверджений численними нашими спостереженнями й опитуваннями вчителів і учнів, потребують додаткового ретельного вивчення.

Ми пропонуємо застосувати конструктивний спосіб для доведення властивості мультиплікативності функції Ейлера, теореми про значення функції Ейлера для натурального числа, що є степенем простого числа, теореми про існування оберненого класу лишків за модулем. При цьому, на нашу думку, доцільно застосовувати як навчання готовим доведенням, так і самостійне винайдення учнями способу доведення.

У теоретичних розвідках і в практиці навчання найбільшого поширення здобули такі способи навчання учнів доведень: 1) аналіз і вивчення готових доведень, проведених учителем біля дошки або викладених у підручнику, з метою їхнього подальшого відтворення; самостійна побудова доведення учнями за аналогією з вивченими доведеннями; самостійне доведення учнів на основі попередньо вказаного способу чи прийому доведення; самостійний пошук і проведення доведень (З. Слєпкань [11], В. Далінгер [5] та ін.); 2) аналіз готового доведення, його відтворення; самостійне відкриття фактів, пошук і конструювання власного доведення; спростування запропонованого доведення (Г. Саранцев [9], Н. Кугай [7] та ін.); 3) аналіз і вивчення готових доведень; виявлення у явному вигляді логічних основ доведень й представлення їх учням чи учнями; самостійна побудова учнями доведення за аналогією або з опорою на допомогу вчителя; самостійний пошук і проведення доведень з опорою на знання логічних основ доведень (А. Столяр [12]). У навчанні учнів конструктивного способу доведень ці способи доцільно модифікувати, зважаючи на варіативність додаткових допоміжних математичних конструкцій (числових послідовностей, виразів, функцій, рівнянь тощо), їх знаково-символьних оболонок (таблиці, схеми, графіки тощо). Ми пропонуємо спиратися на перший із вищеперелічених способів навчання учнів доведень.

Зі способом міркувань у конструктивному доведенні математичного факту учнів доцільно ознайомити на прикладі доведення властивості мультиплікативності функції Ейлера. Розглянемо сумісну діяльність учнів і вчителя поетапно.

Мотивація вивчення теореми проваджується вчителем. Функція Ейлера $\varphi(n)$, визначається для всіх натуральних n і показує кількість невід'ємних цілих чисел, менших від n і взаємно простих з n; при цьому $\varphi(1)=1$. Для невеликих значень натуральних n значення функції $\varphi(n)$ можна знайти простим підрахунком кількості невід'ємних цілих чисел, менших від n і взаємно простих з n, наприклад: $\varphi(2)=1$, $\varphi(3)=2$, $\varphi(4)=2$, $\varphi(5)=4$, $\varphi(6)=2$, $\varphi(7)=6$, $\varphi(8)=4$, $\varphi(9)=6$ і т.д. Але такий спосіб знаходження $\varphi(n)$, очевидно, стає дуже громіздким для великих чисел. Тому бажано б мати формулу для знаходження значень $\varphi(n)$. Для її знаходження зупинимося спочатку на деяких властивостях цієї функції.

Теорема. *Для будь-яких взаємно простих натуральних чисел m і n виконується рівність* $\varphi(mn)=\varphi(m)\varphi(n)$. (Ця властивість називається *мультиплікативністю* функції Ейлера).

«Відкриття» математичного факту за допомогою допоміжних конструкцій. Зразок побудови допоміжної конструкції і проведення подальших міркувань надає вчитель, залучаючи учнів до співбесіди на окремих етапах доведення. Нехай m і n взаємно прості натуральні числа. Знайдемо, скільки є чисел менших від добутку mn і взаємно простих з ним. Для цього побудуємо допоміжну конструкцію – таблицю, що містить m стовпчиків, у яку випишемо натуральні числа від 1 до mn (табл. 1).

Таблиця 1

1	2	3	…	m
$m + 1$	$m + 2$	$m + 3$	…	$2m$
$2m + 1$	$2m + 2$	$2m + 3$	…	$3m$
…	…	…	…	…
$(n - 1)m + 1$	$(n - 1)m + 2$	$(n - 1)m + 3$	…	nm

Число a є взаємно простим із добутком mn тоді, і тільки тоді, коли НСД(a; n) = 1 і НСД(a; m) = 1. Знайдемо спочатку в таблиці числа, що взаємно прості з m. У першому рядку, де всі числа від 1 до m, взаємно простих з m рівно $\varphi(m)$ штук. Вони утворюють зведену систему лишків (ЗСЛ) за модулем m. Позначимо їх b_i. Числа, розміщені в кожному стовпчику, належать до одного і того ж самого класу лишків за модулем m. Тому, якщо число b_i взаємно просте з m, то і будь-яке число зі стовпчика, що містить b_i, також взаємно просте з m. Випишемо стовпчики із числами b_i, де НСД(b_i; m) = 1 (табл. 2).

Таблиця 2

b_1	b_2	b_3	…	$b_{\varphi(m)}$
$m + b_1$	$m + b_2$	$m + b_3$	…	$m + b_{\varphi(m)}$
$2m + b_1$	$2m + b_2$	$2m + b_3$	…	$2m + b_{\varphi(m)}$
…	…	…	…	…
$(n-1)m + b_1$	$(n-1)m + b_2$	$(n-1)m + b_3$	…	$(n-1)m + b_{\varphi(m)}$

Тепер знайдемо, скільки у кожному з отриманих стовпчиків є чисел, що є взаємно простими з n. Розглянемо довільний стовпчик (табл. 3):

Таблиця 3

b_i
$m + b_i$
$2m + b_i$
…
$(n-1)m + b_i$

Маємо n різних чисел. Загальний вигляд цих чисел $mx + b$ де x набуває послідовно значень від 0 до (n – 1), іншими словами, x «пробігає» повну систему лишків (ПСЛ). Доведемо, що всі вони дають різні остачі при діленні на n, тобто, лінійний вираз $mx + b$ також «пробігає» (ПСЛ). Скористаємося ознакою повної системи лишків (вона має містити рівно n елементів й усі вони мають бути попарно не конгруентні за модулем).

Отримана система складається з n чисел, оскільки x у виразі $mx + b$ набуває n різних значень. Доведемо, що всі ці n отриманих значень не конгруентні між собою за модулем n. Припустимо супротивне. Нехай $mx_1 + b \equiv mx_2 + b \pmod n$, при цьому x_1, x_2 не конгруентні між собою за модулем n. Спрощуючи отриману конгруенцію і враховуючи, що (m, n) = 1, отримаємо $x_1 \equiv x_2 \pmod n$. Отримали суперечність із припущенням.

Отже, кожен із стовпчиків є повною системою лишків за модулем n. Відтак, кожен із них містить рівно $\varphi(n)$ чисел менших за n і взаємно простих з n. Загалом чисел, взаємно простих з добутком mn, у таблиці 2 буде $\varphi(n)\cdot\varphi(m)$. Усі вони є меншими за добуток mn і взаємно простими з цим добутком, тобто, значення функції Ейлера для добутку mn визначається рівністю $\varphi(mn) = \varphi(n)\cdot\varphi(m)$.

Зауважимо, що на етапі *закріплення конструктивного способу доведення* важливо провести додаткову роботу щодо виділення структури доведення, пропонуючи учням виділити основну ідею доведення, проаналізувати допоміжну конструкцію (табл. 1, 2), побудувати коротку схему проведеного доведення, зафіксувати посилання на відомі факти. Не менш вагоме значення мають і конструювання учнями доведень за аналогією, за вказаною структурою, за запропонованими вчителем ідеєю чи методом, з використанням аналогічної чи варіативної допоміжної конструкції.

Наприклад, з*акріплення конструктивного способу доведення* можливо здійснити в ході доведення наступної теореми – значення функції Ейлера для степеня простого числа, – виділивши структуру доведення, скеровуючи учнів на пошук способу доведення системою відповідних запитань (завдань).

Теорема 2. *Якщо p – просте число і* $k \in N$, *то*

$$\varphi\left(p^k\right) = p^k - p^{k-1} = p^k\left(1-\frac{1}{p}\right).$$

Доведення виконують учні, даючи відповіді на запитання вчителя.

1) Запишіть у вигляді таблиці, що містить p стовпчиків, усі натуральні числа від 1 до p^k. *Очікувана відповідь учнів (табл. 4).*

Таблиця 4

1	2	3	…	p
$p+1$	$p+2$	$p+3$	…	$2p$
$2p+1$	$2p+2$	$2p+3$	…	$3p$
…	…	…	…	…
…	…	…	…	p^2
…	…	…	…	…
…	…	…	…	p^k

2) Визначте, які числа в таблиці взаємно прості з p і скільки їх.

Очікувані міркування учнів. Числа з останнього стовпчика діляться на p, тому вони не є взаємно простими із числом p, Всі інші числа таблиці не діляться на число p, а, отже, взаємно прості з ним.

3) Зробіть висновок про кількість чисел, що є взаємно простими з числом p^k.

Очікувані міркування учнів. Числа з останнього стовпчика не є взаємно простими з числом p, а відтак, не є взаємно простими з числом p^k. Всі інші числа таблиці взаємно прості з p, тому вони взаємно прості з p^k. Оскільки чисел у таблиці p^k, а в останньому стовпчику їх p^{k-1}, тому чисел, що не перевищують p^k і є взаємно простими з ним буде $p^k - p^{k-1}$.

4) Зробіть висновок щодо значення функції Ейлера $\varphi\left(p^k\right)$.

Очікувані міркування учнів. Отже,

$$\varphi\left(p^k\right) = p^k - p^{k-1} = p^k\left(1-\frac{1}{p}\right).$$

Засвоєння змісту теореми і запам'ятовування формулювання теореми пропонуємо здійснювати в ході виконання вправ.

Вправа 1. Чому дорівнює значення функції Ейлера, $\varphi(p)$, якщо p – просте число?

Очікувані міркування учнів. Якщо p – просте число, то за теоремою 11.2 можна записати рівність:

$$\varphi\left(p^k\right) = p^k - p^{k-1} = p^k\left(1-\frac{1}{p}\right).$$

Якщо $k=1$, то маємо $\varphi(p) = p-1$.

Наслідок 1. *(формулюють учні самостійно) Якщо p – просте число, то* $\varphi(p) = p-1$.

Вправа 2. Як обчислити функцію Ейлера для натурального числа $n>1$, що задано в канонічному вигляді $n = p_1^{k_1}\cdot p_2^{k_2}\cdot\ldots\cdot p_s^{k_s}$?

Очікувані міркування учнів. Оскільки функція Ейлера мультиплікативна, то згідно зауваження до попередньої теореми, виконується рівність:

$$\varphi(n) = \varphi\left(p_1^{k_1}\cdot p_2^{k_2}\cdot\ldots\cdot p_s^{k_s}\right) = \varphi\left(p_1^{k_1}\right)\cdot\varphi\left(p_2^{k_2}\right)\cdot\ldots\cdot\varphi\left(p_s^{k_s}\right) =$$

$$= p_1^{k_1}\left(1-\frac{1}{p_1}\right)\cdot p_2^{k_2}\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot p_s^{k_s}\left(1-\frac{1}{p_s}\right) =$$

$$= n\left(1-\frac{1}{p_1}\right)\cdot\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_s}\right).$$

Наслідок 2. *(формулюють учні самостійно) Якщо натуральне число $n>1$ задано в канонічному вигляді $n = p_1^{k_1}\cdot p_2^{k_2}\cdot\ldots\cdot p_s^{k_s}$, то*

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\cdot\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_s}\right).$$

Як бачимо, допоміжні конструкції можуть бути пред'явлені чи сконструйовані учнями самостійно (таблиці 1–4) у різних знаково-символьних оболонках (Н. Тарасенкова [13]). У навчанні учнів конструктивного способу доведення варто наголосити, що допоміжними конструкціями можуть бути різні математичні об'єкти, як от: формули, послідовності чисел тощо (наприклад, у доведенні теореми Ейлера).

Теорема Ейлера. *Якщо* НСД(a; m) = 1, *то* $a^{\varphi(m)} \equiv 1 \pmod m$.

Доведення. Розглянемо допоміжну конструкцію: послідовність з $\varphi(m)$ довільних чисел $x_1, x_2, \ldots x_{\varphi(m)}$, кожне з яких є взаємно простим з числом m й усі вони попарно не конгруентні між собою. Таку множину чисел називають *зведеною системою лишків* за модулем m (ЗСЛ(m)).

Пропонуємо учням утворити й розглянути ще одну допоміжну конструкцію: множину чисел $ax_1, ax_2, \ldots ax_{\varphi(m)}$. З цією метою помножити кожне число зі зведеної системи лишків на a (НСД(a; m) = 1). Скеровуємо учнів на дослідження властивостей чисел з цієї послідовності: $ax_1, ax_2, \ldots ax_{\varphi(m)}$.

Очікувані міркування учнів.

1. Кількість чисел у множині дорівнює $\varphi(m)$.

2. Оскільки всі x_i взаємно прості з m і число a взаємно просте з m, тому всі ax_i взаємно прості з m.

3. Той факт, що вони попарно не конгруентні між собою доведемо від супротивного. Припустимо, що існує така пара чисел, що $ax_i \equiv ax_{j_i} \pmod m$. Оскільки НСД($a$; m) = 1, тому обидві частини конгруенції можна поділити на a і матимемо $x_i \equiv x_j \pmod m$, що суперечить умові.

Отже, множина чисел $ax_1, ax_2, \dots ax_{\varphi(m)}$ має всі три характеристичні властивості ЗСЛ(m), тому вона утворює ЗСЛ(m). Тобто

$$ax_1 \equiv ax_{j_1} \pmod m$$
$$ax_2 \equiv ax_{j_2} \pmod m$$
$$\dots$$
$$ax_{\varphi(m)} \equiv ax_{j_{\varphi(m)}} \pmod m.$$

Тут числа $ax_1, ax_2, \dots ax_{\varphi(m)}$ – це ті ж числа $x_1, x_2, \dots x_{\varphi(m)}$ але, можливо в іншому порядку.

Утворимо ще одну допоміжну конструкцію – почленні добутки наведених конгруенцій. Перемножимо почленно отримані конгруенції. Отримуємо

$$a^{\varphi(m)}\left(x_1x_2\dots x_{\varphi(m)}\right) \equiv \left(x_1x_2\dots x_{\varphi(m)}\right) \pmod m.$$

Кожне з чисел x_i взаємно просте з m, тому добуток $x_1x_2\dots x_{\varphi(m)}$ взаємно простий з m. Отже, після скорочення маємо

$$a^{\varphi(m)} \equiv 1 \pmod m.$$

Доцільно звернути увагу учнів, що з теореми Ейлера безпосередньо слідує теорема Ферма (мала), з якою вони знайомилися у 8-му класі, однак, спосіб її доведення був іншим (також конструктивним [8, с. 305]).

Теорема Ферма (мала теорема Ферма). Якщо натуральне число a не ділиться на просте число p, *то* $a^{p-1} \equiv 1 \pmod p$.

Пропонуємо учням довести її самостійно, ґрунтуючись не теоремі Ейлера (можливо усно).

Розвиток умінь школярів доводити твердження курсу за вибором має відбуватися шляхом доведення як теоретичних тверджень, так і в ході розв'язування задач. Наведемо приклад.

Вправа 3. Доведіть, що для натуральних чисел $n \geq 3$ значення функції $\varphi(n)$ є парним числом.

Вправа 4. Користуючись теоремою Ейлера доведіть, що виконуються конгруенції:

а) $3^4 \equiv 1 \pmod{10}$; б) $7^{400} \equiv 1 \pmod{1000}$;

в) $9^{41} \equiv 9 \pmod{100}$; г) $11^{102} \equiv 121 \pmod{125}$; д) $13^{40} \equiv 1 \pmod{41}$.

Висновки. Одним із вагомих результатів навчання математики на поглибленому чи профільному рівнях є спроможність учнів не лише відтворювати готові доведення математичних фактів, а й конструювати власні, ґрунтуючись на методах наукового пізнання і прийомах евристичного й логічного мислення. У навчанні учнів конструктивного способу доведення необхідно зосереджувати увагу на: 1) самостійному чи запропонованому вчителем «відкритті» математичного факту за допомогою допоміжних конструкцій; 2) закріпленні конструктивного способу доведення шляхом виокремлення структури, основної ідеї доведення, допоміжної конструкції, побудови короткої схеми проведеного доведення, фіксації посилань на відомі факти в доведенні; 3) здійсненні учнями доведень за аналогією, за вказаною структурою, за запропонованими вчителем ідеєю чи методом, з використанням аналогічної чи варіативної допоміжної конструкції; 4) застосуванні доведених фактів у розв'язуванні вправ на доведення. При цьому необхідно зауважувати варіативність допоміжних конструкцій і їх знаково-символьних оболонок, можливі варіації способів доведень.

Список використаної літератури.

1. Tarasenkova, N. A. & Akulenko, I. A. The Problem of Forming and Developing Students' Logical Thinking in the Context of Subject Specialization in Secondary School [Електронний ресурс] // American Journal of

Educational Research. – 2013. – vol. 2, no. 12B. – p. 33-40. doi: 10.12691/education-2-12B-7. Режим доступу: http://pubs.sciepub.com/education/2/12B/7 – Дата звернення 09.09.2017.
2. Акуленко І. А. Елементи математичної логіки у поглибленому курсі математики: розробки уроків : методичний посібник для вчителів загальноосвітніх навчальних закладів / І. А. Акуленко, Ю. Ю. Лещенко. Черкаси : Вид. від. ЧНУ ім. Б. Хмельницького, 2011. – 62 с.
3. Акуленко І. А. Основи криптології. Матеріали 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.
4. Блонский П. П. Избранные педагогические и психологические сочинения: В 2-х т. / Сост. М. Г. Данильченко, А. А. Никольская / Под редакцией А. В. Петровского. – М. : Педаг., 1979. – Т. 2. – С. 102.
5. Далингер В.А. Методика обучения учащихся доказательству математических предложений / В.А.Далингер. – М. : Просвещение, 2006. – 256 с.
6. Кірман В.К. Методична система вивчення функцій у класах фізико-математичного профілю : автореф. дис. ... канд. пед. наук : 13.00.02 «Теорія та методика навчання математики» / Вадим Кімович Кірман ; Черкаський національний університет ім.Б.Хмельницького. – Черкаси, 2010. – 18с.
7. Кугай Н.В. Розвиток умінь старшокласників доводити твердження у процесі вивчення алгебри і початків аналізу : автореф. дис. ... канд. пед. наук : 13.00.02 «Теорія та методика навчання математики» / Наталія Василівна Кугай; Націон. пед. ун-т ім. М. П. Драгоманова. – К., 2007. – 18 с.
8. Мерзляк А.Г. Алгебра : підруч. для 8 кл. з погл. вивч. Математики / А.Г.Мерзляк, В.Б.Полонський, М.С.Якір. – Харків : Гімназія, 2008 – 368 с.
9. Саранцев Г.И. Обучение математическим доказательствам и опровержениям в школе [Текст] / Г.И.Саранцев. – М. : Гуманитар. изд. центр ВЛАДОС, 2006. – 183 с.
10. Скафа Е. И. Теоретико-методические основы формирования приемов эвристической деятельности при изучении математики в условиях внедрения современных технологий обучения : дис. ... д-ра пед. наук : 13.00.02 «Теория и методика обучения математики» / Елена Ивановна Скафа ; Донецкий нац. ун-т. – Донецк, 2004. – 479 с.
11. Слепкань З.І. Психолого-педагогічні те методичні основи розвивального навчання математики / З.І.Слєпкань. – Тернопіль : Підручники і посібники, 2004. – 240 с.
12. Столяр А.А. Логические проблемы преподавания математики [Текст] / А.А.Столяр. – Минск : Высшая школа, 1965. – 254 с.
13. Тарасенкова Н. А. Теоретико-методичні основи використання знаково-символьних засобів у навчанні математики учнів основної школи : дис. ... д-ра пед. наук : 13.00.02 «Теорія та методика навчання математики» / Ніна Анатоліївна Тарасенкова ; Національний пед. ун-т ім. М. П. Драгоманова. – К., 2004. – 630 с.
14. Халперн Д. Психология критического мышления [Текст] / Д.Халперн. – СПб. : Издательство «Питер», 2000. – 512 с.
15. Ширикова Т.С. Методика обучения учащихся основной школы доказательству теорем при изучении геометрии с использованием GEOGEBRA : дис. ... канд. пед. наук : 13.00.02 «Теория и методика обучения и воспитания (математика) / Татьяна Сергеевна Ширикова ; ФГАОУВПО «Северный (Арктический) федеральный университет имени М. В. Ломоносова». – Архангельск, 2014. – 250 с.
16. Яценко С.Є. Організація навчально-виховного процесу на уроках математики в класах з поглибленим вивченням предмета основної школи : автореф. дис. ... канд. пед. наук : 13.00.02 «Теорія та методика навчання математики» / Світлана Євгенівна Яценко ; Національний пед. ун-т ім. М. П. Драгоманова. – К., 1999. – 18 с.

References.

1. Tarasenkova, N. A., & Akulenko, I. A. (2013). The Problem of Forming and Developing Students' Logical Thinking in the Context of Subject Specialization in Secondary School. *American Journal of Educational Research*, 2 (12B), 33-40. Retrieved from: http://pubs.sciepub.com/education/2/12B/7
2. Akulenko, I. A., & Leshchenko, Yu. Yu. (2011). *Elements of mathematical logic in the math course* (plans of lessons). Cherkasy: Bohdan Khmelnytsky National University of Cherkasy (in Ukr.)
3. Akulenko, I. A., Krasnoshlyk, N. O., & Leshchenko, Yu. Yu. (2016). *Introduction to cryptology*. Cherkasy. (in Ukr.)
4. Blonsky, P. P. (1979). *Selected pedagogical and psychological works*. *Part 2*. In A. V. Petrovsky (Ed.). Moscow: Pedag., 102 (in Rus.)
5. Dalinger, V. A. (2006). *A method of teaching students proofs of mathematical proposals*. – Moscow: Prosveshchenie (in Rus.)
6. Kirman, V. K. (2010). *The system of methods of studying functions in school forms of mathematical profile*. Cherkasy: Bohdan Khmelnytsky National University of Cherkasy (in Ukr.)

7. Kugai, N. V. (2007). *Forming the senior pupils' demonstration skills in the process of algebra and beginning of analysis learning*. Kyiv: National Pedagogical Dragomanov University (in Ukr.)
8. Merzlyak, A. G., Polonsky, V. B., & Yakir, M. S. (2008). Algebra: textbook for 8th grade with in-depth learning of math. – Kharkiv: Gimnazia (in Ukr.)
9. Sarantsev, G. I. (2006). *Teaching mathematical proofs and disproofs in school*. – Moscow: VLADOS (in Rus.)
10. Skafa, E. I. (2004). *Theoretical and methodical bases of formation of methods of heuristic activity at studying of mathematics in the conditions of introduction of modern technologies of training*. Donetsk: Vasyl' Stus Donetsk National University (in Rus.)
11. Slepkan, Z. I. (2004). *Psychological, pedagogical and methodical foundations of the developmental mathematical education*. Ternopil: Textbooks and manuals (in Ukr.)
12. Stolyar, A. A. (1965). *Logical problems of teaching mathematics*. Minsk: Vysshaya shkola (in Rus.)
13. Tarasenkova, N. A. (2004). *The theoretic-methodical principles using of the sign-symbolic means in teaching mathematics of the basic school students*. Kyiv: National Pedagogical Dragomanov University (in Ukr.)
14. Halpern, D. (2000). *Psychology of critical thinking*. Saint Petersburg: Piter (in Rus.)
15. Shirikova, T. S. (2014). *Methodology for teaching students of the basic school proofs of theorems in geometry using Geogebra*. Arkhangelsk: Northern (Arctic) Federal University (in Rus.)
16. Yatsenko, S.Y. (1999). *Education and instruction management for profound math course at base school*. Kyiv: National Pedagogical Dragomanov University (in Ukr.)

AKULENKO I.,
Doctor of Science (Pedagogical Sciences), Professor of the Department of Algebra and Mathematical Analysis, Bogdan Khmelnitsky Cherkasy National University.
LESHCHENKO Yu.,
PhD (Physics, Mathematics), Associate Professor of the Department of Algebra and Mathematical Analysis, Bogdan Khmelnitsky Cherkasy National University.

TEACHING STUDENTS TO PROVE MATHEMATICAL STATEMENTS IN THE SELECTIVE COURSE «INTRODUCTION TO CRYPTOLOGY».

Abstract. Introduction. *Students' mastering in the art of proof is one of the most important educational results of mathematics teaching (especially of profile or in depth math teaching).*

Significant potential in this aspect has both mathematics lessons and elective courses, such as the interdisciplinary elective course «Introduction to Cryptology» (for students of 9th, 10th grades with in depth learning of mathematics). Its theoretical basis are, in particular, the elements of the theory of divisibility and the theory of congruence in the ring of integers, the basis of algorithmization and programming (informatics course for 8th-9th grades). New mathematical facts that we offer to prove in this course: necessary and sufficient condition of the mutual simplicity of two numbers, the property of the multiplicative Euler function, the formula for finding the Euler function's value for an arbitrary natural number and for one that is a power of a prime number, the Euler theorem, Fermat's small theorem. The educational result can be investigated in students' mastering of the ways of thinking in accordance with analytical, synthetic, analytical and synthetic methods of proof, the method by contradiction, the method of complete induction, and the constructive method of the proof of mathematical facts.

Purpose *is to reveal the peculiarities of the teaching the constructive proofs of mathematical statements in the elective course «Introduction to Cryptology» (for students who are learning mathematics in depth).*

Methods. *Theoretical analysis of psychological and pedagogical literature on the problem were used, comparison, generalization, systematization. Empirical systematization and generalization of advanced pedagogical experience in relation to the problematic issues.*

Results. *It is known that the constructive method of proof is widely used in the proof of geometric facts. However, the counts of sets of rational, integer numbers, and Fermat's small theorem are proved constructively in Algebra textbook for 8th grade with in depth math teaching. We offer to use the constructive method for proving the multiplicative Euler function's property, the theorem on value of the Euler function for a natural number, which is a power of a prime number, theorems on the inverse class of residues modulo. At the same time, in our opinion, it is advisable to use both the teaching as a ready-made proof and an independent investigation of the way of proof by the students. It is*

advantageous to familiarize students with the method of thinking in the ready-made constructive proof on the example of proving the multiplicative property of Euler's function. It is possible to teach students to construct proofs by analogy, according to the given structure, according to the proposed teacher's idea or method on the example of theorem of the value of the Euler function for a power of a prime number. An independent students' investigation of the proofs must be ensured while carrying out exercises (to prove that a congruence is performed; to prove that the Euler's function is a pair number for natural numbers not less than 3, etc.)

Originality. *The author's analysis of some points with respect to the teaching of mathematical proofs in the context of the elective course «Introduction to Cryptology» for students who are learning math in depth is provided.*

Conclusion*. In teaching students of the constructive method of proof it makes sense: 1) to carry out the detailed examination of the finished proofs for the purpose of their subsequent reproduction, taking into account the variability of the auxiliary constructions and their symbols; variations of methods of proof are possible; 2) to foresee the students' independent construction of the proof by analogy or on the basis of the teacher's previously prescribed method or the technique of proof; 3) to provide an opportunity of independent search and realization of proofs.*

Keywords: *mathematical proofs, teaching math in depth, elective course.*

Одержано редакцією 25.10.2017 р.
Прийнято до публікації 04.12.2017 р.

УДК 37.013.75:33-051

ТКАЧ Юлія Миколаївна,
кандидат педагогічних наук, доцент
кафедри кібербезпеки та математичного
моделювання Чернігівського
національного технологічного
університету
e-mail: tkachym79@gmail.com

ПЕДАГОГІЧНИЙ ЕКСПЕРИМЕНТ ЩОДО ПРОБЛЕМИ ФУНДАМЕНТАЛІЗАЦІЇ ПРОФЕСІЙНОЇ ПІДГОТОВКИ МАЙБУТНІХ ЕКОНОМІСТІВ

У статті викладено основні етапи педагогічного експерименту щодо фундаменталізації професійної підготовки майбутніх економістів. Викладено основні проміжні результати. Зазначено, про позитивну динаміку рівня сформованості професійних компетентностей та оволодіння методами теоретичного пізнання, підвищення рівня вмотивованості студентів до навчання та якості засвоєння знань в цілому.

Ключові слова: *фундаменталізація, майбутні економісти, інформатизація, математизація, технологізація.*

Постановка проблеми. Посилення глобалізаційних та інтеграційних тенденцій, динамічний розвиток суспільства, соціальні та економічні виклики сучасності вимагають нових підходів до змісту й організації вищої економічної освіти, що ґрунтуються на впровадженні інноваційних технологій навчання, принципово нових методологічних засадах, сучасних дидактичних принципах та психолого-педагогічних теоріях. При цьому значення фундаментальної складової у професійній підготовці постійно зростає, тому виникає потреба у фундаменталізації системи вищої освіти, економічної зокрема.

С. Гончаренко [11, с. 2–6.] зазначав, що фундаменталізація освіти на сучасній основі виступає провідним імперативом освітніх реформ.