УДК 378.511 DOI 10.31651/2524-2660-2018-9-3-10

АКУЛЕНКО Ірина Анатоліївна,
доктор педагогічних наук,
професор кафедри алгебри і
математичного аналізу,
Черкаський національний університет
імені Богдана Хмельницького
e-mail: akulenkoira@ukr.net
https://orcid.org/0000-0003-4603-409X

ЛЕЩЕНКО Юрій Юрійович,
кандидат фізико-математичних наук,
доцент кафедри алгебри і
математичного аналізу,
Черкаський національний університет
імені Богдана Хмельницького
e-mail: ylesch@gmail.com
https://orcid.org/0000-0001-9079-1683

ОЗНАЙОМЛЕННЯ СТУДЕНТІВ (УЧНІВ) ІЗ ПРИКЛАДНИМИ АСПЕКТАМИ ТЕОРІЇ ПОРІВНЯНЬ У КІЛЬЦІ ЦІЛИХ ЧИСЕЛ

У статті розкрито способи з'ясування зі студентами (учнями) окремих прикладних аспектів теорії порівнянь у кільці цілих чисел, зокрема розглянуто формування поняття квадратного кореня за простим і складеним модулем, застосування способів розв'язування квадратних конгруенцій для дешифрування у системі Рабіна.

Ключові слова: *квадратичний лишок і нелишок, квадратний корінь за простим і складеним модулем, критерій Ейлера для квадратичних лишків і нелишків, Китайська теорема про остачі, шифр Рабіна.*

Постановка проблеми. Вивчення студентами (спеціальності 111 – Математика) основ теорії чисел передбачає, зокрема ознайомлення з теорією порівнянь у кільці цілих чисел. У результаті вивчення цього змістового модуля студенти: *формулюють означення* чисел, конгруентних за даним модулем, повної і зведеної системи лишків, числа, оберненого до даного за даним модулем, функції Ейлера, квадратичного лишку і нелишку, конгруенцій (лінійних, квадратних, вищих степенів) та їх розв'язків, показника числа за даним модулем, первісного кореня, індексу за простим модулем, *наводять відповідні приклади*; *застосовують* властивості конгруенцій та різні спеціальні способи до розв'язування конгруенцій першого, другого і вищих степенів, *знаходять* значення функції Ейлера для простих і складених чисел, квадратичні лишки і нелишки за допомогою функції Ейлера, символу Лежандра і символу Якобі, *будують* таблиці індексів за простим модулем, *доводять* теореми про властивості класів лишків як класів еквівалентності, теореми Ейлера і Ферма, теорему про кількість розв'язків лінійної конгруенції тощо. Теоретичні здобутки студентів є досить вагомими. Однак, часто поза увагою залишаються прикладні аспекти отриманих знань, які, зокрема пов'язані із захистом інформації. Оскільки елементи теорії порівнянь вивчають і

учні в поглибленому курсі математики, тому ці аспекти можливо й доцільно розглядати й із ними (наприклад, у курсі за вибором «Основи критпології» [1]).

Аналіз останніх досліджень та публікацій. Методичні аспекти навчання студентів елементів теорії подільності і теорії конгруенцій за кейс-технологією висвітлено у посібнику [2], роль задач практичного змісту розглянуто в роботі [3]. Методиці формування пізнавального інтересу учнів у навчанні спеціальних видів чисел (досконалих, дружніх, іменних, «смугастих») присвячено роботу [4]. У низці публікацій увага зосереджена на прикладних питаннях, а саме, на використанні лінійних конгруенцій та їх систем у процесі ознайомлення учнів, які вивчають математику поглиблено, із окремими видами шифрів, як от із шифрами Цезаря та Віженера [5], лінійним і афінним шифрами [6; 7]. Елементи модулярної математики виокремлюють автори (О. В. Вербіцький [8], М. В. Захарченко [9], В. М. Рудницький [10], В. А. Вільштінський і А. В. Бережний [11], Ю. С. Харін, В. І. Берник, Г. В. Матвеєв, Б. Шнайдер [12] та інші), описуючи математичні основи криптографії, методи й засоби реалізації сучасного криптографічного кодування. Відтак, розроблення методики опанування студентами (учнями) основ теорії подільності і теорії порівнянь у контексті їх прикладних застосувань є актуальною проблемою сучасної дидактики математики.

Мета статті – розглянути пропедевтичну роботу та способи з'ясування зі студентами (учнями) окремих прикладних аспектів теорії порівнянь у кільці цілих чисел, зокрема у криптології, на прикладі шифру Рабіна.

Виклад основного матеріалу. Одним із відомих шифрів, у якому використовують піднесення до квадрату за даним модулем для шифрування відкритих повідомлень і добування квадратних коренів за даним модулем для дешифрування криптотексту, є шифр Рабіна.

Генерування ключів для шифру Рабіна відбувається у такий спосіб: 1) вибирають два великих простих числа p і q; 2) обчислюють їх добуток $n = pq$; 3) утворюють відкритий ключ n, таємний ключ p і q.

Шифрування відбувається блоками, згідно з формулою $E(M) = M^2 (\mathrm{mod}\, n)$. Для дешифрування необхідно розв'язати квадратну конгруенцію $x^2 \equiv k(\mathrm{mod}\, n)$ і добувати квадратний корінь за складеним модулем $n = pq$.

Для опанування студентами (учнями) процедури дешифрування криптотексту, отриманого за допомогою шифру Рабіна, їм необхідно засвоїти поняття «конгруенція другого степеня (повна і неповна)», «квадратичний лишок (квадратичний нелишок) за модулем», застосувати теорему про кількість розв'язків конгруенції $x^2 \equiv k(\mathrm{mod}\, n)$, якщо k – квадратичний лишок за простим модулем p *і* $НСД(k; p) = 1$, $p > 2$, Китайську теорему про остачі, опанувати способи дослідження і знаходження розв'язків систем лінійних конгруенцій, конгруенцій другого степеня за простим і складеним модулем.

На підготовчому етапі студенти (учні) мають засвоїти метод спроб у розв'язуванні неповних квадратних конгруенцій (вправа 1).

Вправа 1. Розв'яжіть конгруенцію способом спроб:

а) $x^2 \equiv 4(\mathrm{mod}11)$; б) $x^2 \equiv -8(\mathrm{mod}11)$; в) $x^2 \equiv 2(\mathrm{mod}11)$;

г) $x^2 \equiv 6(\mathrm{mod}11)$; д) $x^2 \equiv 10(\mathrm{mod}11)$.

Наступним етапом є вивчення теореми про кількість лишків і нелишків у зведеній системі лишків за даним модулем. Для підготовки до її доведення доцільно запропонувати вправу 2.

Вправа 2. Знайдіть усі значення параметра *k*, при яких конгруенція $x^2 \equiv k(\mathrm{mod}\,11)$ матиме розв'язки.

Після виконання вправи 2 доцільно організувати роботу із доведення теореми 1 (у колективній роботі викладача (вчителя) і студентів (учнів), залучаючи учнів до висловлення припущень, встановлення наслідків на окремих етапах доведення, фіксації загальних висновків, отриманих у ході доведення теореми).

Теорема 1. [8, с. 95-98] *Для будь-якого простого числа* $p > 2$ *половина елементів ЗСЛ є квадратичними лишками, інша половина – квадратичними нелишками.*

Оскільки при досить великих модулях процес підстановки елементів представників класів лишків із ЗСЛ стає довготривалим, тому постає проблема: чи не можна до початку розв'язування конгруенції $x^2 \equiv k(\mathrm{mod}\,p)$, $НСД(k;p)=1$, $p > 2$ встановити, чи має вона розв'язки, чи ні. Для цього користуються критерієм Ейлера. Після актуалізації формулювання критерію Ейлера варто запропонувати вправи для його застосування (вправи 3 – 5).

Вправа 3. Встановіть, чи має розв'язки конгруенція:

а) $x^2 \equiv 15(\mathrm{mod}\,37)$; б) $x^2 \equiv 30(\mathrm{mod}\,37)$.

Вправа 4. Розв'яжіть конгруенцію:

а) $x^2 \equiv 42(\mathrm{mod}\,67)$; б) $x^2 \equiv 34(\mathrm{mod}\,11)$; в) $x^2 \equiv 21(\mathrm{mod}\,43)$;

г) $x^2 \equiv 32(\mathrm{mod}\,59)$; д) $x^2 \equiv 5(\mathrm{mod}\,17)$.

Вправа 5. Розв'яжіть у цілих числах рівняння:

а) $5x^2 + 6 - y^2 = 0$; б) $7x + 15 - y^2 = 0$; в) $2y^2 = 11x + 7$.

Після виконання цих вправ варто зосередитися на розв'язуванні повних конгруенцій другого степеня (вправа 6).

Вправа 6. Розв'яжіть конгруенції, звівши їх до двочленних:

а) $3x^2 + 6x + 1 \equiv 0(\mathrm{mod}\,5)$; б) $2x^2 - 4x - 5 \equiv 0(\mathrm{mod}\,7)$;

в) $4x^2 - 7x - 3 \equiv 0(\mathrm{mod}\,11)$; г) $5x^2 + 7x + 1 \equiv 0(\mathrm{mod}\,13)$;

д) $7x^2 + 15x - 11 \equiv 0(\mathrm{mod}\,23)$.

На завершення цього етапу доцільно узагальнити спосіб розв'язування таких конгруенцій і сформулювати зі студентами (учнями) правило-орієнтир зведення повної квадратної конгруенції $ax^2 + bx + c \equiv 0(\mathrm{mod}\,m)$, де $p(a;m)=1$ до двочленної:

1) множимо конгруенцію на $a^{-1}(\mathrm{mod}\,m)$ з метою, щоб старший коефіцієнт квадратного тричлена замінити одиницею;

2) отриману конгруенцію $x^2 + b_1x + c_1 \equiv 0(\mathrm{mod}\,m)$ множимо на 4, щоб виділити повний квадрат, маємо $4x^2 + 4b_1x + 4c_1 \equiv 0(\mathrm{mod}\,m)$;

3) виділяємо повний квадрат:

$$4x^2 + 4b_1x + 4c_1 \equiv 0(\mathrm{mod}\,m),$$
$$4x^2 + 4b_1x + b_1^2 \equiv b_1^2 - 4c_1(\mathrm{mod}\,m),$$
$$(2x + b_1)^2 \equiv b_1^2 - 4c_1(\mathrm{mod}\,m);$$

4) вводимо заміну: $y = 2x + b_1$, $k = b_1^2 - 4c_1$ і розв'язуємо конгруенцію:

$$y^2 \equiv k(\mathrm{mod}\, m).$$

Для закріплення критерію Ейлера і способів розв'язування квадратних конгруенцій за простим модулем можна розв'язати вправи на доведення (вправи 7, 8). Додатковим навчальним результатом є виведені студентами (учнями) формули розв'язків неповних квадратних конгруенцій за простим модулем спеціального виду (де модуль $p = 4k+3$, $p = 8k+5$, $k \in Z$).

Вправа 7 [8, с. 112]. Доведіть, що конгруенція $x^2 \equiv a(\mathrm{mod}\, p)$ має розв'язки $x = \pm a^{k+1}(\mathrm{mod}\, p)$, якщо $p = 4k+3$, $k \in Z$ і a – квадратичний лишок за модулем p.

Вправа 8 [8, с. 112]. Доведіть, що, якщо $p = 8k+5$, $k \in Z$ *і* a – квадратичний лишок за модулем *p*, тоді конгруенція $x^2 \equiv a(\mathrm{mod}\, p)$ має розв'язки;

$$x = a^{k+1}(\mathrm{mod}\, p) \text{ і } x = a^{k+1} \cdot 2^{2k+1}(\mathrm{mod}\, p).$$

Оскільки на попередньому етапі студенти (учні) розв'язували конгруенції другого степеня за простим модулем, природно виникає питання: «Яким способом розв'язувати конгруенції за складеним модулем?». Корисною у цьому випадку виявляється так звана *Китайська теорема про остачі*. Її вивчення доцільно організувати у такий спосіб: 1) розглянути розв'язування системи лінійних конгруенцій; 2) узагальнити результат здійсненого способу математичної діяльності і сформулювати відповідне математичне твердження; 3) навести кілька формулювань Китайської теореми про остачі; 4) довести її (можливо кількома способами).

Сформулювати Китайську теорему про остачі можливо кількома способами.

Спосіб 1 (*його зазвичай формулюють студенти (учні), узагальнюючи спосіб розв'язування системи лінійних конгруенцій*). Нехай $m_1, m_2, ...m_n$ – попарно взаємно прості числа і $a_1, a_2, ...a_n$ довільні цілі числа. Тоді існує ціле число x_0, що задовольняє систему конгруенцій:

$$\begin{cases} x \equiv a_1(\mathrm{mod}\, m_1), \\ x \equiv a_2(\mathrm{mod}\, m_2), \\ ... \\ x \equiv a_n(\mathrm{mod}\, m_n). \end{cases}$$

Додаткові умови:

1) $0 \le x_0 < m_1 m_2 ... m_n$;

2) ціле число y задовольняє систему тоді і тільки тоді, коли $y \equiv x_0(\mathrm{mod}\, m_1 m_2 ... m_n)$.

Спосіб 2. Нехай $m_1, m_2, ..., m_n$ – попарно взаємно прості числа відмінні від 1. Тоді існує єдиний розв'язок $x_0 = a_1 M_1 N_1 + a_2 M_2 N_2 + ... + a_n M_n N_n$ за модулем $M = m_1 m_2 ... m_n$ системи конгруенцій:

$$\begin{cases} x \equiv a_1(\mathrm{mod}\, m_1), \\ x \equiv a_2(\mathrm{mod}\, m_2), \\ ... \\ x \equiv a_n(\mathrm{mod}\, m_n). \end{cases}$$

Тут $M_i = m_1 \cdot ... \cdot m_{i-1} \cdot m_{i+1} \cdot ... \cdot m_n$, а $N_i = M_i^{-1}(\mathrm{mod}\, m_i)$.

Способи доведення існування, які можливо розглянути зі студентами (учнями), наведено, наприклад, у роботі [1, с. 178-179].

У *наслідку* отримуємо, що *якщо модуль конгруенції* $f(x) \equiv a(\mathrm{mod}\, m)$ *є добутком кількох простих чисел* $m = p_1 p_2 ... p_n$, *то розв'язування даної конгруенції можна звести до розв'язування системи конгруенцій за цими простими модулями:*

$$\begin{cases} f(x) \equiv a(\mathrm{mod}\, p_1), \\ f(x) \equiv a(\mathrm{mod}\, p_2), \\ ... \\ f(x) \equiv a(\mathrm{mod}\, p_n). \end{cases}$$

Це є можливим позаяк розв'язок системи конгруенцій задовольняє дану конгруенцію і навпаки.

Отриманий спосіб діяльності уможливлює розв'язування вправ 9, 10.

Вправа 9. Знайдіть квадратні корені за простим модулем: а) $\sqrt{5}$ за модулем 7; б) $\sqrt{7}$ за модулем 19; в) $\sqrt{3}$ за модулем 11; г) $\sqrt{6}$ за модулем 23.

Вправа 10. Знайдіть квадратні корені за складеним модулем: а) $\sqrt{60}$ за модулем 77; б) $\sqrt{10}$ за модулем 129.

Після такої ретельної підготовчої роботи можна переходити до вивчення криптосистеми Рабіна.

Криптосистема Рабіна передбачає таку процедуру [8, с. 137]:

1. Генерування ключів

1. Обирають два досить великих простих числа *p* і *q*.

2. Утворюють їх добуток *n = pq*

Відкритий ключ: *n*.

Таємний ключ: *p*, *q*.

2. Шифрування у системі Рабіна

Шифрування відбувається блоками. Для цього повідомлення записують у числовій формі і розбивають на блоки, так, щоб число із кожного блоку не перевищувало б *n* (величина таких блоків є предметом домовленості для конкретної реалізації алгоритму). Число, що є відповідним блоку *M*, розглядається як елемент повної системи лишків за модулем *n* (Z_n) і підноситься до квадрату за модулем *n*. Записуємо це так:

$$E(M) = M^2 (\mathrm{mod}\, n).$$

У результаті отримується блок криптотексту *C = E* (*M*).

3. Дешифрування у системі Рабіна полягає у відновленні блоку *M* за відомим блоком *C*, тобто, у знаходженні квадратного кореня із числа *C* за модулем *n*: $M = \sqrt{C(\mathrm{mod}\, n)}$. Оскільки можливе існування чотирьох квадратних коренів за складеним модулем *n = pq*, з них обирається той, у результаті застосування якого після дешифрування отримується змістовний текст.

Для закріплення способу діяльності із шифрування відкритих повідомлень шифром Рабіна пропонуємо студентам (учням) зашифрувати повідомлення ШИФР РАБІНА, якщо *p* = 59, *q* = 67.

Розв'язання.

1. Генерування ключів.

Якщо $p = 59$; $q = 67$; $n = 3953$.

Відкритий ключ: $n = 3953$.

Таємний ключ: $p = 59$; $q = 67$.

2. Переходимо до цифрової форми запису повідомлення (відповідні числа під літерами – це номери їх літер в українському алфавіті, нумерація ведеться з 0):

Ш	И	Ф	Р	Р	А	Б	І	Н	А
28	10	24	20	20	00	01	11	17	00

Розбиваємо на блоки по 4 цифри (по дві букви із повідомлення). В результаті маємо:

$$2810^2 \pmod{3953} = 1959;$$
$$2420^2 \pmod{3953} = 2007;$$
$$2000^2 \pmod{3953} = 3517;$$
$$111^2 \pmod{3953} = 0462;$$
$$1700^2 \pmod{3953} = 0357.$$

Отже, криптотекст: 1959 2007 3517 0462 0357.

Для закріплення способу діяльності із дешифрування крипто текстів, зашифрованих шифром Рабіна пропонуємо студентам (учням) розшифрувати криптотекст 0753 2556, якщо відкритий ключ: $n = 3953$ [8, с. 139].

Висновки. Проведене експериментальне навчання показало, що прикладні аспекти застосування теорії подільності і теорії конгруенцій у кільці цілих чисел у криптології доцільно й можливо з'ясовувати зі студентами під час вивчення відповідного змістового модуля у курсі алгебри, у спеціальному курсі за вибором навчального закладу чи за вибором студентів. З учнями, які вивчають математику на поглибленому рівні, також можливо розглядати ці питання, зокрема у курсі за вибором «Основи криптології».

Список використаної літератури.

1. Акуленко І.А. Основи криптології. Матеріали для міжпредметного (математика та інформатика) курсу за вибором для учнів основної школи : навчально-методичний посібник / І. А. Акуленко, Н. О. Красношлик, Ю. Ю. Лещенко. – Черкаси, 2016. – 228 с.

2. Кляцька Л. М. Алгебра і теорія чисел : навч.-метод. пос. / Л. М. Кляцька, І. А. Акуленко, І. В. Ус. – Черкаси : ЧНУ ім. Б. Хмельницького, 2007. – 70 с.

3. Акуленко І. А. Роль задач практичного змісту при вивченні курсу «Алгебра і теорія чисел» / І. А. Акуленко // Вісник Черкаського університету. Серія: Педагогічні науки. – 2007. – Вип. 101. – С. 136–140.

4. Акуленко І. А. Формування пізнавальних інтересів учнів при вивченні спеціальних чисел / І. А. Акуленко, М. О. Завадська // Вісник Черкаського університету. Серія: Педагогічні науки. – 2007. – Вип. 111. – С. 3–7.

5. Акуленко І.А. Шифр Віженера та модульна арифметика у навчанні математики на поглибленому рівні / І. А. Акуленко, Н. О. Красношлик, Ю. Ю. Лещенко // Математика в рідній школі. – 2017. – № 1. – с. 20-25.

6. Акуленко І.А. Вивчення комбінації шифрів у курсі за вибором «Основи криптології» / І. А. Акуленко, Н. О. Красношлик, Ю. Ю. Лещенко // Математика в рідній школі. – 2015. – № 11. – С. 32-37.

7. Акуленко І.А. Інноваційні форми організації занять у позаурочній роботі з математики (на прикладі курсу за вибором «Основи криптології») / І. А. Акуленко, Н. О. Красношлик, Ю. Ю. Лещенко // Математика в рідній школі. – 2015. – № 12. – С. 26-31.

8. Вербіцький О. В. Вступ до криптології / О. В. Вербіцький. – М. : ВНТЛ, 1998. – 249 с.
9. Захарченко М. В. Асиметричні методи шифрування в телекомунікаціях : навч. посіб. / М. В. Захарченко, О. В. Онацький, Л. Г. Йона, Т. М. Шинкарчук. – Одеса : ОНАЗ ім. О. С. Попова, 2011. – 184 с.
10. Криптографическое кодирование: методы и средства реализации : монография / В. Н. Рудницкий, С. В. Пивнева, В. Г. Бабенко, И. В. Миронец и др. – Тольят. гос. ун-т. – Тольятти, 2013. – 196 с.
11. Математичні основи криптографії : конспект лекцій / укладачі: В. А. Фільштінський, А. В. Бережний. – Суми : Сумський державний університет, 2011. – 138 с.
12. Харин Ю. С. Математические основы криптологии : учеб. пос. / Ю.С.Харин, В.И. Берник, Г. В. Матвеев. – Мн. : БГУ, 1999. – 319 с.

References.

1. Akulenko, I. A., Krasnoshlyk, N. O., & Leshchenko, Yu. Yu. (2016). *Introduction to cryptology*. Cherkasy. (in Ukr.)
2. Klyatka, L. M. & Akulenko, I.A. (2007). *Algebra and number theory*. Cherkasy: Bohdan Khmelnytsky National University of Cherkasy (in Ukr.)
3. Akulenko I.A. (2007). The role of real life problems in studying the course «Algebra and Number Theory». *Visnyk Cherkas'koho universytetu. Seriya: Pedahohichni nauky (Bulletin of Cherkasy University. Series: Pedagogical Sciences)*, 101, 136–140. (in Ukr.)
4. Akulenko, I.A. & Zavadskaya, M.O. (2007). Formation of Students' Cognitive Interest in Learning Special Numbers. *Visnyk Cherkas'koho universytetu. Seriya: Pedahohichni nauky (Bulletin of Cherkasy University. Series: Pedagogical Sciences),*, 111, 3–7. (in Ukr.)
5. Akulenko, I. A., Krasnoshlyk, N. O., & Leshchenko, Yu. Yu. (2017). Vigener's Cipher and Modular Arithmetic in Teaching Mathematics. *Matematyka v ridniy shkoli (Mathematics in native school)*, 1, 20-25. (in Ukr.)
6. Akulenko, I. A., Krasnoshlyk, N. O., & Leshchenko, Yu. Yu. (2015). Teaching the Combination of Ciphers in the Elective Course «Introduction to Cryptology». *Matematyka v ridniy shkoli (Mathematics in native school)*, 11, 32-37. (in Ukr.)
7. Akulenko, I. A., Krasnoshlyk, N. O., & Leshchenko, Yu. Yu. (2015). Innovative Forms of Classes in Extra-curricular Work on Mathematics (on an Example of the Elective Course «Introduction to Cryptology». *Matematyka v ridniy shkoli (Mathematics in native school)*, 12, 26-31. (in Ukr.)
8. Verbitsky, O. V. (1998). *Introduction to cryptology*. Moscow: VNTL (in Rus.)
9. Zakharchenko, M. V., Onatsky, O. V., Yona,. L. G., & Shinkarchuk, T. M. (2011). *Asymmetric Methods of Encryption in Telecommunications*. Odessa: ONAT. (in Ukr.)
10. Rudnitsky, V. N., Pivneva, S. V., Babenko, V. G., & Mironets, I. V. (2013). *Cryptographic Encoding: Methods and Means of Realization: monograph*. Tolyatti: Tolyatti State University. (in Rus.)
11. Fil'shtinsky, V. A., & Berezhnyi, A. V. (2011). *Mathematical Foundations of Cryptography*. Sumy: Sumy State University. (in Ukr.)
12. Kharin Yu. S., Bernick, V. I., & Matveyev, G. V. (1999). *Mathematical Foundations of Cryptology*. Minsk: BSU. (in Rus.)

AKULENKO Irina,
Doctor of Science (Pedagogical Sciences), Professor of the Department of Algebra and Mathematical Analysis, Bohdan Khmelnytsky National University of Cherkasy.

LESHCHENKO Yuriy,
PhD (Physics, Mathematics), Associate Professor of the Department of Algebra and Mathematical Analysis, Bohdan Khmelnytsky National University of Cherkasy.

PROVIDING STUDENTS WITH APPLIED ASPECTS OF COMPARISON THEORY IN RING OF INTEGERS.

Abstract. Introduction. *The students' studying the foundations of number theory involves the following results: students formulate the definition of the basic concepts of modular arithmetic in the ring of integers such as: congruence, numbers that are congruent modulo, a complete (reduced) residue system modulo n, a linear (quadratic) congruence, a solution of the linear congruence, equivalent linear congruencies, elementary transformations of congruencies, inverse of a modulo m, linear representation of GCD of two natural numbers, a system of congruencies, a solution of a*

system of congruencies, Euler's totient function, a multiplicative function, a quadratic residue modulo n and quadratic non-residue modulo n, a square root modulo a composite (or a prime) number. Students prove new mathematical facts: necessary and sufficient conditions of the relative simplicity of two numbers, the property of the multiplicativity of Euler's totient function, the formula for Euler's totient function for an arbitrary natural number (or a prime power), Euler's theorem, the theorem on the number of solutions for the congruence $x^2 \equiv k \pmod p$, where k is the quadratic residue modulo a prime p, GCD(k; p) = 1, p > 2, the theorem on the number of the quadratic residues and non-residues in the complete residue system, the Euler's criterion for determining whether an integer is a quadratic residue modulo a prime p, Chinese remainder theorem. Students find inverse of a modulo m, solve linear congruencies and systems of linear congruencies with two variables, solve the simplest quadratic congruencies by completing the square, the reducing of the congruence $ax^2 + bx + c \equiv 0 \pmod m$, where (a; m) = 1, to the binomial, using Chinese remainder theorem; find the square root modulo a composite (or a prime) number. The students' theoretical achievements are significant. However, the applied aspects of theoretical knowledge often are outside of attention, though they are widely used in cryptology.

Purpose. *The purpose is to consider the possible ways of exploration with students some applied aspects of the modular arithmetic in the ring of integers, in particular in cryptology, for example, the Rabin's cipher.*

Methods. *Theoretical analyses of mathematical, psychological and pedagogical literature on the problem were used. The educational curriculum for 111–Mathematics implemented in the Cherkasy Bohdan Khmelnytskyi National University, were analyzed.*

Results. *The results of mathematical, psychological and pedagogical literature on the problem show that the development of methods for students' acquiring the basis of divisibility theory and comparison theory in the context of their applied application is an actual problem of modern didactics of Mathematics. Besides, since the elements of comparison theory are studied by the students in the advanced course of Mathematics, these aspects can be considered with them (for example, in the optional course of «Introduction to Cryptology». Providing students with Caesar and Vigenere ciphers, linear and affine ciphers is possible on the basis of previously acquired theoretical information and basic concepts and facts of modular arithmetic.*

It is convenient to prove the main mathematical facts (Euler's theorem, the theorem on the number of solutions for the congruence $x^2 \equiv k \pmod p$, where k is the quadratic residue modulo a prime p, GCD(k; p) = 1, p > 2, the theorem on the number of the quadratic residues and non-residues in the complete residue system, the Euler's criterion for determining whether an integer is a quadratic residue modulo a prime p, Chinese remainder theorem) in some ways (e.g. Chinese remainder theorem), since it is the way for forming the skills of consistent arguments and techniques of mental activity in the analytical, synthetic, analytical-synthetic proof of mathematical facts.

The concept of a square root modulo a composite (or a prime) number should be paid additional attention, as the students learn the procedure of decrypting messages encrypted with Rabin's cipher on its basis.

Originality. *Some definite examples of the methodical recommendations for including into the learning process the basics of number theory for students of 111 – Mathematics are considered, the respective conclusions are substantiated.*

Conclusion. *The conducted experimental study show that the applied aspects of applying the theory of divisibility and the theory of congruences in the ring of integers should be considered by the students while studying the corresponding content module in the course of Algebra, in an optional course. The pupils learning the advanced Mathematics at school can consider these problems on the optional course of «Introduction to Cryptology».*

Key words: *a quadratic residue modulo n and a quadratic non-residue modulo n, a square root modulo a composite (or a prime) number, the Euler's criterion for determining whether an integer is a quadratic residue modulo a prime p, Chinese remainder theorem, Rabin's Cipher.*

Одержано редакцією 05.06.2018 р.
Прийнято до публікації 15.06.2018 р.