Scientific journal
PHYSICAL AND MATHEMATICAL EDUCATION
Has been issued since 2013.

Науковий журнал
ФІЗИКО-МАТЕМАТИЧНА ОСВІТА
Видається з 2013.

ISSN 2413-158X (online)
ISSN 2413-1571 (print)

http://fmo-journal.fizmatsspu.sumy.ua/

Лукашова Т.Д., Марченко К.В. Модульні арифметики. Фізико-математична освіта. 2018. Випуск 1(15). С. 246-251.

Lukashova T., Marchenko K. The Modular Arithmetics. Physical and Mathematical Education. 2018. Issue 1(15). P. 246-251.

УДК 511.172+512.552.18+512.624

Т.Д. Лукашова[1], К.В. Марченко[2]
Сумський державний педагогічний університет імені А.С. Макаренка, Україна
[1]tanya.lukashova2015@gmail.com, [2]omikomz@gmail.com
DOI 10.31110/2413-1571-2018-015-1-046

МОДУЛЬНІ АРИФМЕТИКИ

Анотація. *У багатьох задачах теорії чисел, дискретної математики та теорії шифрів доводиться знаходити остачі від ділення на деяке натуральне число (модуль) та виконувати арифметичні дії над знайденими остачами. Розглядаючи сукупність остач та вводячи операції додавання, віднімання, множення та ділення на утворених множинах, приходимо до так званих модульних арифметик. Число елементів у цих арифметиках скінченне, тому іноді їх називають скінченними арифметиками.*

Незважаючи на те, що арифметичні дії в модульних арифметиках вводяться аналогічно до того, як вони визначені для цілих чисел, деякі особливості виникають при множенні елементів, піднесенні їх до степеня та добуванні кореня, а відтак – при розв'язуванні рівнянь та їх систем.

В арифметиках за простим модулем результати операцій віднімання та ділення на відмінний від нуля елемент також є елементами відповідних арифметик. Тому в них можна обходитись без від'ємних та дробових виразів. Окрім того, в таких арифметиках зберігається більшість відомих алгоритмів розв'язування алгебраїчних рівнянь та їх систем. З іншого боку, в арифметиках за складеним модулем усталені правила можуть порушуватись, що пояснюється існуванням в них дільників нуля.

Незважаючи на те, що виконання арифметичних операцій у скінченних арифметиках значною мірою спирається на теорію конгруенцій та теорію кілець, які вивчаються у курсі алгебри й теорії чисел, дослідженню модульних арифметик та особливостям виконання в них арифметичних дій присвячено лише окремі публікації.

У даній статті розглядаються особливості виконання арифметичних операцій у модульних арифметиках, які конструюються на основі кілець класів лишків цілих чисел за заданим модулем. Значну увагу приділено питанням піднесення до степеня та добування кореня, наведено відповідні приклади. Матеріал статті може бути використаний при вивченні відповідних тем з теорії чисел та дискретної математики, а також розглянутий на заняттях спецкурсів та математичних гуртків.

Ключові слова: *кільця класів лишків, скінченні арифметики, модульні арифметики, арифметичні операції.*

Постановка проблеми та аналіз актуальних досліджень. У повсякденному житті досить часто доводиться оперувати різноманітними величинами та їх числовими характеристиками. Арифметичні дії над цілими числами – це перше, з чим стикаються школярі молодших класів на уроках математики. Розглядаючи остачі від ділення цілих чисел на деяке натуральне число m – модуль, та вводячи операції додавання та множення на утворених множинах, приходимо до так званих модульних арифметик.

Найпростішим прикладом використання модульних арифметик є годинник: хвилинна стрілка завжди показує остачу від ділення величини часу, що минув з моменту його заведення, на 60, а годинна – на 12. Отже, маємо арифметики по модулям 60 та 12 відповідно.

Зазначимо, що в арифметиках за простим модулем властивості елементів щодо віднімання і ділення аналогічні до властивостей дійсних чисел, і тому в них зберігається більшість відомих алгоритмів розв'язування рівнянь та їх систем. З іншого боку, в арифметиках за складеним модулем усталені правила можуть порушуватися, що пояснюється існуванням у них дільників нуля.

У наш час модульні арифметики знаходять найширше застосовування у теорії кодів та шифрів: існує велика кількість криптографічних протоколів, що базуються саме на застосуванні властивостей скінченних p-арифметик. З іншого боку, у науковій та методичній літературі питання, що стосуються обчислень у модульних арифметиках, висвітлюються недостатньо, а кількість джерел, що стосуються цієї теми є досить обмеженою (див. [1–9]). Тому розгляд даної теми є корисним і цікавим, а матеріал, викладений у статті, може бути використаний при вивченні скінченних кілець у курсах теорії чисел та дискретної математики, а також розглянутий на заняттях спецкурсів та математичних гуртків.

Мета статті. Розглянути особливості виконання арифметичних дій (зокрема, піднесення до степеня та добування кореня) у модульних арифметиках.

Виклад основного матеріалу

1. Арифметичні операції у скінченних арифметиках

Нехай Z – кільце цілих чисел. Розглянемо множину

$$Z_m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\},$$

елементами якої є класи лишків по модулю $m \in \mathbb{N}$ (клас лишків $\bar{r}$ за модулем m складається з цілих чисел виду $\bar{r} = \{r + mt | \ t \in Z\}$).

Як відомо із курсу теорії чисел, над класами лишків природним чином означаються операції додавання, віднімання та множення [10; 134]. Зокрема, *сумою* класів лишків $\bar{a}$ *і* $\bar{b}$ за модулем m називається клас лишків $\overline{a+b}$, який визначається остачею від ділення на m суми $(a+b)$ представників цих класів.

Віднімання класів лишків за модулем m можна визначити як операцію, обернену до додавання: *різницею* класів лишків $\bar{a} - \bar{b}$ назвемо клас лишків $\bar{x}$, що задовольняє умову: $\bar{b} + \bar{x} = \bar{a}$.

Аналогічно, *добутком* класів лишків $\bar{a}$ і $\bar{b}$ називається клас лишків $\overline{a \cdot b}$, який визначається остачею від ділення на m добутку чисел a і b. Нарешті, ділення класів лишків можна ввести як операцію, обернену до множення. При цьому *часткою* від ділення елементів $\bar{a} \in Z_m$ і $\bar{b} \in Z_m$ називають елемент $\bar{q} \in Z_m$, який задовольняє умову: $\bar{a} = \bar{b} \cdot \bar{q}$. Результат ділення позначають як $\bar{q} = \bar{a} : \bar{b}$ або $\bar{q} = \frac{\bar{a}}{\bar{b}}$.

Оскільки арифметичні дії над класами лишків зводяться до відповідних дій над цілими числами, а Z є комутативним кільцем, то у множині Z_m мають місце комутативний, асоціативний та дистрибутивний закони відносно додавання та множення, тобто Z_m також є комутативним кільцем [10; 137].

Множини класів лишків Z_m з уведеними на них арифметичними операціями (додавання, віднімання та множення) надалі будемо називати *модульними арифметиками* або *m-арифметиками,* а елементи відповідних кілець – *елементами m-арифметики* [3].

Для виконання арифметичних обчислень у m-арифметиках зручно користуватися таблицями додавання та множення, які також дозволяють знайти різницю та частку елементів (див., наприклад, [7]). Окрім того, результати додавання і множення можна подати у вигляді графів. Графічну інтерпретацію виконання множення у 5- та 6-арифметиках наведено на рисунках 1.1 - 1.7.

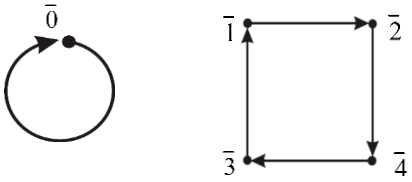

Рис. 1.1. Множення на $\bar{2}$ у 5-арифметиці

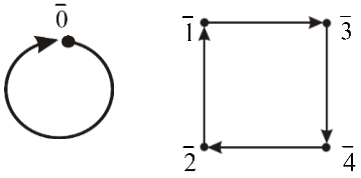

Рис. 1.2 .Множення на $\bar{3}$ у 5-арифметиці

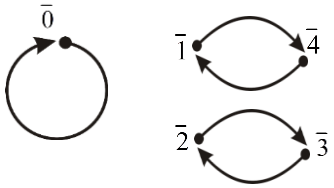

Рис. 1.3. Множення на $\bar{4}$ у 5-арифметиці

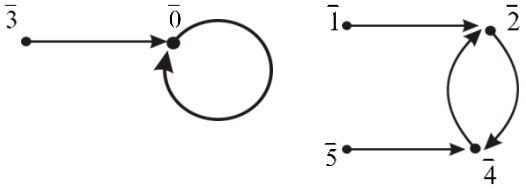

Рис. 1.4. Множення на $\bar{2}$ у 6-арифметиці

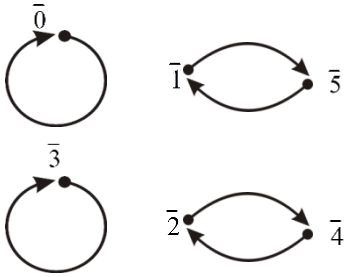

Рис. 1.5. Множення на $\bar{5}$ у 6-арифметиці

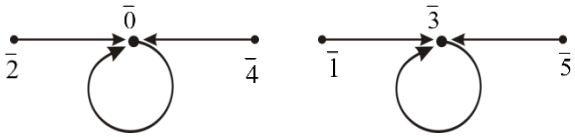

Рис. 1.6. Множення на $\bar{3}$ у 6-арифметиці

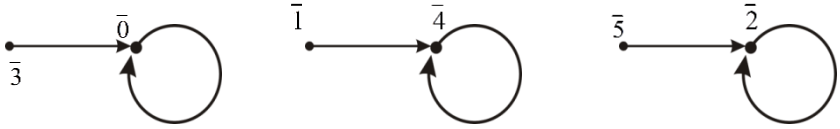

Рис. 1.7. Множення на $\bar{4}$ у 6-арифметиці

Проте, найчастіше виконання арифметичних дій у модульних арифметиках зводиться до виконання відповідних дій над цілими числами та заміною результату остачею від ділення на модуль.

Приклад 1.1. У 5-арифметиці маємо:

$$\overline{2}+\overline{3}=\overline{2+3}=\overline{5}=\overline{0},$$
$$\overline{2}-\overline{3}=\overline{2-3}=\overline{-1}=\overline{-1+5}=\overline{4},$$
$$\overline{2}\cdot\overline{3}=\overline{2\cdot 3}=\overline{6}=\overline{1}.$$

Аналогічно, для арифметики за модулем 6:

$$\overline{2}+\overline{3}=\overline{2+3}=\overline{5},$$
$$\overline{2}-\overline{3}=\overline{2-3}=\overline{-1}=\overline{-1+6}=\overline{5},$$
$$\overline{2}\cdot\overline{3}=\overline{2\cdot 3}=\overline{6}=\overline{0}.$$

Приклад 1.2. Знайдемо частку від ділення $\overline{2}:\overline{3}$ у 5-арифметиці. Для цього додамо до лишка, який визначає ділене, подвоєний модуль $5\cdot 2$ (що належить класу $\overline{0}$). Тоді

$$\frac{\overline{2}}{\overline{3}}=\frac{\overline{12}}{\overline{3}}=\overline{4}.$$

Легко довести, кожен «дріб» у 5-арифметиці можна подати як «цілий» клас, наприклад:

$$\frac{\overline{2}}{\overline{3}}=\overline{2}\cdot(\overline{3})^{-1}=\overline{2}\cdot\overline{2}=\overline{4},\ \frac{\overline{1}}{\overline{3}}=\overline{1}\cdot(\overline{3})^{-1}=\overline{2},\ \frac{\overline{4}}{\overline{3}}=\overline{4}\cdot(\overline{3})^{-1}=\overline{3}.$$

Зазначимо, що 5-арифметика є прикладом модульної арифметики, властивості якої притаманні будь-якій скінченній арифметиці за простим модулем. Як відомо [10; 137], кільця Z_p (p – просте число) є полями, тому кожен елемент $\overline{a}$ такого кільця ділиться націло на довільний елемент $\overline{b}$ ≠0, а дроби $\frac{\overline{a}}{\overline{b}}$ є елементами кільця Z_p. Саме тому p-арифметики за простим модулем p можна побудувати, не використовуючи «дробових» чисел.

У загальному ж випадку дріб $\frac{\overline{a}}{\overline{b}}$ завжди можна подати у вигляді «цілого» елемента лише у тій арифметиці, модуль якої взаємно простий із знаменником дробу, причому таке подання єдине. Що ж стосується арифметик за складеним модулем, то, взагалі кажучи, вони мають інші властивості. В них не завжди виконується операція ділення, більш того, якщо $\overline{a}:\overline{b}$, то частка $\overline{q}$ може визначатися неоднозначно.

Приклад 1.3. У 6-арифметиці $\overline{5}:\overline{2}$, $\overline{3}:\overline{2}$, $\overline{1}:\overline{3}$, проте, $\overline{1}:\overline{5}$, $\overline{3}:\overline{5}$ (рис. 1.4 – 1.7). Звернемо також увагу на те, що на $\overline{3}$ діляться лише класи $\overline{0}$ і $\overline{3}$. При цьому частка від ділення $\overline{3}$ на $\overline{3}$ визначається неоднозначно:

$$\overline{3}=\overline{1}\cdot\overline{3}=\overline{3}\cdot\overline{3}=\overline{3}\cdot\overline{5}$$

тобто: $q_1=\overline{1}$, $q_2=\overline{3}$, $q_3=\overline{5}$.

У 6-арифметиці добуток ненульових класів лишків може бути нулем: $\overline{2}\cdot\overline{3}=\overline{0}$, $\overline{4}\cdot\overline{3}=\overline{0}$, бо кільце Z_6 містить *дільники нуля* – ненульові елементи, добуток яких є нулем. Зазначимо, що у числових множинах дільників нуля немає, як їх немає і у кільці Z_5. У 6-арифметиці дільниками нуля є класи: $\overline{2},\overline{3},\overline{4}$.

Виникає питання: а чи можуть усі ненульові елементи деякої скінченної арифметики бути дільниками нуля? Як показує наступний приклад, відповідь позитивна, проте будова такої арифметики дещо відрізняється від будови арифметик, розглянутих вище.

Приклад 1.4. Візьмемо множину $3Z$, що складається з усіх цілих чисел, кратних 3 і розглянемо її розбиття за модулем 9. Зрозуміло, що утвориться три класи лишків:

$$\overline{0}=\{9t|\ t\in Z\},\ \overline{3}=\{3+9t|\ t\in Z\},\ \overline{6}=\{6+9t|\ t\in Z\}.$$

У цьому випадку $\overline{3}\cdot\overline{3}=\overline{9}=\overline{0}$, $\overline{3}\cdot\overline{6}=\overline{18}=\overline{0}$, $\overline{6}\cdot\overline{6}=\overline{36}=\overline{0}$. Отже, усі класи лишків є дільниками нуля. Більш того, у заданій таким чином арифметиці результатом множення довільних елементів є нуль.

Схожа ситуація спостерігається і в арифметиці, побудованій на основі множини парних чисел $2Z$ за модулем 8 (табл. 1.1). Усі її елементи також є дільниками нуля, проте множення тут ненульове.

Таблиця 1.1.

Множення у $(2Z)_8$

·	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$
$\overline{4}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{6}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$

В такого роду арифметиках дещо незвично може виглядати «одиниця». Як і у випадку чисел, одиницею скінченної арифметики природно називати такий клас лишків, множення на який не змінює інші елементи. Зазначимо, що у m-арифметиках роль одиниці відіграє клас лишків $\overline{1}$.

Приклад 1.5. Розглянемо класи лишків у множині парних чисел $2Z$ за модулем 6:

$$\overline{0}=\{6t|\ t\in Z\},\ \overline{2}=\{2+6t|\ t\in Z\},\ \overline{4}=\{4+6t|\ t\in Z\}.$$

та складемо для них таблицю множення.

Таблиця 1.2.

Множення у $(2Z)_6$

·	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$

Очевидно, клас $\overline{4}$ не змінює множників у результаті множення (табл. 1.2). Отже, він є одиницею у даній арифметиці.

2. Піднесення до степеня та добування коренів у модульних арифметиках

Перейдемо тепер до дослідження операцій піднесення до степеня і добування кореня у m-арифметиках. Зрозуміло, що операція піднесення до степеня в m-арифметиці, як і в звичайній, є окремим випадком множення.

Клас лишків $\bar{a}^n = \underbrace{\bar{a}\cdot\bar{a}\cdot\ldots\cdot\bar{a}}_{n\text{ разів}}$ називається *-м степенем класу лишків* $\bar{a}$. Відповідно, *коренем* n*-го степеня з класу лишків* $\bar{a}$ називається такий клас $\bar{x}$, що $\bar{x}^n = \bar{a}$ (за умови, що він існує).

Користуючись теоремою Ейлера або малою теоремою Ферма [10;139], показник степеня елемента $\bar{a}^n$ можна зменшити по модулю $\varphi(m)$ або, відповідно, по модулю $(p-1)$, якщо модуль p – число просте.

Приклад 2.1. Проілюструємо піднесення до степеня у 5- та 6-арифметиках (таблиці 2.1, 2.2).

За малою теоремою Ферма для довільного цілого числа a маємо $a^5 \equiv a\ (mod\ 5)$, тому у 5-арифметиці $\bar{a}^5 \equiv \bar{a}$. Отже, при піднесенні елемента $\bar{a}$ до n-го степеня досить розглянути лише значення a^n, де $n < 5$. При цьому

$$\bar{a}^{4k+1} = \bar{a},\ \bar{a}^{4k+2} = \bar{a}^2,\ \bar{a}^{4k+3} = \bar{a}^3,\ \bar{a}^{4k} = \bar{a}^4.$$

Таблиця 2.1.

***Піднесення до степеня у* 5-арифметиці**

$\bar{a}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\bar{a}^2$	$\overline{0}$	$\overline{1}$	$\overline{4}$	$\overline{4}$	$\overline{1}$
$\bar{a}^3$	$\overline{0}$	$\overline{1}$	$\overline{3}$	$\overline{2}$	$\overline{4}$
$\bar{a}^4$	$\overline{0}$	$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{1}$
$\bar{a}^5$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

За теоремою Ейлера [10; 138] для $a \in Z, (a,m) = 1$ маємо $a^2 \equiv 1\ (mod\ 6)$. Отже, у 6-арифметиці $\bar{a}^2 \equiv \overline{1}$, якщо $(a,m) = 1$. Окрім того, у цій арифметиці виконується рівність: $\bar{a}^3 \equiv \bar{a}$ (табл. 2.2). Тобто, як і у попередньому прикладі значення степенів елементів періодично повторюються.

Таблиця 2.2.

***Піднесення до степеня у* 6-арифметиці**

$\bar{a}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\bar{a}^2$	$\overline{0}$	$\overline{1}$	$\overline{4}$	$\overline{3}$	$\overline{4}$	$\overline{1}$
$\bar{a}^3$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\bar{a}^4$	$\overline{0}$	$\overline{1}$	$\overline{4}$	$\overline{3}$	$\overline{4}$	$\overline{1}$

Приклад 2.2. Доведемо, що у 6-арифметиці $(\bar{a}^2 + \bar{b}^2) \vdots \overline{3}$ тоді і тільки тоді, коли на $\overline{3}$ діляться $\bar{a}$ і $\bar{b}$ одночасно.

Нехай $(\bar{a}^2 + \bar{b}^2) \vdots \overline{3}$. Як було встановлено вище (табл. 2.2), квадрати елементів у 6-арифметиці дорівнюють: $\overline{0}, \overline{1}, \overline{3}, \overline{4}$. Тому сума $(\bar{a}^2 + \bar{b}^2)$ набуває значень $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}$. При цьому $(\bar{a}^2 + \bar{b}^2) \vdots \overline{3}$ лише коли $(\bar{a}^2 + \bar{b}^2)$ дорівнює $\overline{0}$ або $\overline{3}$ (див. приклад 1.3). Але у такому випадку або $\bar{a} = \bar{b} = \overline{0}$, або $\bar{a} = \overline{3}, \bar{b} = \overline{0}$ або $\bar{a} = \bar{b} = \overline{3}$. У кожному із цих випадків $\bar{a} \vdots \overline{3}$ і $\bar{b} \vdots \overline{3}$.

Зазначимо також, що в m-арифметиках зберігаються формули скороченого множення, добре знайомі зі шкільного курсу математики. Якщо при цьому $m = p$ – просте число, то їх можна спростити, користуючись малою теоремою Ферма. Зокрема, у 2-арифметиці $\bar{a}^2 = \bar{a}$, тому

$$\bar{a}^2 - \bar{b}^2 = (\bar{a} - \bar{b}) = (\bar{a} + \bar{b}),$$
$$(\bar{a} + \bar{b})^2 = \bar{a}^2 + \bar{b}^2 = (\bar{a} + \bar{b}),$$
$$(\bar{a} - \bar{b})^2 = \bar{a}^2 - \bar{b}^2 = (\bar{a} - \bar{b}) = (\bar{a} + \bar{b}).$$

Відповідно, у 3-арифметиці $\bar{a}^3 = \bar{a}$, отже,

$$\bar{a}^3 - \bar{b}^3 = \bar{a} - \bar{b},$$
$$\bar{a}^3 + \bar{b}^3 = \bar{a} + \bar{b}$$
$$(\bar{a} + \bar{b})^3 = \bar{a} + \bar{b},$$
$$(\bar{a} - \bar{b})^3 = \bar{a} - \bar{b}.$$

Нарешті, у p-арифметиках значно спрощується формула бінома Ньютона:

$$(\bar{a} + \bar{b})^p = \bar{a}^p + \overline{pa^{p-1}b} + \frac{\overline{p(p-1)}}{2}\bar{a}^{p-2}\bar{b}^2 + \cdots + \overline{pb^{p-1}}\bar{a} + \overline{b^p} = \bar{a}^p + \overline{b}^p = \bar{a} + \bar{b}$$

Приклад 2.3. Знайдемо значення суми

$$s_k = \bar{a}_1^k + \bar{a}_2^k + \ldots + \bar{a}_p^k,\ k \in N \qquad (2.1)$$

k-х степенів усіх елементів деякої p-арифметики (p – просте непарне число) [3].

Зазначимо спочатку, що можна вважати, що $k < p$, оскільки за малою теоремою Ферма $\bar{a}^p \equiv \bar{a}$ для усіх $\bar{a} \in Z_p$.

Нехай $k = p - 1$. Тоді для усіх елементів $\bar{a} \neq \overline{0}$ маємо $\bar{a}^{p-1} \equiv \overline{1}$. Отже,

$$s_{p-1} = \bar{a}_1^{p-1} + \bar{a}_2^{p-1} + \ldots + \bar{a}_p^{p-1} = \overline{p-1}.$$

Очевидно також, що при $k = 1$: $s_1 = (\bar{a}_1 + \bar{a}_2 + \ldots + \bar{a}_p) = \overline{0} + \overline{1} + \ldots + \overline{p-1} = \overline{0}$.

Нехай тепер $0 \leq k \leq p - 1$. Помножимо обидві частини рівності (2.1) на $\bar{b}^k$, де $\bar{b} \in Z_p, \bar{b}$ – первісний корінь по модулю p (як відомо, по простому модулю $p \neq 2$ такі корені існують [10; 207]). Одержимо:

$$\bar{b}^k s_k = (\bar{b}\overline{a_1})^k + (\bar{b}\overline{a_2})^k + \ldots + (\bar{b}\overline{a_p})^k \quad (2.2)$$

Оскільки $\bar{b} \neq \bar{0}$ і $\bar{b} \neq \bar{1}$, то елементи $\bar{b}\overline{a_m}$ попарно різні і разом з $\overline{a_m}$ пробігають множину Z_p. Отже, вираз у правій частині рівності (2.2) збігається з $\bar{a}_1^k + \bar{a}_2^k + \ldots + \bar{a}_p^k$, тобто з s_k. Отстаточно маємо: $\bar{b}^k s_k = s_k$, звідки $s_k = \bar{0}$. Отже, $s_k = \begin{cases} \bar{0}, \text{якщо } k \vdots (p-1) \\ \overline{p-1}, \text{якщо } k : (p-1) \end{cases}$.

Розглянемо більш детально операцію добування кореня у p-арифметиках. Наведені у таблицях 2.1 та 2.2 дані можна використати для знаходження значень коренів *n-го* степеня з елементів 5- та 6-арифметик.

Приклад 2.4. Знайдемо значення коренів $\sqrt[n]{\bar{a}}$ у 5-арифметиці.

Обчислимо значення коренів з елементів Z_5 для $n \leq 5$. Як бачимо (табл. 2.3), квадратні корені добуваються лише з елементів $\overline{0}$, $\overline{1}$ та $\overline{4}$. При цьому $\sqrt{\overline{4}}$ має два значення: $\overline{2}$ і $\overline{3}$, оскільки $\overline{2}^2 = \overline{3}^2 = \overline{4}$.

Кубічні корені видобуваються з кожного елемента цієї арифметики; корінь четвертого степеня – лише з класів $\overline{0}$, $\overline{1}$, а значення коренів п'ятого степеня збігаються з самими елементами: $\sqrt[5]{\bar{a}} = \bar{a}$ (це випливає з малої теореми Ферма).

Таблиця 2.3.

Добування коренів у 5-арифметиці

$\bar{a}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\sqrt{\bar{a}}$	$\overline{0}$	$\overline{1}, \overline{4}$	–	–	$\overline{2}, \overline{3}$
$\sqrt[3]{\bar{a}}$	$\overline{0}$	$\overline{1}$	$\overline{3}$	$\overline{2}$	$\overline{4}$
$\sqrt[4]{\bar{a}}$	$\overline{0}$	$\overline{1}, \overline{2}, \overline{3}, \overline{4}$	–	–	–
$\sqrt[5]{\bar{a}}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

З останньої рівності слідує також, що для елементів 5-арифметики, з яких добуваються квадратні, кубічні та біквадратні корені відповідно, мають місце рівності:

$$\sqrt[6]{\bar{a}} = \sqrt{\bar{a}},\ \sqrt[7]{\bar{a}} = \sqrt[3]{\bar{a}},\ \sqrt[8]{\bar{a}} = \sqrt[4]{\bar{a}},\ \sqrt[9]{\bar{a}} = \sqrt[5]{\bar{a}} = \bar{a}.$$

Аналогічно, у 6-арифметиці, $\sqrt{\overline{4}}$ відповідають два класи: $\overline{2}$ і $\overline{4}$, $\sqrt{\overline{3}} = \overline{3}$, а $\sqrt{\overline{2}}$ також не існує. Проте, і у цій арифметиці добуваються корені кубічні з усіх класів лишків, причому $\sqrt[3]{\bar{a}} = \bar{a}$, для довільного $\bar{a} \in Z_6$ (табл. 2.4).

Таблиця 2.4.

Добування коренів у 6-арифметиці

$\bar{a}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\sqrt{\bar{a}}$	$\overline{0}$	$\overline{1}, \overline{5}$	–	$\overline{3}$	$\overline{2}, \overline{4}$	–
$\sqrt[3]{\bar{a}}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\sqrt[4]{\bar{a}}$	$\overline{0}$	$\overline{1}, \overline{5}$	–	$\overline{3}$	$\overline{2}, \overline{4}$	–

Зазначимо також, що у деяких арифметиках квадратний корінь може мати більше, ніж два значення. Наприклад, у 8-арифметиці $\sqrt{\overline{1}}$ має чотири значення: $\{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$.

Виникає питання: зі скількох лишків у m-арифметиці добуваються корені квадратні і скільки значень у цьому випадку відповідає кожному квадратному кореню. Відповідь на це питання відома, якщо $m = p$ – просте число. Виявляється, що за цих умов корінь квадратний добувається рівно з половини ненульових класів (їх називають *квадратичними лишками* по даному модулю), причому кожному такому кореню відповідає два класи лишків [10; 169].

Встановити, чи є число a, яке визначає клас $\bar{a}$, квадратичним лишком, можна, скориставшись критерієм Ейлера [10, с.169]: *ціле число a є квадратичним лишком по модулю p тоді і тільки тоді, коли*

$$a^{\frac{p-1}{2}} \equiv 1 (mod\ p).$$

Тобто, в p-арифметиці має виконуватися рівність $\bar{a}^{\frac{p-1}{2}} = \overline{1}$. У випадку довільного m ситуація є більш складною (див., наприклад, [11; 168]).

Приклад 2.5. Покажемо, що у 5-арифметиці лишок $\overline{2}$ має властивості, подібні до властивостей $\sqrt{-1}$ арифметики комплексних чисел.

Справді, степені цього лишку утворюються так само, як і степені комплексного числа i:

$$\overline{2}^1 = \overline{2},\ \overline{2}^2 = \overline{4} = \overline{-1},\ \overline{2}^3 = \overline{-1} \cdot \overline{2} = -\overline{2},\ \overline{2}^4 = -\overline{2} \cdot \overline{2} = \overline{1}.$$

Від'ємне значення кореня $\sqrt{\overline{-1}}$, тобто $-\overline{2} = \overline{3}$, відіграє в 5-арифметиці роль числа, спряженого з уявною одиницею звичайної арифметики.

Число 5 – не єдиний модуль, за яким повна система лишків (тобто, система чисел узятих по одному з кожного класу лишків за даним модулем), містить елемент з властивостями уявної одиниці. Зокрема, у повній системі найменших додатних лишків за будь-яким модулем $(r^2 + 1)$ лишок $(\overline{r^2 + 1})$ розглядається як нуль, тому:

$$\sqrt{\overline{-1}} = \sqrt{\overline{-1 + r^2 + 1}} = \bar{r}.$$

Отже, лишок $\bar{r}$ в $(r^2 + 1)$ – арифметиці – аналог уявної одиниці. Зокрема, в цій арифметиці мають місце рівності:

$$\bar{r}^{4k+1} = \bar{r},\ \bar{r}^{4k+2} = -\overline{1},\ \bar{r}^{4k+3} = -\bar{r},\ \bar{r}^{4k} = \overline{1}.$$

Від'ємне значення $\sqrt{\overline{-1}}$, тобто $-\bar{r}$ відіграє у цій арифметиці роль числа, спряженого з уявною одиницею звичайної арифметики.

Висновки. Виконання арифметичних дій у модульних арифметиках має певні особливості у порівнянні з арифметикою цілих чисел. Зокрема, у арифметиках по простому модулю результат віднімання та ділення ненульових елементів також є елементом даної арифметики. У арифметиках за складеним модулем ділення виконується не завжди, а результат множення ненульових елементів може бути нулем.

Список використаних джерел

1. Бич О. В. Будуємо нові арифметики. У світі математики. 1998. № 1. С. 11-14.
2. Виленкин Н. Сравнения и классы вычетов. Квант. 1978. № 10. С. 4-8.
3. Геронимус А. Сравнения по простому модулю. Квант. 1978. № 11. С. 6-10.
4. Геронимус А. Диофантовы уравнения по простому модулю. Квант. 1978. № 12. С. 2-6.
5. Егоров А. Сравнения по модулю и арифметика остатков . Квант. 1970. №5. С. 27-33.
6. Егоров А., Котова А. Необыкновенные арифметики. Квант. 1993. № 3-4. С. 37-42.
7. Лукашова Т. Д., Пискун К.В. Скінченні арифметики. У світі математики. 2015. № 1. С. 26-34.
8. Хмара Т. М. Незвичайні арифметики. У світі математики. 1974. № 5. С. 7-14.
9. Попов Є. Д. Інтерпретація комплексних чисел у скінченних арифметиках. У світі математики. 1975. № 6. С. 110-121.
10. Окунєв Л.Я. Краткий курс теории чисел. М.: Учпедгиз, 1956. 240 с.
11. Требенко Д.Я., Требенко О.О. Алгебра і теорія чисел. К.: НПУ імені М.П. Драгоманова, 2006. Ч.1. 400с.

References

1. Bych O.V. We are building new Arithmetic. In the world of Mathematics.1998 №1. p. 11-14.
2. Vilenkin N. Comparison and residues classes. Kvant. 1978. № 10. p.4-8
3. Geronimus A. Comparison of a simple module. Kvant . 1978. № 11. p. 6-10.
4. Geronimus A. Diophantine equations of a simple module, Kvant. 1978. №. 12. p. 2-6.
5. Egorov A. Comparison of modulus and Arithmetic of residues. Kvant. 1970. №5. pp. 27-33
6. Egorov A., Kotova A. Uncommon Arithmetic, Kvant. 1993. № 3-4. pp. 37-42.
7. Lukashova T.D., Piskun K.V. Finite Arithmetic. In the world of Mathematics. 2015. № 1. p. 26-34.
8. Khmara T. M. Uncommon Arithmetic. In the world of Mathematics. 1974. № 5. p. 7-14.
9. Popov E. D. Interpretation of complex numbers in Finite Arithmetic. In the world of Mathematics. 1975. № 6. p. 110-121
10. Okunev L.I. Safety education of Number Theory M.: Uchpedgiz, 1956, 240 p.
11. Trebenko D.I., Trebenko O.O. Algebra and Number Theory. K .: Drahomanov's NPU, 2006, p.1. 400 p.

THE MODULAR ARITHMETICS

T.D. Lukashova, K.V. Marchenko

Makarenko Sumy State Pedagogical University

***Abstract**. In many problems of number theory, discrete mathematics and theory of ciphers you have to find the modulo for some positive integer (the modulus) and to perform arithmetic operations on found rest. Considering the totality of the balance and the introducing operations of addition, subtraction, multiplication and division for educated, come to the so-called modular arithmetic. The number of elements in these finite arithmetic, so sometimes called a finite arithmetic.*

Despite the fact that the arithmetic operations in the comparison module are entered the same way as they are defined for integers, some peculiarities arise from the multiplication of the elements, the lifting them to a power and extracting the root, and then in the solution of equations and their systems.

In arithmetic to a Prime modulus, the results of the operations of subtraction and division by a nonzero element is also the relevant elements of arithmetic. So they can do without negative and fractional expressions. In addition, the arithmetic remains the most well-known algorithms for solving algebraic equations and their systems. On the other hand, in the arithmetic module according to the established rules can be violated, owing to the existence in them of zero divisors.

Despite the fact that the arithmetic operations in finite arithmetic relies heavily on the theory of congruences and of the theory of rings that are studied in the course algebra and number theory, the study of modular arithmetic and run them in arithmetic is concerned only separate publication.

This article discusses the features of execution of arithmetic operations in the comparison module, which are constructed on the basis of the residue class rings of integers with a given module. Considerable attention is given to issues of exponentiation, and root extraction, the appropriate examples are given. The material can be used for studying relevant topics on number theory and discrete mathematics, and discussed in the classroom courses and math.

***Key words**: rings of residues classes, modular arithmetic, finite arithmetic, arithmetic operations.*