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., Лукашова М.В., Марченко К.В. Розв'язування алгебраїчних рівнянь в модульних арифметиках. Фізико-математична освіта. 2018. Випуск 2(16). С. 86-90.

Lukashova T., Lukashova M., Marchenko K. Solving Algebraic Equations In Modular Arithmetic. Physical and Mathematical Education. 2018. Issue 2(16). P. 86-90.

УДК 511.172+512.552.18+512.624

Т.Д. Лукашова[1], М.В. Лукашова, К.В. Марченко[2]
Сумський державний педагогічний університет імені А.С. Макаренка, Україна
[1]tanya.lukashova2015@gmail.com, [2]omikomz@gmail.com
DOI 10.31110/2413-1571-2018-016-2-016

РОЗВ'ЯЗУВАННЯ АЛГЕБРАЇЧНИХ РІВНЯНЬ В МОДУЛЬНИХ АРИФМЕТИКАХ

Анотація. *У багатьох задачах теорії чисел та дискретної математики доводиться виконувати арифметичні дії над цілими числами за певним модулем. При такому підході кожне ціле число можна ототожнити з остачею за цим модулем та розглядати множину лишків як нову, модульну арифметику.*

Зазначимо, що арифметичні операції над елементами утвореної таким способом алгебраїчної структури вводяться подібно до того, як вони визначені для цілих чисел, і визначаються відповідними остачами від ділення на модуль. Проте, залежно від модуля, деякі особливості можуть виникати при множенні класів лишків та похідних від нього операцій – піднесенні 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 цих арифметик. Тому в них можна обійтись без від'ємних та дробових числових 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, зокрема, особливостям виконання в них арифметичних дій, розв'язуванню рівнянь та їх систем присвячено лише окремі публікації.

У даній статті розглядаються особливості розв'язування алгебраїчних рівнянь та їх систем у модульних арифметиках. Досліджено питання розв'язності окремих типів алгебраїчних рівнянь (зокрема, лінійних та квадратних) та систем лінійних рівнянь у арифметиках за простим модулем, наведено відповідні алгоритми і 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, модульні арифметики, скінченні арифметики, алгебраїчні рівняння, лінійні рівняння, системи лінійних рівнянь.*

Постановка проблеми та аналіз актуальних досліджень. Цілий ряд математичних задач зводиться до пошуку остачі від ділення цілих чисел на деяке число. До них, зокрема, відносяться теоретико-числові задачі на доведення подільності та встановлення ознак подільності.

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. Число елементів у цих арифметиках скінченне, тому іноді їх називають скінченними арифметиками.

Зазначимо, що в арифметиках за простим модулем виконуються операції віднімання та ділення на відмінний від нуля елемент. Тому в них зберігається більшість алгоритмів розв'язування рівнянь та їх систем, що мають місце у числових полях. З іншого боку, в арифметиках за складеним модулем усталені правила можуть порушуватися, що пояснюється існуванням в них дільників нуля.

Незважаючи на те, що виконання дій у скінченних арифметиках значною мірою спирається на теорію конгруенцій та теорію кілець, які вивчаються у курсі алгебри й теорії чисел, дослідженню модульних арифметик, зокрема, розв'язуванню в них рівнянь та їх систем присвячено лише окремі публікації [1-10]. Тому розгляд даної теми є досить актуальним. Окрім того, відповідний матеріал може бути використаний при вивченні відповідних тем з теорії чисел та дискретної математики, а також розглянутий на заняттях спецкурсів та математичних гуртків.

Мета статті. Розглянути особливості розв'язування алгебраїчних рівнянь та їх систем у модульних арифметиках.

У ході підготовки статті були використані наступні **методи**:

- аналіз і систематизація наукової та навчальної літератури, за якими визначено основні питання щодо дослідження розв'язності алгебраїчних рівнянь та їх систем у модульних арифметиках;

- теоретико-числові методи та методи теорії конгруенцій, на основі яких виконуються дії у модульних арифметиках та з метою дослідження числа розв'язків рівнянь та їх систем у модульних арифметиках;

- узагальнення класичних підходів щодо розв'язування алгебраїчних рівнянь та їх систем на випадок арифметик за простим модулем.

Виклад основного матеріалу

1. Арифметичні операції у скінченних арифметиках

Нехай Z – кільце цілих чисел. Розглянемо множину $Z_m = \{\overline{0}, \overline{1}, \dots, \overline{m-1}\}$, елементами якої є класи лишків по модулю m (клас лишків $\bar{r}$ за модулем m складається з чисел виду $\bar{r} = \{r + mt | \ t \in Z\}$). Над класами лишків природним чином означаються операції додавання, віднімання та множення елементів [10; 134].

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. Відповідно, *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.

Віднімання та ділення класів лишків за модулем m можна визначити як операції, обернені до додавання та множення відповідно. Зокрема, *різницею* класів лишків $\bar{a} - \bar{b}$ називають клас лишків $\bar{x}$, що задовольняє умову: $\bar{b} + \bar{x} = \bar{a}$. Аналогічно, *часткою* від ділення класів $\bar{a}$ і $\bar{b}$ називають клас $\bar{x} \in Z_m$, для якого $\bar{a} = \bar{b} \cdot \bar{x}$. Результат ділення позначають $\bar{x} = \bar{a} : \bar{b}$ або $\bar{x} = \frac{\bar{a}}{\bar{b}}$.

Множини класів лишків Z_m з уведеними на них арифметичними операціями називають *модульними арифметиками* або *m-арифметиками,* а елементи відповідних кілець – *елементами m-арифметики* [4]. Модульні арифметики є прикладами так званих скінченних арифметик, в яких число елементів скінченне.

У роботах [7, 12] розглядалися особливості виконання арифметичних дій та операцій піднесення до степеня й добування кореня n-го степеня у m-арифметиках. Розглянемо у цих арифметиках питання розв'язності алгебраїчних рівнянь та їх систем.

1. Розв'язування алгебраїчних рівнянь у модульних арифметиках

Нехай у арифметиці за модулем m задано лінійне рівняння

$$\bar{a}x = \bar{b}, \tag{1.1}$$

де a і b – цілі числа, $0 \le a \le m-1$ і $0 \le b \le m-1$.

Зрозуміло, що розв'язання такого рівняння зводиться до розв'язання лінійної конгруенції

$$ax \equiv b (mod\ m).$$

З курсу теорії чисел добре відомо, що дослідження кількості розв'язків останньої конгруенції залежить від значень чисел a, b і m [13; 64]. Відповідно, у m-арифметиці число розв'язків рівняння (1.1) описує наступна теорема.

Теорема 1.1. *Нехай у m-арифметиці задано лінійне рівняння $\bar{a}x = \bar{b}$. Тоді:*

1) *це рівняння має єдиний розв'язок $x = \bar{a}^{-1}\bar{b}$, якщо $(a, m) = 1$,*

2) *рівняння не має розв'язків, якщо $(a, m) = d > 1$ і число b не ділиться на d,*

3) *рівняння має d розв'язків, якщо $(a, m) = d > 1$ і число b ділиться на d.*

Зазначимо, що елемент $\bar{a}$, для якого виконується умова $(a,m) = d > 1$, є дільником нуля відповідного кільця класів лишків. Тому для розв'язності рівняння (1.1) потрібно, щоб дільником нуля був і елемент $\bar{b}$ (причому b має ділитися на d).

Приклад 1.1. Розв'язати рівняння

$$\overline{4}x = \overline{2}$$

у арифметиках за модулями $m = 5$ та $m = 6$.

1) Нехай $m = 5$. Оскільки $(5, 4) = 1$, то у цій арифметиці дане рівняння має один розв'язок, причому

$$x = \overline{4}^{-1} \cdot \overline{2} = \overline{4} \cdot \overline{2} = \overline{8} = \overline{3}.$$

2) Нехай тепер $m = 6$. Оскільки $(4,6) = 2$ і $2 \vdots 2$, то дане рівняння має два розв'язки. Неважко переконатися, що ними є: $x = \overline{2}$ та $x = \overline{5}$.

Оскільки випадку простого числа m $(m = p)$ кільце класів лишків Z_p є полем, то у p-арифметиці алгоритм дослідження рівняння (1.1) подібний до алгоритма дослідження лінійного рівняння у множині дійсних чисел.

Наслідок. *Нехай задано лінійне рівняння* (1.1), *де $\bar{a}$ і $\bar{b}$ – елементи деякої p-арифметики (p – просте число),* $0 \le \bar{a}, \bar{b} \le p-1$. *Тоді:*

1) *якщо $\bar{a} \ne \overline{0}$, то дане рівняння має єдиний розв'язок $x = \bar{a}^{-1}\bar{b}$;*

2) *якщо $\bar{a} = \overline{0}$ і $\bar{b} = \overline{0}$, то розв'язками рівняння є усі p елементів даної арифметики;*

3) *якщо $\bar{a} = \overline{0}$ і $\bar{b} \ne \overline{0}$, то дане рівняння розв'язків не має.*

Приклад 1.2. Розв'язати рівняння $\overline{27}x = \overline{8}$ у 43-арифметиці.

Маємо: $a = 27$, $p = 43$, $b = 8$. За наслідком це рівняння має один розв'язок. Додамо до лівої частини рівняння вираз $-\overline{43x}$, кратний модулю. Дістанемо рівняння:

$$-\overline{16}x = \overline{8},$$

рівносильне даному. Поділимо тепер обидві частини рівняння на 8 та додамо до правої частини модуль:

$$-\overline{2}x = \overline{1},\ -\overline{2}x = \overline{44}.$$

Поділимо обидві частини рівняння на -2. Одержимо: $x = -\overline{22}$ або $x = \overline{21}$.

Перейдемо до розв'язування ***квадратних рівнянь*** в p-арифметиках (p – просте непарне число).

Розглянемо спочатку двочлення рівняння:

$$x^2 = \bar{a} \tag{1.2}$$

Виходячи з відомих результатів теорії конгруенцій, таке рівняння при $\bar{a} = \bar{0}$ має *єдиний розв'язок*, а при $\bar{a} \neq \bar{0}$ – або *два розв'язки*, або *жодного*, залежно від того, буде число a квадратичним лишком чи нелишком за модулем p. Визначити, чи є a квадратичним лишком можна за критерієм Ейлера [14; 79].

Приклад 1.3. Розв'язати рівняння $x^2 = \bar{2}$ у 5- та 7-арифметиках.

Задача зводиться до знаходження значень кореня квадратного з $\bar{2}$, який у 5-арифметиці не існує [12], бо 2 – квадратичний нелишок за модулем 5. Отже, у 5-арифметиці дане рівняння розв'язків не має.

З'ясуємо тепер, чи має дане рівняння розв'язки у арифметиці за модулем 7. Скористаємось критерієм Ейлера: $\bar{2}^{\frac{p-1}{2}} = \bar{2}^{\frac{7-1}{2}} = \bar{2}^3 = \bar{1}$. Отже, у 7-арифметиці це рівняння має два розв'язки. Неважко перевірити, що ними є: $x_1 = \bar{3}$, $x_2 = \bar{4}$.

Зазначимо, що у довільних m-арифметиках рівняння (1.2) може мати більше, ніж два розв'язки, що підтверджує наступний приклад.

Приклад 1.4. Розв'язати рівняння $x^2 = \bar{1}$ у 8-арифметиці.

Простим перебором елементів 8-арифметики неважко переконатися, що рівняння має 4 розв'язки: $x_1 = \bar{1}$, $x_2 = \bar{3}, x_3 = \bar{5}$, $x_4 = \bar{7}$.

Розглянемо тепер повне квадратне рівняння

$$ax^2 + bx + c = \bar{0} \tag{1.3}$$

у p-арифметиці (p – просте число) та знайдемо формулу обчислення його коренів.

Оскільки

$$ax^2 + bx + c = a(x + \frac{b}{2a})^2 + \frac{4ac - b^2}{4a},$$

то рівняння (1.3) еквівалентне рівнянню

$$a(x + \frac{b}{2a})^2 + \frac{4ac - b^2}{4a} = 0 \text{ або } (x + \frac{b}{2a})^2 = \frac{b^2 - 4ac}{4a^2}.$$

З останньої рівності знайдемо x:

$$x + \frac{b}{2a} = \frac{\pm\sqrt{b^2 - 4ac}}{2a}.$$

Отже рівняння (1.3) *не має розв'язків*, якщо у даній арифметиці не можна визначити значення кореня з дискримінанта $\sqrt{\overline{b^2 - 4ac}}$ (тобто, дискримінант є квадратичним нелишком), і має *два розв'язки*, якщо дана арифметика містить значення $\sqrt{\overline{b^2 - 4ac}}$ (тобто, дискримінант є квадратичним лишком). Ці розв'язки різні, якщо $\overline{b^2 - 4ac} \neq \bar{0}$ і співпадають, коли $\overline{b^2 - 4ac} = \bar{0}$. У випадку 2-арифметики формула втрачає зміст, через те, що виконується ділення на 2.

Приклад 1.5. Розв'язати рівняння $x^2 + \bar{2}x + \bar{4} = \bar{0}$ у 7-арифметиці.

$D = \overline{4 - 4 \cdot 4} = \overline{4 - 16} = \bar{2} \Rightarrow \sqrt{D} = \bar{3}$ або $\sqrt{D} = -\bar{3} = \bar{4}$. Остаточно маємо:

$x_1 = \frac{-\bar{2} - \bar{3}}{\bar{2}} = \frac{\overline{-5}}{\bar{2}} \equiv \frac{\overline{-5+7}}{\bar{2}} = \frac{\bar{2}}{\bar{2}} = \bar{1}$, $x_2 = \frac{-\bar{2} + \bar{3}}{\bar{2}} = \frac{\bar{1}}{\bar{2}} \equiv \frac{\overline{1-7}}{\bar{2}} = -\frac{\bar{6}}{\bar{2}} = -\bar{3} \equiv \bar{4}$.

Приклад 1.6. Розв'язати рівняння $\bar{3}x^2 + \bar{4}x - \bar{5} = \bar{0}$ у 11-арифметиці

Знайдемо дискримінант: $D = \overline{16 - 4 \cdot 3 \cdot (-5)} = \overline{5 + 1 \cdot 5} = \overline{10}$.

Оскільки $\overline{10}$ є квадратичним нелишком по модулю 11 (бо $10^{\frac{11-1}{2}} \equiv -1\ (mod\ 11)$), то $\sqrt{D}$ не існує. Отже, дане рівняння розв'язків не має.

Перейдемо до розгляду *алгебраїчних рівнянь вищих степенів* у p-арифметиках та дослідимо число їх розв'язків. Нехай маємо рівняння

$$\overline{a_n}x^n + .. + \overline{a_1}x + \overline{a_0} = \bar{0} \tag{1.4}$$

де n – натуральне число, $\overline{a_1}, \dots, \overline{a_n}$ – елементи p-арифметики.

Число n називають *степенем* рівняння (1.4), якщо a_n не ділиться на m.

Виходячи з відомих тверджень теорії конгруенцій, у випадку простого модуля ($m = p$) і за умови, що $n \leq p - 1$, рівняння (1.4) має не більше n розв'язків. Якщо ж вказане рівняння має більше n розв'язків, то всі коефіцієнти діляться на p.

Зауважимо, що у випадку $n \geq p$ степінь конгруенції можна зменшити, використовуючи малу теорему Ферма [13; 139] та поділивши ліву частину (1.4) на двочлен $(x^p - x)$. Отримане таким чином рівняння у даній арифметиці буде рівносильне даному та матиме степінь, що не перевищує $p - 1$.

Зрозуміло також, що в p -арифметиці за простою основою p рівняння

$$x^{p-1} = \bar{1} \tag{1.5}$$

має точно $(p - 1)$ розв'язків: його згідно з малою теоремою Ферма задовольняють усі ненульові елементи даної арифметики. Більш того, якщо d – натуральний дільник числа $(p - 1)$, то рівняння $x^d = \bar{1}$ або не має розвязків, або має має $\varphi(d)$ розв'язків [14;132]. Знайти ці розв'язки можна методом перебору множини Z_p.

У загальному випадку розв'язати двочленне рівняння

$$\bar{a}x^n = \bar{b}$$

у p-арифметиці можна, спираючись на теорію індексів (або дискретне логарифмування) [14; 141]. Зокрема, рівняння виду $x^n = \bar{a}$, $n < p$ розв'язне у p-арифметиці тоді і тільки тоді, коли має місце рівність $\bar{a}^{\frac{p-1}{n}} = \bar{1}$ [14; 144].

Приклад 1.7. Розв'язати в 3-арифметиці рівняння: $x^4 + \bar{2}x^3 - \bar{2}x^2 + x + \bar{1} = \bar{0}$.

Використаємо метод перебору та підставимо у рівняння елементи даної арифметики. Його задовольняють значення $x = \bar{1}$, $x = \bar{2}$.

Зазначимо, що можна було спочатку понизити степінь цього рівняння, поділивши ліву частину на $x^p - x = x^3 - x$ або виконуючи заміну $x^3 = x$. У цьому випадку маємо

$$x^2 + \bar{2}x - \bar{2}x^2 + x + \bar{1} = \bar{0},$$
$$-x^2 + \bar{3}x + \bar{1} = \bar{0},$$
$$-x^2 + \bar{1} = \bar{0}, x^2 = \bar{1},$$

звідки $x=\bar{1}$, $x=\bar{2}$.

Приклад 1.8. Розв'язати у 5-арифметиці рівняння: $x^{10}-\bar{2}x+\bar{1}=\bar{0}$.

Спростимо рівняння, виконуючи заміну $x^5=x$:

$$x^2-\bar{2}x+\bar{1}=\bar{0},$$
$$(x-\bar{1})^2=\bar{0},$$

звідки $x=\bar{1}$.

Приклад 1.9. З'ясувати, при яких значеннях параметрів $\bar{a}$ і $\bar{b}$ рівняння $x^3+\bar{a}x+\bar{b}=\bar{0}$ має три розв'язки у 5-арифметиці.

Позначимо $\bar{x}_1,\bar{x}_2,\bar{x}_3$ – розв'язки даного рівняння ($\bar{x}_i\neq\bar{x}_j$ при $i\neq j$. Підставимо кожне з цих значень у дане рівняння та віднімемо з першої рівності другу та третю:

$$\bar{x}_1^3-\bar{x}_2^3+\bar{a}(\bar{x}_1-\bar{x}_2)=\bar{0},\ \bar{x}_1^3-\bar{x}_3^3+\bar{a}(\bar{x}_1-\bar{x}_3)=\bar{0}.$$

Скоротимо першу рівність на $(\bar{x}_1-\bar{x}_2)$, а другу – на $(\bar{x}_1-\bar{x}_3)$:

$$\bar{x}_1^2+\bar{x}_1\bar{x}_2+\bar{x}_2^2+\bar{a}=\bar{0},\ \bar{x}_1^2+\bar{x}_1\bar{x}_3+\bar{x}_3^2+\bar{a}=\bar{0}.$$

Віднявши почленно та скоротивши на $\bar{x}_2-\bar{x}_3$, дістанемо: $\bar{x}_1+\bar{x}_2+\bar{x}_3=\bar{0}$. Оскільки значення $\bar{x}_i$ різні, то останню рівність задовольняють лише класи: $\bar{0},\bar{1},\bar{4}$ та $\bar{0},\bar{2},\bar{3}$.

У першому випадку, підставивши значення $\bar{0},\bar{1},\bar{4}$ у рівняння, маємо:

$$\bar{b}=\bar{0},\bar{1}+\bar{a}+\bar{b}=\bar{0},\ \bar{4}+\bar{4}\bar{a}+\bar{b}=\bar{0},$$

звідки $\bar{b}=\bar{0}$ і $\bar{a}=\bar{4}$. Аналогічно, для значень $\bar{0},\bar{2},\bar{3}$, дістанемо $\bar{b}=\bar{0}$ і $\bar{a}=\bar{1}$.

Отже, вказане рівняння має три розв'язки, якщо $\bar{b}=\bar{0}$ і $\bar{a}=\bar{4}$ і $\bar{b}=\bar{0}$ і $\bar{a}=\bar{1}$.

2. Розв'язування систем лінійних рівнянь у p-арифметиках

Розглянемо систему лінійних рівнянь з невідомими $x_1,x_2,\dots,x_n$ у p-арифметиці (p – просте число):

$$\begin{cases}\bar{a}_{11}x_1+\bar{a}_{12}x_2+\cdots+\bar{a}_{1n}x_n=\bar{b}_1\\ \bar{a}_{21}x_1+\bar{a}_{22}x_2+\cdots+\bar{a}_{2n}x_n=\bar{b}_2\\ \dots\dots\dots\dots\dots\\ \bar{a}_{m1}x_1+\bar{a}_{m2}x_2+\cdots+\bar{a}_{mn}x_n=\bar{b}_m\end{cases}. \qquad (2.1)$$

де $\bar{a}_{ij}$ і $\bar{b}_i$ – елементи p-арифметики.

Оскільки кільце Z_p, на основі якого будується дана арифметика є полем, то для розв'язування системи (2.1) можна використати усі результати, відомі з курсу лінійної алгебри для систем лінійних рівнянь над числовими полями [13; 194]. Зокрема, для розв'язання системи (2.1) можна використати метод виключення невідомих (або метод Гаусса), а у випадку, коли число рівнянь дорівнює числу невідомих, – теорію визначників і правило Крамера.

Для дослідження системи (2.1) можна використовувати також критерій сумісності системи лінійних рівнянь, що полягає у порівнянні рангів основної та розширеної матриць системи. Єдиною відмінністю від систем лінійних рівнянь над числовими полями є те, що у випадку сумісності системи вона завжди має скінченне число розв'язків.

Теорема 2.1. [13; 194] *Нехай у системі (2.1), що розглядається у p-арифметиці, $m=n$ і визначник основної матриці $\Delta\neq\bar{0}$. Тоді система (2.1) має єдиний розв'язок, який визначається з рівностей:*

$$\Delta x_1=\Delta_1,\Delta x_2=\Delta_2,\dots,\Delta x_n=\Delta_n.$$

Зазначимо, що твердження теореми залишається правильним і у випадку довільної m-арифметики за умови $(\Delta,m)=1$.

Приклад 2.1. Розв'язати у 11-арифметиці систему рівнянь: $\begin{cases}x_1+x_2+x_3=\bar{1}\\ x_1+\bar{2}x_2-x_3=\bar{0}\\ \bar{3}x_1+\bar{3}x_2+\bar{8}x_3=\bar{5}\end{cases}$.

Обчислимо визначник основної та допоміжних матриць, користуючись властивостями визначників та виконуючи арифметичні дії за правилами 11-арифметики.

$$\Delta=\begin{vmatrix}\bar{1}&\bar{1}&\bar{1}\\ \bar{1}&\bar{2}&-\bar{1}\\ \bar{3}&\bar{3}&\bar{8}\end{vmatrix}=\bar{5}\neq\bar{0},\ \Delta_1=\begin{vmatrix}\bar{1}&\bar{1}&\bar{1}\\ \bar{0}&\bar{2}&-\bar{1}\\ \bar{5}&\bar{3}&\bar{8}\end{vmatrix}=\bar{4},\ \Delta_2=\begin{vmatrix}\bar{1}&\bar{1}&\bar{1}\\ \bar{1}&\bar{0}&-\bar{1}\\ \bar{3}&\bar{5}&\bar{8}\end{vmatrix}=\overline{10},\ \Delta_3=\begin{vmatrix}\bar{1}&\bar{1}&\bar{1}\\ \bar{1}&\bar{2}&\bar{0}\\ \bar{3}&\bar{3}&\bar{5}\end{vmatrix}=\bar{2}.$$

За теоремою 2.1 маємо: $x_1=\frac{\bar{4}}{\bar{5}}=\bar{4}\cdot\bar{9}=\bar{3},:x_2=\frac{\bar{1}}{\bar{5}}=\overline{10}\cdot\bar{9}=\bar{2},:x_3=\frac{\bar{2}}{\bar{5}}=\bar{2}\cdot\bar{9}=\bar{7}$.

Приклад 2.2. Розв'язати у 7-арифметиці систему рівнянь: $\begin{cases}x_1+x_2+x_3=\bar{1}\\ x_1+\bar{2}x_2-\bar{3}x_3=\bar{0}\\ \bar{2}x_1+\bar{3}x_2+\bar{5}x_3=\bar{1}\end{cases}$.

У даному випадку $\Delta=\begin{vmatrix}\bar{1}&\bar{1}&\bar{1}\\ \bar{1}&\bar{2}&-\bar{3}\\ \bar{2}&\bar{3}&\bar{5}\end{vmatrix}=\bar{0}$, тому теорему 2.1 застосувати неможливо. Оскільки ранги основної і розширеної матриці дорівнюють 2, то система сумісна. Знайдемо її розв'язки. Для цього використаємо метод Гаусса:

$$\left(\begin{array}{ccc|c}\bar{1}&\bar{1}&\bar{1}&\bar{1}\\ \bar{1}&\bar{2}&-\bar{3}&\bar{0}\\ \bar{2}&\bar{3}&\bar{5}&\bar{1}\end{array}\right)\sim\left(\begin{array}{ccc|c}\bar{1}&\bar{1}&\bar{1}&\bar{1}\\ \bar{0}&\bar{1}&-\bar{4}&-\bar{1}\\ \bar{0}&\bar{1}&\bar{3}&-\bar{1}\end{array}\right)\sim\left(\begin{array}{ccc|c}\bar{1}&\bar{1}&\bar{1}&\bar{1}\\ \bar{0}&\bar{1}&-\bar{4}&-\bar{1}\\ \bar{0}&\bar{0}&\bar{0}&\bar{0}\end{array}\right).$$

Отже, система має одну вільну змінну. Нехай це буде x_3. Тоді:

$$\begin{cases}x_2-\bar{4}x_3=-\bar{1}\\ x_1+x_2+x_3=\bar{1}\end{cases},\begin{cases}x_2=\bar{4}x_3-\bar{1}\\ x_1=-x_2-x_3+\bar{1}\end{cases},\begin{cases}x_2=\bar{4}x_3-\bar{1}\\ x_1=-\bar{5}x_3+\bar{2}\end{cases},\text{ де } x_3\in\{\bar{0},\bar{1},\dots,\bar{6}\}.$$

Висновки. У арифметиках за простим модулем розв'язування алгебраїчних рівнянь та їх систем має багато спільного з тим, як вони розв'язуються у числових множинах. Зокрема, працюють твердження про число розв'язків, схожими є алгоритми розв'язування лінійних та квадратних рівнянь та систем лінійних рівнянь. У арифметиках за складеним модулем вказані алгоритми працюють не завжди, що ілюструють наведені приклади.

Список використаних джерел

1. Бич О. В. Будуємо нові арифметики. У світі математики. 1998. № 1. С. 11-14.
2. Геронимус А. Диофантовы уравнения по простому модулю. Квант. 1978. № 12. С. 2-6.
3. Виленкин Н. Сравнения и классы вычетов. Квант. 1978. № 10. С. 4-8.
4. Геронимус А. Сравнения по простому модулю. Квант. 1978. № 11. С. 6-10.
5. Егоров А., Котова А. Необыкновенные арифметики. Квант. 1993. № 3-4. С. 37-42.
6. Егоров А. Сравнения по модулю и арифметика остатков. Квант. 1970. №5. С. 27-33.
7. Лукашова Т. Д., Пискун К.В. Скінченні арифметики. У світі математики. 2015. № 1. С. 26-34.
8. Михелович Ш. Х. Материалы для факультативных занятий по дополнительным вопросам арифметики в средней школе Ч. 1. Даугавпилс: Даугавпилсский пед. Инст-т, 1973. 178 с.
9. Попов Є. Д. Інтерпретація комплексних чисел у скінченних арифметиках. У світі математики. 1975. № 6. С. 110-121.
10. Хмара Т. М. Незвичайні арифметики. У світі математики. 1974. № 5. С. 7-14.
11. Окунев Л.Я. Краткий курс теории чисел. М.:Учпедгиз, 1956. 240 с.
12. Лукашова Т.Д., Марченко К.В. Модульні арифметики. Фізико-математична освіта. 2018. Випуск 1(15). С. 246-251
13. Михелович Ш. Х. Теория чисел. М.: «Высшая школа». 1967. 336 с.
14. Бородін О. І. Теорія чисел. К. : «Радянська школа», 1960. 246 с.

References

1. Bych O.V. We are building new Arithmetic. In the world of Mathematics.1998 №1. P. 11-14.
2. Geronimus A. Diophantine equations of a simple module, Kvant. 1978. №. 12. P. 2-6.
3. Vilenkin N. Comparison and residues classes. Kvant. 1978. № 10. P.4-8.
4. Geronimus A. Comparison of a simple module. Kvant . 1978. № 11. P. 6-10.
5. Egorov A., Kotova A. Uncommon Arithmetic, Kvant. 1993. № 3-4. P. 37-42.
6. Egorov A. Comparison of modulus and Arithmetic of residues. Kvant. 1970. №5. P. 27-33
7. Lukashova T.D., Piskun K.V. Finite Arithmetic. In the world of Mathematics. 2015. № 1. P. 26-34.
8. Mikhelovich Sh. H. Materials for facultative studies on additional questions of Arithmetic in secondary school. Ch. 1. Daugavpils: Daugavpils Ped. Inst., 1973. 178 p.
9. Popov E. D. Interpretation of complex numbers in Finite Arithmetic. In the world of Mathematics. 1975. № 6. P. 110-121.
10. Khmara T. M. Uncommon Arithmetic. In the world of Mathematics. 1974. № 5. P. 7-14.
11. Okunev L.I. Safety education of Number Theory M.: Uchpedgiz, 1956. 240 p.
12. Lukashova T., Marchenko K. The Modular Arithmetics. Physical and Mathematical Education. 2018. Issue 1(15). P. 246-251.
13. Mikhelovich Sh. H. . Number Theory. M.: "Hight school", 1967. 336 p.
14. Borodin O. I. Number Theory. K.: "Soviet school", 1960. 246 p.

SOLVING ALGEBRAIC EQUATIONS IN MODULAR ARITHMETIC

T.D. Lukashova, M.V. Lukashova, K.V. Marchenko

Makarenko Sumy State Pedagogical University, Ukraine

Abstract. *It is necessary to perform arithmetic operations for a particular module in many tasks of Theory of Numbers, Discrete Mathematics and Cipher Theory. In this case, each integer can be identified with the remainder of this module and consider a plurality of residues as a new Modular Arithmetic.*

In spite of the fact arithmetic operations over elements of an algebraic structure formed in this way are introduced in the same way as they are defined for integers, and are determined by the corresponding residues from division into a module. However, depending on the module, some features may arise when multiplying the classes of residues and derivative operations, elevation to degree and extraction of the root, when solving equations and their systems.

In Arithmetics for a simple module, the results of the operations of subtraction and division for a non-zero element also are the elements of the corresponding Arithmetics. Therefore, they can be considered without negative and fractional expressions. Moreover, in such an Arithmetics, most of well-known algorithms of solving algebraic equations and their systems are preserved. On the other hand, in the Arithmetics for the compiled module, the established rules may be violated, what is explained by the existence of dividers of zero in them.

Despite the fact that the implementation of arithmetic operations in finite Arithmetics basing mostly on the Theory of Congruences and the Theory of Rings, which are studied in the course of Algebra and Theory of Numbers, only some individual publications are devoted to the study of Modular Arithmetics, the peculiarities of the implementation of arithmetic operations and the solving algebraic equations and their systems, in them.

In this article peculiarities algebraic equations and their systems in Modular Arithmetic. The solvability of certain types of algebraic equations (in partiqular, linear and square equations), as well as systems of linear equations in arithmetic by a simple module, is explored, and the corresponding algorithms and examples are given. The problem of solvability of certain types of algebraic equations, as well as systems of linear equations in Modular Arithmetic is explored. Corresponding algorithms and examples are given in this article. The material of the article can be used in the study of relevant topics in the Theory of Numbers and Discrete Mathematics, as well as at the lessons of the special courses and mathematical circles.

Key words: *rings of residues classes, Modular Arithmetic, Finite Arithmetic, algebraic equations, linear equations, systems of linear equations.*