Лекція 2

Розвиток теорій алгебраїчних структур

БАЗОВІ ВІДОМОСТІ ПРО АЛГЕБРАЇЧНІ СТРУКТУРИ

Група (алгебраїчна структура з однією алгебраїчною операцією)

Означення. *Алгебраїчною операцією* на множині A називається відображення $A\times A\to A$, при якому кожній впорядкованій парі (a,b) елементів із A відповідає елемент цієї ж множини. Цей елемент зазвичай позначають через $a*b$ (або $a+b$, або ab і т.ін.). В цьому випадку говорять, що *множина A є замкнутою відносно операції $*$*.

Означення. *Групою* називається непуста множина G разом із заданою на ній алгебраїчною операцією $*$, для якої виконуються аксіоми:

1) Для будь-яких трьох елементів a,b,c множини G $a*(b*c)=(a*b)*c$ *(асоціативність операції $*$).*

2) Існує такий елемент e множини G, що для будь-якого елемента a цієї ж множини $a*e=a$ *(існування нейтрального елемента).*

3) Для кожного елемента a множини G існує такий елемент a' цієї ж множини, що $a*a'=e$ *(існування симетричного елемента).*

Групу позначають символом $(G,*)$.

Означення. *Група* $(G,*)$ називається *абелевою (*або *комутативною),* якщо для будь-яких її елементів a,b виконується умова $a*b=b*a$.

Якщо група $(G,*)$ містить скінченну кількість елементів, то вона називається *скінченною*, а число елементів в ній називається *порядком групи* та позначається символом $|G|$. Група з нескінченою кількістю елементів називається *нескінченною.* Скінчена група $(G,*)$ називається p - *групою,* якщо $|G|=p^k$, де p - просте число, а k - натуральне.

Запис результату бінарної операції в групі у вигляді $(x, y) \to xy$ називають мультиплікативним, а саму групу називають *мультиплікативною*. Нейтральний *елемент* мультиплікативної групи прийнято називати *одиничним*, а симетричний *елемент – оберненим*. Іноді зручніше використовувати адитивний запис $(x, y) \to x + y$ і називати *групу адитивною*. В такій групі нейтральний *елемент* називають *нульовим,* а симетричний – *протилежним.*

В мультиплікативній групі замість запису $\underbrace{x \cdot x \cdot \ldots \cdot x}_{n}$ пишуть x^n, а в адитивній групі замість $\underbrace{x + x + \ldots + x}_{n}$ прийняте позначення nx.

Означення. Нехай x - елемент мультиплікативної групи. Найменше натуральне число n таке, що $x^n = e$ називається *порядком елемента* x. Позначають $|x|$ або $ord\, x$. Якщо такого n не існує то говорять, що x - *елемент нескінченного порядку.*

Означення. Підмножина H групи G називається її *підгрупою*, якщо вона є групою відносно алгебраїчної операції в групі. Позначають $H < G$. *Підгрупи* $E = \{e\} < G$ і $G < G$ називаються *невласними* або *тривіальними*, всі інші підгрупи називаються *власними.*

Завдання:

1. Чи є групами відносно вказаних операцій наступні числові множини: Z, Q, R, C відносно операції додавання, $Q \setminus \{0\}$, $R \setminus \{0\}$, $C \setminus \{0\}$ відносно операції множення?

2. Чи є групою множина всіх невироджених матриць n - го порядку з дійсними елементами відносно операції множення матриць?

3. Довести, що $(a * b)' = a' * b'$ тоді і лише тоді, коли $a * b = b * a$.

4. Чому дорівнює порядок групи рухів, які суміщають із самим собою правильний n - кутник?

5. В мультиплікативній групі U_8 виписати всі елементи та знайти порядки всіх елементів.

6. 13. В групі G_3 самосуміщень правильного трикутника знайти:

A) $\left(R_0^{120^0}\right)^{n+29}$; B) $\left(R_0^{120^0} \circ S_a\right)^{n+4}$.

7. 14. В групі S_8 знайти: A) порядок елемента $\alpha\beta$; B) α^{n+1};

8. C) представити β у вигляді добутку транспозицій, де

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 4 & 1 & 7 & 6 & 8 & 5 \end{pmatrix},$$

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 8 & 3 & 1 & 2 & 4 & 6 & 7 \end{pmatrix}.$$

Приклади: 1) Множини Z, Q, R, C є адитивними групами. Крім того, $Z < Q < R < C$. 2) Множина $Z_6 = \{0,1,2,3,4,5\}$, на якій операція «+» задається таблицею (детальніше у додатку в кінці лекції):

+	**0**	**1**	**2**	**3**	**4**	**5**
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

є групою. Крім того, $M = \{0,2,4\} < Z_6$, $P = \{0,3\} < Z_6$.

Теорема (Лагранжа) Порядок скінченної групи ділиться на порядок будь-якої її підгрупи.

Наслідок. Група простого порядку не має власних підгруп.

Означення. Нехай $(G,*)$ і $(H,\circ)$ групи. Відображення $f: G \to H$ називається *ізоморфізмом* цих груп, якщо воно бієктивне і $f(a*b) = f(a) \circ f(b)$ для будь-яких $a,b \in G$. Якщо такий ізоморфізм існує, то *групи* називають *ізоморфними* і позначають $G \cong H$.

Ізоморфні групи мають одні і ті самі властивості.

Властивості ізоморфізмів. Нехай $f: G \to H$ - ізоморфізм. Тоді:

1) Образом нейтрального елемента групи G є нейтральний елемент групи H, тобто $f(e) = e'$.

2) Образом елемента a', який є симетричним до елемента $a \in G$, є елемент групи H, симетричний до образа елемента a, тобто $f(a') = (f(a))'$.

3) Відображення, обернене до ізоморфізму, є ізоморфізмом.

4) Якщо $f(g) = h$, то порядки елементів g і h однакові.

5) Якщо $f: G \to H$ і $g: H \to F$ - ізоморфізми, то композиція $(g \circ f): G \to F$ теж є ізоморфізмом.

Завдання:

1. Довести, що групи $(R,+)$ і $(R_+,\cdot)$ ізоморфні.

2. В мультиплікативній групі $(G,\cdot)$ зафіксовано елемент a і задано нову операцію за правилом $x \circ y = x \cdot a \cdot y$**.** Довести, що відносно цієї операції G є групою, ізоморфною заданій.

Кільце (алгебраїчна структура з двома алгебраїчними операціями)

Означення. *Кільцем* називається непуста множина K разом із заданими на ній алгебраїчними операціями $+$ і $*$, для яких виконуються аксіоми:

1) Для будь-яких трьох елементів a,b,c множини K $a + (b + c) = (a + b) + c$ *(асоціативність операції +).*

2) Існує такий елемент Θ множини K, що для будь-якого елемента a цієї ж множини $a+\Theta=a$ *(існування нейтрального елемента відносно додавання).* Прийнято елемент Θ називати *нулем*.

3) Для кожного елемента a множини K існує такий елемент a' цієї ж множини, що $a+a'=\Theta$ *(існування протилежного елемента).* Позначають $a'=-a$.

4) Для будь-яких двох елементів a,b множини K $a+b=b+a$ *(комутативність операції +).*

5.1) Для будь-яких трьох елементів a,b,c множини K $a*(b+c)=a*b+a*c$ *(ліва дистрибутивність).*

5.2) Для будь-яких трьох елементів a,b,c множини K $(a+b)*c=a*c+b*c$ *(права дистрибутивність).*

Кільце позначають символом $(K,+,*)$.

Крім вказаних аксіом, які визначають на множині структуру кільця, на цій множині можуть виконуватись й інші аксіоми. Тоді кільця мають спеціальну назву.

Означення Кільце називається:

- *асоціативним*, якщо виконується аксіома 6) Для будь-яких трьох елементів $a,b,c\in K$ $a*(b*c)=(a*b)*c$ *(асоціативність операції *)*;
- *комутативним*, якщо виконується аксіома 7) Для будь-яких двох елементів $a,b\in K$ $a*b=b*a$ *(комутативність операції *)*;
- *кільцем з одиницею*, якщо виконується аксіома 8) Існує такий елемент e, що для будь-якого елемента $a\in K$ $a*e=a$ (існування нейтрального елемента відносно множення). Елемент e називають *одиницею*.

Означення. *Полем* називається асоціативне комутативне кільце з одиницею, в якому виконується аксіома

9) Для кожного елемента $a \in K, a \neq \Theta$ існує такий елемент $\bar{a} \in K$, що $a * \bar{a} = e$ *(існування оберненого елемента)*. Позначають $\bar{a} = a^{-1}$.

Означення. Елемент $a \neq \Theta$ кільця *K* називається *дільником нуля*, якщо існує такий елемент $b \neq \Theta$, що $a * b = \Theta$. Якщо кільце є асоціативним, комутативним і в ньому відсутні дільники нуля, то воно називається *областю цілісності.*

Означення. Підмножина *M* кільця *K* називається його *підкільцем*, якщо вона є кільцем відносно тих самих алгебраїчних операцій. Позначають $M < K$.

Приклади. 1) Множини Z, Q, R, C є кільцями і областями цілісності. Крім того, $Z < Q < R < C$. 2) Множина $Z_6 = \{0,1,2,3,4,5\}$, на якій операції задаються таблицями (дивись додаток в кінці лекції).

+	**0**	**1**	**2**	**3**	**4**	**5**
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

.	**0**	**1**	**2**	**3**	**4**	**5**
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

є кільцем, але не є областю цілісності. Крім того, $M=\{0,2,4\}<Z_6$, $P=\{0,3\}<Z_6$.

Існування розкладу на прості співмножники для кожного цілого числа

Прості числа представляють великий інтерес ще й тому, що з ними пов'язано велика кількість проблем, які легко поставити, але дуже важко вирішити. Багато проблем, щодо простих чисел, не вирішені до цих пір.

Першими простими числами є 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, … .

Грецьким математикам був відомий спосіб виділення простих чисел з

Теорема Кожне ненульове ціле число може бути представлене у вигляді добутку простих чисел.

Означення *Канонічним розкладом цілого числа* $n>1$ називається представлення n у вигляді $n=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_m^{\alpha_m}$, де p_1, …, p_m − попарно різні прості числа, α_1, …, α_m − натуральні числа. Канонічним розкладом цілого числа $n<-1$ називається аналогічне представлення у вигляді $n=-p_1^{\alpha_1}p_2^{\alpha_2}\dots p_m^{\alpha_m}$ [1].

Сформулюємо теорему про однозначність розкладу на прості множники.

Теорема. Для будь-якого ненульового цілого числа n існує розклад на прості множники

$$n=(-1)^{\varepsilon(n)}\prod_p p^{\alpha(p)}$$

з показниками степеня, які однозначно визначаються числом n. Різні розклади цілого числа на прості множники відрізняється лише порядком цих множників.

Означення. Нехай є кільця $(K,+,*)$ і $(L,\oplus,\circ)$. *Гомоморфізмом із К в L* називається відображення $f: K \to L$, яке зберігає операції, тобто виконуються вимоги:

а) $(\forall x, y \in K) \quad f(x+y) = f(x) \oplus f(y)$,

б) $(\forall x, y \in K) \quad f(x*y) = f(x) \circ f(y)$.

Ізоморфізмом кілець $(K,+,*)$ і $(L,\oplus,\circ)$ називається бієктивний гомоморфізм $f: K \to L$. Пишуть $K \cong L$.

Означення. *Ядром гомоморфізму* $f: K \to L$ називається множина $Kerf = \{x \in K \mid f(x) = \Theta_L\}$. *Образом гомоморфізму* $f: K \to L$ називається множина $\mathrm{Im}\, f = \{y \in L \mid (\exists x \in K)\ f(x) = y\}$.

Завдання:

1. Нехай A - деяка множина, B - сукупність всіх підмножин множини A. На множині B задамо операцію додавання і множення наступним чином: $X + Y = (X \cup Y) \setminus (X \cap Y)$, $X \cdot Y = X \cap Y$. Довести, що B відносо цих операцій є кільцем з одиницею.

2. Довести, що оборотні елементі комутативного кільця утворюють групу відносно операції множення.

3. Довести, що поле є областю цілісності.

4. З'ясуйте, чи є в кільцях Z_6 , Z_8, Z_9 , Z_{10} дільники нуля. При яких m кільце Z_m є областю цілісності?

5. Знайти всі підкільця кілець Z_3, Z_4, Z_6.

СТРУКТУРА КІЛЬЦЯ В МНОЖИНІ МАТРИЦЬ З ЕЛЕМЕНТАМИ З КІЛЬЦЯ Z_m. ОБОРОТНІ ЕЛЕМЕНТИ

Розглянемо кільце $Z_m = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{m-1}\}$ класів лишків по модулю m. Якщо m − просте число, то Z_m буде полем [5]. Нагадаємо, що операції над класами визначаються рівностями:

$$\bar{a} + \bar{b} = \overline{a+b},$$
$$\bar{a} \cdot \bar{b} = \overline{ab}.$$

Далі через $M(2, Z_m)$ будемо позначати множину квадратних матриць другого порядку з елементами із кільця Z_m. Множина матриць $M(2, Z_m)$ є кільцем відносно операцій множення і додавання матриць, так як виконуються аксіоми кільця.

Множина $M(2, Z_m)$ є кільцем з одиницею. Одиницею даного кільця є матриця $E = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}$, так як при множенні будь-якої матриці зліва (справа) на матрицю $E = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}$ отримуємо в результаті ту ж саму матрицю.

Нагадаємо, що умовою існування оберненої до A матриці над числовим полем є відмінність від нуля її визначника. В кільці $M(2, Z_m)$ існують матриці з відмінним від нуля визначником, які не мають оберненої.

Приклад. Розглянемо матрицю $A = \begin{pmatrix} \bar{6} & \bar{4} \\ \bar{5} & \bar{3} \end{pmatrix}$ над кільцем Z_8. Припустимо, що вона має обернену матрицю $A^{-1} = \begin{pmatrix} \bar{x} & \bar{y} \\ \bar{z} & \bar{t} \end{pmatrix}$. Тоді

$AA^{-1}=\begin{pmatrix}\bar{6} & \bar{4}\\ \bar{5} & \bar{3}\end{pmatrix}\begin{pmatrix}\bar{x} & \bar{y}\\ \bar{z} & \bar{t}\end{pmatrix}=\begin{pmatrix}\bar{6}x+\bar{4}z & \bar{6}y+\bar{4}t\\ \bar{5}x+\bar{3}z & \bar{5}y+\bar{3}t\end{pmatrix}=\begin{pmatrix}\bar{1} & \bar{0}\\ \bar{0} & \bar{1}\end{pmatrix}$. Отримаємо наступну систему порівнянь

$$\begin{cases}6x+4z\equiv 1(\mathrm{mod}8),\\ 5y+3t\equiv 1(\mathrm{mod}8),\\ 5x+3z\equiv 0(\mathrm{mod}8),\\ 6y+4t\equiv 0(\mathrm{mod}8).\end{cases}$$

Різницею першого та третього порівнянь є порівняння $x+z\equiv 1(\mathrm{mod}8)$. Тоді третє порівняння набуває вигляду $2z\equiv 5(\mathrm{mod}8)$. Таке порівняння не має розв'язків за властивостями порівнянь. Таким чином, наше припущення невірне і матриця A не має оберненої. Аналізуючи причини такого негативного результату, помічаємо, що визначник даної матриці порівняний з числом 2, а, отже не взаємно простий з модулем.

Для того, щоб знайти обернену матрицю в кільці Z_m введемо наступні теореми.

Теорема. Нехай $A=\begin{pmatrix}\bar{a} & \bar{b}\\ \bar{c} & \bar{d}\end{pmatrix}$ – матриця з кільця $M(2,Z_m)$, $\det A=\bar{k}$ і $НСД(k,m)=1$. Тоді A є оборотною і $A^{-1}=\bar{l}\begin{pmatrix}\bar{d} & -\bar{b}\\ -\bar{c} & \bar{a}\end{pmatrix}$, де $k\cdot l\equiv 1(\mathrm{mod}m)$.

Теорема (обернена). Якщо матриця $A\in M(2,Z_m)$ має обернену, то $\det A=\bar{k}$ задовольняє умову $НСД(k,m)=1$.

Приклад. Знайдемо для матриці $A=\begin{pmatrix}\bar{5} & \bar{6}\\ \bar{4} & \bar{6}\end{pmatrix}\in M(2,Z_{17})$ обернену матрицю. Матриця A невироджена, оскільки $\det A=\bar{5}\cdot\bar{6}-\bar{4}\cdot\bar{6}=\bar{6}$ і $НСД(6,17)=1$. Тоді $\det(A^{-1})=\overline{16}$, тому що $\bar{6}\cdot\bar{3}=\overline{18}=\bar{1}$. Далі знаходимо

матрицю з алгебраїчних доповнень та транспонуємо її. В результаті маємо $A^{-1}=\overline{3}\begin{pmatrix}\overline{6} & \overline{11}\\ \overline{13} & \overline{5}\end{pmatrix}=\begin{pmatrix}\overline{1} & \overline{16}\\ \overline{5} & \overline{5}\end{pmatrix}$.

ОБ ОДНОЙ ИЗ ЗАДАЧ – МОНСТРОВ

Речь пойдет о следующей **задаче**: Доказать, что для двух целочисленных матриц A,B таких, что $\det A=1$, $\det B\neq 0$, существует $n\in N$ такое, что $B^{-1}A^nB$ – тоже целочисленная матрица.

Ее условие мы взяли из журнала «Математическое просвещение», № 11 за 2007 год в отделе задач. В последующих номерах журнала решение не появилось. Эта задача попала также в сборник Белова А.Я. задач – монстров по математике.

Мы приведем здесь решение этой задачи, полученное путем разбиения ее на подзадачи, объединенные общей идеей. Прежде всего, отметим, что, желая рассматривать эту задачу как исследовательскую, следовало бы изменить ее формулировку следующим образом.

Задача. Пусть даны две целочисленные матрицы A,B такие, что $\det A=1$, $\det B\neq 0$. Существует ли $n\in N$ такое, что $B^{-1}A^nB$ – тоже целочисленная матрица?

Решение. Первые попытки провести исследование для произвольной унимодулярной матрицы не дали результата, поэтому поиск алгоритма решения пришлось начать с рассмотрения частных случаев и попытаться их обобщить.

Самым простым примером унимодулярной матрицы, определитель которой равен 1, является единичная матрица E. Для нее, очевидно, $n=1$, так как

$B^{-1}EB = B^{-1}B = E$ по определению обратной матрицы. Из этого ясно, что для тех унимодулярных матриц, некоторая натуральная степень которых равна единичной матрице E, ответ на поставленный вопрос положительный. Такие матрицы существуют. Действительно, множество унимодулярных матриц с определителем 1 образует мультипликативную группу $SL(n,Z)$ бесконечного порядка, в которой роль нейтрального элемента играет единичная матрица. Безусловно, в этой группе существуют элементы конечного порядка. Порядок каждого такого элемента и будет искомым натуральным числом. Например, матрица $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ является элементом группы $SL(2,Z)$ унимодулярных матриц с равным 1 определителем. Порядок этой матрицы равен 4, а значит, при $n = 4$, матрица $B^{-1}A^4B$ будет целочисленной. Действительно, $B^{-1}A^4B = B^{-1}EB = B^{-1}B = E$.

Итак, нам удалось сделать обобщение простого частного случая и выделить класс матриц, для которых искомое натуральное число совпадает с их порядком. Но в группе $SL(n,Z)$ содержатся и элементы бесконечного порядка. Например, в группе $SL(2,Z)$ таким элементом является матрица $L = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Тем не менее, и в этом случае ответ остается положительным. Для описания решения задачи в этом случае нам понадобится сделать еще одно обобщение, более высокого уровня.

До сих пор целочисленность матрицы $B^{-1}A^nB$ следовала из определения обратной матрицы, так как во всех рассмотренных случаях эта матрица была единичной. Целочисленность матрицы $B^{-1}A^nB$ будет следовать также из того, что все элементы матрицы CA^nB, где C - союзная для B матрица, делятся на число $\det B$. Этот факт позволяет рассматривать не сами элементы матрицы CA^nB, а их остатки от деления на число $\det B$. Поэтому, будет естественным каждой матрице A из $SL(n,Z)$ поставить в соответствие матрицу $\overline{A}$, элементами которой являются классы вычетов по модулю $m = detB$.

Полученное множество матриц, по сравнению с исходным множеством $SL(n,Z)$, является конечным. Наделим его структурой кольца относительно операций сложения и умножения матриц. Каждый элемент этого кольца имеет конечный порядок. Например, если в условии даны матрицы $A=\begin{pmatrix}3 & 7\\ 2 & 5\end{pmatrix}$ и $B=\begin{pmatrix}3 & 3\\ 3 & 4\end{pmatrix}$, то соответствующая матрица для матрицы A имеет вид $\overline{A}=\begin{pmatrix}\overline{0} & \overline{1}\\ \overline{2} & \overline{2}\end{pmatrix}$, так как $\det B=3$. Понятно, что при нахождении натуральных степеней матрицы $A=\begin{pmatrix}3 & 7\\ 2 & 5\end{pmatrix}$ мы никогда не получим единичную матрицу, то есть в группе $SL(2,Z)$ эта матрица имеет бесконечный порядок. Напротив, матрица $\overline{A}$ в указанном кольце имеет порядок 3, то есть $\overline{A}^3=\begin{pmatrix}\overline{1} & \overline{0}\\ \overline{0} & \overline{1}\end{pmatrix}$.

Можем вернуться к рассмотрению общего случая. Если $\det B=m$, порядок матрицы $\overline{A}$ равен $n\in N$, то переходя от матрицы $\begin{pmatrix}\overline{1} & \overline{0}\\ \overline{0} & \overline{1}\end{pmatrix}$ к ее прообразам в указанном соответствии, получим

$$B^{-1}A^nB=B^{-1}\begin{pmatrix}qm+1 & rm\\ sm & tm+1\end{pmatrix}B=B^{-1}\left(\begin{pmatrix}qm & rm\\ sm & tm\end{pmatrix}+\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\right)B=B^{-1}\begin{pmatrix}qm & rm\\ sm & tm\end{pmatrix}B+B^{-1}EB,$$

где $q,s,t,r\in Z$.

Матрица $B^{-1}A^nB$ является целочисленной как сумма двух целочисленных матриц.

Мы провели исследование для всех возможных унимодулярных матриц с равным 1 определителем и дали положительный ответ на поставленный вопрос. Наше рассуждение было основано на рассмотрении частных случаев, разбиении задачи на подзадачи и использовании свойств конечных алгебраических структур.

Додаток

МНОЖИНА КЛАСІВ ЛИШКІВ

Означення. Цілі числа a і b називаються *конгруентними за модулем* m, якщо їх різниця ділиться без остачі на m.

Іншими словами, цілі числа a і b називаються конгруентними за модулем m, якщо їх остачі при діленні на m одинакові.

Якщо числа a і b конгруентні за модулем m, то пишуть

$$a \equiv b(\mathrm{mod}\, m).$$

Приклад. Так як різниця $16-30=-14$ ділиться на 7, то $16 \equiv 30(\mathrm{mod}\, 7)$, а $72 \equiv 45(\mathrm{mod}\, 8)$, так як $72-45=27$ не ділиться на 8.

Для фіксованого натурального числа m відношення конгруентності за модулем m має наступні властивості:

- рефлексивність: для будь-якого цілого числа a справедливо $a \equiv a(\mathrm{mod}\, m)$;

- симетричність: якщо $a \equiv b(\mathrm{mod}\, m)$, то $b \equiv a(\mathrm{mod}\, m)$;

- транзитивність: якщо $a \equiv b(\mathrm{mod}\, m)$ і $b \equiv c(\mathrm{mod}\, m)$, то $a \equiv c(\mathrm{mod}\, m)$.

Дійсно,

- для будь-якого m і будь-якого a різниця $(a-a) \vdots m$;

- з $a \equiv b(\mathrm{mod}\, m)$ випливає $(a-b) \vdots m$. $b-a=-(a-b) \vdots m$. Таким чином, $b \equiv a(\mathrm{mod}\, m)$.

- з $a \equiv b(\mathrm{mod}\, m)$ випливає $(a-b) \vdots m$, а з $b \equiv c(\mathrm{mod}\, m)$ випливає $(b-c) \vdots m$. Отже, $(a-c) \vdots m$, а значить $a \equiv c(\mathrm{mod}\, m)$.

Таким чином, відношення конгруентності за модулем m являється відношенням еквівалентності на множині цілих чисел.

Означення. Множина всіх чисел, конгруентних з a за модулем m, називається *класом лишків за модулем* m, породженим елементом a.

При діленні на m можна отримати m різних остач: $0, 1, 2, ..., m-1$. Кожній з них відповідає свій клас лишків. Остачі r відповідає клас лишків $\bar{r}$, що складається з чисел вигляду $r + km$, де k - ціле число:

$$\bar{r} = \{r + km | k \in Z\}.$$

Вся множина Z цілих чисел розпадається на m класів лишків за модулем m. Множина всіх цих класів позначається через $Z_m : Z_m = \{\bar{0}, \bar{1}, \bar{2}, ..., \overline{m-1}\}$.

Операції на множині класів лишків за модулем m

Введемо на множині Z_m операцію додавання. В кожному з доданків $\bar{a}$ і $\bar{b}$ беруть по представнику і додають їх, а потім дивляться, до якого класу лишків відноситься сума. Цей клас позначають $\overline{a+b}$ і називають сумою даних класів.

Приклад. Додамо класи лишків $\bar{4}$ і $\bar{5}$ за модулем 6. Виберемо в них по представнику, візьмемо самі лишки $\bar{4}$ і $\bar{5}$. Їх сума дорівнює 9. Але $9 \equiv 3 (\mathrm{mod} 6)$ і тому $\bar{4} + \bar{5} = \bar{3}$. Якщо ж ці класи беруться не в Z_6, а в Z_8, то отримаємо іншу суму: $\bar{4} + \bar{5} = \bar{1}$. А в Z_9: $\bar{4} + \bar{5} = \bar{0}$.

Теорема. Якщо $a \equiv a_1 (\mathrm{mod} m)$ і $b \equiv b_1 (\mathrm{mod} m)$, то $a + b \equiv a_1 + b_1 (\mathrm{mod} m)$.

Доведення. Так як $a \equiv a_1 (\mathrm{mod} m)$, $a = a_1 + km$, де $k \in Z$, а так як $b \equiv b_1 (\mathrm{mod} m)$, $b = b_1 + lm$, де $l \in Z$. Тому $a + b \equiv a_1 + b_1 + (k + l)m$, де $k + l \in Z$, і $a + b \equiv a_1 + b_1 (\mathrm{mod} m)$.

Наслідок. Операція додавання класу лишків не залежить від вибору представників.

Ми звели додавання класів лишків до додавання цілих чисел. Тому додавання класів лишків комутативне і асоціативне, тобто $\bar{a}+\bar{b}=\bar{b}+\bar{a}$ і $(\bar{a}+\bar{b})+\bar{c}=\bar{a}+(\bar{b}+\bar{c})$, додавання класу $\bar{0}$ не міняє клас лишків, тобто $\bar{a}+\bar{0}=\bar{a}$.

Віднімання і множення класів лишків визначаються аналогічно – в класах обирають по представнику і виконують операції над ними. Результат цих операцій також не залежить від вибору представників.

Означення. Поділити клас лишків $\bar{b}$ на клас лишків $\bar{a}$ - значить знайти такий клас лишків $\bar{x}$, що $\bar{a}\bar{x}=\bar{b}$.

Для цілих чисел задача ділення розв'язується не завжди, але якщо вона розв'язується, то єдиним чином. Це пов'язано з тим, що добуток двох цілих чисел дорівнює нулю лише у випадку, коли один із множників дорівнює нулю. Але в Z_m справа дещо інша.

Приклад. Розглянемо таблицю множення Z_6.

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Таблиця множення

Бачимо, що нулі стоять в ній не тільки в першому рядку і в першому стовпчику (там, де один із множників дорівнює нулю). Наприклад, $\bar{2}\cdot\bar{3}=\bar{0}$ і $\bar{3}\cdot\bar{4}=\bar{0}$.

Означення. Клас лишків $\bar{a}$ називається дільником нуля, якщо він відмінний від $\bar{0}$, але існує такий клас $\bar{b}\neq\bar{0}$, що $\bar{a}\cdot\bar{b}=\bar{0}$.

В розглянутому прикладі 4.3 нулю дорівнюють добутки $\bar{2}\cdot\bar{3}$, $\bar{3}\cdot\bar{4}$, хоча множники відмінні від нуля. Отже, в Z_6 класи $\bar{2}$, $\bar{3}$, $\bar{4}$ є дільниками нуля. Звернемо увагу на той факт, що представники цих класів - числа 2, 3, 4 – мають спільну властивість, а саме вони не являються взаємо простими з модулем 6. Має місце наступна теорема:

Теорема. Клас лишків $\bar{a}$ в Z_m не являється дільником нуля в тому і лише і тому випадку, коли a і m взаємо прості.

Доведення. Нехай a і m взаємо прості. Якщо $\bar{a}\cdot\bar{b}=\bar{0}$, то число ab ділиться на m. Але в силу взаємної простоти a і m, це може бути лише у випадку, коли b ділиться на m, тобто $\bar{b}=\bar{0}$. Це значить, що $\overline{ab}=\bar{0}$ лише при $\bar{b}=\bar{0}$, тобто клас $\bar{a}$ не являється дільником нуля.

Припустимо тепер, що найбільший спільний дільник d чисел a і m відмінний від 1, $a=a_1d$, $m=m_1d$, $d>1$. Тоді число $m_1<m$ - ціле, причому відмінне від m, і тому $\overline{m_1}\neq\bar{0}$. Але $am_1=a_1dm_1=a_1m$, тобто $\bar{a}\overline{m_1}=\bar{0}$. А значить $\bar{a}$ - дільник нуля.

Означення. Якщо число a взаємно просте з модулем m, то всі числа з класу лишків $\bar{a}$ взаємно прості з m. В цьому випадку говорять, що клас $\bar{a}$ взаємо простий з m.

Наслідок. Якщо клас лишків $\bar{a}$ взаємно простий з m, то в Z_m можна однозначно ділити на $\bar{a}$, тобто для будь-якого $\bar{b} \in Z_m$ рівняння $\bar{a}\bar{x} = \bar{b}$ має один і тільки один розв'язок.

Доведення. Спочатку доведемо, що це рівняння не може мати різні розв'язки. Якщо $\bar{a}\bar{x}_1 = \bar{b}$ і $\bar{a}\bar{x}_2 = \bar{b}$, то $\bar{a}(\bar{x}_1 - \bar{x}_2) = \bar{0}$, а так як $\bar{a}$ не дільник нуля, то $\bar{x}_1 - \bar{x}_2 = \bar{0}$, тобто $\bar{x}_1 = \bar{x}_2$. Значить, розв'язок може бути лише один.

Залишилось показати, що розв'язок існує. Ми довели, що серед класів лишків $\bar{a} \cdot \bar{0}$, $\bar{a} \cdot \bar{1}$, …, $\bar{a} \cdot (\overline{m-1})$ не має однакових. Отже, це ті ж класи $\bar{0}, \bar{1}, ..., \overline{m-1}$, тільки, можливо, взяті в іншому порядку. А тоді для будь-якого класу $\bar{b}$ знайдеться такий клас $\bar{x}$, що $\bar{a} \cdot \bar{x} = \bar{b}$.

Проілюструємо доведений факт таблицею множення за модулем 6. З неї видно, що тільки в рядках для класів $\bar{1}$ і $\bar{5}$ зустрічаються всі класи лишків. В інших рядках є лише частина класів: в рядках $\bar{2}$ і $\bar{4}$ класи $\bar{0}$, $\bar{2}$, $\bar{4}$, а в рядку для $\bar{3}$ – класи $\bar{0}$ і $\bar{3}$. Ці спостереження дозволяють сформулювати наступний наслідок:

Наслідок. Якщо $НСД(a, m) = d$, то рівняння $\bar{a} \cdot \bar{x} = \bar{b}$ має розв'язок лише при умові, що b ділиться на d. В цьому випадку число розв'язків дорівнює d.

У випадку, коли модуль являється простим числом, можна ділити на будь-який ненульовий клас лишків – в цьому випадку всі такі класи взаємно прості з модулем.

Існують і інші властивості пов'язані з діленням в кільці класів лишків. В теорії чисел для кільця цілих чисел дуже часто використовується так звана мала теорема Ферма:

Теорема. Якщо p - просте число і a не ділиться на p, то остача при діленні числа a^{p-1} на p дорівнює 1.

Ця теорема має місце і в кільці класів лишків. Сформулюємо її в термінах цього кільця.

Теорема. Якщо $\bar{a}$ - ненульовий клас лишків за простим модулем p, то $\bar{a}^{p-1} = \bar{1}$.

Доведення. Так як $0 < a < p$, а модуль p - просте число, то a і p взаємно прості. Тому класи $\bar{a} \cdot \bar{1}$, $\bar{a} \cdot \bar{2}$, …, $\bar{a} \cdot (\overline{p-1})$ являються тими ж, що й $\bar{1}, \bar{2}, ..., \overline{p-1}$, тільки взятими в іншому порядку. Так як Z_p комутативне і асоціативне кільце, то $(\bar{a} \cdot \bar{1})(\bar{a} \cdot \bar{2})..(\bar{a} \cdot (\overline{p-1})) = \bar{1} \cdot \bar{2} \cdot ... \cdot (\overline{p-1})$. Залишилось скоротити це рівняння на відмінний від $\bar{0}$ множник $\bar{1} \cdot \bar{2} \cdot ... \cdot (\overline{p-1})$, щоб пересвідчитись в тому, що $\bar{a}^{p-1} = \bar{1}$.

В теоремі Ферма модуль p повинен бути простим числом. Ейлер відкрив чудове узагальнення цієї теореми на випадок складеного модуля m. Класи лишків $\bar{1}, \bar{2}, ..., \overline{p-1}$, які ми множили на $\bar{a}$, взаємно прості з p. Візьмемо для складеного модуля m лише класи лишків, взаємно простих з m, і позначимо їх через $\varphi(m)$. Множення цих класів лишків на $\bar{a}$, взаємно простий з m, лише переставляє їх. Перемноживши ці добутки і розмірковуючи так, як при доведенні Малої теореми Ферма, приходимо до наступного твердження:

Теорема. Якщо клас лишків $\bar{a}$ взаємно простий з модулем m, то $\bar{a}^{\varphi(m)} = \bar{1}$.

Тобто, якщо число a взаємно просте з m, то при діленні $a^{\varphi(m)}$ на m отримаємо остачу 1. Для невеликих чисел m число $\varphi(m)$ можна знайти безпосередньо. Вони будуть представниками класів лишків.

Приклад. Для числа 12 маємо $\varphi(12)=4$, тобто з модулем 12 взаємно прості класи лишків $\bar{1}$, $\bar{5}$, $\bar{7}$, $\overline{11}$. Число $a=31$ взаємно просте з модулем 12. Тому при діленні $\overline{31}^4$ на 12 отримуємо остачу $\bar{1}$.