

**ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»
ФАКУЛЬТЕТ МАТЕМАТИКИ ТА ЦИФРОВИХ ТЕХНОЛОГІЙ
Кафедра алгебри та диференціальних рівнянь**

«ЗАТВЕРДЖУЮ»
Декан факультету математики
та цифрових технологій
Микола МАЛІЯР
« 30 » _____ 2023 року



РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ЕЛЕМЕНТАРНА ТЕОРІЯ ЧИСЕЛ

Рівень вищої освіти **перший (бакалаврський)**
Галузь знань **11 Математика та статистика**
Спеціальність **113 Прикладна математика**
Освітня програма **Системи штучного інтелекту**
Статус дисципліни **вибіркова**
Мова навчання **українська**

Ужгород 2023

Робоча програма навчальної дисципліни «Елементарна теорія чисел» для здобувачів вищої освіти галузі знань **11 Математика та статистика** спеціальності **113 Прикладна математика** освітньої програми **Системи штучного інтелекту**.

Розробник: Юрченко Н. В., канд. фіз.-мат. наук, доцент, доцент кафедри алгебри та диференціальних рівнянь

Робочу програму розглянуто та затверджено на засіданні

кафедри алгебри та диференціальних рівнянь

Протокол № 9 від «14» 06 2023 року

Завідувач кафедри Рейтій Олександр РЕЙТІЙ

Схвалено науково-методичною комісією **факультету математики та цифрових технологій**

Протокол № 10 від «20» червня 2023 року.

Голова науково-методичної комісії Юрченко Наталія ЮРЧЕНКО

Юрченко Н.В., 2023 р.

ДВНЗ «Ужгородський національний університет», 2023 р.

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Найменування показників	Розподіл годин за навчальним планом
	Денна форма навчання
Кількість кредитів ЄКТС – 4	Рік підготовки:
Загальна кількість годин – 120.	2-й
Кількість модулів – 2	Семестр:
Тижневих годин для денної форми навчання: аудиторних – 3 год., самостійної роботи студента – 3 год.;	3-й
	Лекції:
	30
	Практичні (семінарські):
	30
Вид підсумкового контролю: залік	Лабораторні:
	-
Форма підсумкового контролю: усна	Самостійна робота:
	60

2. МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою вивчення навчальної дисципліни «Елементарна теорія чисел» є ознайомлення студентів з основами теорії чисел, фундаментальними методами алгебри, вивчення основних алгебраїчних структур, теоретичними положеннями та основними застосуваннями деяких розділів алгебри та теорії чисел в різних задачах математики та інформатики, сприяння розвитку логічного та аналітичного мислення студентів.

Відповідно до освітньої програми, вивчення дисципліни сприяє формуванню у здобувачів вищої освіти таких компетентностей:

- ЗК01. Здатність учитися і оволодівати сучасними знаннями.
- ЗК02. Здатність застосовувати знання у практичних ситуаціях.
- ЗК04. Здатність бути критичним і самокритичним.
- ЗК05. Здатність проведення досліджень на відповідному рівні.
- ЗК06. Здатність до абстрактного мислення, аналізу та синтезу.
- ЗК07. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
- ЗК08. Знання та розуміння предметної області та розуміння професійної діяльності.
- ФК01. Здатність використовувати й адаптувати математичні теорії, методи та прийоми для доведення математичних тверджень і теорем.
- ФК02. Здатність виконувати завдання, сформульовані у математичній формі.
- ФК03. Здатність обирати та застосовувати математичні методи для розв'язання прикладних задач, моделювання, аналізу, проектування, керування, прогнозування, прийняття рішень.
- ФК14. Здатність сформулювати математичну постановку задачі, спираючись на постановку мовою предметної галузі, та обирати метод її розв'язання, що забезпечує потрібні точність і надійність результату.

3. ПЕРЕДУМОВИ ДЛЯ ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Передумовами вивчення навчальної дисципліни «Елементарна теорія чисел» є опанування таких навчальних дисциплін (НД) освітньої програми (ОП):

ОК 07 Алгебра і геометрія.

4. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Очікувані результати навчання, які повинні бути досягнуті здобувачами освіти після опанування навчальної дисципліни «Елементарна теорія чисел»:

Знання з предметної області включають: основні поняття абстрактної алгебри і теорії чисел, зокрема такі як бінарна алгебраїчна операція, алгебраїчна структура, ізоморфізм алгебраїчних структур, група, абелева група, порядок елемента групи, циклічна група, підгрупа, суміжний клас, індекс підгрупи, нормальна підгрупа, фактор-група, гомоморфізм груп, ядро та образ гомоморфізму, автоморфізм групи, p -група, прямий добуток груп, кільце, комутативне кільце, кільце з одиницею, дільник нуля, оборотній елемент, цілісне кільце, ідеал кільця, гомоморфізм кільця, кільце головних ідеалів, евклідове кільце, простий елемент, факторіальне кільце, найбільший спільний дільник і найменше спільне кратне елементів кільця, кільце класів лишків, функція Ейлера, конгруенція 1-го степеня, конгруенція n -го степеня, алгебраїчне та трансцендентне число, ціле алгебраїчне число, поле, просте число, розв'язування рівнянь в цілих числах, ланцюгові дроби

Когнітивні компетентності включають: здатність перевіряти, чи є задана алгебраїчна структура групою; здатність перевіряти, чи задане відображення є гомоморфізмом груп;

знаходження порядку елемента групи; побудову фактор-групи; здатність перевіряти, чи буде кільцем задана алгебраїчна структура; здатність перевіряти, чи задане відображення є гомоморфізмом кілець; здатність описувати дільники нуля та оборотні елементи в кільці; знаходження ідеалів кільця; обчислення найбільшого спільного дільника елементів кільця; здатність розв'язувати лінійні конгруенції; розв'язувати діафантові рівняння; розкласти числа в неперервний дріб.

До практичних вмінь та навичок входять: вміння розпізнавати і визначати алгебраїчні структури; вміння застосовувати апарат теорії груп; вміння розв'язувати системи лінійних конгруенцій та квадратичних конгруенцій; навички використання апарату теорії груп та кілець до розв'язання деяких задач на практиці.

5. ЗАСОБИ ДІАГНОСТИКИ ТА КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Методи навчання

При вивченні дисципліни використовуються інформаційні, ілюстративні, абстрактно-дедуктивні (теоретичні) та навчально-продуктивні (практичні) методи навчання із застосуванням: лекцій у супроводі мультимедійних матеріалів, евристичних лекцій-бесід, виконання студентами індивідуальних завдань, контрольних завдань.

Засоби оцінювання та методи демонстрування результатів навчання

Для визначення рівня засвоєння студентами навчального матеріалу використовуються такі методи оцінювання знань: проведення контрольних робіт після вивчення певних змістовних модулів; перевірка домашніх робіт; опитування під час практичних занять; підсумкова модульна контрольна робота, залік. Для діагностики знань використовується кредитно-рейтингова система за 100-бальною шкалою оцінювання.

Форми контролю та критерії оцінювання результатів навчання

Форми поточного контролю: виконання практичних та домашніх завдань.

Форма модульного контролю: письмова контрольна робота.

Форма підсумкового семестрового контролю: залік.

Форми поточного контролю. Поточний контроль знань студентів упродовж одного семестру включає бали за роботу на практичних заняттях, а також оцінювання всіх видів самостійної роботи. В кожному семестрі проводяться також дві модульні контрольні роботи і викладаються дві модульні контрольні оцінки. Вплив поточного контролю та модульного контрольного оцінювання на 100 бальну модульну оцінку відповідно 30 та 70 балів максимально. У разі пропуску модульного контрольного оцінювання здобувачем у графах контролю викладачі роблять позначку "н". Здобувач вищої освіти, який з поважних причин, підтверджених документально, не мав можливості брати участь у формах поточного контролю та виконати індивідуальне завдання і самостійну роботу, має право на відпрацювання у двотижневий термін після повернення, але до початку екзаменаційної сесії. Після завершення вивчення дисципліни викладач виводить підсумкову модульну оцінку як середнє арифметичне результатів двох модульних контролів (Модульних оцінок) округлену до цілих та виставляється за 100-бальною шкалою, шкалою ЄКТС та національною шкалою.

Форми модульного контролю. До модульного контролю допускаються всі студенти. Модульний контроль проводиться за розкладом, затвердженим деканом факультету. Результати модульного контролю мають бути внесені до відомості обліку успішності здобувачів вищої

освіти протягом 2-х днів після його проведення, але обов'язково до початку екзаменаційної сесії. У випадку відсутності студента на модульному контролі з поважної причини, підтвердженої документально, рішенням кафедри узгоджується додатковий розклад модульного контрольного оцінювання.

Форми підсумкового контролю. Форма підсумкового контролю полягає в оцінюванні рівня опанування студентами навчального матеріалу виключно на підставі результатів виконання ними певних видів робіт, зазначених у робочій програмі навчальної дисципліни. Оцінка за семестр з дисципліни виставляється після закінчення її вивчення та здачі заліка чи, як максимум підсумкової модульної оцінки та залікової оцінки.

Розподіл балів, які отримують здобувачі вищої освіти (модуль 1)

Поточне оцінювання та самостійна робота			Модульна контрольна робота	Сума
T1	T2	T3	70	100
10	10	10		

T1, T2, T3 – теми

Розподіл балів, які отримують здобувачі вищої освіти (модуль 2)

Поточне оцінювання та самостійна робота			Модульна контрольна робота	Сума
T1	T2	T3	70	100
10	10	10		

T1, T2, T3 – теми

Оцінювання окремих видів навчальної роботи з дисципліни

Вид діяльності здобувача вищої освіти	Модуль 1		Модуль 2	
	Кількість	Максимальна кількість балів (сумарна)	Кількість	Максимальна кількість балів (сумарна)
Практичні заняття	6	30	7	30
Модульна контрольна робота	1	70	1	70
Разом		100		100

Критерії оцінювання модульної контрольної роботи

Матеріал кожного модуля, який здобувачі вищої освіти повинні засвоїти протягом семестру, виноситься на одну з двох модульних контрольних робіт, що проводяться в семестр. Оцінювання модульного контролю здійснюється за шкалою від «0» до «70».

Здобувач вищої освіти, який не з'явився на модульну контрольну роботу, або ж його модульна оцінка складає від 0 до 34 балів, зобов'язаний скласти (перескласти) модуль до початку підсумкового контролю у строки, визначені викладачем дисципліни та погоджені деканатом факультету.

Критерії оцінювання підсумкового семестрового контролю

Оцінювання знань студента здійснюється за 100-бальною шкалою.

Залікова методика оцінювання. Підсумкова рейтингова дозалікова оцінка визначається як середнє арифметичне значення двох модульних балів.

До складання заліку допускаються здобувачі вищої освіти, які мають підсумковий рейтинговий бал не менше 35.

Здобувач вищої освіти, рейтинговий бал якого складає від 0 до 34 балів, зобов'язаний покращити його до початку заліку під час чергування викладачів на кафедрі у строки, визначені викладачем дисципліни та погоджені деканатом факультету. В протилежному випадку, здобувач не допускається до заліку, і у нього виникає академічна заборгованість.

У випадку, якщо за поточну успішність студент набрав більше 59 балів, то за його бажанням може бути виставлена відповідна набраним балам підсумкова оцінка з дисципліни з записом «зараховано» без складання заліку.

Здобувачі вищої освіти, рейтинговий бал яких становить від 35 до 59, залік здають обов'язково. Здобувач освіти може підвищити на заліку рейтинговий бал, при цьому, за результатами складання заліку оцінка не може бути менша за дозаліковий рейтинговий бал.

Залік проводиться в усній формі. Залікові завдання складаються з двох теоретичних питань та двох практичних завдань. Оцінка за залік вноситься у відомість обліку успішності.

Таблиця відповідності оцінок за різними шкалами оцінювання

Оцінка в балах	Оцінка ECTS	Екзаменаційна оцінка за національною шкалою
90–100	A	<i>зараховано</i>
82–89	B	<i>зараховано</i>
74–81	C	
64–73	D	<i>зараховано</i>
60–63	E	
35–59	FX	<i>Незараховано з можливістю повторного складання</i>
0–34	F	<i>Незараховано з обов'язковим повторним вивченням дисципліни</i>

Критерій оцінювання з дисципліни

— ” **зараховано** ” (90 та вище балів) заслуговує студент, який виявив всебічне і глибоке знання програмового матеріалу, вміння вільно виконувати завдання, передбачені програмою, засвоїв основну і ознайомився з додатковою літературою, розуміє взаємозв'язок головних понять дисципліни та їх значення для майбутньої професії;

— ” **зараховано** ” (82–89 балів) заслуговує студент, який виявив повне знання програмного матеріалу, успішно виконує передбачені програмою завдання, засвоїв основну літературу рекомендовану програмою, виявив систематичний характер знань з дисциплін і здатний до самостійного доповнення, але під час відповіді допустив деякі неточності;

— ” **зараховано** ” (74–81 балів) заслуговує студент, що виявив не цілком повне знання програмного матеріалу, не завжди успішно виконує передбачені програмою завдання, частково засвоїв основну літературу, рекомендовану програмою, виявив не систематичний характер знань з дисциплін і не завжди здатний до їх самостійного доповнення і під час відповіді допускає деякі неточності;

— ” **зараховано** ” (64–73 балів) заслуговує студент, що виявив знання основного програмного матеріалу в обсязі, що передбачені програмою, знайомий з основною рекомендованою

літературою. Як правило, оцінка “D” виставляється студентам, що допустили помилки у відповіді на заліку та при виконанні залікових завдань, але які

володіють необхідними знаннями для їх усунення за допомогою викладача;

— ” **зараховано** ” (60–63 балів) заслуговує студент, що виявив часткове знання основного програмового матеріалу, не завжди вмів виконувати завдання, передбачені програмою, знайомий лише частково з основною рекомендованою літературою. Як правило, оцінка “E” виставляється студентам, що допустили грубі помилки у відповіді на заліку та при виконанні залікових завдань, але які частково володіють

необхідними знаннями для їх усунення за допомогою викладача;

— ” **не зараховано** ” (35–59 балів) виставляється студенту, який виявив суттєві прогалини в знаннях основного програмового матеріалу, допустив принципові помилки у виконанні передбачених програмою завдань;

— ” **не зараховано** ” (0–34 балів) виставляється студенту коли протягом семестру він допустив грубі помилки у виконанні передбачених програмою завдань.

6. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

6.1. Зміст навчальної дисципліни

Модуль 1

Тема 1. Групи

Групи, підгрупи. Суміжні класи, теорема Лагранжа, нормальна підгрупа, фактор-група. Гомоморфізми груп. Основна теорема про гомоморфізми груп.

Тема 2. Абелеві групи.

Циклічні групи. Внутрішній і зовнішній прямий добуток груп. Будова скінченної абелевої групи

Тема 3. Кільця

Кільця, підкільця, ідеали, факторкільця. Гомоморфізми кілець. Основна теорема про гомоморфізми кілець. Кільця головних ідеалів. Евклідові кільця.

Модуль 2

Тема 1. Подільність в кільці

Відношення подільності на множині цілих чисел. Алгоритм Евкліда. Канонічний розклад натуральних чисел. Мультиплікативні функції. Мультиплікативна група кільця класів лишків.

Тема 2. Конгруентність чисел за модулем

Ознаки подільності чисел. Конгруенції. Властивості конгруенцій. Теорема Ферма-Ейлера. Алгебраїчні конгруенції 1-го степеня. Системи конгруенцій 1-го степеня. Алгебраїчні конгруенції 2-го степеня. Символ Лежандра.

Тема 3. Розв’язування рівнянь в цілих числах

Неперервні дроби. Підхідні дроби. Розв’язування лінійних діофантових рівнянь від двох змінних. Розв’язування деяких типів нелінійних діофантових рівнянь від двох змінних. Піфагорові трійки.

6.2. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин: 120					
	Форма навчання: денна					
	у тому числі					
	Усього	лекції	практичні (семінарські)	лабораторні	індивідуальна робота	самостійна робота
3-й семестр						
Модуль 1						
Тема 1. Групи.	20	6	4			10
Тема 2. Абелеві групи.	18	4	4			10
Тема 3. Кільця.	20	6	4			10
Модульна контрольна робота	2		2	-	-	-
Разом за модуль	60	16	14	-	-	30
Модуль 2						
Тема 1. Подільність в кільці.	18	4	4			10
Тема 2. Конгруентність чисел за модулем.	20	6	6			8
Тема 3. Розв'язування рівнянь в цілих числах.	20	4	4			12
Модульна контрольна робота	2		2	-	-	-
Разом за модуль	60	14	16			30
Разом за семестр	120	30	30	-	-	60

6.3. Тематики практичних занять

№ з/п	Назва теми	Кількість годин
Модуль 1		
1.	Групи, підгрупи. Суміжні класи, теорема Лагранжа, нормальна підгрупа. Фактор-група.	2
2.	Гомоморфізми груп. Основна теорема про гомоморфізми груп.	2
3.	Циклічні групи. Внутрішній і зовнішній прямий добуток груп.	2
4.	Будова скінченної абелевої групи	2
5.	Кільця, підкільця, ідеали, факторкільця. Гомоморфізми кілець. Основна теорема про гомоморфізми кілець.	2
6.	Кільця головних ідеалів. Евклідові кільця.	2
7.	Модульна контрольна робота	2
	Разом	14

Модуль 2		
1.	Відношення подільності на множині цілих чисел. Алгоритм Евкліда. Канонічний розклад натуральних чисел.	2
2.	Мультиплікативні функції. Мультиплікативна група кільця класів лишків.	2
3.	Ознаки подільності чисел. Конгруенції. Властивості конгруенцій. Теорема Ферма-Ейлера.	2
4.	Алгебраїчні конгруенції 1-го степеня. Системи конгруенцій 1-го степеня. Алгебраїчні конгруенції 2-го степеня. Символ Лежандра.	2
5.	Неперервні дроби. Підхідні дроби.	2
6.	Розв'язування лінійних діофантових рівнянь від двох змінних.	2
7.	Розв'язування деяких типів нелінійних діофантових рівнянь від двох змінних. Піфагорові трійки.	2
8.	Модульна контрольна робота	2
Разом		16
Разом за семестр		30

6.4. Самостійна робота

№ з/п	Назва теми	Кількість годин
Модуль 1		
1.	Групи, підгрупи. Суміжні класи, теорема Лагранжа, нормальна підгрупа. Фактор-група.	6
2.	Гомоморфізми груп. Основна теорема про гомоморфізми груп.	4
3.	Циклічні групи. Внутрішній і зовнішній прямий добуток груп.	6
4.	Будова скінченної абелевої групи	4
5.	Кільця, підкільця, ідеали, факторкільця. Гомоморфізми кілець. Основна теорема про гомоморфізми кілець.	6
6.	Кільця головних ідеалів. Евклідові кільця.	4
Разом		30
Модуль 2		
1.	Відношення подільності на множині цілих чисел. Алгоритм Евкліда. Канонічний розклад натуральних чисел.	6
2.	Мультиплікативні функції. Мультиплікативна група кільця класів лишків.	4
3.	Ознаки подільності чисел. Конгруенції. Властивості конгруенцій. Теорема Ферма-Ейлера.	4
4.	Алгебраїчні конгруенції 1-го степеня. Системи конгруенцій 1-го степеня. Алгебраїчні конгруенції 2-го степеня. Символ Лежандра.	6
5.	Неперервні дроби. Підхідні дроби.	4
6.	Розв'язування лінійних діофантових рівнянь від двох змінних.	4
7.	Розв'язування деяких типів нелінійних діофантових рівнянь від двох змінних. Піфагорові трійки.	2
Разом		30
Разом за семестр		60

7. ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВИКОРИСТАННЯ ЯКИХ ПЕРЕДБАЧАЄ НАВЧАЛЬНА ДИСЦИПЛІНА

Технічні засоби: система дистанційного навчання «Moodle», сервіс Google Meet.

8. РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основна література

1. Забавський Б., Андрійчук В., Гаталевич А., Пігура О. Загальна алгебра: навч. посібник. Львів : ЛНУ імені Івана Франка, 2018. 186 с.
2. Гудивок П.М., Кирилюк О.А., Погоріляк Є.Я., Тилищак О.А., Юрченко Н.В. Практикум з алгебри і теорії чисел. Ужгород: Видавництво УжНУ «Говерла», 2008. 64 с.
3. Ковальчук, Л. В. Прикладна алгебра: основні поняття алгебри та теорії чисел. Київ : НТУУ «КПІ», 2011.
4. Головащук Н.С., Є.А. Кочубінська Є.А., Овсієнко С.А. Практикум з прикладної алгебри.: для студентів механіко – математичного факультету. К., 2015. 59 с.
5. Безущак О.О., Ганюшкін О.Г. Елементи теорії чисел: Навчальний посібник. К.: Видавничо-поліграфічний центр “Київський університет”, 2003. 203 с.
6. Юрченко Н.В. Методичні вказівки до розв’язування діофантових рівнянь. Ужгород: ДВНЗ «УжНУ», 2015. 51 с.
7. Безущак О.О., Ганюшкін О.Г. Елементи теорії чисел: навчальний посібник. К.: ВПЦ «Київський університет», 2003.

Допоміжна література

1. Богуч В.М, Мухачов В.А. Криптографічні застосування елементарної теорії чисел. Навчальний посібник. К.: ДУІКТ, 2006. 126 с.
2. Стасюк М. Елементи математичних основ криптографії : навчальний посібник. Львів : ЛДУ БЖД, 2021. 216 с.
3. Безущак О.О., Ганюшкін О.Г. Завдання до практичних занять з алгебри і теорії чисел (теорія груп). К.: ВПЦ “Київський університет”, 2007. 103 с.
4. Головащук Н.С., Кочубінська Є.А., Овсієнко С.А. Збірник задач з теорії кілець (базовий курс) К.: ВПЦ «Київський університет», 2013. 86 с.

Інформаційні ресурси в мережі Інтернет

1. <https://dspace.uzhnu.edu.ua/jspui/handle/123456789/103> — репозитарій, методичні роботи науково-педагогічних працівників кафедри алгебри ДВНЗ «Ужгородський національний університет».
2. <http://e-learn.uzhnu.edu.ua> — сайт електронного навчання ДВНЗ «Ужгородський національний університет».
3. <http://www.nbuv.gov.ua> — Національна бібліотека України імені В. І. Вернадського.