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 МАЛЯР/
«27» ____06_____2025 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ТЕОРІЯ ЧИСЕЛ ТА ЕЛЕМЕНТИ КРИПТОГРАФІЇ

Рівень вищої освіти	**перший (бакалаврський)**
Галузь знань	**11 Математика і статистика**
Спеціальність	**111 Математика**
Освітня програма	**Комп'ютерна та бізнес-математика**
Статус дисципліни	**обов'язкова**
Мова навчання	**українська**

Ужгород 2025

Робоча програма навчальної дисципліни «**ТЕОРІЯ ЧИСЕЛ ТА ЕЛЕМЕНТИ КРИПТОГРАФІЇ**» для здобувачів вищої освіти галузі знань **11 Математика і статистика** спеціальності **111 Математика** освітньої програми **Комп'ютерна та бізнес-математика.**

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

Робочу програму розглянуто та затверджено на засіданні кафедри ***алгебри та диференціальних рівнянь***

протокол № 10, від 18.06.2025 р

Завідувач кафедри _____ Олександр РЕЙТІЙ

Схвалено науково-методичною комісією факультету математики та цифрових технологій

протокол № 10 від 26.06.2025 р

Голова науково-методичної комісії _____ Наталія ЮРЧЕНКО

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><td rowspan="2">Найменування показників</td><td colspan="2">Розподіл годин за навчальним планом</td></tr>
<tr><td>Денна форма навчання</td><td>Заочна форма навчання</td></tr>
<tr><td>Кількість кредитів ЄКТС –4</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Загальна кількість годин –120</td><td>2-ий</td><td>2-ий</td></tr>
<tr><td>Кількість модулів –2</td><td colspan="2">Семестр:</td></tr>
<tr><td rowspan="6">Тижневих годин
для денної форми навчання:

аудиторних –4

самостійної роботи студента –4</td><td>3-ій</td><td>3-ій, 4-ий</td></tr>
<tr><td colspan="2">Лекції:</td></tr>
<tr><td>30</td><td>10</td></tr>
<tr><td colspan="2">Практичні (семінарські):</td></tr>
<tr><td>30</td><td>10</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td rowspan="2">Вид підсумкового контролю: екзамен</td><td colspan="2">Лабораторні:</td></tr>
<tr><td>–</td><td>–</td></tr>
<tr><td rowspan="2">Форма підсумкового контролю: усна</td><td colspan="2">Самостійна робота:</td></tr>
<tr><td>60</td><td>100</td></tr>
</table>

2. МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою вивчення навчальної дисципліни **«Теорія чисел і елементи криптографії»** є ознайомлення студентів з сучасними методами, теоретичними положеннями та основними застосуваннями абстрактної алгебри та алгебраїчної теорії чисел в деяких задачах математики та криптології , сприяння розвитку логічного та аналітичного мислення студентів.

Відповідно до освітньої програми «Компютерна та бізнес-математика» спеціальності Математика, вивчення дисципліни сприяє формуванню у здобувачів вищої освіти таких загальних (ЗК) та спеціальних (СК) компетентностей:

− здатність до абстрактного мислення, аналізу та синтезу (ЗК-01);
− здатність застосовувати знання у практичних ситуаціях (ЗК-02);
− знання й розуміння предметної області та професійної діяльності (ЗК-03);
− здатність формулювати проблеми математично та в символьній формі з метою спрощення їхнього аналізу й розв'язання (СК-01) ;
− здатність до аналізу математичних структур, у тому числі до оцінювання обґрунтованості й ефективності використовуваних математичних підходів (СК-08).

3. ПЕРЕДУМОВИ ДЛЯ ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Передумовами вивчення навчальної дисципліни «**Теорія чисел і елементи криптографії**» є опанування таких навчальних дисциплін (НД) освітньої програми (ОП):

НД Алгебра (ОК.07)
НД Лінійна алгебра (ОК.08)

4. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Відповідно до освітньої програми **«Теорія чисел і елементи криптографії»,** вивчення навчальної дисципліни повинно забезпечити досягнення здобувачами вищої освіти таких програмних результатів навчання (ПРН)**:**

Програмні результати навчання	Шифр ПРН
Знати основні етапи історичного розвитку математичних знань і парадигм, розуміти сучасні тенденції в математиці.	РН-01
Знати принципи modus ponens (правило виведення логічних висловлювань) та modus tollens (доведення від супротивного) і використовувати умови, формулювання, висновки, доведення та наслідки математичних тверджень.	РН-03
Розуміти фундаментальну математику на рівні, необхідному для досягнення інших вимог освітньої програми.	РН-04
Розв'язувати задачі придатними математичними методами, перевіряти умови виконання математичних тверджень, коректно переносити умови та твердження на нові класи об'єктів, знаходити й аналізувати відповідності між поставленою задачею й відомими моделями.	РН-10
Розв'язувати конкретні математичні задачі, які сформульовано у формалізованому вигляді; здійснювати базові перетворення математичних моделей.	РН-11

Знати теоретичні основи і застосовувати алгебраїчні методи для вивчення математичних структур.	РН-15

Очікувані результати навчання з дисципліни
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, прямий добуток груп, кільце, комутативне кільце, кільце з одиницею, найбільший спільний дільник і найменше спільне кратне елементів кільця, кільце класів лишків, мультиплікативна функція, конгруенція 1-го степеня, конгруенція n-го степеня, поняття симетричні та асиметричні шифри, деякі криптоалгоритми та криптопротоколи.
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 встановлювати ізоморфізм груп; встановлення ізоморфізм груп; знаходження порядку елемента групи; побудову фактор-групи; здатність встановлювати ізоморфізм груп; здатність знаходити кількість попарно неізоморфних абелевих груп заданого порядку; здатність перевіряти, чи ізоморфні задані абелеві групи; обчислення кількості елементів заданого порядку в абелевій групі; знаходження підгруп скінченних абелевих груп; описувати гомоморфізми заданих абелевих груп; здатність розкладати задану абелеву групу в прямий добуток циклічних груп; здатність перевіряти, чи буде кільцем задана алгебраїчна структура; здатність перевіряти, чи задане відображення є гомоморфізмом кілець обчислення найбільшого спільного дільника елементів кільця; здатність розв’язувати лінійні конгруенції; вміти застосовувати матриці для шифрування та дешифрування, вміти застосовувати деякі симетричні алгоритми.
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 кілець класів лишків до розв’язання деяких задач з шифрування та дешифрування.

5. ЗАСОБИ ДІАГНОСТИКИ ТА КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

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 змістових модулів; перевірка домашніх робіт; опитування під час практичних занять; підсумкова модульна контрольна робота. Для діагностики знань використовується кредитно-рейтингова система за 100-бальною шкалою оцінювання.

Форми контролю та критерії оцінювання результатів навчання

Форми поточного контролю. Поточний контроль знань студентів упродовж одного семестру включає бали за роботу на практичних заняттях, а також оцінювання всіх видів самостійної роботи. Оцінювання роботи на практичних заняттях, індивідуальної та самостійної роботи здійснюється за шкалою від «0» до «10». У разі пропуску заняття 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 до навчання, але до початку екзаменаційної сесії. Студент, який не використав надане йому право у встановлений термін або пропустив заняття без поважних причин, отримує за кожне пропущення заняття 0 балів. Після завершення вивчення дисципліни викладач виводить середньозважений бал, який переводиться у 100-бальну шкалу з відповідним ваговим коефіцієнтом. Підрахунки середньозваженого балу здійснюють з точністю до другого знака після коми. Кількість балів за поточний контроль округлюють до цілих.

Форми модульного контролю. До модульного контролю допускаються всі студенти. Модульний контроль проводиться за розкладом, затвердженим деканом факультету. Оцінювання модульного контролю здійснюється за шкалою від «0» до «70». 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, деканатом складається додатковий розклад.

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, з якої передбачений екзамен, виставляється після закінчення її вивчення (до початку екзаменаційної сесії) за результатами поточного (ваговий коефіцієнт – 0,3) та модульного (ваговий коефіцієнт – 0,7) контролю.

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

Поточне оцінювання та самостійна робота									**Модульна контрольна робота**	**Сума**
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	Т9	**70**	**100**
3	3	3	3	3	3	4	4	4		

Т1, Т2 ... – теми

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

Поточне оцінювання та самостійна робота												**Модульна контрольна робота**	**Сума**
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	Т9	Т10	Т11	Т12	**70**	**100**
3	3	3	3	3	2	3	2	2	2	2	2		

Т1, Т2 ... – 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 (семінарські) заняття		10		10
Виконання самостійних домашніх робіт		20		20
Модульна контрольна робота	1	70	1	70
Разом		**100**		**100**

Критерії оцінювання модульної контрольної роботи

Оцінювання модульного контролю здійснюється за шкалою від «0» до «70».

Критерії оцінювання підсумкового семестрового контролю

Оцінювання знань студента здійснюється за 100-бальною шкалою (для екзаменів і заліків).

Максимальна кількість балів при оцінюванні знань студентів з дисципліни, яка завершується екзаменом, становить за поточну успішність 100 балів, на екзамені – 100 балів.

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 без складання іспиту.

При оформленні документів за екзаменаційну сесію використовується таблиця відповідності оцінювання знань студентів за різними системами.

Шкала оцінювання: національна та ECTS

Оцінка в балах	Оцінка ECTS	Екзаменаційна оцінка за національною шкалою
90–100	**A**	*Відмінно*
82–89	**B**	*Добре*
74–81	**C**	
64–73	**D**	*Задовільно*
60–63	**E**	
35–59	**FX**	*Незадовільно з можливістю повторного складання*
0–34	**F**	*Незадовільно з обов'язковим повторним вивченням дисципліни*

Критерій оцінювання з дисципліни

— **"A"** (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;

— **"B"** (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;

— **"C"** (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;

— **"D"** (64–73 балів) заслуговує студент, що виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та майбутньої роботи за професією, вміє виконувати завдання, передбачені програмою, знайомий з основною рекомендованою літературою. Як правило, оцінка "D" виставляється студентам, що допустили помилки у відповіді на екзамені та при виконанні екзаменаційних завдань, але які володіють необхідними знаннями для їх усунення за допомогою викладача;

— **"E"** (60–63 балів) заслуговує студент, що виявив часткове знання основного програмового матеріалу в обсязі, необхідному для подальшого навчання та майбутньої роботи за професією, не завжди вміє виконувати завдання, передбачені програмою, знайомий лише частково з основною рекомендованою літературою. Як правило, оцінка "E" виставляється студентам, що допустили грубі помилки у відповіді на екзамені та при виконанні екзаменаційних завдань, але які частково володіють необхідними знаннями для їх усунення за допомогою викладача;

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

— **"F"** (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
Теорія груп та кілець

Тема 1. Групи, підгрупи.
Тема 2. Суміжні класи, теорема Лагранжа, нормальна підгрупа, фактор-група.
Тема 3. Гомоморфізми груп. Основна теорема про гомоморфізми груп.
Тема 4. Циклічні групи.
Тема 5. Внутрішній і зовнішній прямий добуток груп.
Тема 6. Абелеві групи. Будова скінченної абелевої групи
Тема 7. Кільця, підкільця, ідеали, факторкільця.
Тема 8. Гомоморфізми кілець. Основна теорема про гомоморфізми кілець.
Тема 9. Кільця головних ідеалів. Евклідові кільця.

Модуль 2
Теорія конгруенцій та математичні основи криптографії

Тема 1. Відношення подільності на множині цілих чисел. Канонічний розклад натуральних чисел. Мультиплікативні функції.
Тема 2. Мультиплікативна група кільця класів лишків.
Тема 3. Конгруенції. Теорема Ферма-Ейлера. Алгебраїчні конгруенції 1–го степеня.
Тема 4. Системи конгруенцій 1-го степеня.
Тема 5. Алгебраїчні конгруенції n–го степеня.
Тема 6. Алгебраїчні конгруенції 2–го степеня. Символ Лежандра.
Тема 7. Застосування матриць для шифрування.
Тема 8. Шифр Хілла. Шифр Віженера.
Тема 9. Симетричні шифри.

Тема 10. Криптоалгоритми Ель-Гамаля.
Тема 11. Можливі атаки на шифри.
Тема 12. Криптографічні протоколи.

6.2. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин: 120						Кількість годин: 120					
	Форма навчання: денна						Форма навчання: заочна					
	Усього	у тому числі					Усього	у тому числі				
		лекції	практичні (семінарські)	лабораторні	індивідуальна робота	самостійна робота		лекції	практичні (семінарські)	лабораторні	індивідуаль-на робота	самостійна робота
3-й семестр												
Модуль 1												
Теорія груп та кілець												
Тема 1. Групи, підгрупи.	5	1	2	-	-	2	5	0,5	0,5	-	-	4
Тема 2. Суміжні класи, теорема Лагранжа, нормальна підгрупа, фактор-група.	5	1	2	-	-	2	6	0,5	0,5	-	-	5
Тема 3. Гомоморфізми груп. Основна теорема про гомоморфізми груп.	5	1	2	-	-	2	5	0,5	0,5	-	-	4
Тема 4. Циклічні групи.	5	1	1	-	-	3	5	0,5	0,5	-	-	4
Тема 5. Внутрішній і зовнішній прямий добуток груп.	5	1	1	-	-	3	5	0,5	0,5	-	-	4
Тема 6. Абелеві групи. Будова скінченної абелевої групи	5	1	1	-	-	3	5	0,5	0,5	-	-	4
Тема 7. Кільця, підкільця, ідеали, факторкільця.	6	2	2	-	-	2	6	0,5	0,5	-	-	5
Тема 8. Гомоморфізми кілець. Основна теорема про гомоморфізми кілець.	6	2	1	-	-	3	6	0,5	0,5	-	-	5
Тема 9. Кільця головних ідеалів. Евклідові кільця.	6	2	2	-	-	2	6	-	-	-	-	6
Модульна контрольна робота	2	2	-	-	-	-	1	1	-	-	-	-
Разом за модуль	50	14	14	-	-	22	50	5	4	-	-	41
Модуль 2												
Елементи теорії конгруенцій та математичні основи криптографії												
Тема 1. Відношення подільності на множині цілих чисел. Канонічний розклад натуральних чисел. Мультиплікативні функції.	6	2	2	-	-	2	6	0,5	0,5	-	-	5
Тема 2. Мультиплікативна група кільця класів лишків.	6	1	1	-	-	4	6	0,5	0,5	-	-	5
Тема 3. Конгруенції. Теорема Ферма-Ейлера. Алгебраїчні конгруенції 1–го степеня.	6	1	2	-	-	3	6	0,5	0,5	-	-	5
Тема 4. Системи конгруенцій 1-го	5	1	2	-	-	2	5	0,5	0,5	-	-	4

степеня.												
Тема 5. Алгебраїчні конгруенції n–го степеня.	5	1	2	-	-	2	5	-	0,5	-	-	4,5
Тема 6. Алгебраїчні конгруенції 2–го степеня. Символ Лежандра.	6	1	2	-	-	3	6	0,5	0,5	-	-	5
Тема 7. Застосування матриць для шифрування.	6	1	1	-	-	4	6	0,5	0,5	-	-	5
Тема 8. Шифр Хілла. Шифр Віженера.	6	1	1	-	-	4	6	0,5	0,5	-	-	5
Тема 9. Симетричні шифри.	6	1	1	-	-	4	6	-	0,5	-	-	5,5
Тема 10. Криптоалгоритми Ель-Гамаля.	6	2	1	-	-	3	6	0,5	0,5	-	-	5
Тема 11. Можливі атаки на шифри.	5	1	1	-	-	3	5		0,5	-	-	4,5
Тема 12. Криптографічні протоколи.	5	1	1	-	-	3	6	-	0,5	-	-	5,5
Модульна контрольна робота	2	2	-	-	-	-	1	1	-	-	-	-
Разом за модуль	70	16	16	-	-	45	70	5	6	-	-	59
Разом за семестр	120	30	30	-	-	60	120	10	10	-	-	100

6.3. Теми практичних (семінарських, лабораторних) занять

№ з/п	Назва теми	Кількість годин	
		Денна форма	*Заочна Форма*
1.	Групи, підгрупи.	2	0,5
2	Суміжні класи, теорема Лагранжа, нормальна підгрупа, факторгрупа.	2	0,5
3	Гомоморфізми груп. Основна теорема про гомоморфізми груп.	2	0,5
4	Циклічні групи.	1	0,5
5	Внутрішній і зовнішній прямий добуток груп.	1	0,5
6	Абелеві групи. Будова скінченної абелевої групи.	1	0,5
7	Кільця, підкільця, ідеали, факторкільця.	2	0,5
8	Гомоморфізми кілець. Основна теорема про гомоморфізми кілець.	1	0,5
9.	Кільця головних ідеалів. Евклідові кільця.	2	-
10.	Відношення подільності на множині цілих чисел. Канонічний розклад натуральних чисел. Мультиплікативні функції.	2	0,5
11.	Мультиплікативна група кільця класів лишків.	1	0,5
12.	Конгруенції. Теорема Ферма-Ейлера. Алгебраїчні конгруенції 1–го степеня.	2	0,5
13.	Системи конгруенцій 1-го степеня.	2	0,5
14.	Алгебраїчні конгруенції n–го степеня.	2	0,5
15.	Алгебраїчні конгруенції 2–го степеня. Символ Лежандра.	2	0,5
16.	Застосування матриць для шифрування.	1	0,5
17.	Шифр Хілла. Шифр Віженера.	1	0,5
18.	Симетричні шифри.	1	0,5
19.	Криптоалгоритми Ель-Гамаля.	1	0,5
20.	Можливі атаки на шифри.	1	0,5
21.	Криптографічні протоколи.	1	0,5
Разом		**30**	**10**

6.4. Самостійна робота

№ з/п	Назва теми	Кількість годин	
		Денна форма	*Заочна форма*
1.	Групи, підгрупи.	2	4
2.	Суміжні класи, теорема Лагранжа, нормальна підгрупа, фактор-група.	2	5
3.	Гомоморфізми груп. Основна теорема про гомоморфізми груп.	2	4
4.	Циклічні групи.	3	4
5.	Внутрішній і зовнішній прямий добуток груп.	3	4
6.	Абелеві групи. Будова скінченної абелевої групи	3	4
7.	Кільця, підкільця, ідеали, факторкільця.	2	5
8.	Гомоморфізми кілець. Основна теорема про гомоморфізми кілець.	3	5
9.	Кільця головних ідеалів. Евклідові кільця.	2	6
10.	Відношення подільності на множині цілих чисел. Канонічний розклад натуральних чисел. Мультиплікативні функції.	2	5
11.	Мультиплікативна група кільця класів лишків.	4	5
12.	Конгруенції. Теорема Ферма-Ейлера. Алгебраїчні конгруенції 1–го степеня.	3	5
13.	Системи конгруенцій 1-го степеня.	2	4
14.	Алгебраїчні конгруенції n–го степеня.	2	4,5
15.	Алгебраїчні конгруенції 2–го степеня. Символ Лежандра.	3	5
16.	Застосування матриць для шифрування.	4	5
17.	Шифр Хілла. Шифр Віженера.	4	5
18.	Симетричні шифри.	4	5,5
19.	Криптоалгоритми Ель-Гамаля.	3	5
20.	Можливі атаки на шифри.	3	4,5
21.	Криптографічні протоколи.	3	5,5
	Разом	**60**	**100**

7. 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.