

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет імені Івана Франка
Механіко-математичний факультет
Кафедра алгебри, топології та основ математики

Затверджено

на засіданні кафедри алгебри, топології та
основ математики
механіко-математичного факультету
Львівського національного університету
імені Івана Франка
(протокол № 1 від 29.08.2022)



Завідувач кафедри:

проф. Банах Т.О.

Силабус з навчальної дисципліни

“ Теорія чисел”,

що викладається в межах ОПП “Комп’ютерна алгебра, криптологія та теорія ігор”, “Комп’ютерний аналіз математичних моделей”, “Математика. Математична економіка та економетрика”, “Середня освіта (Математика)” першого (бакалаврського) рівня вищої освіти для здобувачів із спеціальностей 111 – Математика та 014 – Середня освіта

Львів 2022

Назва дисципліни	Теорія чисел
Адреса викладання дисципліни	м. Львів, вул. Університетська 1
Факультет та кафедра, за якою закріплена дисципліна	Механіко-математичного факультет Кафедра алгебри, топології та основ математики
Галузь знань, шифр та назва спеціальності	Галузь знань: 11 Математика і статистика Спеціальність: 111 Математика; Галузь знань: 01 Освіта/Педагогіка Спеціальність: 014 Середня освіта (Математика)
Викладачі дисципліни	Романів Олег Миколайович , кандидат фізико-математичних наук, доцент, доцент кафедри алгебри, топології та основ математики
Контактна інформація викладачів	oleh.romaniv@lnu.edu.ua
Консультації з питань навчання по дисципліні відбуваються	Консультацію з теоретичної чи практичної частини курсу можна отримати на нараді MS Teams і групі курсу в Telegram у будь-який зручний для студентів та викладача час, а також очно в день проведення лекцій чи практичних занять за попередньою домовленістю.
Сторінка курсу	http://mmf.lnu.edu.ua/algstu/302
Інформація про дисципліну	Дисципліна “Теорія чисел” є нормативною дисципліною зі спеціальності 111 Математика для освітніх програм “Комп’ютерна алгебра, криптологія і теорія ігор”, “Комп’ютерний аналіз математичних моделей”, “Математика. Математична економіка та економетрика”, а також зі спеціальності 014 – Середня освіта для освітньої програми “Середня освіта (Математика)”. Вона викладається в 4-му семестрі в обсязі 3 кредити (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Навчальну дисципліну розроблено таким чином, щоб надати здобувачам першого (бакалаврського) рівня необхідні знання для отримання загальних і фахових компетенцій з теорії чисел, які дозволять засвоювати пов’язані з нею дисципліни та використовувати набуті знання в професійній діяльності. Ця діяльність може, зокрема, бути пов’язаною з побудовою і дослідженням математичних моделей захисту інформації, основами криптографії.
Мета та цілі дисципліни	Мета: ознайомлення з основними поняттями та методами теорії чисел. Цілі: викласти основні положення теорії чисел, ознайомити з методами розв’язування задач з теорії чисел, які можуть бути використані в математичними моделями різних природних процесів.
Література для вивчення дисципліни	1. <i>О.М. Романів</i> . Електронний текст лекцій по курсу «Теорія чисел» // http://mmf.lnu.edu.ua/algstu/302 2. <i>О.М. Романів</i> . Електронний текст матеріалів для практичних занять по курсу «Теорія чисел» // http://mmf.lnu.edu.ua/algstu/302 3. <i>Андрійчук В.І., Забавський Б.В.</i> Алгебра і теорія чисел // -Львів. -2005..

	<p>4. <i>Flath D. E.</i> Introduction to Number Theory // American Mathematical Society, 2018</p> <p>5. <i>Dujella A.</i> Number Theory // Školska knjiga, 2021.</p> <p>6. <i>Завало С.Т. та інші.</i> Алгебра та теорія чисел. Практикум. Частина 2 // Київ: Вища школа, 1996.</p> <p>7. Онлайн-курс «Number Theory and Cryptography» на Coursera: https://www.coursera.org/learn/number-theory-cryptography</p>
Обсяг курсу	<p>Загальний обсяг: 90 годин. Аудиторних занять: 32 год., з них 16 год. лекцій та 16 годин практичних занять.</p> <p>Самостійна робота: 58 год. Кредитів: 3.</p>
Очікувані результати навчання	<p><u>В результаті вивчення даного курсу студент повинен знати:</u> основні поняття абстрактної теорії чисел, зокрема: просте число, основна теорема арифметики, теореми Ферма, Ейлера, Вільсона, ланцюговий дріб, конгруенція в кільці цілих чисел, квадратичний лишок та нелишок, символ Лежандра, квадратичний закон;</p> <p>вміти: перетворювати конгруенції у еквівалентні, розкласти дійсне число в ланцюговий дріб, застосувати алгоритм Евкліда для знаходження НСД цілих чисел, знаходити кількість і суму всіх дільників числа, значення функції Ейлера, застосовувати ланцюгові дроби до знаходження раціонального наближення дійсних чисел, розв'язувати лінійні конгруенції з одним невідомим та їх системи, розв'язувати лінійні діофантові рівняння з використанням конгруенцій та ланцюгових дроби, перевіряти, чи буде задане число квадратичним лишком за модулем n, знаходити значення символу Лежандра.</p> <p>Після успішного завершення курсу студент має набути такі загальні компетентності (ЗК) та спеціальні (фахові) компетентності (СК):</p> <p>ЗК-1 Здатність до абстрактного мислення, аналізу та синтезу;</p> <p>ЗК-2 Здатність застосовувати знання у практичних ситуаціях;</p> <p>ЗК-3 Знання й розуміння предметної області та професійної діяльності;</p> <p>ЗК-7 Здатність учитися і оволодівати сучасними знаннями;</p> <p>ЗК-9 Здатність приймати обґрунтовані рішення.</p> <p>СК-1 Здатність формулювати проблеми математично та в символічній формі з метою спрощення їхнього аналізу й розв'язання;</p> <p>СК-2 Здатність подавати математичні міркування та висновки з них у формі, придатній для цільової аудиторії, а також аналізувати та обговорювати математичні міркування інших осіб, залучених до розв'язання тієї самої задачі;</p> <p>СК-3 Здатність здійснювати міркування та виокремлювати ланцюжки міркувань у математичних доведеннях на базі аксіоматичного підходу, а також розташовувати їх у логічну послідовність, у тому числі відрізняти основні ідеї від деталей і технічних викладок;</p> <p>СК-4 Здатність конструювати формальні доведення з аксіом та постулатів і відрізняти правдоподібні аргументи від формально бездоганних;</p> <p>СК-8 Здатність до аналізу математичних структур, у тому числі до оцінювання обґрунтованості й ефективності використовуваних математичних підходів,</p>

	<p>і здобути такі програмні результати навчання (РН):</p> <p>РН-1 Знати основні етапи історичного розвитку математичних знань і парадигм, розуміти сучасні тенденції в математиці;</p> <p>РН-3 Знати принципи <i>modus ponens</i> (правило виведення логічних висловлювань) та <i>modus tollens</i> (доведення від супротивного) і використовувати умови, формулювання, висновки, доведення та наслідки математичних тверджень;</p> <p>РН-4 Розуміти фундаментальну математику на рівні, необхідному для досягнення інших вимог освітньої програми;</p> <p>РН-7 Пояснювати математичні концепції мовою, зрозумілою для нефахівців у галузі математики;</p> <p>РН-10 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;</p> <p>РН-11 Розв'язувати конкретні математичні задачі, які сформульовано у формалізованому вигляді; здійснювати базові перетворення математичних моделей.</p>
Ключові слова	Просте число, основна теорема арифметики, теорема Ферма, теорема Ейлера, ланцюговий дріб, конгруенція в кільці цілих чисел, квадратичний лишок, символ Лежандра, символ Якобі, квадратичний закон взаємності.
Формат курсу	Лекції та практичні заняття, контрольні роботи, колоквиуми і консультації.
Теми	Див. Схема курсу
Підсумковий контроль, форма	Іспит в 4-ому семестрі.
Пререквізити	Для вивчення даного курсу студенти повинні мати базові знання з: <ul style="list-style-type: none"> - лінійної алгебри та аналітичної геометрії, - математичного аналізу.
Навчальні методи та техніки, які будуть використовуватися під час викладання	Проведення лекцій і практичних занять.

курсу	
Необхідне обладнання	Комп'ютер із необхідним програмним забезпеченням, доступ до Internet мережі.
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	<p>Оцінювання проводиться за 100-бальною шкалою.</p> <p>Бали нараховуються так: контрольні роботи №1, №2 : $2 \times 10 = 20$; колоквиуми №1, №5: $2 \times 10 = 20$; самостійні роботи -- $8 \times 0,5 = 4$; премія за активну роботу на заняттях -- 6; всього – 50 за роботу в семестрі.</p> <p>Іспит – 50. Всього – 100.</p> <p>Остаточна кількість балів, які отримує студент на іспиті: загальна кількість балів, набраних за семестр і на іспиті.</p> <p><i>Примітка: Самостійні роботи студенти пишуть під час проведення практичних занять для перевірки засвоєння ними матеріалу цього заняття (5-10 хв). Написанням самостійних робіт також є контролем за відвідуванням занять, оскільки навіть за незначний результат самостійної роботи виставляється якась частина максимальної кількості балів за цю роботу і це фіксується в журналі.</i></p> <p>Академічна доброчесність: Очікується, що роботи студентів будуть оригінальними дослідженнями чи міркуваннями. Списування та втручання в роботу інших студентів становлять, але не обмежують, приклади можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в написанні завдань є підставою для її незарахування викладачем, незалежно від масштабів плагіату чи обману.</p> <p>Відвідання занять є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та практичні заняття курсу. Студенти повинні інформувати викладача про неможливість відвідати заняття. У будь-якому випадку студенти зобов'язані дотримуватися термінів визначених для виконання всіх видів робіт, передбачених курсом.</p> <p>Література. Уся література, яку студенти не зможуть знайти самостійно, буде надана викладачем виключно в освітніх цілях без права її передачі третім особам. Студенти заохочуються до використання також й іншої літератури та джерел, яких немає серед рекомендованих.</p> <p>Політика виставлення балів. Враховуються бали, набрані при поточному контролі та бали підсумкового тестування. При цьому обов'язково враховуються присутність на заняттях та активність студента під час практичного заняття; недопустимість пропусків та запізнень на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття в цілях не пов'язаних з навчанням; списування та плагіат; несвоєчасне виконання поставленого завдання і т. ін.</p> <p>Жодні форми порушення академічної доброчесності не толеруються.</p>
Питання до заліку чи екзамену	<p>Відношення подільності. Ділення з остачею. Прості та складені числа. НСД і НСК. Взаємно прості числа. Числові функції. Системи числення. Ланцюгові дроби. Конгруенції в кільці цілих чисел та їх найпростіші властивості. Класи лишків. Повна і зведена системи лишків за даним модулем. Теорема Ейлера та Ферма. Конгруенції першого степеня з одним невідомим та їх застосування. Конгруенції вищих степенів з одним невідомим. Конгруенції другого степеня. Квадратичні лишки, квадратичні</p>

	нелишки, символ Лежандра. Порядок числа. Первісні корені. Індеси за простим модулем. Арифметичні застосування теорії конгруенцій. <i>Додаткові завдання розміщені на сторінці курсу.</i>
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.

Схема курсу “Теорія Чисел”

Тиж- день	Лекції		Практичні заняття		СР К-ть год Л-ра
	Назва теми	К- сть год	Назва теми	К- сть год	
1	Тема №1. Арифметика цілих та натуральних чисел	2			2 [1-7]
2			Відношення подільності. Ділення з остачею. Прості та складені числа. НСД і НСК. Взаємно прості числа	2	2 [1-7]
3	Тема №2. Числові функції. Системи числення	2			2 [1-7]
4			Числові функції. Системи числення	2	2 [1-7]
3	Тема №3. Ланцюгові дроби	2			2 [1-7]
			Ланцюгові дроби	2	2 [1-7]
5	Колоквіум № 1	2			2 [1-7]
6			Контрольна робота № 1	2	2 [1-7]
7	Тема №4. Конгруенції і кільця класів лишків	2			2 [1-7]
8			Класи лишків. Повна і зведена	2	2

			системи лишків за даним модулем. Теорема Ейлера та Ферма.		[1-7]
9	Тема №5. Конгруенції з невідомою. Конгруенції вищих степенів	2			2 [1-7]
10			Конгруенції першого степеня з одним невідомим та їх застосування. Конгруенції вищих степенів з одним невідомим.	2	2 [1-7]
11	Тема №6. Степеневі лишки. Первісні корені. Індекси	2			2 [1-7]
12			Конгруенції другого степеня. Квадратичні лишки, квадратичні нелишки, символ Лежандра. Порядок числа. Первісні корені. Індекси за простим модулем. Арифметичні застосування теорії конгруенцій	2	2 [1-7]
15	Колоквіум № 2	2			2 [1-7]
16			Контрольна робота №2	2	2 [1-7]
	Разом за семестр	16		16	32
	Лектор Романів О.М.		Викладач Романів О.М.		

Примітка: В [1] викладений повністю весь теоретичний матеріал по даному курсу, а --- в [2] --- матеріали до всіх практичних занять.