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 р.)

Завідувач кафедри: проф. Банах Т.О.

_____

Силабус з навчальної дисципліни

“ Теорія чисел ”,

що викладається в межах ОПП “Комп’ютерна алгебра, криптологія і 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 (предметна спеціальність 014.04 Середня освіта (Математика))

Львів 2022

Назва дисципліни	**Теорія чисел**
Адреса викладання дисципліни	м. Львів, вул. Університетська 1
Факультет та кафедра, за якою закріплена дисципліна	Механіко-математичний 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) Предметна спеціальність 014.04 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. *О.М. Романів.* Електронний текст лекцій по курсу «Теорія чисел» // http://mmf.lnu.edu.ua/algstu/302 2. *О.М. Романів.* Електронний текст матеріалів для практичних занять по курсу «Теорія чисел» // http://mmf.lnu.edu.ua/algstu/302 3. *Андрійчук В.І., Забавський Б.В.* Алгебра і теорія чисел // -Львів. -2005.. 4. *Flath D. E.* Introduction to Number Theory // American Mathematical Society, 2018

	5. *Dujella A.* Number Theory // Školska knjiga, 2021. 6. *Завало С.Т. та інші.* Алгебра та теорія чисел. Практикум. Частина 2 // Київ: Вища школа,1996. 7. Онлайн-курс «Number Theory and Cryptography» на Coursera: https://www.coursera.org/learn/number-theory-cryptography
Обсяг курсу	**Загальний обсяг:** 90 годин. Аудиторних занять: 32 год., з них 16 год. лекцій та 16 годин практичних занять. Самостійна робота: 58 год.
Очікувані результати навчання	В результаті вивчення даного курсу студент повинен **знати:** 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; **вміти:** перетворювати конгруенції у еквівалентні, розкладати 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 дробів, перевіряти, чи буде задане число квадратичним лишком за модулем n, знаходити значення символу Лежандра. Після успішного завершення курсу студент має набути такі **загальні компетентності (ЗК)** та **спеціальні** (фахові) **компетентності (СК):** ЗК-1 Здатність до абстрактного мислення, аналізу та синтезу; ЗК-2 Здатність застосовувати знання у практичних ситуаціях; ЗК-3 Знання й розуміння предметної області та професійної діяльності; ЗК-7 Здатність учитися і оволодівати сучасними знаннями; ЗК-9 Здатність приймати обґрунтовані рішення. СК-1 Здатність формулювати проблеми математично та в символьній формі з метою спрощення їхнього аналізу й розв'язання; 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; 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; СК-4 Здатність конструювати формальні доведення з аксіом та постулатів і відрізняти правдоподібні аргументи від формально бездоганних; СК-8 Здатність до аналізу математичних структур, у тому числі до оцінювання обґрунтованості й ефективності використовуваних математичних підходів і здобути такі програмні **результати навчання** (**РН**): РН-1 Знати основні етапи історичного розвитку математичних знань і парадигм, розуміти сучасні тенденції в математиці; РН-3 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-4 Розуміти фундаментальну математику на рівні, необхідному для досягнення інших вимог освітньої програми;

	РН-7 Пояснювати математичні концепції мовою, зрозумілою для нефахівців у галузі математики; 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; РН-11 Розв'язувати конкретні математичні задачі, які сформульовано у формалізованому вигляді; здійснювати базові перетворення математичних моделей.
Ключові слова	Просте число, алгоритм Евкліда, 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	Очний
Теми	Див. **Схема курсу**
Підсумковий контроль, форма	Іспит в 4-ому семестрі.
Пререквізити	Для вивчення даного курсу студенти повинні мати базові знання з: - лінійної алгебри та аналітичної геометрії, - математичного аналізу.
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Основними методами навчання, що використовуються в процесі викладання навчальної дисципліни «Теорія чисел» є: • метод передачі і сприйняття навчальної інформації, пробудження наукового інтересу (розповідь, пояснення, бесіда, лекція, презентація, демонстрація, спостереження, аналіз); • метод практично-орієнтованого засвоєння курсу з допомогою розв'язування задач за темами курсу для набуття умінь і практичних навичок (практичні заняття); • метод контролю з допомогою періодичного складання колоквіумів та контрольних робіт за тематикою лекційних та практичних занять; • метод самостійного засвоєння студентами навчального матеріалу у вигляді виконання домашніх завдань та розв'язування задач підвищеної складності, зокрема на доведення, з визначених тем курсу на підставі самостійно опрацьованої базової літератури та додаткових джерел інформації, інтернет-ресурсів з метою конкретизації й поглиблення базових знань, необхідних умінь та практичних навичок (самостійна робота); • інтерактивні методи (демонстраційні вправи, мозковий штурм, дискусії, діалогова форма набуття знань, обговорення складних дискусійних питань і проблем тощо) на лекціях, лабораторних заняттях та консультаціях. Під час навчання застосовуватимуться лекції, презентації, комплексні завдання, електронні матеріали з навчального курсу, спільні розробки, практично-орієнтоване навчання, інтерактивні методи, виконання індивідуальних завдань.

Необхідне обладнання	Для вивчення навчальної дисципліни «Теорія чисел» потрібно: дошка, крейда, навчальні посібники, мультимедійний проектор, комп'ютер, доступ до мережі «Інтернет», доступ до платформ Microsoft Teams, Zoom, Telegram, електронна пошта.
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються так: контрольні роботи №1, №2 : 2 х 10 = 20; колоквіуми №1, №2: 2 х 10 = 20; самостійні роботи -- 8 х 0,5 =4; премія за активну роботу на заняттях -- 6; всього – 50 за роботу в семестрі. **Іспит** – 50. Всього – 100. **Остаточна кількість балів**, які отримує студент на іспиті: загальна кількість балів, набраних за семестр і на іспиті. *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.* **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 незарахуванння викладачем, незалежно від масштабів плагіату чи обману. **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. **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. **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. **Жодні форми порушення академічної доброчесності не толеруються.**
Питання до екзамену	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. Теореми Ейлера та Ферма. Конгруенції першого степеня з одним невідомим та їх застосування. Конгруенції вищих степенів з одним невідомим. Конгруенції другого степеня. Квадратичні лишки, квадратичні нелишки, символ Лежандра. Порядок числа. Первісні корені. Індекси за простим модулем. Арифметичні застосування теорії конгруенцій. *Додаткові завдання розміщені на сторінці курсу.*

Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.

Схема курсу "Теорія Чисел"

Тиждень	Лекції		Практичні заняття		СР
	Назва теми	К-сть год	Назва теми	К-сть год	К-ть год Л-ра
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 системи лишків за даним модулем. Теореми Ейлера та Ферма.	2	2 [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.