МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

КАФЕДРА КІБЕРБЕЗПЕКИ

Ахмаметьева Г.В., Баландіна Н. М.

МАТЕМАТИЧНІ ОСНОВИ КРИПТОГРАФІЇ

МЕТОДИЧНІ ВКАЗІВКИ

(для бакалаврів галузі знань 12 «Інформаційні технології», спеціальності 125 «Кібербезпека та захист інформації» факультету кібербезпеки та інформаційних технологій)

Одеса
2024

УДК 512.624.95
А 954

Рекомендовано навчально-методичною радою Національного університету «Одеська юридична академія» (протокол № 3 від 26.12.2024 р.)

Укладачі:
Ахмаметьева Г.В. - кандидат технічних наук, доцент, доцент кафедри кібербезпеки Національного університету «Одеська юридична академія», ORCID iD: https://orcid.org/0000-0002-0567-902X;
Баландіна Н. М. – старший викладач кафедри кібербезпеки Національного університету «Одеська юридична академія», ORCID iD: https://orcid.org/0000-0002-3121-4517.

Рецензенти:
Тимошенко Л.М. кандидат економічних наук, доцент, завідувач кафедри кібербезпеки та програмного забезпечення Національного університету «Одеська політехніка»;
Щербина Ю.В. – кандидат технічних наук, доцент, доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія».

Математичні основи криптографії: методичні вказівки (для бакалаврів галузі знань 12 «Інформаційні технології», спеціальності 125 «Кібербезпека та захист інформації» факультету кібербезпеки та інформаційних технологій) [Електронне видання] / Г.В. Ахмаметьева, Н.М. Баландіна; кафедра кібербезпеки НУ «Одеська юридична академія». - Одеса, 2024. - 40 с. - Режим доступу: https://doi.org/10.32837/11300.28997

Методичні вказівки з курсу «Математичні основи криптографії» розроблено відповідно до навчального плану, вони складаються з навчальної програми курсу, методичних рекомендацій із проведення практичних занять, питань для самоконтролю, завдань для самостійної роботи, переліку рекомендованих джерел. Вивчення дисципліни «Математичні основи криптографії» допоможе студентам розвинути навички застосування методів та засобів математичних основ криптографії та криптографічного аналізу, що застосовуються до захисту інформації в інформаційних системах.

Матеріали призначені для здобувачів факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія», які навчаються за спеціальністю 125 «Кібербезпека та захист інформації».

УДК 512.624.95
А 954

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Навчальна дисципліна «Математичні основи криптографії» призначена для студентів, що навчаються за освітньо-кваліфікаційним рівнем «бакалавр». Вивчення дисципліни «Математичні основи криптографії» полягає у формуванні у майбутніх спеціалістів загальних і фахових компетенцій з теорії чисел, які дозволять засвоювати пов’язані з нею дисципліни та використовувати набуті знання в професійній діяльності. Студенти мають ознайомитися з теоретичними основами теорії чисел та поліноміальної арифметики при розв’язанні практичних задач криптографії. Необхідно навчити студентів вільно оперувати основними поняттями, твердженнями та позначеннями з теорії чисел та теорії груп, кілець та полів; розв'язувати завдання з використанням отриманих знань; підготувати студентів до використання набутих знань в подальших навчальних курсах.

Міждисциплінарні зв’язки. Вивчення курсу «Математичні основи криптографії» передбачає наявність систематичних та ґрунтовних знань, отриманих при вивченні дисциплін «Лінійна алгебра та аналітична геометрія», «Математичний аналіз», «Дискретна математика».

В свою чергу, дана дисципліна повинна забезпечити ґрунтовну основу для вивчення курсів «Криптографія», «Перспективні системи асиметричної криптографії».

Програма навчальної дисципліни розрахована на один семестр і передбачає читання лекцій, проведення практичних занять, консультацій, самостійної роботи та іспиту; містить 5 тем, для кожної з яких наведено перелік питань, що розкривають її зміст.

ЗАПЛАНОВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Метою викладання навчальної дисципліни «Математичні основи криптографії» є формування у студентів умінь та компетенцій для забезпечення реалізації ефективного криптографічного захисту інформації та застосуванню відповідних алгоритмів, методів і засобів криптографічного захисту при розробці сучасних інформаційних систем.

Для досягнення мети передбачається вивчення таких основних розділів: теорія подільності цілих чисел; найважливіші числові функції, що зустрічаються в теорії чисел; класи за даним модулем; порівняння і класи лишків; порівняння з невідомою величиною; степеневі лишки; множини з дією, елементи теорії груп; основи теорії кілець та полів, обчислення в скінченних полях.

Основними завданнями вивчення дисципліни «Математичні основи криптографії» є встановлення математичного та термінологічного фундаменту в галузі криптографії та формування компетентностей майбутніх фахівців в галузі сучасних технологій захисту інформації в комп'ютерних системах.

Згідно з вимогами освітньо-професійної програми студенти повинні:

знати:

основні фундаментальні поняття абстрактної теорії чисел, зокрема: просте число, основна теорема арифметики, властивості простих та складених чисел. взаємно прості числа, канонічний розклад складеного числа, основні числові функції, півгрупа, група, теорема Лагранжа, порядок елемента у групі, циклічні підгрупи у групі. циклічні групи та їх властивості, твірні елементи циклічних груп, кільце, комутативне кільце, кільце з одиницею, найбільший спільний дільник і найменше спільне кратне елементів кільця, числові функції, теореми Ферма, Ейлера, Вільсона, ланцюгові дроби, підхідні дроби, порівняння в кільці цілих чисел, квадратичний лишок та нелишок, символ Лежандра, квадратичний закон взаємності, первісні корені, індекси за простим модулем, поняття класичної теорії полів та теорії Галуа.

вміти:

виконувати арифметичні дії з цілими числами, виконувати ділення з остачею, застосувати алгоритм Евкліда для знаходження НСД цілих чисел, розкладати цілі числа на прості множники, знаходити кількість і суму всіх дільників, значення функції Ейлера, виконувати арифметичні дії з класами лишків, розв'язувати лінійні порівняння з одним невідомим та їх системи, перетворювати порівняння у еквівалентні, знаходити залишок від ділення за модулем, застосовувати теорему Ейлера, перевіряти натуральне число на простоту, користатись китайською теоремою, розкладати раціональне число у ланцюговий дріб, розкладати квадратичну ірраціональність у нескінченний періодичний ланцюговий дріб, розв'язувати лінійні діофантові рівняння з використанням порівнянь та ланцюгових дробів, перевіряти, чи буде задане число квадратичним лишком за модулем m, знаходити значення символу Лежандра, первісні корені, складати таблиці індексів, володіти методами розпізнавання найважливіших алгебраїчних структур, вмінням класифікувати алгебраїчні структури, обчислювати порядок елемента у скінченних групах, виділяти циклічні підгрупи у групах, будувати прості розширення полів, знаходити степінь розширення, виконувати арифметичні дії у скінченних розширеннях полів, будувати скінченні поля, застосовувати стандартні методи і алгоритми теорії полів і теорії Галуа при розв'язанні практичних задач.

бути ознайомленими:

з основними поняттями, фактами класичної теорії чисел, теорії груп, кілець, полів; основними методами алгебри і теорії чисел та способами їх застосування до розв'язування теоретичних і прикладних задач;

з сучасними методами, теоретичними положеннями та основними застосуваннями алгебраїчної теорії чисел в деяких задачах криптографії;

з теоретичними основами основних сучасних методів шифрування та дешифрації.

з основами теорії чисел та поліноміальної арифметики при розв'язанні практичних задач криптографії.

ТЕМАТИЧНИЙ ПЛАН НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «МАТЕМАТИЧНІ ОСНОВИ КРИПТОГРАФІЇ»

№ теми	Назва теми	Лекційні заняття (год.)		Практичні заняття (год.)		Самостійна робота (год.)	
	Тема	очна	заоч-на	очна	заоч-на	очна	заоч-на
1	Теорія подільності цілих чисел	2	2	10	2	15	25
2	Теорія порівнянь	2	2	10	2	15	20
3	Первісні корені. Індекси	2	0	6	0	10	18
4	Алгебраїчні структури	2	2	6	2	14	20
5	Обчислення в скінченних полях Галуа	2	0	4	0	20	25
	Всього	10	6	36	6	74	108

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1. Теорія подільності цілих чисел

Відношення подільності, його найпростіші властивості в кільці цілих чисел. Теорема про ділення з остачею. Прості і складені числа. Решето Ератосфена. Теорема Евкліда. Основна теорема арифметики. Канонічний розклад натурального числа. Найбільший спільний дільник. Алгоритм Евкліда. Найменше спільне кратне. Лінійне зображення НСД. Взаємно прості числа. Числові функції. Ціла і дробова частини числа. Число і сума натуральних дільників. Функція Ейлера, її властивості. Функція Мебіуса. Системи числення, операції над системними числами, перехід від однієї системи числення до іншої. Ознаки подільності. Ланцюгові дроби. Підхідні дроби ланцюгового дробу, їх ввластивості. Застосування ланцюгових дробів до розв'язування діофантових рівнянь.

Тема 2. Теорія порівнянь

Порівняння в кільці цілих чисел та їхні найпростіші властивості. Класи лишків, повна і зведена системи лишків за даним модулем. Теореми Ейлера і Ферма. Порівняння першого ступеня з одним невідомим. Системи порівнянь першого ступеня з одним невідомим. Китайська теорема про лишки. Порівняння вищих ступенів з одним невідомим за простим модулем. Порівняння другого ступеня. Квадратичні лишки і квадратичні нелишки. Критерій Ейлера. Символ Лежандра, його властивості. Квадратичний закон взаємності. Символ Якобі.

Тема 3. Первісні корені. Індекси

Показники за даним модулем. Первісні корені, їх існування та кількість за простим модулем. Індекси і їх властивості. Двочленні порівняння за простим модулем. Таблиці індексів. Застосування таблиць індексів.

Тема 4. Алгебраїчні структури

Множини з дією: групоїд, півгрупа, група. Поняття ступеня та порядку елемент. Підгрупа. Циклічні підгрупи у групі. Циклічні групи та їх властивості. Твірні елементи циклічних груп. Розклад групи за підгрупою. Суміжні класи. Теорема Лагранжа та наслідки з неї. Нормальний дільник. Фактор-група. Кільце, підкільце. Кільце цілісності. Кільце з одиницею. Оборотні елементи кільця. Фактор-кільце. Поле, підполе, характеристика поля.

Тема 5. Обчислення в скінченних полях Галуа

Скінченні поля Галуа. Форми представлення елементів поля Галуа. Представлення n-бітових слів в полі GF(2^n). Основні операції над n-бітовими словами в полі GF(2^n). Алгоритми комп'ютерного множення поліномів. Обчислення в полі GF(2^n) на основі генератора.

ТЕМИ ПРАКТИЧНИХ ЗАНЯТЬ

Тема 1. Теорія подільності цілих чисел

При вивченні теми відбувається знайомство з основними поняттями і твердженнями теорії чисел: формулюються теорема про ділення з остачею, теорема Евкліда про нескінченність множини простих чисел, основна теорема арифметики, розглядаються поняття, пов'язані з простими числами, числові функції, системи числення, ланцюгові дроби.

Важливо звернути увагу на те, що уявлення

$$a = bq + r, \text{ де } 0 \le r < |b| \qquad (1)$$

при a > 0 можна отримати ділячи a на b з недоліком до отримання залишку r < b і при a < 0 – ділячи – a на b з надлишком.

Слід зазначити, що в (1) залишок завжди буде невід'ємним.

Треба зауважити, що для того, щоб знайти неповну частку q і остачу r при діленні цілого числа a на ціле число b, треба знайти найбільше ціле число k, яке кратне b і не перевищує число a. Тоді неповну частку q дістають як частку від ділення k на b, а остачу r як різницю між a та k.

Якщо в задачах на подільність мова йде про числа, записані за допомогою ступенів, то доцільно слідкувати за тим, які остачі дають при діленні на те чи інше число послідовні ступені основи.

Необхідно також ознайомитися з основною теоремою арифметики, яка призводить до канонічного представлення чисел, що дозволяє легко отримати вираз для найбільшого спільного дільника та найменшого спільного кратного двох даних чисел.

Продовжуючи вивчення теми, варто розглянути алгоритм Евкліда та придбати навік у знаходженні найбільшого спільного дільника.

Важливо звернути увагу на те, що послідовне ділення треба починати з правого верхнього кута листа, отримавши залишок, записати перед ним дільник і продовжувати подальше ділення.

Слід зазначити, що при знаходженні лінійного виразу НСД може трапитись, що у виразах для остач деякі неповні частки збігаються з якоюсь остачею. Тоді потрібно уважно стежити, щоб замість таких часток не було поставлено вираз для остачі.

Наступним етапом є вивчення основних числових функцій та їх властивостей.

Під час вивчення теми запроваджується дуже важлива функція Ейлера φ(a), треба зауважити, що її значення можна тлумачити і як кількість чисел ряду 1, 2, 3….,(a-1), a, взаємно простих з a.

При доказі мультипликативності функції Мебіуса зверніть увагу на

необхідність взаємної простоти аргументів a і b.

Здобувачам слід дослідити, як з мультиплікативності функції Ейлера φ(n) можна отримати формулу для обчислення φ(n).

Продовжуючи вивчення теми, необхідно розглянути системи числення, перехід від однієї системи числення до іншої.

Слід знати, що при виконанні арифметичних операцій, записаних в десятковій системі числення, користуються правилами додавання, віднімання та множення чисел «стовпчиком» і ділення «кутом». За цими правилами виконують операції і над числами, які записані в будь-якій іншій позиційній системі числення.

Також варто розглянути ланцюгові дроби, які використовуються в криптографії для створення складних алгоритмів шифрування.

Під час підготовки до практичного заняття рекомендується дослідити приклади застосування ланцюгових дробів до розв'язування рівнянь першого ступеня з двома невідомими та діофантових рівнянь.

Питання до підготовки:

1. Відношення подільності цілих чисел, його властивості. Теорема про ділення з остачею.
2. Означення і властивості простих та складених чисел. Решето Ератосфена. Основна теорема арифметики. Канонічний розклад натурального числа. Розподіл простих чисел серед чисел натурального ряду.
3. Найбільший спільний дільник і найменше спільне кратне, способи їх знаходження. Взаємно прості числа та їх властивості. Розширений алгоритм Евкліда.
4. Числові функції. Мультиплікативні функції та їх властивості. Ціла і дробова частини числа. Сума та кількість дільників натурального числа. Функція Ейлера. Функція Мебіуса.
5. Обчислення остач від ділення.
6. Системи числення, операції над системними числами, перехід від однієї системи числення до іншої.
7. Перевірка натуральних чисел на простоту. Ознаки подільності: загальна теорема про ознаки подільності.
8. Скінченні ланцюгові дроби та їх властивості. Зображення раціональних чисел ланцюговими дробами. Підхідні дроби ланцюгового дробу. Рекурентні формули для обчислення чисельника і знаменника підхідного дробу. Властивості підхідних дробив. Квадратичні ірраціональності та періодичні ланцюгові дроби. Застосування ланцюгових дробів до розв'язування рівнянь першого

ступеня з двома невідомими. Наближення дійсних чисел підхідними дробами.

9. Лінійні діофантові рівняння від двох змінних. Застосування ланцюгових дробив до розв’язування діофантових рівнянь.

Література:
Основна: 1-21
Допоміжна: 1-15

Тема 2. Теорія порівнянь

Тема спрямована на опанування поняття порівняння, яке є одним з найсильніших засобів теоретико-числових досліджень.

Вивчаючи теорію порівнянь, потрібно добре знати поняття порівнянності двох чисел за даним модулем та вміти у різних випадках вибирати найзручніше з рівносильних формулювань порівнянності чисел.

Важливо звернути увагу на те, що порівняння багато в чому схожі на рівності, тому треба бути особливо обережним там, де їх властивості відрізняються. Так, скорочувати порівняння можна тільки на числа, взаємно прості з модулем. При скороченні на інші числа можна прийти до невірного порівняння.

Необхідно добре усвідомити, що рішенням порівняння буде не тільки дане число (якщо воно існує), але і весь клас чисел за тим самим модулем, що і дане порівняння.

Слід зазначити, що порівняння може не мати рішень зовсім. Якщо ж порівняння має рішення, то треба пам'ятати, що оскільки класів лишків за модулем m всього m, то порівняння може мати лише скінчену кількість розв’язків, які можна знайти пробуючи по черзі всі лишки повної системи.

Для опанування теми, здобувачам рекомендується ретельно розібрати різні методи вирішення порівнянь першого ступеня з одним невідомим.

Треба зауважити, що використання способу Ейлера чи застосування ланцюгових дробів справедливі тільки при (a, m)=1. Тому розв'язування порівнянь першого ступеня з одним невідомим будь-яким способом треба починати з відшукання (a, m).

Перш ніж застосовувати ланцюгові дроби при розв'язуванні порівнянь, слід спочатку, використовуючи властивості порівнянь, зробити коефіцієнт при невідомому невід' ємним і меншим за модуль.

Варто звернути увагу на те, що при розв’язуванні порівнянь з використанням ланцюгових дробів треба обчислити тільки P_{n-1}*, проте*

доцільно заповнювати всю таблицю, оскільки, обчисливши P_n *можна здійснити проміжний контроль*

Процес розв'язування порівняння першого ступеня з одним невідомим будь-яким способом слід закінчувати перевіркою.

Так як при вирішенні порівнянь вищих ступенів доводиться стикатися з порівняннями першого ступеня, необхідно на конкретних числових прикладах набути гарної навички їх вирішення.

Здобувачам необхідно добре усвідомити умову розв'язання системи порівнянь першого ступеня. Крім методу побудови рішення системи порівнянь з попарно взаємно простими модулями, потрібно розглянути метод знаходження рішення, придатний для випадку довільних модулів (спосіб підстановки).

Слід врахувати, що якщо деяке з порівнянь системи має кілька розв'язків, то їх слід об'єднати і записати як один розв'язок за меншим модулем, бо в противному разі треба буде розв'язувати стільки систем, скільки розв'язків має порівняння.

Продовжуючи вивчення теми, необхідно розглянути порівняння вищих ступенів, вони мають складнішу теорію, ніж порівняння першого ступеня.

Важливо пам'ятати, що число рішень порівняння n-ого ступеня за простим модулем не перевищує ступеня порівняння, а порівняння n-го ступеня з одним невідомим за складеним модулем може мати рішень більше, ніж ступінь.

Корисно помітити, що рішення порівняння n-го ступеня з одним невідомим за складеним модулем може бути зведене до вирішення того ж порівняння, але за модулем, рівним мірою простого числа, з подальшим розв'язанням систем лінійних порівнянь з попарно взаємно простими модулями.

Під час вивчення цієї теми слід приділити увагу вивченню критерія Ейлера та символів Лежандра і Якобі.

Особливу увагу слід звернути увагу на те, що ймовірнісні криптосистеми вимагають володіння поняттями квадратичного лишка, символів Лежандра і Якобі. Здобувачам пропонується детально ознайомитися з властивостями символів Лежандра і Якобі.

Слід зазначити, що незручність обчислень символа Лежандра полягає у необхідності розкладання на множники чисельника. Цього можна уникнути для непарного чисельника запровадженням спеціального символу Якобі. Таким чином, символ Лежандра є окремим випадком символу Якобі, тому можна для його обчислення користуватися властивостями символу Якобі.

Властивості символу Якобі, крім критерію Ейлера, збігаються з властивостями символу Лежандра і дозволяють обчислити символи Лежандра як окремий випадок символу Якобі без розкладання непарного чисельника на множники.

Питання до підготовки:

1. Порівняння в кільці цілих чисел та їх найпростіші властивості. Класи лишків. Повна і зведена системи лишків за даним модулем. Теореми Ейлера та Ферма.
2. Порівняння першого ступеня з одним невідомим, існування їх розв'язків. Методи розв'язування таких порівнянь.
3. Розв'язування порівнянь з використанням теореми Ейлера.
4. Розв'язування порівнянь з використанням ланцюгових дробів.
5. Системи порівнянь першого ступеня з одним невідомим. Китайська теорема про лишки
6. Застосування порівнянь до розв'язування діофантових рівнянь.
7. Порівняння вищих степенів з одним невідомим.
8. Порівняння n-го ступеня з одним невідомим за простим модулем, побудова еквівалентних порівнянь, кількість розв'язків. Порівняння n-го ступеня з одним невідомим за складеним модулем. Теорема Вільсона.
9. Порівняння другого ступеня. Квадратичні лишки, квадратичні нелишки, критерій Ейлера.
10. Символ Лежандра, його властивості. Квадратичний закон взаємності. Символ Якобі.

Література:
Основна: 1-21
Допоміжна: 1-15

Тема 3. Первісні корені. Індекси.

Для успішного опанування теми рекомендується розпочати з ознайомлення із сутністю поняття показника числа за даним модулем.

Поняття показника і первісного кореня характеризують властивості алгебраїчні властивості сукупності класів лишків, взаємно простих з модулем, відносно операції множення класів. Відповідно до властивостей показник числа a за модулем m є дільником числа $\varphi(m)$. Тому для практичного визначення показника числа a достатньо випробувати дільники $\varphi(m)$ в

порядку їх зростання.

Важливо звернути увагу на питання існування первісних коренів за модулем m. Якщо m-складне число, то первісні корені за модулем m можуть і не існувати. За простим модулем p завжди існують первісні корені, причому їх число дорівнює φ(p-1).

Якщо знайдено первісний корінь a за модулем p, то інші первісні корені слід шукати серед ступенів виду a^k*, де (k, p-1)=1, 1< k< p-1.*

З первісними коренями пов'язане поняття індексу. Оскільки послідовні ступеня первісного кореня породжують всю зведену систему лишків, то кожне число, взаємно просте з модулем порівняно з деяким ступенем первісного кореня.

Користуючись означенням індексу, можна скласти таблицю індексів за даною основою і модулем. Таблиці індексів за кожним простим модулем p містять дві таблиці: одна – для знаходження індексу за числом (таблиця індексів), а друга - для знаходження числа за індексом (таблиця анти індексів).

Номер рядка в таблиці індексів означає число десятків, а номер стовпчика – число одиниць заданого числа. На перетині рядка і стовпчика знаходиться індекс.

Здобувачам знань рекомендується розібрати теорію та навчиться користатися таблицею індексів.

Важливо звернути увагу на те. що оскільки вибір основи для складання таблиць індексів за даним модулем є довільний, то в різних підручниках і посібниках такі таблиці не завжди збігаються. Проте це не впливає на остаточний результат при розв'язуванні задач за допомогою індексів.

Питання до підготовки:

1. Показник числа і класу лишків за модулем.
2. Первісні корені, їх існування та кількість за простим модулем.
3. Індекси за простим модулем та їх властивості.
4. Розв’язування двочленних порівняння вищих ступенів за простим модулем за допомогою індексів.
5. Таблиці індексів та їх застосування.

Література:
Основна: 1-21
Допоміжна: 1-15

Тема 4. Алгебраїчні структури

Для успішного опанування теми рекомендується розпочати з ознайомлення із сутністю одного найважливішого і фундаментального поняття, якому приділяється значна увага – з поняття групи.

Необхідно звернути увагу на те, що порядок перевірки аксіом групи можна змінювати, особливо цим фактом доцільно користуватись у разі не існування структури групи на заданій множині.

Також треба враховувати, що в скінченій групі порядок кожного елемента є натуральним числом, в нескінченій групі можуть існувати елементи як скінченого так і нескінченого порядків.

При вивченні ізоморфізмів груп слід звернути увагу на основну вимогу ізоморфізму – існування взаємно однозначного відображення φ між множинами елементів груп. Слід зазначити, що на практиці не завжди вдається відразу вдало підібрати відображення, тому значно легше перевіряти, чи буде задане відображення ізоморфізмом груп, ніж знаходити таке відображення.

Поняття ізоморфізму дозволяє підкреслити велику важливість теорії кінцевих груп симетричної групи підстановок S_n, мається на увазі теорема Келі: кожна кінцева група G порядку n ізоморфна деякій підгрупі симетричної групи підстановок S_n.

Треба враховувати, що таблиця Келі, є зручною формою завдання групи, але для груп з великою кількістю елементів, таблиця Келі непридатна. Для таких груп істотне значення набуває поняття твірної множини або системи твірних групи.

Під час вивчення цієї теми слід особливу увагу приділити вивченню циклічних груп.

Продовжуючи вивчення теми, здобувачам варто дослідити поняття суміжних класів і приділити увагу теоремі Лагранжа та наслідків з неї.

При підготовці до практичного заняття, варто уважно вивчити означення фактор-групи, оскільки часто в ньому забувають про те, що треба розглядати нормальну підгрупу. Для подолання цих труднощів слід потренуватись виконувати дії над суміжними класам для конкретних груп, наприклад, групи підстановок або адитивної групи цілих чисел.

Поняття нормального дільника та фактор групи тісно пов'язані з одним природним узагальненням поняття ізоморфізму груп- гомоморфізмом.

Обов'язковими для вивчення є властивості гомоморфних (ізоморфних) відображень.

На завершення здобувачам рекомендується ретельно розібрати основні визначення і поняття теорії кілец та полів.

Питання до підготовки:

1. Алгебри з однією бінарною алгебраїчною операцією.
2. Основні алгебраїчні структури: групи, підгрупи, кільця, поля.
3. Властивості елементів групи. Класифікація груп за властивостями групової операції та за кількістю елементів групи.
4. Поняття порядку елемента в групі.
5. Підстановки; симетрична група, група підстановок деякої множини; скінченні та нескінченні цикли, транспозиції.
6. Означення та деякі властивості знакозмінної групи.
7. Системи твірних знакозмінної групи.
8. Ізоморфізм груп. Приклади. Скінчена група, її порядок.
9. Суміжні класи. Розклад групи за підгрупою. Теорема Лагранжа та наслідки з неї.
10. Нормальний дільник, фактор-група, гомоморфізм груп.
11. Алгебри з двома алгебраїчними операціями: півкільця, кільця, підкільця. Основні властивості, приклади.
12. Поля, підполя. Числові поля. Алгебраїчні і трансцендентні числа. Поле алгебраїчних чисел.

Література:
Основна: 1-21
Допоміжна: 1-15

Тема 5. Обчислення в скінченних полях Галуа

При вивченні теми почати слід з поняття простого поля GF(p), де p – просте число, та форм його представлення. Зручним способом представлення простого поля є табличний. Для кожної бінарної операції будується таблиця, яка має назву таблиця групової операції, або таблиця Келі групи.

Введення понять степеню поліному A(x), незвідного поліному p(x) та порівняності поліномів A(x) та B(x) за подвійним модулем (F(x),p) дозволяє прийти до розуміння розширеного поля або розширення степені n простого поля GF(p).

В публікаціях, присвячених сучасним криптографічним перетворення, подання обчислень в розширених полях $GF(p^n)$ може бути наведеним в різних формах: степеневій, цілочисельній, поліноміальній, векторній. Тому слід приділити увагу тому, який зв'язок між переліченими поданнями є та яким чином відбувається перехід від однієї форми до іншої.

Сучасні криптографічні перетворення працюють з розширеними

полями GF(2^n), але в табличному представленні за умови звичайних операцій множення і додавання в цілочисельній формі певні значення повторюються, а певні відсутні зовсім. Оскільки часто на основі обчислень в полі GF(2^n) формуються S-блоки заміни, які не передбачають повторюваних значень, то подання значень в поліноміальній формі, які дозволяють отримати бієктивне відображення поліномів, тобто кожному поліному ставиться у відповідність інший неповторюваний поліном.

Студентам важливо приділити увагу, яким чином здійснюються операції додавання, віднімання, обчислення за модулем, множення, ділення, мультиплікативна інверсія, та в чому полягає різниця цих операцій з цілочисельними обччисленнями.

На практичних заняттях слід звернути увагу на алгоритми, які дозволяють прискорити обчислення на поліномах, зокрема операцій множення та ділення. А також дослідити процес побудови генератора для поля GF(2^n) та його застосування при знаходженні мультиплікативної інверсії, операцій множення і ділення поліномів.

Питання до підготовки:

1. Поля, приклади та основні властивості. Розширення полів. Прості поля. Степінь розширення поля. Характеристика поля.
2. Виконання операцій додавання і множення в простих скінченних полях.
3. Прості розширення полів. Алгебраїчні і трансцендентні елементи над полем. Алгебраїчні розширення полів. Скінченні поля та їх основні властивості.
4. Побудова скінченних полів. Мультиплікативна група скінченного поля.
5. Незвідні многочлени над скінченим полем.
6. Побудова простого алгебраїчного розширення.
7. Скінченні поля Галуа. Форми представлення елементів поля Галуа.
8. Властивості полів Галуа та їх застосування в криптографії.
9. Представлення n-бітових слів в полі GF(2^n). Основні операції над n-бітовими словами в полі GF(2^n).
10. Алгоритми комп'ютерного множення поліномів. Обчислення в полі GF(2^n) на основі генератора.

Література:
Основна: 1-21
Допоміжна: 1-15

ЗАВДАННЯ ДЛЯ САМОСТІЙНОЇ РОБОТИ

Тема 1. Теорія подільності цілих чисел

1. Контрольні запитання і завдання:

- Дайте визначення відношення подільності та сформулюйте його властивості.
- У чому полягає суть ділення з остачею?
- Як знайти канонічний розклад цілого числа?
- Сформулюйте основну теорему арифметики та наслідки з неї.
- Опишіть решето Ератосфена.
- Розкрийте поняття НСД, НСК. Наведіть приклади.
- Опишіть алгоритм Евкліда знаходження НСД.
- Наведіть визначення взаємно простих чисел.
- Розкрийте сутність розширеного алгоритма Евкліда.
- Що називається цілою та дробовою частинами числа? які значення може набувати дробова частина?
- Як знайти кількість дільників і суму всіх дільників цілого числа?
- Які основні властивості функції Ейлера вам відомі? Вкажіть формули для обчислення її значень.
- Як задається функція Мебіуса?
- Що називається мультиплікативною функцією?
- Виведіть ознаки подільності на 2, 3, 6, 9, 5, 7, 11, 13.
- Що таке ланцюговий дріб?
- Як пов'язаний алгоритм Евкліда з ланцюговими дробами?
- Які застосування ланцюгових та підхідних дробів вам відомі?
- Наведіть рекурентні формули для обчислення чисельника і знаменника підхідного дробу.
- Якими властивостями володіють підхідні дроби?
- Як зобразити раціональний дріб ланцюговим дробом?
- Довести, що добуток двох послідовних чисел ділиться на 2, трьох на 6, чотирьох на 24.
- Довести, що квадрат непарного числа при діленні на 8 дає остачу 1.
- Довести, що при простих $p > 5$ число (p^2-25) ділиться на 24.
- Довести, що при простих $p > 7$ число (p^4-1) ділиться на 240.
- Довести, що різниця $n^5 - n$ ділиться на 5 при будь- якому $n \in N$.
- Довести, що різниця квадратів двох цілих чисел, які не діляться ні на 2, ні на 3, кратна 24.
- Довести, що для довільного натурального числа n: $(10^{n+1}-9n-10) \vdots 81$.

- складіть таблицю простих чисел, менших за 150
- При ділені цілого числа a на ціле число b утворюється неповна частка q і остача r. Знайти b і r, якщо a=371, q=14.
- Знайти найбільше ціле, що дає при діленні на 17 частку 19.
- Знайти остачу від ділення числа n на 30, якщо відомо, що остача від ділення n на 15 дорівнює 7, а остача від ділення n на 6 дорівнює 4.
- Знайти остачу від ділення 5^{20} на 24.
- Знайти остачу від ділення $2^{60}+7^{30}$ на 13.
- Знайти остачу від ділення $3^{105}+4^{105}$ на 181.
- Знайти остачу від ділення 15^{231} на 14.
- Знайти остачу від ділення 1532^5-1 на 9.
- Довести, що число $43^{43}-17^{17}$ ділиться на 10.
- Знайти останню цифру числа 9^9.
- На яку цифру закінчується 2^{25} ?
- Знайти дві останні цифри числа 9^{9^9}.
- Знайти останні дві цифри числа 243^{402}.
- Знайти число і суму всіх натуральних дільників числа n=360.
- Обчислити функцію Ейлера для числа n=17.
- Обчислити функцію Ейлера для числа n=1200.
- Знайти натуральне число n, якщо $n=3^k5^l7^s$,де $k, l, s \in \mathbb{N}$, $\varphi(n)$=3600.
- Знайти канонічний розклад числа 18!.
- Скількома нулями закінчується число n!, якщо n=50?
- Розв'язати рівняння $[3{,}4\,x]=1$.
- Знайти $\mu(63)$.
- Обчислити всі підхідні дроби для дробу $\frac{1240}{706}$.
- Розв'язати рівняння 23x + 17y = 2 за допомогою ланцюгових дробів.

2. Підготувати доповіді на теми:
- Числа-близнюки, число Шехерезади, цікаві теореми з теорії натуральних чисел.
- Алгоритми обчислення числових функцій.
- Алгоритми тестування чисел на простоту.
- Псевдопрості числа Ейлера.
- Числа Кармайкла.
- Алгоритми переходу від однієї основи систем числення до іншої основи. Складність таких алгоритмів та їх реалізація.
- Арифметичні застосування теорії подільності.
-

Тема 2. Теорія порівнянь

1. Контрольні запитання і завдання:
   - Дайте визначення поняттю класів лишків за модулем.
   - Наведіть визначення поняттям повної і зведеної системи лишків та вкажіть різницю між ними.
   - Як додавати та множити класи лишків за модулем? Пояснити алгоритми та наведіть приклад.
   - Сформулюйте теореми Ейлера та Ферма.
   - Порівняння першого ступеня з одним невідомим та їх застосування.
   - Які властивості порівнянь вам відомі?
   - Сформулюйте властивості порівнянь які не збігаються з властивостями рівностей.
   - Які способи розв'язання порівнянь першого ступеня з одним невідомим використовуються? Наведіть приклади.
   - Сформулюйте китайську теорему про залишки.
   - Як розв'язуються порівнянь вищих ступенів з одним невідомим.
   - Які способи розв'язання систем порівнянь ви знаєте?
   - Що розуміють під символом Лежандра? Наведіть означення та приклади.
   - Які властивості символу Лежандра вам відомі?
   - Дайте визначення поняттю символ Якобі.
   - Яка різниця між символами Лежандра та Якобі?
   - Які арифметичні застосування теорії порівнянь ви знаєте?
   - Чи порівняні числа 78, 210 і 346 з числом 27 за модулем 11?
   - Які з чисел a, b, c порівняні з числом d=11 за модулем m, якщо a=217, b=201, c=186, m=19.
   - Записати у вигляді порівнянь умову: при діленні на 8 число 53 дає остачу 5.
   - Знайти за модулем m=12 зведену систему лишків.
   - Чи утворює повну систему лишків за модулем m система чисел {-7, 2, 16, 20, 27, 39, 46, -3}, якщо m=8?
   - За способом спроб розв'язати порівняння $3x \equiv 1 (\mathrm{mod}\ 4)$.
   - За штучним способом розв'язати порівняння $7x \equiv 8 (\mathrm{mod}\ 5)$.
   - За способом Ейлера розв'язати порівняння $5x \equiv 7 (\mathrm{mod}\ 13)$.
   - Застосовуючи ланцюгові дроби, розв'язати порівняння $143x \equiv 41 (\mathrm{mod}\ 227)$.
   - Застосовуючи ланцюгові дроби, розв'язати порівняння $236x \equiv 44 (\mathrm{mod}\ 388)$.

- Знайти розв'язки системи порівнянь $\begin{cases} 3x \equiv 5 (\mathrm{mod}\ 7) \\ 4x \equiv 2 (\mathrm{mod}\ 5). \end{cases}$
- Знайти розв'язки системи порівнянь $\begin{cases} x \equiv 3 \ (\mathrm{mod}\ 5) \\ x \equiv 2 \ (\mathrm{mod}\ 12) \\ x \equiv 7 \ (\mathrm{mod}\ 3). \end{cases}$
- Знайти розв'язки системи порівнянь $\begin{cases} 3x \equiv 11 (\mathrm{mod}\ 17) \\ 15x \equiv 35 (\mathrm{mod}\ 13) \\ 21x \equiv 33 (\mathrm{mod}\ 3. \end{cases}$
- За способом спроб розв'язати порівняння $x^2 \equiv 4 (\mathrm{mod}\ 7)$.
- Обчислити символ Лежандра $\left(\frac{323}{607}\right)$.
- Визначити, скільки розв'язків має порівняння $x^2 \equiv 728 (\mathrm{mod}\ 919)$.

2. Підготувати доповіді на теми:
   - Гамма-функція Ейлера.
   - Дзета-функція Рімана. Нулі дзета-функції.
   - L-функції Діріхле.
   - L-ряди Діріхле.
   - Асимптотичний закон розподілу простих чисел.
   - Арифметичні застосування теорії порівнянь.

Тема 3. Первісні корені. Індекси

1. Контрольні запитання і завдання:
   - Що розуміють під показником за заданим модулем? Наведіть приклади.
   - Якому показнику належить первісний корінь за простим модулем?
   - Пояснить, що таке первісний корінь.
   - Як зайти первісні корені?
   - Сформулюйте достатню умову існування первісних коренів за простим модулем.
   - Як обчислити кількість первісних коренів за простим модулем?
   - Що називають індексом числа за заданим модулем?
   - Які властивості індексів ви знаєте?
   - Як розв'язати двочленні порівняння n-го ступеня за простим модулем за допомогою індексів?
   - Як скласти таблиці індексів та антиіндексів за заданим модулем?
   - Наведіть приклади застосування таблиць індексів.
   - Знайти порядок числа 2 за модулем 5.
   - Знайти всі первісні корені за модулем 11.

- Знайти число первісних коренів і найменший з них модулем 19.
- Знайти найменший первісний корінь за модулем 41.
- Знаючи, що 3 є первісним коренем за модулем 29, знайти решту первісних коренів за цим модулем.
- Скласти таблицю індексів та антиіндексів за модулем 11.
- Розв'язати лінійне порівняння $7x \equiv 23 \pmod{17}$.
- Розв'язати двочленне порівняння $28x^8 \equiv 70 \pmod{13}$.
- Розв'язати порівняння $7 \cdot 5^x + 1 \equiv 0 \pmod{73}$.
- Користуючись критерієм Ейлера, з'ясувати, які з чисел 15, 16, 17, 18, 19, 20 є квадратичними лишками за модулем 89.
- Чи є первісним коренем за модулем 59 число 12?

2. Підготувати доповіді на теми:
- Застосування чисел, обернених за модулем.
- Алгоритм знаходження чисел, обернених за модулем.
- Адитивні шифри. Показник кореня за модулем.

Тема 4. Алгебраїчні структури

1. Контрольні запитання і завдання:
- Що таке бінарна операція та n-арна?
- Сформулюйте визначення підгрупи та групи. Наведіть приклади.
- Розкрийте поняття множини твірних групи.
- Дайте визначення підстановки n-го ступеня.
- Яка підстановка називається транспозицією?
- Що таке циклічна група? Як будуються циклічні групи?
- Як знайти порядок елемента? Наведіть приклади.
- Розкрийте сутність поняття періодичної групи та групи без кручень.
- Яка група називається симетричною групою ступеня n? Знакозмінною групою?
- Що називають правим суміжним класом групи G по підгрупі H?
- Яка різниця між ізоморфізмом та гомоморфізмом груп?
- Як зайти розклад групи за підгрупою?
- Розкрийте поняття нормального дільника групи.
- Сформулюйте теорему Лагранжа та наслідки з неї.
- Що таке кільце? Які бувають кільця? Чи може кільце бути оберненим?
- Наведіть основні властивості кільця.
- Опішить кільце лишків цілих чисел та його властивості.
- Як визначити дільники нуля?
- Що розуміють під фактор-групою?
- Як побудувати фактор-групу?

- Що таке поле? Які бувають поля? Коли поле називається нескінченним?
- Чи утворює групу множина:
  a) симетричних матриць відносно додавання;
  b) діагональних матриць відносно додавання;
  c) діагональних матриць відносно множення;
  d) верхніх трикутних матриць відносно множення?
- Довести, що множина парних цілих чисел є підгрупою адитивної групи цілих чисел.
- Знайти підгрупи симетричної групи S_3.
- Дано множину H =$\{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ підстановок із симетричної групи S_4.
  a) перевірити, чи є H підгрупою групи S_4;
  b) встановити порядок елемента σ_2;
  c) визначити парність підстановки σ_3;
  d) розкласти в добуток циклів підстановку σ_4.
- Який порядок можуть мати елементи групи S_6?
- Скільки різних циклічних підгруп містить група S_4?
- Знайти всі нетривіальні підгрупи групи коренів з одиниці для $\sqrt[28]{1}$.
- Побудувати таблиці Келі для групи $\mathbb{Z}_5^*$.
- Які серед даних груп циклічні: a) $\mathbb{Z}_{10}^*$; b) $\mathbb{Z}_{11}^*$; c) $\mathbb{Z}_{12}^*$; d) $\mathbb{Z}_{14}^*$?
- Знайти порядки елементів в групі $(\mathbb{Z}_{12}, +)$, вказати циклічні підгрупи.
- Скільки різних підгруп має циклічна група порядку 6120?
- Знайти порядки всіх елементів групи $\mathbb{Z}_{11}^*$ і з'ясувати, які з елементів будуть її твірними.
- Знайти твірні елементи скінченної циклічної групи лишків за модулем 29.
- Чи може добуток двох елементів:
  a) скінченного порядку мати нескінченний порядок;
  b) порядку 2 мати нескінченний порядок;
  c) нескінченного порядку мати скінченний порядок?
- Чи можуть дві різні підгрупи циклічної групи бути ізоморфними?
- Опишіть з точністю до ізоморфізму всі групи порядку 4. Побудуйте їх таблиці Келі. Зобразіть ці групи як групи підстановок.
- Опишіть усі нормальні підгрупи групи S_3. і доведіть, що в цій групі властивість "бути нормальною підгрупою" є транзитивною.
- Опишіть усі гомоморфізми $\varphi : \mathbb{Z}_6 \to \mathbb{Z}_{18}$ і для кожного з них укажіть ядро та образ.
- Чи є кільцем відносно операцій додавання і множення множина парних цілих чисел? Відповідь поясніть.
- Множина цілих чисел є полем відносно операцій додавання і множення?

- Написати таблиці додавання і множення в кільці $17\mathbb{Z}/85\mathbb{Z}$. Знайти одиницю в цьому кільці та переконатись, що $17\mathbb{Z}/85\mathbb{Z}$ – поле
- Знайти протилежні та обернені елементи до елементів кільця$17\mathbb{Z}/85\mathbb{Z}$.
- Чи є фактор- кільце $\mathbb{Z}/5\mathbb{Z}$ полем?
- Чи має кільце $\mathbb{Z}/6\mathbb{Z}$ дільники нуля?

2. Підготувати доповіді на теми:
- Групи симетрій і діедральні групи. Група Клейна.
- Автоморфізми та спряжені елементи.
- Групи, кільця та поля. Основні властивості цих алгебр та їх роль у криптографії.
- Алгоритми і приклади застосування методів теорії груп в криптографії.
-

Тема 5. Обчислення в скінченних полях Галуа

1. Контрольні запитання і завдання:
   - Наведіть визначення скінченного поля.
   - Сформулюйте визначення простого поля Галуа.
   - Наведіть визначення та приклади незвідного поліному.
   - Що розуміють під розширеним полем Галуа?
   - Які форми представлення елементів скінченного поля вам відомі?
   - Розкрийте сутність обчислення елементів в скінченних полях.
   - Як відбувається додавання і множення в полях Галуа?
   - Які типи розширень полів ви знаєте?
   - Що розуміють під полями лишків за модулем простого числа?
   - Побудувати поле з 9 елементів та навести його таблицю Келі для операцій додавання та множення.
   - Переконатись, що многочлен x^3+x+1 є незвідним над полем $\mathbb{Z}/2\mathbb{Z}$.
   - В полі $(\mathbb{Z}/101)$ вирішити рівняння $4x=1$.
   - Чи справджується рівність $x^2+1=(x+1)(x-1)$ над полем $\mathbb{Z}/2\mathbb{Z}$?
   - Дослідити на звідність многочлен x^2+1 над полем $GF(2)$.
   - Як задати операцію множення у полі $GF(2^8)$?
   - Знайти в полі $GF(13)$ обернені адитивні елементи для 3, 5, 8, 9.
   - Побудувати поле F_3^2.
   - Побудувати скінченні прості поля Галуа для модулів Pi = 7, 11, 13, 17, 19, 23, 29, 31, 37, 41. Визначити множину первісних елементів для кожного Pi.
   - Обчислити $P_1 \oplus P_2$, якщо $P_1 = x^4 + x^2 + x + 1$, $P_2 = x^6 + x^5 + x^3 + x + 1$ в полі $GF(2^8)$.

- Згенерувати елементи поля $GF(2^5)$ за допомогою генератора, використовуючи многочлен $f(x) = x^5 + x^3 + 1$.

2. Підготувати доповіді на теми:
   - Функція Мебіуса та незвідні многочлени.
   - Алгоритми побудови незвідних многочленів та скінченних полів.
   - Генератори псевдовипадкових чисел.
   - Корені з одиниці та кругові многочлени.
   - Еліптичні криві над полем дійсних чисел.
   - Еліптичні криві та криптосистеми на цих кривих.
   - Використання полів Галуа для виконання операцій над блоками даних під час процесів шифрування та дешифрування в AES.

ТЕМИ РЕФЕРАТІВ

1. Зв’язок між теорією чисел та криптографією.
3. Алгоритм Евкліда. Розширений алгоритм Евкліда. Алгоритм знаходження чисел, обернених за модулем.
4. Системи лінійних діофантових рівнянь.
5. Діофантові рівняння вищих степенів.
6. Розподіл простих чисел, застосування у криптографії.
7. Складність алгоритмів обчислення додавання, віднімання, множення та ділення в різних системах числення.
8. Метод обчислення квадратних коренів за модулем n=pq.
9. Алгоритми і приклади застосування методів теорії груп в криптографії.
10. Застосування матриць для шифрування.
11. Методи оптимізації арифметичних операцій з великими числами у криптографії.
12. Шифрування. Блокове шифрування. Шифрування зі зв’язком блоків.
13. Шифрування та розшифрування повідомлень, створення ключів та захист інформації.
14. Алгоритми обчислення теоретико-числових функцій. Класифікація криптосистем, основні загрози таким системам.
15. Застосування лінійних порівнянь в криптосистемах RSA.
16. Шифр Цезаря. Шифрація. Дешифрація. Арифметика за модулем.
17. Шифр Хілла. Системи лінійних рівнянь за модулем.
18. Аддитивні шифри. Криптоаналіз. Принцип Керкхофса.
19. Мультиплікативні шифри. Числа, обернені за модулем.
20. Застосування чисел, обернених за модулем. Криптоаналіз мультиплікативних шифрів.
21. Експоненціальні шифри. Шифрування. Показник кореня за модулем.
22. Експоненціальні шифри. Криптоаналіз. Односторонні функції. Алгоритм Крайчика.
23. Можливі атаки на шифри.

24. Алгоритм Сільвера-Поліга-Хелмана.
25. Криптосистеми з відкритими ключами. Головоломки Меркла. Метод Діффі-Хелмана.
26. Криптографічні системи та їх класифікація. Характеристика криптосистем.
27. Симетричні системи та асиметричні системи. Асиметричні системи та їх властивості.
28. Основні області застосування симетричних та асиметричних криптосистем.
29. Проблеми обміну ключами та основні методи генерації та обміну ключами.
30. Принципи побудови асиметричних криптосистем. Приклади асиметричних шифрів.
31. Криптосистема RSA Ключові пари RSA.
32. Метод RSA. Доведення. Атаки на RSA.
33. Рюкзачна система. Метод Ель-Гамаля.
34. Цифровий підпис. Сліпий цифровий підпис.
35. Цифровий підпис. Стандарти цифрового підпису.
36. Цифровий підпис RSA. Безпека RSA.
37. Криптографічні протоколи та атаки на них.
38. Електронні вибори на базі RSA.
39. Електронні гроші на базі RSA.
40. Тестування на простоту з допомогою еліптичних кривих.
41. Криптосистема Ель-Гамаля над еліптичною кривою.
42. Хешування. Вимоги до хешфункцій.
43. Схема Меркеля–Дамгарда. Розподіл ключів за схемою Діффі-Хелмана.
44. Аналіз ефективності алгоритмів шифрування на основі теорії чисел.
45. Дослідження швидкості та стійкості алгоритмів шифрування, їхніх переваг та недоліків на основі теорії чисел.

ПИТАННЯ ДО ПІДСУМКОВОГО КОНТРОЛЮ ЗНАНЬ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

1. Відношення подільності, його найпростіші властивості в кільці цілих чисел. Теорема про ділення з остачею.
2. Прості числа. Теорема Евкліда.
3. Властивості простих і складених чисел.
4. Решето Ератосфена для пошуку простих чисел.
5. Основна теорема арифметики. наслідки.
6. Канонічний розклад натурального числа.
7. Теорема про розподіл простих чисел. Наслідки.
8. Алгоритм Евкліда.
9. Найбільший спільний дільник та найменше спільне кратне та способи їх знаходження.
10. Взаємно прості числа та їх властивості.
11. Знаходження лінійного зображення НСД за допомогою алгоритму Евкліда.
12. Числові функції.
13. Мультиплікативні функції, властивості та приклади.
14. Ціла та дробова частина дійсного числа, застосування.
15. Кількість дільників натурального числа.
16. Сума дільників натурального числа.
17. Функція Ейлера, властивості, формули для обчислення її значень.
18. Функція Мебіуса та її властивості.
19. Ланцюгові дроби. Зображення раціональних чисел ланцюговими дробами.
20. Підхідні дроби ланцюгового дробу. Рекурентні формули для обчислення чисельника і знаменника підхідного дробу.
21. Властивості підхідних дробів.
22. Застосування ланцюгових дробів до розв’язування діофантових рівнянь.
23. Системи числення, операції над системними числами, перехід від однієї системи числення до іншої.

24. Ознаки подільності.
25. Порівняння в кільці цілих чисел та їх найпростіші властивості.
26. Класи лишків за даним модулем. Повна і зведена системи лишків.
27. Теореми Ейлера і Ферма.
28. Тестування простоти на основі теореми Ферма.
29. Теорема Вільсона.
30. Порівняння першого ступеня з одним невідомим, існування їх розв'язків.
31. Розв'язання конгруенції першого ступеня, що мають декілька розв'язків. Приклади.
32. Розв'язування лінійних порівнянь з використанням теореми Ейлера.
33. Розв'язування лінійних порівнянь з використанням ланцюгових дробів.
34. Лінійні діофантові рівняння.
35. Системи порівнянь першого ступеня з одним невідомим.
36. Китайська теорема про лишки.
37. Конгруенції n-го ступеня за простим модулем.
38. Побудова рівносильних конгруенцій. Число розв'язків конгруенцій n-го ступеня за простим модулем.
39. Конгруенції n-го ступеня за складеним модулем.
40. Порівняння n -го ступеня з одним невідомим за простим модулем.
41. Порівняння n -го ступеня з одним невідомим за складеним модулем.
42. Двочленні порівняння другого ступеня. Квадратичні лишки і нелишки.
43. Критерій Ейлера.
44. Символ Лежандра, його властивості.
45. Квадратичний закон взаємності.
46. Символ Якобі.
47. Арифметичні застосування теорії порівнянь.
48. Показники чисел за даним модулем та їх властивості.
49. Первісні корені за простим модулем і їх існування.
50. Індекси та їх властивості.
51. Таблиці індексів.

52. Застосування таблиць індексів.
53. Означення групи. Приклади.
54. Підгрупа. Критерій підгрупи.
55. Циклічні групи, їх властивості.
56. Твірні елементи групи. Приклади.
57. Підстановки, симетрична група, група підстановок деякої множини.
58. Означення та властивості знакозмінної групи. Системи твірних знакозмінної групи.
59. Порядок елемента в групі. Циклічні підгрупи.
60. Суміжні класи.
61. Розклад групи за підгрупою.
62. Теорема Лагранжа та наслідки з неї.
63. Ізоморфне зображення груп підстановками і матрицями. Теорема Келі.
64. Нормальний дільник, Приклади.
65. Фактор-група. Приклади.
66. Гомоморфізм груп.
67. Кільце, підкільце. Приклади числових кілець.
68. Типи кілець. Властивості кілець. Асоціативні кільця. Комутативні кільця. Кільця з одиницею.
69. Дільники нуля. Оборотні елементи. Область цілісності.
70. Кільце класів лишків з дільниками нуля.
71. Фактор-кільце.
72. Означення поля. Приклади. Характеристика поля.
73. Поле, підполе, приклади та основні властивості.
74. Прості підполя. Теорема про прості підполя.
75. Ізоморфізм полів.
76. Прості розширення полів.
77. Будова простого алгебраїчного розширення.
78. Алгебраїчні розширення, алгебраїчні елементи, мінімальний многочлен.
79. Теорема про зв’язок між алгебраїчними та скінченними розширеннями.

80. Алгебраїчне замикання, алгебраїчні числа. Приклад трансцендентного числа.
81. Скінченні поля та їх основні властивості.
82. Виконання операцій додавання і множення в простих скінченних полях.
83. Теорема про мультиплікативну групу скінченного поля. Наслідки.
84. Незвідні многочлени над скінченним полем.
85. Кільце многочленів над полем Галуа.
86. Форми представлення елементів поля Галуа.
87. Представлення n-бітових слів в полі GF(2^n).
88. Основні операції над n-бітовими словами в полі GF(2^n).
89. Алгоритми комп'ютерного множення многочленів.
90. Властивості полів Галуа та їх застосування в криптографії.

ФОРМИ ПІДСУМКОВОГО КОНТРОЛЮ УСПІШНОСТІ ЗДОБУВАЧІВ

Поточний контроль здійснюється під час проведення практичних занять і має на меті перевірку рівня засвоєння здобувачем вивченої теми.

При поточному контролі оцінці підлягають: рівень теоретичних знань та вміння працювати з науковою літературою, знання матеріалу, продемонстрованого у виконаних завданнях самостійної роботи; активність та систематичність роботи на заняттях; результати виконання домашніх завдань, тестів, експрес-опитувань, доповідей, рефератів тощо.

Форми проведення поточного контролю: усне опитування здобувачів, розв’язування практичних завдань, тестові завдання, доповіді, реферати.

Проміжний контроль проводиться після вивчення відповідних тем або блоку тем з метою з`ясування ступеню засвоюваності здобувачами відповідного об’єму опрацьованого та вивченого матеріалу та подальшої оцінки рівня отриманих знань. Форми проведення проміжного контролю: контрольна робота, тестове опитування, співбесіда (усне спілкування).

Підсумковий контроль здійснюється у формі іспиту.

КРИТЕРІЇ ОЦІНЮВАННЯ

При використанні форми контролю у вигляді заліку враховується поточна, зокрема самостійна робота, наукова діяльність здобувача. Крім того, здобувач має надати відповідь на залікове запитання. Оцінка рівня знань виконується за принципом "відповідь вірна" або "відповідь невірна". При вірній відповіді виставляється оцінка "зараховано", при невірній, неповній відповіді виставляється оцінка "не зараховано".

Оцінка з національної шкали переводиться у 100-бальну та шкалу ECTS у відповідності до результатів навчальної успішності здобувача протягом семестру.

СХЕМА НАРАХУВАННЯ БАЛІВ (СКЛАДОВІ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ)

Пункт оцінки	% підсумкової оцінки або максимальна оцінка в балах	Групове чи індивідуальне оцінювання
Поточний контроль, разом, у т.ч.:	**50**	
доповіді та повідомлення на семінарах	25	Групове та індивідуальне
виконання письмових індивідуальних завдань, рефератів, контрольних робіт	15	Індивідуальне
опитування на практичних заняттях	10	Групове та індивідуальне
Підсумковий контроль, разом, у т.ч.:	**50**	
письмова компонента	25	Індивідуальне
усна компонента	25	Індивідуальне

ШКАЛА ЗА ECTS

<table>
<tr><th rowspan="2">Сума балів</th><th rowspan="2">Оцінка за 7-бальною шкалою</th><th colspan="2">Оцінка за 4-бальною шкалою</th></tr>
<tr><th>екзамен</th><th>залік</th></tr>
<tr><td>A</td><td>90-100</td><td>Відмінно</td><td rowspan="5">зараховано</td></tr>
<tr><td>B</td><td>82-89</td><td rowspan="2">Добре</td></tr>
<tr><td>C</td><td>74-81</td></tr>
<tr><td>D</td><td>64-73</td><td rowspan="2">Задовільно (достатньо)</td></tr>
<tr><td>E</td><td>60-63</td></tr>
<tr><td>Fx</td><td>35-59</td><td>Незадовільно з можливістю повторного складання</td><td>не зараховано</td></tr>
</table>

ПЕРЕЛІК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

ОСНОВНІ ДЖЕРЕЛА

1) Кузнецов Г.В. Математичні основи криптографії : Навч. посіб. / Г.В. Кузнецов, В.В. Фомичов, С.О. Сушко, Л.Я. Фомичова. — Національний гірничий ун- т. — Д.: НГУ, 2004. –Ч.1. 392 с.

2) Щур Н.О., Покотило О.А. Основи криптології: навч. посібник. – Житомир: Державний університет «Житомирська політехніка», 2021. 120 с.

3) Оглобліна О. І., Сушко Т. С., Шрамко Ю. В. Елементи теорії чисел: навч. посіб. Суми: Сумський державний університет, 2015. 186 с.

4) Андрійчук В.І., Забавський Б.В. Алгебра і теорія чисел. Львів. Видавничий центр ЛНУ ім. Івана Франка 2005. 238 с.

5) Клесов О.І., Елементарна теорія чисел та елементи криптографії, ТВіМС, Київ, 2017. 394 с.

6) Безущак О.О., Ганюшкін О.Г. Елементи теорії чисел: Навч. посібник.— К.: Видавничо–поліграфічний центр “Київський університет”, 2003. 202 с.

7) Євсеєв С.П., Остапов С.Е., Король О.Г. Кібербезпека: основи кодування та криптографії: навчальний посібник / С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. – Харків: Вид. “Новий Світ-2000”, 2023. 658с.

8) Ганюшкін О.Г. Теорія груп / О.Г. Ганюшкін, О.О. Безущак. — К. : «ВПЦ Київський ун-т», 2005. 122 с.

9) Фільштинський В.А. Математичні основи криптографії. Конспект лекцій/ В.А.Фільштинський, А.В. Бережний. – Суми.: Сумський державний університет, 2011. 138 с.

10) Богуш В.М. Криптографічні застосування елементарної теорії чисел : навч. посібник / В.М. Богуш, В.А. Мухачов. — Державний ун-т інформаційно-комунікаційних технологій. — К.: ДУІКТ, 2006. 126 с.

11) Sokolov A.V., Ihnatenko O.O., Balandina N.M. Increasing the Efficiency of Blind Decoding of the Steganographic Method with Code Control of Additional

Information Embedding. Problems of regional energetics. 2024. Vol. 62, No. 2. P. 121-137. doi: 10.52254/1857-0070.2024.2-62.11 (Scopus, Web of Science)

12) Kazakova N.F., Sokolov A.V., Balandina N.M. Dependence of the Algebraic Nonlinearity of 4-Functions of Two Variables from the Cryptographic Properties of Their Component Boolean Functions. Proceedings of the Workshop Cybersecurity Providing in Information and Telecommunication Systems. 2024. Kyiv, Ukraine, February 28, 2024. P. 479–484. (Scopus)

13) Bakunina O. V., Balandina N. M., Sokolov A. V. Synthesis method for S-boxes based on Galois field transform matrices. Ukrainian Journal of Information Technology. 2023. Vol. 5, No. 2. P. 41-48. DOI: 10.23939/ujit2023.02.041. URL: https://doi.org/10.23939/ujit2023.02.041

14) Козіна Г.Л. Криптографія від історії до сучасних стандартів : навч.посібник / Г. Л. Козіна. – Запоріжжя: НУ «Запорізька політехніка», 2020. 192 с.

15) Криптологія: навч. посібник / М.Н. Курко, П.М. Лісовський, Ю.П. Лісовська. — К.: Видавничий дім «Кондор», 2020. 248 с.

16) Flath D. E. Introduction to Number Theory // American Mathematical Society, 2018. 212 c.

17) Rosen K. H., Elementary Number Theory, 2011, 6th edition, Addison Wesley, Boston MA.

18) Стєганцев Є.В. Теорія груп: методичні вказівки для студентів напряму підготовки «Математика» спеціалізації «Алгебра і теорія чисел».– Запоріжжя: ЗНУ, 2013. – 45 с.

19) Ахмаметьєва Г.В. Методичні вказівки до виконання практичних занять з дисципліни «Спеціальні розділи математики» для іноземних студентів першого освітньо-кваліфікаційного рівня спеціальності 122 Комп’ютерні науки, 125 Кібербезпека. – Одеса: ОНПУ, 2019. –- 47 с.

20) Алгебра і теорія чисел: Практикум. Частина 2 / Завало С.Т., Левищенко С.С., Пилаєв В.В. Рокіцький І.А. – К.: Вища шк. Головне видавництво, 1986. 264 с.

21) Практикум з алгебри і теорії чисел / Гудивок П. М., Кирилюк О. А., Погоріляк Є. Я., Тилищак О. А., Юрченко Н. В. – Ужгород: Говерла, 2008. 64 с.

ДОПОМІЖНІ ДЖЕРЕЛА

1) Пащенко З.Д. Алгебра і теорія чисел. Змістовий модуль «Теорія конгруенцій»: навчальний посібник/ З.Д.Пащенко, Т. В. Турка. – Слов'янськ: СДПУ, 2009. 56 с.

2) Пащенко З.Д. Алгебра і теорія чисел. Змістовий модуль «Групи. Кільця. Поля»: навчальний посібник/ З.Д.Пащенко, Т. В. Турка. – Слов'янськ: СДПУ, 2008. 33 с.

3) Бобало Ю. Я. Інформаційна безпека: навч. посібник / Ю. Я. Бобало, І.В. Горбатий, М. Д. Кіселичник та ін.; за заг. ред. д-ра техн. наук, проф. Ю.Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. – Львів: Видавництво Львівської політехніки, 2019. 580 с.

4) Горбенко Ю.І., Горбенко І.Д. Інфраструктура відкритих ключів. Електронний цифровий підпис. Теорія та практика: монографія. Харків: Видавництво «Форт», 2010. 608 с.

5) Євсеєв С.П., Остапов С.Е., Король О.Г. Кібербезпека: сучасні технології захисту: навч. посіб. для студ. вищ. навч. закл. Львів: «Новий Світ- 2000», 2019. 678 с.

6) Криптологія: навч. посібник / М.Н. Курко, П.М. Лісовський, Ю.П. Лісовська. — К.: Видавничий дім «Кондор», 2020. 248 с.

7) Глинчук Л.Я. Криптологія: навч. посібник / Л.Я. Глинчук. — Луцьк: РВВ «Вежа» Волин. нац. ун-т ім. Лесі Українки, 2011. 132 с.

8) Горбенко Ю.І., Горбенко І.Д. Інфраструктура відкритих ключів. Електронний цифровий підпис. Теорія та практика: монографія. Харків: Видавництво «Форт», 2010. 608 с.

9) Ігнатєв І.В., Кондратюк В.М., Алгоритм перевірки числа на простоту Збірник матеріалів проблемно-наукової міжгалузевої конференції

«Автоматизація та комп'ютерно – інтегровані технології» (АКІТ -2022), Тернопіль, 2022. 70-73 с.

10) Посвятовська О.Б., Стефурак Н.А., Кондратюк В.М., Дослідження властивостей простих чисел для BPSW. Збірник матеріалів науково-практичної конференції молодих вчених, аспірантів та студентів» (КБКІТ-2020), Тернопіль, 2022, С. 73-79.

11) Остапов С.Е. Основи криптографії/ С.Е. Остапов, Л.О.Валь.- Чернівці.: Книги XXL, 2008. –188 с.

12) Ємець В. Сучасна криптографія/ В.Ємець, А.Мельник, Р.Попович.- Львів.: БАК, 2003. 144 с.

13) Трофименко О.Г., Прокоп Ю.В., Чепурна О.Є., Баландіна Н.М. Роль математики у різних сферах розробки програмного забезпечення. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія «Технічні науки».* 2023. Т. 34 (73). № 4. С. 117-123. DOI: 10.32782/2663-5941/2023.4/19. URL: https://www.tech.vernadskyjournals.in.ua/34-73-4.

14) Zazkis, R. (2007). Number Theory in Mathematics Education: Queen and Servant. SEMT 07: International Symposium Elementary Maths Teaching, Prague, Czech Republic, 46-59.

15) Qiu, S.Y., & Liu, L.A. (2010). On Teaching Reform of Elementary Number Theory in Colleges. International Conference on Education and Sports Education, Wuhan, China, 1, 246-248.

РЕСУРСИ ВІДКРИТОГО ДОСТУПУ

1) http://cyber.onua.edu.ua – сайт факультету кібербезпеки та інформаційних технологій, на якому розміщено робочі матеріали з курсу

2) О.І. Клесов «Елементарна теорія чисел та елементи криптографії». URL: https://ela.kpi.ua/handle/123456789/30046

3) Лукашова, Т. Д., & Марченко К.В. (2018). Модульні арифметики. Фізико-математична освіта, 1(15), 246-251. URL: https://doi.org/10.31110/2413-1571-

2018-015-1-046.

4) Pramasdyahsari, A.S., Setyawati, R.D., & Albab, I.U. (2020). How group theory and school mathematics are connected: an identification of mathematics in-service teachers. Journal of Physics: Conference Series, 1663, 012068. https://doi.org/10.1088/1742-6596/1663/1/012068.

5) Ганюшкін О.Г. Завдання до практичних занять з алгебри і теорії чисел / О.Г. Ганюшкін, О.О. Безущак. – К. : ВПЦ «Київський університет», 2007. – 103 с. http://www.mechmat.univ.kiev.ua/wp-content/uploads/2018/03/group_s.pdf

6) Збірник задач з теорії чисел. [Навчальний посібник длястудентів фізикоматематичного факультету] За редакцією І.О.Рокіцького, Вінниця, 2003 – 140с. URL: http://amnm.vspu.edu.ua/wp-content/uploads/2016/02/Rokitskiy-Zbirnik-zadach-z-teoriyichisel.pdf

7) http://dspace.onua.edu.ua – eNUOLAIR – депозитарій (архів) НУ ОЮА

ЗМІСТ

Навчальне видання

Ахмаметьева Ганна Валеріївна

Баландіна Наталія Миколаївна

МАТЕМАТИЧНІ ОСНОВИ КРИПТОГРАФІЇ

Методичні вказівки

(для бакалаврів галузі знань 12 «Інформаційні технології», спеціальності 125 «Кібербезпека та захист інформації» факультету кібербезпеки та інформаційних технологій)

В авторській редакції