

Міністерство освіти і науки України
Харківський національний університет імені В.Н. Каразіна
Кафедра вищої математики та інформатики

“ЗАТВЕРДЖУЮ”
Проректор
з науково-педагогічної роботи
А.В. Пайтелеймонов
« _____ » _____ 2018 р.



РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Дискретна математика

рівень вищої освіти	перший (бакалаврський) рівень
галузь знань	12 Інформаційні технології
спеціальність	122 Комп'ютерні науки
освітня програма	Комп'ютерні науки
галузь знань	12 Інформаційні технології
спеціальність	123 Комп'ютерна інженерія
освітня програма	Комп'ютерна інженерія
галузь знань	12 Інформаційні технології
спеціальність	125 Кібербезпека
освітня програма	Кібербезпека
галузь знань	15 Автоматизація та приладобудування
спеціальність	151 Автоматизація та комп'ютерно-інтегровані технології
освітня програма	Автоматизація та комп'ютерно-інтегровані технології
вид дисципліни	обов'язкова
факультет	комп'ютерних наук

2018 / 2019 навчальний рік

Програму рекомендовано до затвердження вченою радою факультету математики і інформатики

“27” серпня 2018 року, протокол № 7

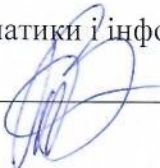
РОЗРОБНИКИ ПРОГРАМИ:

кандидат фізико-математичних наук, доцент Курінний Григорій Чарльзович

Програму схвалено на засіданні кафедри вищої математики та інформатики факультету математики і інформатики

Протокол від “27” серпня 2018 року, № 1


Завідувач кафедри вищої математики і інформатики


_____ (Лисиця В.Т.)

Програму погоджено методичною комісією факультету комп'ютерних наук

Протокол від “ ____ ” _____ 2018 року № ____

Голова методичної комісії факультету комп'ютерних наук


_____ (Васильєва Л.В.)

ВСТУП

Програма навчальної дисципліни «Дискретна математика» складена відповідно до освітньо-професійної (освітньо-наукової) освітньо-професійної програми підготовки (бакалаврського) рівня вищої освіти спеціальностей: 122 «Комп'ютерні науки та інформаційні технології», 125 «Кібербезпека», 151 «Автоматизація та комп'ютерно-інтегровані технології», 123 «Комп'ютерна інженерія»

1. Опис навчальної дисципліни

1.1. Мета викладання навчальної дисципліни: формування систематизованих знань із базових взаємозалежних розділів математики, які не вимагають залучення понять нескінченності, неперервності, нескінченно малих та нескінченно великих величин, - знань і умінь в царині дискретної математики.

1.2. Основні завдання вивчення дисципліни:

- розділити всю дискретну математику на окремі розділи;
- навчити студента формально-логічному мисленню - синтаксису і семантиці;
- в кожному розділі дискретної математики виділити базову термінологію і факти, які дають можливість переходити до вузькоспеціалізованого вивчення цього розділу;
- сформувати інтелектуальні навички і вміння в кожному розділі за допомогою активних дій, обґрунтування тих чи інших положень розділу, розв'язування задач і виконання вправ;
- навчити студента творчо користуватися набутими знаннями та вміннями;
- перевірити належне засвоєння вивченого матеріалу за допомогою контрольних робіт, заліку та іспиту.

1.3. Кількість кредитів - 8

1.4. Загальна кількість годин - 240

1.5. Характеристика навчальної дисципліни	
Нормативна	
Денна форма навчання	Денна форма навчання
Рік підготовки	
1-й	1-й
Семестр	
1-й	2-й
Лекції	
32 год.	32 год.
Практичні, семінарські заняття	
32 год.	32 год.
Самостійна робота	
56 год.	56 год.
В т.ч. індивідуальні завдання (2 контрольні роботи)	
5 год.	5 год.

1.6. Заплановані результати навчання:

Студент в процесі вивчення дискретної математики набуває наступної динамічної комбінації знань, вмінь, навичок, уявлень, розуміння з кожного із наступних виділених розділів дискретної математики.

знати:

- формально-логічну та теоретико-множинну термінологію, вміти нею користуватися; знати властивості формул логіки висловлювань та логіки предикатів, булевих функцій;
- означення кільця і приклади кілець – кільце цілих чисел, кільце поліномів, кільце квадратних матриць з дійсними елементами, кільце класів лишків;
- означення алгоритму Евкліда;
- основну теорему цілих чисел (про розкладення натурального числа у добуток простих) і вміти її доводити;
- приклад шифру відкритого ключа і приклад лінійного коду;
- аксіому індукції і принцип найменшого числа для натуральних чисел;
- означення поля і знати приклад чотириелементного поля та поля класів лишків за простим модулем
- означення групи і знати приклади адитивних і мультиплікативних груп;
- означення класів суміжності по підгрупі;
- теорему Лагранжа про подільність порядку групи на порядок підгрупи;
- приклади необчислюваних функцій;
- означення графа і означення різних типів графів – звичайний граф, мультиграф, орієнтований граф, змішаний мультиграф з петлями, плоский граф, дерево, ліс, кістякове дерево, графи з усталеними позначеннями (повний, двочастинний, колесо, мельниця, цикл, шлях, порожній, поміщений і зважений граф), діаграми Хассе для частково впорядкованих множин;
- три аксіоми комбінаторики: аксіому рівності, суми і добутку. Розуміти важливість комбінаторних чисел і модельних задач;
- означення кільця формальних степеневих рядів і кільце многочленів;
- приклади комбінаторних задач, де підрахунок ведеться «з точністю до симетрії» - задачі про намисто, задача по фарбування вершин квадрата;
- приклади дії групи підстановок на множині;
- означення чисел Стірлінга (першого і другого роду);

вміти:

- давати формальний запис змістовних фактів формулами логіки висловлювань та логіки предикатів;
- працювати з основними типами відношень (еквівалентності, часткового порядку);
- працювати з основними типами відображень (бієктивне, ін'єктивне, сюр'єктивне);
- користуватися алгоритмом Евкліда для знаходження найбільшого спільного дільника двох натуральних чисел і для знаходження оберненого елемента в кільці класів лишків;

- доводити твердження методом повної математичної індукції;
- доводити формулу для біномних коефіцієнтів методом повної математичної індукції;
- використовувати китайську теорему про остачі для розв'язування рівнянь;
- працювати в адитивній групі цілих чисел, в мільтиплікативній групі підстановок і в мультиплікативній циклічній групі;
- доводити обчислюваність функції з використанням машин Тьюрінга і методом частково рекурсивних функцій;
- зобразити граф до задачі про кенігсберзькі мости, до задачі про «три хати і три колодязі»;
- задавати граф матрицею суміжності, матрицею інцидентності, списком суміжності;
- зображати відображення і відношення графами;
- доводити формули для відомих комбінаторних чисел (сполуки, розміщення, перестановки, кількість підмножин множини);
- використовувати метод «включення – виключення», метод рекурентних співвідношень і метод твірних (генератрис);
- обчислити числа Каталана а допомогою твірних;
- застосовувати метод твірних для встановлення властивостей біномних коефіцієнтів;
- ділити многочлен на многочлен з остачею;
- знаходити НСД двох многочленів за допомогою алгоритма Евкліда;
- розкладати відношення двох многочленів з дійсними коефіцієнтами в суму найпростіших дробів над полем комплексних чисел;
- знаходити загальний член послідовності, у якої твірна є найпростішим дробом;
- доводити формулу для довільного члена послідовності, яка задовольняє лінійному рекурентному співвідношенню;
- обчислювати числа Фібоначчі;
- обчислити числа Стірлінга при малих значеннях параметрів;
- записати матрицю переходу від стандартного базису лінійного простору многочленів (складається із степенів змінної менше заданого натурального числа) до базису із спадних та зростаючих степенів змінної.
- користуватися «лемою Бернсайда» для підрахунків «з точністю до симетрії»
- підраховувати ймовірність події у випробуваннях Бернуллі, за рівномірного розподілу, за заданого нерівномірного розподілу, за розподілу ймовірності на інтерпретаціях формули логіки висловлювань – «світах». Знати теорему Байеса.
- обчислювати умовну ймовірність, доводити залежність чи незалежність подій;
- знаходити характеристики випадкової величини – математичне очікування та дисперсію.

мати:

- навички доведення в численнях висловлювань та численні секвенцій;
- уявлення про актуальну і потенційну нескінченність, уявлення про відношення та відповідності;

- уявлення про двійкову та шістнадцяткову арифметику;
- навички піднесення ``великого`` числа до ``великого`` степеня за ``великим`` модулем;
- уявлення про існування 16-елементного поля;
- уявлення про дільники нуля в кільці класів лишків.
- навички виконувати дії (множення і знаходження оберненого) в групі підстановок.
- уявлення про групу замощень площини (про паркету);
- уявлення про групи симетрій геометричних тіл, фігур;
- навички розв'язування комбінаторних задач з використанням аксіом, комбінаторних чисел, за допомогою методу «включення-виключення», рекурентних співвідношень, методу твірних;
- навички розв'язування комбінаторних задач, що зводяться до обчислення уже відомих комбінаторних чисел, в тому числі сполуки з повтореннями, розміщення з повтореннями, вибірки, вибірки з повтореннями;
- розуміння глибинних зв'язків між алгеброю і комбінаторикою;
- розуміння відношення ортогональності для чисел Стірлінга першого та другого роду;
- уявлення про розподіли ймовірності на множині і розподіли ймовірності величини;
- уяву про щільність розподілу неперервної величини, про нормальний розподіл Гаусса.

2. Тематичний план навчальної дисципліни

Перший семестр

Розділ 1. Логіки і множини

Тема 1. Логіка висловлювань, - синтаксис (формули) і семантика (інтерпретації) логіки висловлювань, числення висловлювань і числення секвенцій, тавтології та теореми в логіці висловлювань. Метод резолюцій формального доведення формули логіки висловлювань. Пролог-подібні мови програмування. Програмно орієнтовані логіки.

Тема 2. Алгебра булевих функцій — інфіксний, постфіксний і префіксний записи булевих виразів, Двійковий запис натурального числа і задання булевої функції рядком. Задання булевої функції поліномом Жегалкіна, досконалі форми (ДДНФ і ДКНФ). Регістр зсуву із зворотним зв'язком. Лінійне кодування — розв'язування рівнянь над полем $GF(2)$. Теорема Поста про 5 замкнених класів

Тема 3. Множини і логіка предикатів 1-го порядку, - інтуїтивна теорія множин, квантори і формули логіки предикатів, підмножини, відношення, відповідності, множини із стандартними позначеннями. Відношення часткового порядку, відношення еквівалентності,

Тема 4. Функціональне відношення (функція, відображення, відповідність). Композиція відображень, комутативні діаграми, Ін'єктивні, сюр'єктивне та бієктивне відображення. Ліве обернене. Праве обернене і ліве обернене відображення. Розкладення довільного відображення в добуток сюр'єктивного, бієктивного та ін'єктивного відображень

Розділ 2. Арифметика цілих чисел

Тема 1. Кільце цілих чисел: Ділення з остачею . Найбільший спільний дільник двох натуральних чисел і знаходження НСД за допомогою алгоритма Евкліда. Взаємно прості натуральні числа. Функція Ойлера, її мультиплікативність .

Тема 2. Основна теорема цілих чисел: Представлення натурального числа у вигляді добутку простих чисел. Решето Ератосфена. Частковий порядок дільників натурального числа. Розв'язування лінійних рівнянь в цілих числах

Розділ 3. Арифметика класів лишків

Тема 1. Кільце класів лишків по заданому модулю: Коректність визначення операцій в кільці класів лишків . Група оборотних елементів в кільці класів лишків. Піднесення “великого” числа до “великого” степеня по заданому модулю. Шифр відкритого ключа (без доведення коректності). Китайська теорема про остачі. Дільники нуля в кільці.

Тема 2. Поле класів лишків по простому модулю. Розв'язування лінійних однорідних і неоднорідних систем рівнянь. Алгебричне розширення поля галуа $GF(2)$ за допомогою многочлена x^2+x+1 .

Розділ 4. Індукція і біномні коефіцієнти

Тема 1. Необхідна і достатня умови, пряма і обернена теореми, Метод повної математичної індкції. Принцип найменшого числа. Нескінченість множини простих чисел.

Тема 2. Біномні коефіцієнти

Розділ 5. Групи.

Тема 1. Група підстановок. Цикли. Парність підстановки.

Тема 2. Підгрупи. Суміжні класи. Теорема Лагранжа. Мала теорема Ферма.

Тема 3. Доведення коректності шифра з відкритим ключем.

Тема 4. Дія групи на множині.

Розділ 6. Обчислюваність.

Тема 1. Машина Тьюрінга.

Тема 2. Частково рекурсивні функції.

Другий семестр

Розділ 1. Теорія графів

Тема 1. Означення і приклади графів. Сагайдаки. Матриці суміжності і матриці інцидентності. Діаграми Хассе, комутативні діаграми, діаграми відображення та еквівалентностей, що узгоджені з відображенням (конгруенції унара)

Тема 2. Окремі типи графів: повні, двочастинні, планарні, ациклічні (дерева, ліс), помічені і зважені графи.

Тема 3. Задачі на графах — Ойлерів шлях і Гамільтонів шлях. Кістякове дерево.

Розділ 2. Комбінаторика — аксіоми, комбінаторні числа і модельні задачі

Тема 1. Взаємно однозначна відповідність, аксіома рівності, аксіом суми, аксіома добутку.

Комбінаторні числа — спослуки і сполуки з повтореннями, розміщення і розміщення з повтореннями, перестановки, кількість всіх підмножин скінченної множини

Тема 2. Три комбінаторні методи — метод включення-виключення, метод рекурентних співвідношень і метод генератрис (породжуючих функцій)

Розділ 3. Лінійні рекурентні співвідношення.

Тема 1. Формальні степеневі ряди, многочлени, оборотні ряди, ряди, що обернені до многочлена.

Тема 2. Розкладення дробу (відношення двох многочленів з дійсними коефіцієнтами) у суму найпростіших дробів над полем комплексних чисел

Тема 3. Знаходження елементів послідовності, яка задовольняє лінійному рекурентному співвідношенню. Числа Фібоначчі.

Розділ 4. Числа Стірлінга

Тема 1. Числа Стірлінга першого роду

Тема 2. Числа Стірлінга другого роду. Співвідношення ортогональності.

Розділ 5. Перерахування «з точністю до симетрії»

Тема 1. Дія групи на множині. Індекс підгрупи. Лема Бернсайда про кількість орбіт дії групи на множині

Тема 2. Задача про намисто.

Розділ 6. Дискретна ймовірність. Розподіли.

Тема 1. Рівномірний розподіл і нерівномірні розподіли на множині. Підрахунки ймовірності події

Тема 2. Розподіл ймовірності на “світах” - інтерпретаціях формули логіки висловлювань

Тема 3. Біномний, геометричний та гіпергеометричний розподіли.

Розділ 7. Ймовірність величини і її характеристики

Тема 1. Умовна ймовірність. Теорема Байєса. Незалежні величини.

Тема 2. Математичне очікування (сподівання) та дисперсія

Тема 3. Неперервні величини. Нормальний закон Гауса.

2. Структура навчальної дисципліни

Назви розділів і тем	Кількість годин					
	денна форма					
	усьог о	у тому числі				
л		п	лаб.	інд.	с. р.	
1	2	3	4	5	6	7
1 семестр						
Розділ 1. Логіки і множини						
Тема 1. Логіка висловлювань	8	2	2			4
Тема 2. Булеві функції	16	4	4			8
Тема 3. Множини і предикати	18	6	6			6
Разом за розділом 1	42	12	12			18
Розділ 2. Арифметика цілих чисел						
Тема 1. Цілі числа	8	2	2			4
Тема 2. Основна теор. Арифметики	8	2	2			4
Разом за розділом 2	16	4	4			8
Розділ 3. Арифметика класів лишків						
Тема 1. Класи лишків	8	2	2			4
Тема 2. Поле $GF(2)$	8	2	2			4
Разом за розділом 3	16	4	4			8
Розділ 4. Індукція і біномні коефіцієнти.						
Тема 1. Індукція	8	2	2			4
Тема 2. Біномні коефіцієнти.	8	2	2			4
Разом за розділом 4	16	4	4			8
Розділ 5. Групи.						
Тема 1. Група S_n	5	1	1			3
Тема 2. Підгрупи	5	1	1			3
Тема 3. Шифр з відкритим ключем.	8	2	2			4
Разом за розділом 5.	18	4	4			10
Розділ 6. Обчислюваність.						
Тема 1. Машини Тьюрінга.	6	2	2			2
Тема 2. Частково рекурсивні функції.	6	2	2			2
Разом за розділом 6.	12	4	4			4
Усього годин за 1 семестр						
	120	32	32			56
2 семестр						
Розділ 1. Теорія графів						
Тема 1. Означення і приклади графів.	4	1	1			2
Тема 2. Окремі типи графів	4	1	1			2
Тема 3. Задачі на графах	4	1	1			2
Разом за розділом 1	12	3	3			6
Розділ 2. Комбінаторика — аксіоми, комбінаторні числа і модельні задачі						
Тема 1. Аксіоми і комбінаторні числа	10	2	2			6
Тема 2. Комбінаторні методи	10	2	2			6
Разом за розділом 2	20	4	4			12
Розділ 3. Лінійні рекурентні співвідношення						
Тема 1. Степеневі ряди	8	2	2			4
Тема 2. Найпростіші дроби	8	2	2			4
Тема 3. Лінійні рекурентні співвідношення	10	3	3			4
Разом за розділом 3	26	7	7			12
Розділ 4. Числа Стірлінга						
Тема 1. Числа Стірлінга 1-го роду	8	2	2			4

1	2	3	4	5	6	7
Тема 2. Числа Стірлінга 2-го роду.	8	2	2			4
Разом за розділом 4	16	4	4			8
Розділ 5. Задача про намисто						
Тема 1. Лема Берн сайда	6	2	2			2
Тема 2. Задача про намисто	6	2	2			2
Разом за розділом 5.	12	4	4			4
Розділ 6. Дискретна ймовірність. Розподіли.						
Тема 1. Рівномірний і нерівномірний розподіли на множині	8	2	2			4
Тема 2. Розподіл ймовірності на «світах» - інтерпретаціях формули логіки висловлювань	4	1	1			2
Тема 3. Біномний розподіл.	4	1	1			2
Разом за розділом 6.	16	4	4			8
Розділ 7. Ймовірність величини						
Тема 1 Умовна ймовірність	6	2	2			2
Тема 2. Математичне очікування і дисперсія	6	2	2			2
Тема 3. Неперервна величина. Закон Гаусса	6	2	2			2
Разом за розділом 7	18	6	6			6
<i>Усього годин за 2 семестр</i>	120	32	32			56
<i>Разом</i>	240	64	64			112

4. Темі семінарських (практичних, лабораторних) занять

№ з/п	Назва теми	Кількість годин
1 семестр		
1	Запис висловлювання у вигляді формули. Інтерпретація (тлумачення) формул. Формальна мова ЛВ. Постфіксна нотація	2
2	Різні способи задання булевої функції. Класи Поста. Шифрування шифром одноразового блокнота. Кодування кодом з перевіркою на парність.	4
3	Множини, підмножини, еквівалентність і розбиття, відображення та їх суперпозиція, частковий порядок та діаграми Хассе.	6
4	Арифметика цілих чисел — знаходження НСД, НСК розв'язування рівнянь	6
5	Арифметика класів лишків — знаходження оберненого, розв'язування рівнянь, піднесення до степеня, знаходження логарифма. Шифрування шифром з відкритим ключем	4
6	Індукція та біномні коефіцієнти	2
	Група S_n . Підгрупи. Шифр з відкритим ключем.	4
7	Машини Тьюрінга	2
8	Рекурсивні функції	2
	Разом	32
2 семестр		
1	Графи	3
2	Комбінаторика	4
3	Групи і кільця	3
4	Лінійні рекурентні співвідношення	4
5	Теорія Пойя, задача про намисто	4
6	Числа Стірлінга	4
7	Дискретна ймовірність — розподіли на множині елементарних подій	4
8	Випадкові величини і їх характеристики	6
	Разом	32

5. Завдання для самостійної роботи

№ з/п	Види, зміст самостійної роботи	Кількість годин
1 семестр		
1	Довести теорему в численні секвенцій і методом резолюцій.	4
2	Довести повноту заданої сукупності булевих функцій	4
3	Розв'язати систему лінійних однорідних рівнянь над двоелементним полем.	4
4	Розв'язати систему лінійних неоднорідних рівнянь в кільці цілих чисел і в кільці класів лишків.	4
5	В симетричній групі знайти клас суміжності заданого елемента відносно циклічної підгрупи, що породжена заданим елементом	4
6	Побудувати машину Тьюрінга, яка обчислює задану функцію	4
7	Застосувати оператор примітивної рекурсії до двох функцій.	4
8	Знайти результат композиції двох функцій дійсного аргумента.	4
9	Знайти логарифм числа по основі 3 в кільці класів лишків за заданим модулем.	4
10	Підготовка до контрольної роботи	5
11	Знайти породжуючу матрицю коду, якщо відома перевірна матриця	5
12	Знайти перевірочну матрицю лінійного коду, якщо відома породжуюча	5
13	Знайти логарифм заданого цілого числа по основі два з точністю до 1 без використання обчислювального пристрою.	5
	Разом	56
2 семестр		
1	Побудова мінімального кістякового дерева	4
2	Довести рівнопотужність двох множин	5
3	Підрахувати ймовірність події	4
4	З'ясувати залежність чи незалежність подій	5
5	Побудувати факторгрупу	4
6	Побудувати граф факторвідображення	5
7	Побудувати діаграму Хассе чвм з тими чи іншими умовами на найбільший та максимальні елементи	5
8	Підготовка до контрольної роботи	5
9	Підрахувати математичне очікування та дисперсію випадкової величини	5
10	Знайти виграшну стратегію у грі тітоньки Пенні (стор.446 Грехем-Кнут-Паташнік, Penney ante)	5
11	Послідовності випробувань Бернуллі	4
12	Побудувати генератрису для чисел Стірлінга	5
	Разом	56

6. Індивідуальні завдання

2 контрольні роботи.

7. Методи контролю

1-й семестр.

Поточне тестування.

Приклад завдань:

1. Записати формулою логіки висловлень, позначивши прості складові речення пропозиційними (висловлювальними) символами ``Неправда, що із подільності числа 95 на 5 випливає подільність числа 95 на 6. Такж неправдою є те, що із подільності числа 95 на 6 випливає подільність цього числа на 5``
2. Записати таблицю значень булевого виразу $(x \rightarrow \neg(xy)) \square \neg(x \square z)$
3. Записати ДДНФ (ДКНФ) для булевої функції, що задана рядком 0000 0100 1000 0010
4. Перевірити, чи рівносильні формули $f, g: f = (x \rightarrow (xy)) \square \neg(x \square z), \quad g = \neg(x y) \rightarrow (z \square y)$.
5. Довести рівнопотужність множин A, B , встановивши взаємно однозначну відповідність між елементами $A = \mathbf{Z} \setminus \{2,3\}$ і $B = \mathbf{Z} \cup \{a,b,c,d\}$
6. Записати формулою логіки предикатів ``множина A має не більше двох елементів.``
7. Зобразити підмножину (заштрихувати) кругами Ойлера $A \cup (B \setminus C)$.
8. Розв'язати рівняння $x(x-1)(x-5)(x+6)\sqrt{4-x}=0$.
9. Знайти двійковий запис числа 198.
10. Знайти обернене відображення для $f: \mathbf{Z} \rightarrow \mathbf{Z}, \quad f(1)=2, f(2)=0, f(0)=-2, f(-1)=-1, f(-2)=1; f(n)=-n$, якщо $n \in \mathbf{Z} \setminus \{-2,-1,0,1,2\}$.

Критерії оцінювання:

Всього 10 завдань, повне виконання одного завдання оцінюється 2 балами. Часткове виконання – 1 балом. Всього за тестування можна отримати 20 балів.

Контрольна робота, що передбачена робочим планом.

Приклад завдань

1. Обчислити біномний коефіцієнт.
2. Довести твердження методом повної математичної індукції: при $n > 1$.
3. Розв'язати систему рівнянь над полем $\mathbf{Z} / \text{mod } 23$
4. Знайти обернений елемент в полі класів лишків використовуючи алгоритм Евкліда.
5. Розв'язати систему порівнянь (китайська теорема про остачі)
6. Піднести до степеня, використовуючи китайську теорему про остачі
7. Зашифрувати алгоритмом RSA перші дві букви в слові ПРОДАЙ: $P=19, R=20, PR=1920, p=53, q=67, n=3551, \phi(n)=3432, e=1021, d=1021^{-1} \text{ mod } 3432 = 1237$.
8. Дешифрувати повідомлення 41, яке зашифроване алгоритмом RSA з ключем $n=p \cdot q=7 \cdot 13, e=5$.
9. В системі лінійного кодування mod 5 з із заданою перевіркою матрицею A на декодер прийшло слово a . Перевірити, чи не пошкодилося кодове слово в процесі передавання.
10. Створити машину Тьюрінга, яка обчислює функцію $f(x)$.

Критерії оцінювання:

Всього 10 завдань, повне виконання одного завдання оцінюється 2 балами. Часткове виконання – 1 балом. Всього за тестування можна отримати 20 балів.

Завдання на самостійну роботу.

Приклад вправ для самостійної роботи:

i означає номер студента в списку групи, завдання залежать від i .

1. Записати таблицю істиносних значень формули логіки висловлень .
2. Булева функція B_i задана рядком f_i . Задати її ДДНФ чи ДКНФ, таблично і поліномом Жегалкіна
3. Число $n_i = 3011 + i$ задане десятковим записом, задати його двійковим записом. Знайти m для якого $m < \log_2 n_i < m + 1$.
4. Виписати всі підмножини множини M_i
5. Зобразити кругами Ойлера області істинності предикатів $x \in A, x \in B, x \in C$ і заштрихувати область істинності предиката $x \in P_i$

Критерії оцінювання:

Завдання містить 5 задач, кожне з яких оцінюється (в залежності від повноти відповіді) від 0 до 4 балів. Всього можна одержати 20 балів.

Залік.

Приклад залікового завдання:

1. Побудувати таблицю істинності формули логіки висловлень
2. Розв'язати рівняння вигляду $\$ax=b\$$ над скінченним полем (завдання індивідуальні).
3. Встановити взаємно однозначну відповідність між елементами двох множин.
4. Зашифрувати шифром відкритого ключа.

Критерії оцінювання:

Залікове завдання оцінюється від 0 до 40 балів в залежності від повноти відповіді – від 0 до 10 балів за кожну вправу.

2-й семестр.

Методи контролю: поточне тестування, аудиторна контрольна, що передбачена планом, індивідуальні завдання, іспит.

Поточне тестування.

Приклади завдань для поточного тестування.

1. Скількома способами із гральної колоди карт (52 карти, 4 масті - дві чорні і дві червоні, в кожній масті 13 зростів) можна взяти 5 карт так, щоб
 - а) вони були розташовані підряд по зросту;
 - б) дві з них були червоні а три чорні.
2. Скільки чисел від 1 до 1000 (включно) а) не діляться ні на 5 ні на 6; б) діляться на 5 але не діляться на 6.
3. Скільки дільників має число $\$a=4^7 \cdot 6^{15} \cdot 5^8\$$; $\$b=3072.\$$
4. Використовуючи рекурентні співвідношення для чисел Стірлінга першого та другого роду обчислити числа Стірлінга першого чи другого роду з малими значеннями параметрів.

5. Скільки розв'язків в цілих числах має система

$$x_1 + x_3 + x_5 = 11, \quad x_i > 0;$$

$$x_2 + x_4 + x_6 = 5, \quad x_i > 0.$$

6. Підрахувати суму

$$\sum_{i=0}^{23} 5^i C^i_{23}.$$

7. Підрахувати коефіцієнт при $x^3 \cdot y^2 \cdot z^7$ в

$$(x+y+z)^{12}.$$

\end{enumerate}

8. Виписати перші чотири доданки формального степеневого ряду, що обернений до ряду а) $f=1-5x+7x^2+2x^3+x^4+\dots$; б) $f=1-5x$.

9. Скільки матриць

а) з 4 рядками і 7 стовпчиками, елементами яких є 0 та 1, мають різні рядки;

б) з 3 рядками і 8 стовпчиками, елементами яких є 0, 1 та 2, мають різні рядки.

10. Скільки ребер має граф а) K_7 ; б) $C_7 \circ K_2$.

Критерії оцінювання:

В поточному тестуванні пропонується 10 завдань, кожне з яких оцінюється від 0,1 або 2 бали в залежності від того завдання виконане повністю, частково, чи не виконане. Всього повністю виконані всі завдання оцінюються 20 балами.

Контрольна робота, що передбачена навчальним планом.

Приклад завдань, які пропонуються в контрольній роботі: k в умовах задач означає номер студента за списком групи.

1. Знайти кількість дільників натурального числа $15^{3+k} 6^{510^4}$.

2. Знайти кількість найкоротших шляхів з південно-західного рогу до північно-східного рогу в місті, що має $6+k$ вулиць із півдня на північ та 7 вулиць із заходу на схід

3. Знайти формулу для загального члена a_n , $n=0, 1, 2, 3, 4, \dots$ рекурентної послідовності $a_0, a_1, a_2, \dots, a_n, \dots$ де $a_0=1, \quad a_1=2, \quad a_{n+2}-(3+k)a_{n+1}+3 \cdot k \cdot a_n=0$.

$$a_{n+2}-(3+k)a_{n+1}+3 \cdot k \cdot a_n=0.$$

4. Для $1 \leq k \leq 5$: Знайти кількість сюр'єктивних відображень із множини A в множину B , якщо $|A|=k+3, \quad |B|=3$.

Для $6 \leq k \leq 10$: Знайти кількість сюр'єктивних відображень із множини A в множину B , якщо $|A|=k-3, \quad |B|=k-4$.

Для $11 \leq k \leq 16$: Знайти кількість ін'єктивних відображень із множини A в множину B , якщо $|A|=3, \quad |B|=k-5$.

Для $17 \leq k$: Знайти кількість ін'єктивних відображень із множини A в множину B , якщо $|A|=k-11, \quad |B|=k-10$.

5. Із групи, яка складається із $5k+3$ особи, вибрали $5k$ осіб. Скількома способами це можна зробити?

Критерії оцінювання:

Всього в контрольній пропонується 5 завдань, кожне з яких оцінюється від 0 до 4 балів – нічого незробилено - 0, Зроблені певні кроки у виконанні вправи - 1, завдання

виконане, але не повністю – 3, завдання виконане повністю 4 бали. Всього контрольна в залежності від виконання вправ оцінюється від 0 до 20 балів.

Завдання для самостійної роботи.

1. Задати граф з номером k (див. файл ``графи з малою кількістю вершин.jpg``)
 - а) матрицею інцидентності,
 - б) матрицею суміжності; \item списком суміжності.
2. Еквівалентність α на множині $\{22, k, 71, 72, 25, 27\}$ має три класи $A = \{27, 72\}$, $B = \{71, k, 22\}$, $C = \{25\}$. Зобразити граф цього відношення.
3. Підрахувати кількість відношень часткового порядку на множині $\{a, b, c, d\}$ які мають елемент d найбільшим - зобразити ці відношення у вигляді графів (діаграми Хассе).
4. Зобразити граф (діаграму Хассе) подільності на частково впорядкованій множині дільників числа $57+k$.
5. Граф з вершинами $\{A, B, C, D, E\}$ заданий матрицею суміжності. а) Задати його діаграмою - зобразити ребра і вершини, б) задати списком суміжності;
6. Знайти степінь вершини C в графі із попереднього прикладу.
7. Знайти мінімальне кістякове дерево для графа $W(7)$ --- ``колесо``, в якому кожна спиця (іх 7) має вагу 4, а ребра ободу (послідовно) мають вагу 2, 3, 4, 6, 7, 9
8. Відображення $f: M \rightarrow N$ де $M = \{a, b, c, d, e, f\}$ задане двома рядками.
Задати це відображення орієнтованим графом.
9. Вказати номери графів, що ізоморфні графу за номером k .

Критерії оцінювання:

Кожне завдання оцінюється або 0, 1, 2, 3 або 4 балами в залежності від ступеню виконання – Якщо завдання виконане повністю – 4 бали; якщо завдання виконане частково – 1, 2 або 3 бали, якщо завдання не виконане навіть частково – 0 балів. Всього студент за виконання роботи одержує від 0 до 40 балів.

Екзамен.

Приклад завдань:

1. (10 балів) Правило рівності в комбінаториці. Модельні задачі. Комбінаторні числа. Урнова схема.
2. (10 балів) Відображення $f: M \rightarrow N$, $M = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, $N = \{a, b, c, d, e, f\}$ задане таблично. Скільки класів має еквівалентність $x \sim y \iff f(x) = f(y)$?

$$f = \left(\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ b & a & c & b & f & b & d & e & e \end{array} \right)$$
3. (10 балів) Простір подій, генеральна сукупність, елементарна подія, ймовірність елементарної події. Подія, ймовірність події. Ріномірний ймовірнісний розподіл
4. (10 балів) Знайти степінь довіри до висловлення $p \rightarrow \neg q$ при заданому приєднаному розподілі ймовірності (0.25; 0.35; 0.3; 0.1).

Критерій оцінювання:

Екзаменаційний білет містить 4 завдання (2 теретичні і два практичні). За повне виконання завдання нараховується 10 балів. Якщо завдання не виконане навіть частково, за роботу нараховується 0 балів, повністю виконане завдання оцінюється в 10 балів. Частково виконане завдання оцінюється від 1 до 9 балів в залежності від ступеню виконання. За виконання всіх завдань студент отримує від 0 до 40 балів.

9. Схема нарахування балів**1-й семестр**

Поточний контроль, самостійна робота, індивідуальні завдання															Контрольна робота, передбачена навчальним планом	Разом	Залік	Сума
Розділ 1			Розділ 2		Розділ 3		Розділ 4		Розділ 5			Розділ 6						
T1	T2	T3	T1	T2	T1	T2	T1	T2	T1	T2	T3	T1	T2					
2	2	4	2	4	2	4	2	4	2	2	4	2	4	20	60	40	100	

2-й семестр

Поточний контроль, самостійна робота, індивідуальні завдання																	Контрольна робота, передбачена навчальним планом	Разом	Екзамен	Сума	
Розділ 1			Розділ 2		Розділ 3			Розділ 4		Розділ 5		Розділ 6			Розділ 7						
T1	T2	T3	T1	T2	T1	T2	T3	T1	T2	T1	T2	T1	T2	T3	T1	T2					T3
2	2	4	2	2	2	2	4	2	2	2	2	2	2	2	2	2	2	20	60	40	100

Шкала оцінювання

Сума балів за всі види навчальної діяльності протягом семестру	Оцінка	
	для чотирирівневої шкали оцінювання	для дворівневої шкали оцінювання
90 – 100	відмінно	зараховано
70-89	добре	
50-69	задовільно	
1-49	незадовільно	

10. Рекомендована література**Основна література**

1. Андрійчук В.І, Комарницький М.Я. Іщук Ю.Б. Вступ до дискретної математики. - Львів:Видавничий центр ЛНУ імені Івана Франка, 2003. - 254 с.
2. Бондаренко М.Ф., Білоус Н.В., Руткас А.Г. Комп'ютерна дискретна математика. - Харків, Компанія СМІТ, 2004. - 480 с.

3. И.П.Ильинская, А.И.Ильинский Дискретная математика. Сборник задач. Комбинаторика, графы, вероятность. Учебно-методическое пособие. - Харьков, 2008
4. Джеймс А.Андерсон Дискретная математика и комбинаторика - Университет Южной Каролины, Спартанбург. - Москва, Санкт-Петербург, Киев, Издательский дом Вильямс , 2004, 960 с.
5. Р. Грэхем, Д.Кнут, О.Паташник, Конкретная математика. Основание информатики — М:Мир, 1998
6. Kenneth H. Rosen “Discrete mathematics and its applications” , seven edition – 2012
7. Г.П.Гаврилов, А.А.Сапоженко «Сборник задач по дискретной математике» - М:Наука, 1977
8. Лавров И.А., Максимова Л.Л. «Задачи по теории множеств, математической логике и теории алгоритмов.- 3-изд — М:Физматлит, 1995
9. Бойко І.В. Петрик Р.М. Цуприк Г.Б. “Дискретні структури (Алгебраїчні та числові системи, комбінаторний аналіз) — Тернопіль, 2017
10. А.Шень “Математическая индукция” - М: МЦНМО, -32с.

Допоміжна література

1. Adnan Darwiche “Modeling and reasoning with Bayesian networks.” – Cambridge University Press -2009
2. Р.Хаггарти «Дискретная математика для программистов» -Москва:Техносфера, 2003 — 320 с.
3. Ю.П.Жураковський, В.В.Гніліцький “Теорія інформації та кодування в задачах”- ЖІТІ, Житомир , 2002.
4. Вербіцький О.В. “Вступ до криптології” - Львів: Науково технічна література, 1998 — 248 с.
5. Ф.Харари «Теория графов» -М:2003 (Graph Theory by Frank Harary)
6. В.В.Тишин «Дискретная математика в примерах и задачах» - Самара, 2007
7. Юрій Дрозд “Основи математичної логіки” - Київський університет імені Тараса Шевченка, механіко-математичний факультет
8. М.Г.Проценко “Логіка” - Суми, 2005
9. І.Спекторський “Навчальний посібник з дисципліни “Дискретна математика” - 2002
10. Чень Ч, Ли Р., Математическая логика и автоматическое доказательство теорем
11. С.С.Шкільняк “Математична логіка. Приклади і задачі” Навчальний посібник.- Київ, ВПЦ “Київський університет”, 2007