КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ НАУК ТА КІБЕРНЕТИКИ

Кафедра інтелектуальних програмних систем

«ЗАТВЕРДЖУЮ»
Заступник декана
з навчальної роботи

_____ Кашпур О.Ф.

«____»_____2019 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
ПРОГРАМУВАННЯ З ОБМЕЖЕННЯМИ

для студентів

галузь знань	**12 «Інформаційні технології»** *(шифр і назва)*
спеціальність	**121 «Інженерія програмного забезпечення»** *(шифр і назва спеціальності)*
освітній рівень	**бакалавр** *(молодший бакалавр, бакалавр, магістр)*
освітня програма	**«Програмна інженерія»** *(назва освітньої програми)*

вид дисципліни обов'язкова

Форма навчання	**денна**
Навчальний рік	**2018/2019**
Семестр	7
Кількість кредитів ECTS	**3**
Мова викладання, навчання та оцінювання	**українська**
Форма заключного контролю	**залік**

Викладачі: **д.ф.-м.н., проф. Кривий С. Л.** (лекції),

Пролонговано: на 20__/20__ н.р. _____(_____) «__»___ 20__р.
(підпис, ПІБ, дата)

на 20__/20__ н.р. _____(_____) «__»___ 20__р.
(підпис, ПІБ, дата)

КИЇВ – 2019

Розробник: Кривий Сергій Лук’янович д.ф.-м.н., професор кафедри «інтелектуальних програмних систем

»

ЗАТВЕРДЖЕНО

Зав. кафедри «інтелектуальних програмних систем»

_____ (Провотар О.І.)
(підпис) (прізвище та ініціали)

Протокол № від « » 2019 р.

Схвалено науково-методичною комісією факультету комп’ютерних наук та кібернетики _____

Протокол від « X » xxxxxxx 2019 року №___

Голова науково-методичної комісії _____ (Омельчук Л.Л)
(підпис) (прізвище та ініціали)

«_____» _____ 20___ року

1. Анотація дисципліни. Дисципліна „Програмування з обмежегннями” є дисципліною за вибором студентів спеціальності „Програмна інженерія”, що викладається у 7 семестрі для бакалаврів в обсязі 90 год (3-х кредитів), зокрема: 28 годин лекційних, 60 години самостійної роботи, 2 години консультації. Викладання дисципліни закінчується **заліком**.

2. Предмет навчальної дисципліни „ Програмування з обмеженнями ” включає в себе основні поняття проблеми виконуваності обмежень і, зокрема, лінійних діофантових обмежень, які ґрунтуються на застосуваннях методів лінійної алгебри, теорії складності алгоритмів, теорії груп, кілець, полів, теорії чисел та алгоритмах, які використовуються в цих теоріях (найефективніші з алгоритмів). До таких алгоритмів відносяться алгоритми тестування чисел на простоту, алгоритми модульної арифметики та чисельні алгоритми розв’язання систем лінійних обмежень в скінченних полях, кільцях, множині натуральних та цілих чисел. Розглядаються численні застосування побудованих методів розв’язання такого типу обмежень.

3. Попередні вимоги до опанування або вибору навчальної дисципліни

Базовими дисциплінами є «Основи загальної алгебри», «Основи лінійної алгебри». Для успішного вивчення дисципліни «Програмування з обмеженнями» студент повинен відповідати наступним вимогам:

1. Успішне опанування курсів:
    1. Дискретна математика.
    2. Основи загальної та лінійної алгебри.
    3. Основи теорії чисел та скінченних автоматів.
    4. Теорія складності алгоритмів і програм.
    5. Основи програмування.
2. Знання:
    1. Основних понять та методів лінійної та загальної алгебри.
    2. Основних алгоритмів теорії скінченних автоматів.
    3. Основних класів складності та аналізу складності алгоритмів.
    4. Основних алгоритмів теорії чисел.
3. Вміти:
    1. Виконувати аналіз проблеми, що виникає.
    2. Будувати математичні моделі відповідних предметних областей.
    3. Оцінювати часову і ємнісну складність алгоритмів і програм.
4. Володіти:
    1. Базовими навичками використання інтегрованих середовищ розробки програмного забезпечення.
    2. Англійською мовою на рівні не нижче Intermediate.

4. Завдання (навчальні цілі):

Основними завданнями дисципліни «Математичні основи захисту інформації» є засвоєння основних математичних ідей, методів та програмних засобів захисту інформації, відповідно до кваліфікації фахівець з інформаційних технологій. Зокрема, розвивати:

- Здатність до абстрактного мислення, аналізу та синтезу (ЗК-1).
- Здатність застосовувати знання у практичних ситуаціях (ЗК-2).
- Здатність спілкуватися державною мовою як усно, так і письмово (ЗК-3).
- Здатність спілкуватися іноземною мовою як усно, так і письмово (ЗК-4).

- Здатність вчитися і оволодівати сучасними знаннями (ЗК-5).
- Здатність до пошуку, обробки та аналізу інформації з різних джерел (ЗК-6).
- Здатність працювати в команді (ЗК-7).
- Здатність приймати обґрунтовані рішення (ЗК-14).

5. Результати навчання за дисципліною:

Результат навчання (1. знати; 2. вміти; 3. комунікація; 4. автономність та відповідальність)		**Форми (та/або методи і технології) викладання і навчання**	**Методи оцінювання та пороговий критерій оцінювання (за необхідності)**	**Відсоток у підсумковій оцінці з дисципліни**
Код	**Результат навчання**			
РН1.1	*Знати основні математичні поняття, які використовуються в системах перевірки виконуваності обмежень.*	*Лекція, самостійна робота*	*Тест, 60% правильних відповідей, Залік*	15%
РН1.2	*Знати базові типи обмежень, їх класифікацію, технології проектування, налагодження та тестування правильності роботи*	*Лекція, самостійна робота*	*Тест, 60% правильних відповідей, Залік*	20%
РН1.3	*Знати основні алгоритми, які складають основу первірки виконуваності лінійних обмежень*	*Лекція, самостійна робота*	*Тест, 60% правильних відповідей, Залік*	15%
РН2.1	*Вміти застосовувати на практиці інструментальні програмні засоби проектування та розробки програмного забезпечення.*	*Лекція, самостійна робота*	*Поточне оцінювання*	24%
РН3.1	*Обґрунтовувати власний погляд на задачу, спілкуватися з колегами з питань проектування та розробки програм, складати письмові звіти*	*Лекція, самостійна робота*	*Поточне оцінювання*	5%
РН3.2	*Знати методи загальної алгебри, які використовуються в задачах перевірки виконуваності обмежень*	*Лекція, самостійна робота*	*Поточне оцінювання*	5%
ЗН3.3	*Знати методи лінійної алгебри, які використовуються в задачах перевірки виконуваності обмежень*	*Лекція, самостійна робота*	*Поточне оцінювання*	
РН4.1	*Організовувати свою самостійну роботу для досягнення результату*	*Лекція, самостійна робота*	*Поточне оцінювання*	8%
РН4.2	*Відповідально ставитися до виконуваних робіт, нести відповідальність за їх якість*	*Лекція, самостійна робота*	*Поточне оцінювання*	4%
РН4.3	*Застосовувати методи перевірки виконуваності обмежень для розв'язання конкретних задач (математичної логіки, теорії інформації, класифікації тощо)*	*Лекція, самостійна робота*	*Поточне оцінювання*	4%

6. Співвідношення результатів навчання дисципліни із програмними результатами навчання

Результати навчання дисципліни **Програмні результати навчання**	**РН 1.1**	**РН 1.2**	**РН 1.3**	**РН 2.1**	**РН 3.1**	**РН 3.2**	**РН 3.3**	**РН 4.1**	**РН 4.2**	**РН 4.3**
ПРН-1. Знати, аналізувати, цілеспрямовано шукати і вибирати необхідні для вирішення професійних завдань інформаційно-довідникові ресурси і знання з урахуванням сучасних досягнень науки і техніки.	+	+		+	+			+	+	
ПРН-2. Знати кодекс професійної етики, розуміти соціальну значимість та культурні аспекти інженерії програмного забезпечення і дотримуватись їх в професійній діяльності.	+	+	+	+		+				
ПРН-3. Знати основні процеси, фази та ітерації життєвого циклу програмного забезпечення.	+	+	+					+	+	+
ПРН-4. Знати і застосовувати професійні стандарти і інші нормативно-правові документи в галузі інженерії програмного забезпечення.	+	+	+		+					
ПР-5. Знати і застосовувати відповідні математичні поняття, методи побудови криптографічних систем захисту інформації.	+		+	+	+	+	+			
ПРН-6. Уміння вибирати та використовувати відповідну задачі методологію створення програмного забезпечення.					+	+	+	+		
ПРН-7. Знати і застосовувати на практиці фундаментальні концепції, парадигми і основні принципи функціонування мовних, інструментальних і обчислювальних засобів інженерії програмного забезпечення.	+		+	+	+	+				
ПРН-9. Знати і вміти використовувати методи та засоби збору, формулювання та аналізу вимог до програмного забезпечення.	+	+	+	+	+	+				+
ПРН-10. Проводити передпроектне обстеження предметної області, системний аналіз об'єкта проектування.				+	+	+		+	+	
ПР-12. Знати ефективні підходи щодо проектування програмного забезпечення.			+	+					+	+
ПР-13. Знати і застосовувати методи розробки алгоритмів, конструювання програмного забезпечення та структур даних.	+		+	+						

ПРН-14. Застосовувати на практиці інструментальні програмні засоби доменного аналізу, проектування, тестування, візуалізації, вимірювань та документування програмного забезпечення				+	+	+	+	+		
ПРН-15. Мотивовано обирати мови програмування та технології розробки для розв'язання завдань створення і супроводження програмного забезпечення.	+	+	+				+	+		
ПРН-16. Мати навички командної розробки, погодження, оформлення і випуску всіх видів програмної документації.			+		+		+	+		
ПРН-17. Вміти застосовувати методи компонентної розробки програмного забезпечення.			+	+	+	+		+	+	+
ПРН-18. Знати та вміти застосовувати інформаційні технології обробки, зберігання та передачі даних.	+	+	+	+	+		+			
ПРН-19. Знати та вміти застосовувати методи верифікації та валідації програмного забезпечення.	+	+	+	+				+	+	+
ПРН-20. Знати підходи щодо оцінки та забезпечення якості програмного забезпечення.	+	+	+		+			+		
ПРН-22. Знати та вміти застосовувати методи та засоби управління проектами.	+	+	+			+	+			
ПР-23. Уміння документувати та презентувати результати розробки програмного забезпечення.				+					+	+

7. Схема формування оцінки

7.1. Форми оцінювання студентів

Семестрове оцінювання:

1. Контрольна робота 1: РН 1.1, РН 1.2, РН 3.1, РН 4.1, РН 4.2 – 30 балів/15 балів.
2. Контрольна робота 2: РН1.2, РН 1.3, РН 3.1, РН 4.1, РН 4.2 – 30 балів/15 балів.

Підсумкове оцінювання (у формі заліку):

- максимальна кількість балів які можуть бути отримані студентом: 40 балів;
- результати навчання які будуть оцінюватись: РН1.1, РН1.2, РН1.3, РН2.1;
- форма проведення і види завдань: письмова;
- види завдань: 5 письмових завдань (2 теоретичних питання та 3 практичних завдання);
- для отримання загальної позитивної оцінки з дисципліни оцінка за залік повинна бути не меншою ніж 24 бали;
- студент не допускається до заліку, якщо протягом семестру він набрав менше ніж 36 балів;

Критерії оцінювання на екзамені

Завдання	Тема завдання	Максимальний відсоток від 40 балів	Всього відсотків
Завдання 1	Теоретичні питання за матеріалами курсу	15%	15%
Завдання 2		22,5%	22,5%
Завдання 3	Практичне завдання на основі теоретичного матеріалу курсу	25%	25%
Завдання 4		20%	20%
Завдання 5		17,5%	17,5%
			100%

7.2. Терміни проведення форм оцінювання:

1. Контрольна робота 1: до 7 тижня семестру.
2. Контрольна робота 2: до 14 тижня семестру.

Студент має право на одне перескладання кожної контрольної роботи у визначений викладачем термін.

У випадку відсутності студента з поважних причин відпрацювання та перездачі контрольних робіт здійснюються у відповідності до «Положення про порядок оцінювання знань студентів при кредитно-модульній системі організації навчального процесу» від 1 жовтня 2010 року. Якщо студент пропустив без поважних причин більше половини занять, не виконав хоча б однієї лабораторної роботи або не писав контрольної роботи, то він не допускається до складання екзамену.

Студент повинен здавати лабораторні роботи у назначені викладачем терміни. Якщо лабораторні робота не здається в назначені терміни, вона вважається такою, що не виконана студентом.

8. Шкала відповідності оцінок

Відмінно / Excellent	90-100
Добре / Good	75-89
Задовільно / Satisfactory	60-74
Незадовільно / Fail	0-59
Зараховано / Passed	60-100
Не зараховано / Fail	0-59

ТЕМАТИЧНИЙ ПЛАН ЛЕКЦІЙ І ЛАБОРАТОРНИХ ЗАНЯТЬ

№ Лекції	Назва лекції	Лекції	Лаборат роботи	Самост. робота
1	Предмет курсу програмування з обмеженнями. Лінійні обмеження, класифікація обмежень, числові обмеження.	2		3
2	Лінійні обмеження над полем дійсних чисел, полем комплексних чисел. Основні алгоритми.	2		3
3	Метод Гауса та TSS-метод розв’язання систем лінійних рівнянь в полі дійсних чисел. Складність.	2		3
4	TSS-метод розв’язання систем лінійних однорідних і неоднорідних нерівностей в полі дійсних чисел. 9-та проблема 21-го століття. Складність.	2		3

5	Розв'язання несумісних систем лінійних рівнянь. Псевдообернені матриці та метод Гренвіля. Приклади застосування.	2		3
6	Лінійні діофантові обмеження над множиною натуральних чисел. TSS-метод. Складність. Властивості методу.	2		3
7	Методи Контежан-Деві, Комона, Ромеуфа. Автоматні методи побудови базису множини розв'язків.	2		3
Контрольна робота 1				
8	Порівняння методів. Критерій сумісності ЛНДР і ЛНДН. Достатні умови сумісності. Приклади застосування.	2		3
9	Алгоритми побудови базису множини розв'язків в області {0,1}. Складність та приклади застосування.	2		3
10	TSS-метод розв'язання систем лінійних рівнянь в полі лишків за модулем простого числа. Складність та приклади застосування.	2		3
11	TSS-метод розв'язання систем лінійних рівнянь в полі за модулем p^k, де p – просте число. Складність алгоритму та приклади застосування.	2		3
12	TSS-метод розв'язання систем лінійних рівнянь в кільці лишків за модулем простого числа. Складність та приклади застосування.	2		3
13	TSS-метод розв'язання систем лінійних рівнянь в кільці цілих чисел. Складність та приклади застосування.	2		3
14	Застосування алгоритмів: математичний сейф, суперечність системи диз'юнктів, мережі Петрі, арифметика Пресбургера. Підсумки.	2		3
Контрольна робота 2				
ВСЬОГО		**28**		**42**

Загальний обсяг **120 годин**, в тому числі:
Лекцій – 20 **год.**,
Лабораторних робіт – 18 **год.**,
Самостійної роботи – 80 **год.**,
Консультації – 2 **год**.

Змістовна частина 1. *Задачі і проблематика теорії виконуваності обмежень.*

Лекція 1. Предмет математичних основ розв'язання проблеми виконуваності обмежень. Класифікація обмежень: лінійні і нелінійні, числові та символьні. Приклади. – **2год.**

Вступ до області математичних основ розв'язання проблеми перевірки виконуваності обмежень. Вступні приклади та методи їх аналізу. Класифікація обмежень. [1,2,8,9,10].

Завдання для самостійної роботи. (3 год.)

Ознайомлення з основними підходами до розв'язання числових обмежень. Симплекс метод, метод еліпсоїдів, метод Хачіяна. [6-14].

Лекція 2. Лінійні обмеження в полі дійсних чисел. Метод Гауса та TSS-метод. Складність побудови базису СЛР. Порівняння методів. Приклади. – **2год.**

Основні етапи застосування методів Гауса та TSS-методу. Ілюстрація на прикладах. Складність, спільні риси, різниця.

Завдання для самостійної роботи. (3 год.)

Обчислення базисів СЛОР (5 систем) двома методами. Порівняння часових залежностей алгоритмів. [6-14].

Лекція 3. Системи лінійних рівнянь в полі комплексних чисел. Метод редукції до поля дійсних чисел та TSS-метод розв'язання СЛР. Порівняння складності в арифметичній моделі. Приклади для ілюстрації. **– 2год.**

Розглядається два способи розв'язання СЛР в полі комплексних чисел: спосіб зведення розв'язання до СЛР в полі дійсних чисел та прямий TSS-метод розв'язання. Порівнюються методи за складністю. [5-8].

Завдання для самостійної роботи. (3 год.)

Алгоритми реалізації обох способів в мовах С і Pyton. Складність обох реалізацій. Висновки та обгрунтування. [5-12].

Лекція 4. TSS-метод розв'язання систем лінійних однорідних і неоднорідних нерівностей. 9-та проблема Смейла та підходи до її розв'язання. Ілюстрація на прикладах. **- 2год.**

TSS-метод *розв'язання СЛОН і СЛННН в полі дійсних чисел. Ілюстрація складності проблеми. Експоненціальна оцінка складності проблеми. Класи поліноміальної складності.* [5-9].

Завдання для самостійної роботи. (3 год.)

Реалізувати TSS-метод розв'язання СЛОН і СЛНН в трьох мовах програмування. Вивести середні оцінки складності реалізації. [5-10].

Лекція 5. Метоли розв'язання несумісних СЛР. Псевдообернені матриці та їх застосування в розв'язанні задачі. Метод Гренвіля побудови псевдо оберненої матриці СЛР. Складність алгоритму та приклади застосування. – **2 год.**

Завдання для самостійної роботи. (3 год.)

Реалізувати метод Гренвіля та розв'язати 4 несумісні СЛР в полі дійсних чисел.

Лекція 6. TSS-метод розв'язання систем лінійних однорідних і неоднорідних СЛР в множині натуральних чисел. Ілюстрація методу та його обґрунтування. Складність алгоритму та приклади застосування. – **2 год.**

Завдання для самостійної роботи. (3 год.)

Реалізувати TSS-метод розв'язання систем лінійних однорідних і неоднорідних рівнянь. Обгрунувати складність та вказати клас систем, які розв'язуються в поліноміальному часі. [5-9]

Лекція 7. TSS-метод розв'язання систем лінійних однорідних і неоднорідних нерівностей в множині натуральних чисел. Ілюстрація методу та його обґрунтування. Складність алгоритму та приклади застосування. – **2 год.**

Завдання для самостійної роботи. (3 год.)

Методи Контежан-Деві, Комона, Ромеуфа побудови базису множини розв'язків систем. Реалізувати TSS-метод розв'язання систем лінійних однорідних і неоднорідних нерівностей. Складність встановити та казати клас систем, які розв'язуються в поліноміальному часі. [5-14]

ТИПОВЕ ЗАВДАННЯ КОНТРОЛЬНОЇ РОБОТИ

1. Знайти базис множини розв'язків СЛОР в полі дійсних і комплексних чисел.
2. Навести класифікацію систем обмежень та вказати методи перевірки їх виконуваності.
3. Автоматні методи розв'язання СЛОР і СЛНН.
4. Методом Контежан-Деві розв'язати СЛОР.
5. TSS-методом знайти мінімальну породжуючи множину розв'язків СЛОН в полі дійсних чисел.

Контрольні запитання до змістовної частини І.

1. Дати означення проблеми виконуваності обмежень. Навести їх класифікацію. Приклади проблем.
2. Охарактеризувати загальні підходи до аналізу проблеми побудови базису множини розв'язків системи обмежень.

3. Лінійні та лінійні діофантові обмеження. Дискретні та неперервні області. Дати означення складності алгоритму в часі і пам'яті. Навести класифікацію проблем, виходячи з цього означення.
4. Арифметична модель складності и модель складності Тьюрінга. Приклади. Багатосрічкові МТ. Який часовий зв'язок існує між цими моделями обчислень.
5. Означення групи, кільця та поля. Навести основні властивості цих алгебр. СЛОР над цими областями.
6. Алгоритми обчислення теоретико-числових функцій НСД, НСК, порівняння за складеним і простим модулем.
7. Охарактеризувати методи Контежан-Деві, Комона та Потьє. Метод Гауса скорочення числа рівнянь. Порівняльна характеристика.

Змістовна частина II. *Основні методи побудови базису множини розв'язків СЛОН і СЛНН в множині цілих чисел, а також в області {0,1}. Основні алгоритми побудови базису множини розв'язків в скінченних кільцях та полях. Застосування побудованих алгоритмів для аналізу властивостей мереж Петрі, арифметики Пресбургера, суперечності системи диз'юнктів, розпізнавання зображень на площині.. Приклади.*

Лекція 8. Системи лінійних однорідних і неоднорідних нерівностей в області {0,1}. Критерій сумісності. Застосування до розв'язання задачі побудови незалежних множин вершин в графах. **-2 год.** [5-12].

СЛОН і СЛНН та методи їх розв'язання. Критерії сумісності та оцінки складності. Класи систем з поліноміальними оцінками складності. [5-12].

Завдання для самостійної роботи. (3 год.)

Розглянути відповідні розділи лінійної алгебри та лінійних нерівностей. Дати означення конуса розв'язків, поліедра розв'язків та загального розв'язку СЛО. [6,8,14].

Лекція 9. Алгоритми побудови базису множини розв'язків СЛОР і СЛНР в кільцях лишків. Загальний розв'язок СЛНР та метод його побудови. Приклади застосування. – **2год.**

Декомпозиція СЛОР за модулем складеного числа на СЛОР за простими модулями.Розв'язання СЛОР в примарних кільцях. Складність алгоритмів. Основна теорема арифметики та наслідки з неї. Проблема факторизації та її зв'язок з проблемою розв'язання СЛОР. Приклади використання. [1-9].

Завдання для самостійної роботи. (3 год.)

Методи розв'язання рівнянь та порівнянь в кільцях лишків. Алгоритм розв'язання системи порівнянь та його реалізація TSS-метод та алгоритм його реалізації в різних мовах програмування: C, JAVA, Pyton. Порівняння часових оцінок виконання алгоритмів в різних реалізаціях. [1-8].

Лекція 10. TSS-метод розв'язання систем лінійних рівнянь в полі лишків за модулем простого числа. Складність та приклади застосування. Можливість розширення поля лишків. Приклади. – **2 год.**

Розглядаються TSS-метод *розв'язання СЛР в полі лишків за модулем простого числа та його розширення за модулем незвідного полінома. Складність алгоритмів та приклади їх застосування.* [1-8].

Завдання для самостійної роботи. (3 год.)

Методи побудови поля лишків та його розширень. Приклади побудови поля порядку 8 і 27. Реалізація основних алгоритмів та їх часова характеристика. [5-12].

Лекція 11. TSS-метод розв'язання СЛОР в полях лишків та його застосування в криптографії та математичних іграх. Складність алгоритмів та їх застосування. **– 2 год.**

Розглядаються методи побудови розширення поля лишків за допомогою незвідного полінома на д полем лишків за модулем простого числа. Алгоритми тестування незвідності полінома. Побудова поля та складність цієї побудови. [1-8].

Завдання для самостійної роботи. (3 год.)

Реалізація алгоритмів тестування на незвідність поліномів, алгоритм Шаміра. Побудова 6-7 полів, які ілюструють роботу алгоритму, оцінити складність кожного приклада. [1-8].

Лекція 12. Порівняння методів. Критерій сумісності ЛНДР і ЛНДН. Достатні умови сумісності. Приклади застосування. **– 2 год.**

Розглядаються порівняльні характеристики розроблених алгоритмів відносно часових оцінок складності. Визначення класів систем обмежень, які мають поліноміальні оцінки складності. Ілюстрація методів на прикладах.

Завдання для самостійної роботи. (3 год.)

Розв'язання систем обмежень для знайдених окремих класів та загального типу систем. Визначення середньої оцінки складності. Яка основна проблема широкого застосування побудованих алгоритмів. Порівняння часових характеристик реалізацій шифрів в різних мовах програмування. [5,6,10,14].

Лекція 13. TSS-метод розв'язання систем лінійних рівнянь в кільці цілих чисел. Складність та приклади застосування. **– 2 год.**

Розглядається TSS-метод розв'язання систем лінійних рівнянь в кільці цілих чисел. Побудова предбазису та базису СЛОР і СЛНР, Досліджуються його властивості та недоліки. Ілюстрація методів на прикладах. [1-8].

Завдання для самостійної роботи. (3 год.)

Побудувати 6-7 прикладів, які ілюструють роботу алгоритмів. Оцінити складність кожного приклада та порівняти часові характеристики реалізації алгоритму в різних мовах програмування. [1-12].

Лекція 14. Застосування алгоритмів: математичний сейф, суперечність системи диз'юнктів, мережі Петрі, арифметика Пресбургера. Підсумки. **– 2 год.**

Розглядаються застосування розроблених алгоритмів до розв'язання задач перевірки виконуваності множини диз'юнктів, формул арифметики Пресбургера, математичних ігор та аналізу властивостей мереж Петрі. [3-8].

Завдання для самостійної роботи. (3 год.)

Розглянути 6-7 задач та їх розв'язання для перелічених областей. Підготовка до складання заліку. [1-16].

ТИПОВЕ ЗАВДАННЯ КОНТРОЛЬНОЇ РОБОТИ

1. Побудувати поле з 9 елементів та навести його таблицю Келі для операцій додавання та множення.
2. Охарактеризувати переваги та недоліки методів розв'язання СЛОР, СЛНР. Та СЛНН в множині натуральних та цілих чисел.
3. Побудувати таблиці операцій кілець за модулями 12, 8 та 24. Які з цих кілець будуть примарними? Декомпозиція на підсистеми.
4. Розв'язати СЛОР і СЛНР в кільці зо модулем 12 та 24. Знайти загальний розв'язок СЛНР.
5. Виконати побудову полів за модулем 8, 9 та 16. Розв'язати задачу про математичний сейф
6. в цих полях.
5. Перевірити суперечність мнодини диз'юнктів. Знайти мінімальні суперечні підмножини диз'юнктів, якщо вони є. Перевірити виконуваність формул арифметики Пресбургера.

Типу рівності і нерівності.

3,11 та 9.

Контрольні запитання до змістовної частини II.

1. Яке поле називається простим, полем характеристики 0 та простої характеристики. Навести приклади та їх обґрунтувати. В яких задачах використовуються поля?
2. Побудувати комутативне кільце порядку 6 та за модулем 6. В чому різниця між цими кільцями і що є спільного? Розв'язати СЛОР і СЛНР в цих кільцях.
3. Охарактеризувати методи розв'язання СЛР над множинами натуральних та цілих чисел.
4. Застосування методів до перевірки виконуваності формул арифметики Пресбургера та суперечності множини диз'юнктів.
5. Основні задачі, які розв'язуються в скінченних кільцях та полях. Їх характеристика.
6. Методи аналізу властивостей мереж Петрі за допомогою розроблених алгоритмів. Які властивості мереж Петрі досліджуються цими алгоритмами?

Рекомендована література

1. Виноградов И.М. Основы теории чисел. - М.: Наука. - 1972.- 167 с.
2. Вирт Н. Систематическое программирование. - М.: Мир. - 1985.- 183 с.
3. Кнут Д. Искусство программирования для ЭВМ. т. 2 Получисленные алгоритмы. - М.: Мир. - 1977.- 723 с.
4. Коблиц Н. Курс теории чисел и криптографии. - М.: Изд-во ТВП. - 2001.- 260 с.
5. Кривий С.Л. Дискретна математика: вибрані питання. - Київ: Видавничий дім ``Києво-Могилянська академія". - 2007. - 570 с.
6. Кривий С.Л. Дискретна математика. - Чернівці: Букрек. - 2017. - 567 с.
7. Кривий С.Л. Лінійні діофантові обмеження та їх застосування. - Чернівці: Букрек. – 2015. - 222 с.
8. Чарин В..С. Линейные преобразования и выпуклые множества. – К.:Вища школа. – 1978. – 188 с.
9. Черников С.Н. Линейные неравенства. М.: Наука. – 1968. – 488 с.
10. Hadbook of Constraint Programming (ed. F.Rossi, van Beek and T. Walsh). – Elsevier. – 2006 . – 955 p.
11. Rabin M. Probabilistic Algorithm for Primality Testing. - Journal of Number Theory, December. 1980. - P. 70-79.
12. Matyas S., Le A., Abracham D. A Key Management Scheme Based onh Control Vektors. – IBM System Journ. N 3. - 1991. - P. 21--29.
13. Papadimtriou C. H. Zlozonosc obliczeniowa. - Wydawnictwo Naukowo-Techniczne, Warszawa. - 2002. - 540 s.
14. Bockmair A., Weispfenning V. Solving Numerical Constraints. - In Handbook of Automated Reasoning. - Elsevier Science Publishers B.V. - 2001. - P. 753-842.

Додаткова література

15. Yuval C. How to Swindle Rabin. - Cryptologia. - July. - 1979.
16. Menezes A., van Oorschot P., Vanstons S. Handbook of Applied Cryptography. -CRC Press. - 1996. - 661 p.