КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА

Механіко-математичний факультет
Кафедра алгебри і комп'ютерної математики

«ЗАТВЕРДЖУЮ»
Заступник декана/директора
з навчальної роботи
Харитонов О.М.
«31» серпня 2020 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Алгебраїчна геометрія і її застосування в криптографії

(повна назва навчальної дисципліни)

для студентів

галузь знань 11 математика та статистика
(шифр і назва)

спеціальність 111 математика
(шифр і назва спеціальності)

освітній рівень магістр
(молодший бекалавр, бакалавр, магістр)

освітня програма математика
(назва освітньої програми)

вид дисципліни обов'язкова

Форма навчання	денна
Навчальний рік	2020/2021
Семестр	2
Кількість кредитів ECTS	4
Мова викладання, навчання та оцінювання	українська
Форма заключного контролю	залік

Викладачі: професор А.П.Петравчук

Пролонговано: на 2021/2022 н.р. _____(Харитонов)_ «31» серпня 2021р.
(підпис, ПІБ, дата)

на 20__/20__ н.р. _____(_____)_ «___»_____20__р.
(підпис, ПІБ, дата)

КИЇВ – 2020

Розробник Петравчук Анатолій Петрович, д.ф.-м. н., професор завідувач кафедри алгебри і комп'ютерної математики

ЗАТВЕРДЖЕНО
Завідувач кафедри _____

_____ (Петравчук А.П.)
(підпис) (прізвище та ініціали)
Протокол № 1 від "11" серпня 2020 року

Схвалено науково-методичною комісією механіко-математичного факультету

Протокол № 1 від « 31 » серпня 2020 року

Голова науково-методичної комісії _____ (Олійник А.С.)
(підпис) (прізвище та ініціали)
« 31 » серпня 20 20 року

ВСТУП

Навчальна дисципліна «Алгебраїчна геометрія і її застосування в криптографії» є складовою освітньої програми підготовки фахівців за освітнім рівнем «магістр» галузі знань 11 математика та статистика зі *спеціальності* 111 математика освітньої програми «математика».

Дана дисципліна є обовязковою.

Викладається у **2** семестрі 1 курсу в обсязі **120 год**. ***(4 кредити ECTS[1])*** зокрема: *лекції – всього 20 год., практичні заняття – всього 16 год., самостійна робота – 80 год, консультації 4 год.* У курсі передбачено 2 *змістових модулі* та 2 *модульні контрольні роботи*. Завершується дисципліна **заліком.**

1. Мета дисципліни – ознайомлення та оволодіння основами алгебраїчної геометрії, зокрема, теорії алгебраїчних кривих, та їх застосуваннями до сучасних методів захисту інформації. Завданням дисципліни є підготовка студентів до самостійного вивчення відповідної науково-технічної літератури та використання набутих знань та навичок у практичній роботі.

2. Попередні вимоги до опанування або вибору навчальної дисципліни

1. *Знати* основні поняття, факти і теореми аналітичної геометрії, лінійної алгебри, алгебри і теорії чисел, математичного аналізу.

2. *Вміти* активно використовувати та творчо застосовувати зазначені вище знання в процесі опрацювання матеріалу курсу «Алгебраїчна геометрія і її застосування в криптографії».

3. *Володіти елементарними навичками* роботи з многочленами над полями, з комутативними кільцями, ідеалами, фактор-кільцями, досліджувати функції однієї та кількох змінних засобами математичного аналізу, вміти проводити обчислення в скінченних полях, вміти працювати зі скінченнопородженими абелевими групами

3. Анотація навчальної дисципліни. В курсі «Алгебраїчна геометрія і її застосування в криптографії» висвітлюються базові відомості, поняття, факти алгебраїчної геометрії та комутативної алгебри. Зокрема, розглядаються: афінні простори над полями, афінні алгебраїчні многовиди, проективні простори, проективні алгебраїчні многовиди, регулярні відображення многовидів, дивізори, теореми Гільберта про базис і про нулі, проективні криві, еліптичні криві і їх застосування в криптографії.

4. Завдання (навчальні цілі). Досягнення основних *загальних компетентностей*, зокрема, здатностей: 1) Здатність учитися, здобувати нові знання, уміння, у тому числі в галузях, відмінних від математики (ЗК–1); 2) Здатність використовувати у професійній діяльності знання з галузей математичних, природничих, соціально-гуманітарних та економічних наук (ЗК-2); 3) вирішувати проблеми у професійній діяльності на основі абстрактного мислення, аналізу, синтезу та прогнозу (ЗК-3); 4) Здатність до пошуку, оброблення й аналізу інформації з різних джерел, необхідної длярозв'язування наукових і професійних завдань (ЗК-4); 5) Здатність генерувати нові ідеї (ЗК-5); Здатність спілкуватися державною мовою і усно, і письмово (ЗК-8); 9) Здатність спілкуватися іноземною мовою (ЗК-9);
10) Здатність грамотно будувати комунікацію, виходячи з мети і ситуації спілкування (ЗК-10); 11) Здатність критично оцінювати та переосмислювати власний і чужий досвід, аналізувати свою професійну й соціальну діяльність (ЗК-11);. Досягнення основних *спеціальних компетентностей*: Знання на рівні новітніх досягнень, необхідні для дослідницької та/або інноваційної діяльності у сфері математики та її практичних застосувань (ФК-1); 11) Спроможність розуміти проблеми та виділяти їхні суттєві риси (ФК-4); 12)

[1] кредитів ECTS – кредит кратний 30 годинам.

Спроможність розробляти математичну модель ситуації з реального світу та переносити математичні знання у нематематичні контексти (ФК-5); 13)Здатність доводити знання та власні висновки до фахівців та нефахівців (ФК-6); 14) Здатність до розвитку нових та удосконалення існуючих математичних методів аналізу, моделювання, прогнозування, розв'язування нових проблем у нових галузях знань (ФК-8).

5. Результат навчання за дисципліною. **Табл.1**

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**			
1.	**Студент повинен знати:**	лекційні заняття, практичні заняття, самостійна робота	Письмові модульні контрольні роботи, оцінювання роботи під час лекцій, оцінювання виконання завдань для самостійної роботи, опитування під час практичних занять, іспит	До 50%
1.1	Знати: поняття афінного алгебраїчного многовиду, визначального ідеалу многовиду, нетерового кільця і модуля над комутативним кільцем			10%
1.2	Знати основні властивості топології Зариського на афінних алгебраїчних многовидах,			10%
1.3	Знати: теорему Гільберта про базис і теорему Гільберта про нулі			10%
1.4	Знати основні поняття, повязані з застосуванням еліптичних кривих в криптографії.			20%
2.	**Студент повинен уміти:**	лекційні заняття, практичні заняття, самостійна робота	Письмові модульні контрольні роботи, оцінювання роботи під час лекцій, оцінювання виконання завдань для самостійної роботи, опитування під час практичних занять, іспит	До 35%
2.1	Уміти будувати проективне замикання афінної кривої і знаходити проекції проективної кривої на відповідні афінні частини			10%
2.2	Уміти знаходити кількість точок на еліптичній кривій над скінченним полем, а також будувати еіптичні криві випадковим чином			10%
2.3	Уміти виконувати дії з дивізорами на кривих, будувати головні дивізори, знаходити відповідні простори.			10%
2.4	Уміти виконувати операцію додавання точок на еліптичній кривій.			10%
3.	**Комунікація**	лекційні заняття, самостійна робота	*Активна робота на лекційних*	До 5%

			заняттях, іспит	
3.1	Володіти знаннями грамотної побудови комунікації в освітньому і науковому процесі, відбору вихідних даних дослідження, складання списку використаних джерел, опису наукових результатів			
4.	**Автономність та відповідальність**	Лекційні заняття, практичні заняття, самостійна робота	Письмові модульні контрольні роботи, оцінювання під час практичних занять, оцінювання виконання завдань для самостійної	До 10%
4.1	Уміти самостійно планувати виконання дослідницького та/або інноваційного завдання та формулювати висновки за його результатами	Лекційні заняття, практичні заняття, самостійна робота	Письмові модульні контрольні роботи, оцінювання під час практичних занять, оцінювання виконання завдань для самостійної	До 10%

1. Активна робота на лекційних заняттях: РН1.1 – РН1.4, РН 2.1-РН2.4, РН 3.1, – 10 балів/6 балів;

2. Виконання завдань, винесених на самостійну роботу: РН 2.1-РН2.4, РН4.1 – 10 балів/6 балів;

3. Контрольна робота 1: РН1.1-РН1.2, РН2.1-2.2 – 15 балів/9 балів;

4. Контрольна робота 2: РН1.3-РН1.4, РН2.3, РН2.4 – 15 балів/9 балів;

5. Розв'язання задач на практичних заняттях: РН1.1 – РН1.4, РН 2.1-РН2.4, 4.1 – 10 балів/5 балів;

Разом має бути 60/35

- підсумкове оцінювання: іспит.

- *максимальна кількість балів, які можуть бути отримані:* 40 балів;
- *результати навчання, які будуть оцінюватись:* РН1.1 – РН1.4, РН 2.1-РН2.4, РН 3.1

форма проведення і види завдань: письмова робота.

6. Співвідношення результатів навчання дисципліни з програмними результатами

Табл.2

Результати навчання (код) / Програмні результати навчання	1.1	1.2	1.3	1.4	1.5	2.1	2.2	2.3	2.4	2.5	3.1	4.1
Знання												
Знати та розуміти фундаментальні і прикладні аспекти наук у сфері математики (ПРН-З-1)	+	+	+	+	+	+	+	+	+			
Відтворювати знання фундаментальних розділів математики в обсязі, необхідному для володіння математичним апаратом відповідної галузі знань і використання математичних методів у обраній професії (ПРН-З-2)	+	+	+	+	+	+	+	+	+			
Володіти основами математичних дисциплін і теорій, зокрема які вивчають моделі природничих і соціальних процесів (ПРН-З-3);	+	+	+	+	+	+	+	+	+			
Володіти математичними методами аналізу, прогнозування та оцінки параметрів моделей, математичними способами інтерпретації числових даних та принципами функціонування природничих процесів (ПРН-З-4).	+	+	+	+	+	+	+	+	+			
Уміння												
Уміти використовувати фундаментальні математичні закономірності у професійній діяльності (ПРН-У-1)	+	+	+	+	+	+	+	+	+			
Читати і розуміти фундаментальні розділи математичної літератури та демонструвати майстерність їх відтворення в аргументованій усній та/або письмовій доповіді (ПРН-У-2);	+	+	+	+	+	+	+	+	+			
Доносити професійні знання, власні обґрунтування і висновки до фахівців і широкого загалу (ПРН-У-3);											+	+
Бути наполегливим у досягненні мети під час вирішення математичної проблеми (ПРН-У-8);	+	+	+	+	+	+	+	+	+			
Усно й письмово спілкуватися рідною та іноземною мовами в науковій, виробничій та соціально-суспільній сферах діяльності із професійних питань; читати спеціальну літературу; знаходити, аналізувати та використовувати інформацію з різних довідкових джерел (ПРН-У-10);	+	+	+	+	+	+	+	+	+		+	
Використовувати раціональні способи пошуку та використання науково-технічної інформації, включаючи засоби електронних інформаційних мереж; застосовувати інформаційні ресурси, у тому числі електронні, для пошуку відповідних математичних моделей (ПРН-У-	+	+	+	+	+	+	+	+	+	+		

11);												

7. Схема формування оцінки

7.1 Форми оцінювання студентів:

- результати навчання 1.1 – 1.4 [**знання**] до 50 %;
- результат навчання 2.1 – 2.4 [**вміння**] – до 35%;
- результат навчання 3.1 [**комунікація**] – до 5%;
- результат навчання 4.1 [**автономність та відповідальність**] – до 10%.

- семестрове оцінювання **Табл.3**

Вид оцінювання	***ЗМ 1***		***ЗМ 2***	
	Min. – _ балів	*Max. – __ балів*	*Min. – _ балів*	*Max. – __ балів*
Активність на заняттях і виконання позааудиторної самостійної роботи	6	10	6	10
Модульна контрольна робота	12	20	12	20

- підсумкове оцінювання:

- форма оцінювання у 2 семестрі – залік;

- максимальна кількість балів, які можуть бути отримані студентом на заліку, становить 40 балів;

- оцінюватися будуть результати навчання з кодами 1.1 – 1.4, 2.1 – 2.4;

- форма заліку в 2 семестрі – письмово-усна; екзаменаційний білет заліку складається із 3 завдань, два з яких є теоретичним і оцінюються від 0 до 12 балів, а останнє – задача, які оцінюються від 0 до 16 балів; додатково від 0 до 8 балів студент отримує за усне опитування;

- мінімальний пороговий рівень для отримання загальної позитивної оцінки за залік не може бути меншим за **20 балів**. У випадку, коли студент на заліку набрав менше вказаної кількості балів (незалежно від кількості балів, отриманих під час семестру), в відомості у колонці «бали за залік» ставиться «0», а в колонку «результуюча оцінка» переноситься лише кількість балів, отриманих під час семестру.

7.2 Організація оцінювання.

На кожній лекції викладачем фіксується активність студентів, рівень сприйняття матеріалу шляхом усного опитування, а також виконання завдань для позааудиторної роботи. Модульні контрольні роботи проводяться на 10-му та 14 тижнях 2-го семестру. Р

Критично-розрахунковий мінімум балів за навчання впродовж семестру становить **20** балів, рекомендований мінімум, розрахований з урахуванням специфіки дисципліни, становить **35** балів. Студенти, які протягом семестру набрали сумарно меншу кількість балів, ніж рекомендований мінімум – **35** балів, для підвищення балів отримують можливість написати додаткову контрольну роботу та виконати додаткові завдання з самостійної роботи. Мінімальна кількість балів, які додаються до семестрових – 20 балів, тобто, якщо оцінка студента на заліку є нижчою від мінімального порогового рівня (20 балів), то бали за залік не додаються до семестрової оцінки.

У випадку відсутності студента з поважних причин відпрацювання та перездачі форм контролю здійснюються у відповідності до „Положення про організацію освітнього процесу в Київському національному університеті імені Тараса Шевченка" (2018), http://www.univ.kiev.ua/pdfs/official/Organization-of-the-educational-process.pdf.

7.3 Шкала відповідності оцінок

Зараховано/ Passed	60 – 100
Не зараховано/ Fail	0 – 59

8. Структура навчальної дисципліни. Тематичний план лекцій та самостійної роботи

10 семестр

№ теми	Назва теми	Кількість годин			
		Лекції	практичні	самост. робота	Консульта-тації
Змістовий модуль 1 **Афінні та проективні алгебраїчні многовиди**					
1	*Афінні алгебраїчні многовиди, топологія Зариського, приклади. Поняття нетерового кільця і нетерового модуля над комутативним кільцем, теорема Гільберта про базис. Регулярні функції на многовидах, кільце регулярних функцій, його властивості. Регулярні і раціональні відображення многовидів, раціональні многовиди.*	4	4	20	
2	*Радикальні ідеали кілець, теорема Гільберта про нулі. Поняття проективного простору, проективні многовиди, приклади. Теорема Гільберта про нулі для проективних многовидів. Алгебраїчні криві, особливі точки.*	6	4	20	2
Модульна контрольна робота 1					
Змістовий модуль 2 **Еліптичні криві, їх застосування в криптографії**					
3	*Поняття еліптичної кривої, основні властивості. Приклади еліптичних кривих, зв'язок з комплексним аналізом. Еліптичні криві над скінченними полями. Задача дискретного логарифмування на еліптичних кривих. Еквівалентність геометричного і алгебраїчного додавання точок на еліптичній кривій.*	6	4	20	
4	*Явні обчислення на еліптичних кривих. Оцінка точок на еліптичній кривій. Застосування еліптичних кривих в криптографії. Теоретико-числові застосування еліптичних кривих.*	4	4	20	2
Модульна контрольна робота 2					
	ВСЬОГО	**20**	**16**	**80**	**4**

Загальний обсяг ***120*** *год.,* в тому числі:
Лекції – ***20*** *год.*
Практичні – **16** *год.*
Самостійна робота -**80** *год.*
Консультації – **4** *год.*

Перелік питань до заліку за 10-й семестр

1. Афінні многовиди. Приклади
2. Нетерові кільця. Теорема Гільберта про базис.
3. Регулярні та раціональні відображення.
4. Раціональні многовиди.
5. Проективні многовиди
6. Алгебраїчні криві, їх зв'язок з полями раціональних функцій.
7. Дивізори на кривих.
8. Теорема Рімана-Роха.
9. Еліптичні криві.
10. Еліптичні криві над скінченними полями.
11. Задача дискретного логарифмування на еліптичних кривих.
12. Явні обчислення на еліптичних кривих.
13. Еквівалентність «геометричного» та «алгебраїчного» додавання точок на кривій.
14. Оцінка кількості точок на еліптичній кривій над скінченним полем.
15. Теоретико-числові застосування еліптичних кривих.

Типовий білет для заліку

1. Проективні многовиди. (12 балів)
2. Теорема Гільберта про базис (12 балів)
3. Знайти всі точки еліптичної кривої $E(F_5) : y^2 = x^3 + x + 1$ над полем F_5: (16 балів)

Рекомендована література

Базова

1. Ю.Дрозд. Вступ до алгебричної геометрії. ВНТЛ-Класика, Львів, 2004.
2. Н.Коблиц. Курс теории чисел и криптографии. Научное изд. ТВП. Москва, 2001.
3. И.Р.Шафаревич. Основы алгебраической геометрии. Том 1. Наука, Москва, 1988.
4. Б.Я.Рябко, А.Н.Фионов. Криптографические методы защиты информации. Горячая линия–Телеком. Москва, 2005.
5. Н.Смарт. Криптография. Техносфера. Москва, 2005.

Додаткова

6. А.Гурвиц, Р.Курант. Теория функций. Наука. Москва, 1968.
7. Д.Кокс, Дж.Литтл, Д.О'Ши. Идеалы, многообразия и алгоритмы. Мир. Москва, 2000.
8. S.Goldwasser, M.Bellare. Lecture Notes on Criptography. MIT, 2008.
9. J.Hoffstein, J.Pipher, J.H.Silverman. An Introduction to Mathematical Cryptography. Springer, 2008.
10. D.R.Stinson. Cryptograhy. Theory and Practice. Chapman and Hall, Boca Raton, 2006.