Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Новгородский государственный университет имени Ярослава Мудрого»
Институт электронных и информационных систем
Кафедра прикладной математики и информатики

УТВЕРЖДАЮ
Директор ИЭИС
_____ Б.И. Селезнев
«23» апреля 2014 г.

ПРИКЛАДНЫЕ ЗАДАЧИ ТЕОРИИ ЧИСЕЛ

Дисциплина для направления
010400.62 Прикладная математика и информатика

Рабочая программа

СОГЛАСОВАНО
Начальник учебного отдела
_____ О.Б. Широколобова
«23» апреля 2014 г.

Разработал
профессор кафедры ПМИ
_____ В.А. Едемский
Принято на заседании кафедры ПМИ

Протокол № 9 от 08.04 2014 г.
Заведующий кафедрой
_____ А.В. Колногоров
«08» 04 2014 г.

1 Цели и задачи дисциплины

Целью дисциплины является формирование навыков студентов в области применения современного математического аппарата теории чисел в исследовательской деятельности, способствующей становлению их готовности к решению задач профессиональной деятельности.

Основными задачами дисциплины являются:

- формирование у студентов необходимого объема знаний по специальным разделам теории чисел;
- ознакомление студентов с особенностями применения теории чисел для решения прикладных задач;
- овладение уменьем решать практические задачи и производить обработку данных на ЭВМ;
- выработка навыков активного применения пакетов прикладных программ для ПЭВМ.

2 Место дсциплины в структуре ООП направления подготовки

Дисциплина «Прикладные задачи теории чисел» входит в учебный план подготовки бакалавров по направлению 010400.62 - Прикладная математики и информатика, Б2.ВВ7.1 и читается в 8-м семестре. Она использует соответствующие разделы дисциплин «Дискретная математика», «Геометрия и алгебра». Для успешного усвоения дисциплины студент должен знать основные понятия и методы теории чисел, абстрактной алгебры.

Базовые знания по прикладным задачам теории чисел, полученные при изучении данного курса, используются при научно-исследовательской работе бакалавров и выполнении выпускных квалификационных работ.

3 Структура и содержание рабочей программы

3.1 Трудоемкость рабочей программы

В структуре дисциплины выделены следующие темы в качестве самостоятельных разделов: специальные разделы теории чисел и алгебры; математический аппарат для синтеза и формирования последовательностей; математический аппарат для анализа последовательностей.

Учебная работа (УР)	Всего	Распределение по семестрам
		8 сем.
Трудоемкость дисциплины в зачетных единицах (ЗЕ)	2	2
Распределение трудоемкости по видам УР в академических часах (АЧ):	72	72

1) Раздел 1 Специальные разделы теории чисел и алгебры		
- лекции	5	4
- практические занятия	6	5
- аудиторная СРС	4	4
- внеаудиторная СРС	12	12
2) Раздел 2 Математический аппарат для синтеза и формирования последовательностей		
- лекции	5	5
- практические занятия	7	7
- аудиторная СРС	4	4
- внеаудиторная СРС	12	12
3) Раздел 3 Математический аппарат для анализа последовательностей		
- лекции	5	5
- практические занятия	7	7
- аудиторная СРС	4	4
- внеаудиторная СРС	13	13
Аттестация: - зачет		

3.2 Содержание и структура разделов дисциплины

Раздел 1 Специальные разделы теории чисел и алгебры (5/6/4/12)

Сравнения и их свойства. Первообразные корни и циклотомические классы. Разностные множества. Конечные поля. Разбиения множества целых чисел. Циклотомические числа и их свойства.

Раздел 2 Математический аппарат для синтеза и формирования последовательностей (5/7/4/12)

Математические методы формирования псевдослучайных последовательностей на основе теории сравнений и конечных полей. Обобщенное правило кодирования последовательностей на основе циклотомических классов. Последовательности Лежандра, Холла, Сидельникова. Обобщенные циклотомические последовательности.

Раздел 3 Математический аппарат для анализа последовательностей (5/7/4/13)

Циклотомические числа и корреляционные свойства циклотомических последовательностей. Методы анализа линейной сложности циклотомических последовательностей. Свойства последовательностей Лежандра, Холла, Сидельникова и других. Исследование обобщенных циклотомических последовательностей.

Календарный план, наименование разделов дисциплины с указанием трудоемкости по видам учебной работы представлены в технологической карте дисциплины (приложение Б).

3.3 Организация изучения дисциплины

Методические рекомендации по организации изучения дисциплины с учетом использования в учебном процессе активных и интерактивных форм проведения учебных занятий даются в Приложении А.

4 Контроль и оценка качества освоения дисциплины

Контроль качества освоения студентами дисциплины «Прикладные задачи теории чисел» осуществляется непрерывно в течение всего периода обучения с использованием балльно-рейтинговой системы (БРС), являющейся обязательной к использованию всеми структурными подразделениями университета.

Для оценки качества освоения модуля используются формы контроля: текущий – регулярно в течение всего семестра; семестровый – по окончании изучения дисциплины.

Текущий контроль осуществляется во время выполнения практических аудиторных и внеаудиторных заданий, проведения контрольной работы.

Максимальное количество баллов по модулю – 100.

В качестве оценочных средств на протяжении семестра используются: разноуровневые задачи, опросы, индивидуальные домашние задания, контрольные работы.

Содержание видов контроля и их график отражены в технологической карте дисциплины (Приложение Б).

5 Учебно-методическое и информационное обеспечение

Учебно-методическое и информационное обеспечение дисциплины представлено Картой учебно-методического обеспечения (Приложение Г).

6 Материально-техническое обеспечение дисциплины

Для осуществления образовательного процесса по дисциплине используется лекционная аудитория, оборудованная мультимедийными средствами, а также лаборатория.

Приложения (обязательные):

А – Методические рекомендации по организации изучения дисциплины

Б – Технологическая карта

Г – Карта учебно-методического обеспечения дисциплины

Приложение А
(обязательное)

Методические рекомендации по организации изучения дисциплины «Прикладные задачи теории чисел»

Дисциплина «Прикладные задачи теории чисел» разделена на три учебных раздела: «специальные разделы теории чисел и алгебры»; «математический аппарат для синтеза и формирования последовательностей»; «математический аппарат для анализа последовательностей». В таблице А.1 отражены разделы дисциплины, технологии и формы проведения занятий, задания по самостоятельной работе студента и ссылки на необходимую литературу.

А.1 Методические рекомендации по теоретической части дисциплины

Теоретическая часть дисциплины направлена на формирование системы знаний об основных аспектах прикладных теоретико-числовых методов с выделением возможностей применения современного математического аппарата теории чисел в исследовательской деятельности. Основное содержание теоретической части излагается преподавателем на лекционных занятиях, а также усваивается студентом при знакомстве с дополнительной литературой, которая предназначена для более глубокого овладения знаниями основных дидактических единиц соответствующего раздела и указана в таблице А.1.

Таблица А.1 - Организация изучения дисциплины «Прикладные задачи теории чисел»

Тема	Технология и форма проведения занятий	Задания на СРС	Дополнительная литература и интернет-ресурсы
Раздел 1 Специальные разделы теории чисел и алгебры			
1.1 Сравнения и их свойства. Первообразные корни и циклотомические классы. Разностные множества.	Вводная лекция. Формирование умений и навыков решения задач по теме. Решение задач. Самообразовательная деятельность.	– решить задачи (ауд. СРС)	2
1.2. Конечные поля. Разбиения множества целых чисел. Циклотомические числа и их свойства.	Информационная лекция. Решение задач. Работа в группах. Самообразовательная деятельность.	– решить задачи (ауд. СРС)	2
Раздел 2 Математический аппарат для синтеза и формирования последовательностей (5/7/3/12)			
2. Математические методы формирования псевдослучайных последовательностей на основе теории сравнений и конечных полей.	Вводная лекция. Решение задач. Работа в группах. Формирование умений и навыков решения задач по теме.	– решить задачи (ауд. СРС)	2
2.2 Обобщенное правило кодирования последовательностей на основе циклотомических классов. Последовательности Лежандра,	Информационная лекция. Решение задач по теме. Самообразовательная деятель-	– решить задачи (ауд.	2

Тема	Технология и форма проведения занятий	Задания на СРС	Дополнительная литература и интернет-ресурсы
Холла, Сидельникова. Обобщенные циклотомические последовательности.	ность.	СРС)	
Раздел 3 Математический аппарат для анализа последовательностей (5/7/3/13)			
3.1 Циклотомические числа и автокорреляционные свойства циклотомических последовательностей.	Информационная лекция. Решение задач. Работа в группах. Самообразовательная деятельность.	– решить задачи (ауд. СРС)	2
3.2 Методы анализа линейной сложности циклотомических последовательностей. Свойства последовательностей Лежандра, Холла, Сидельникова и других.	Информационная лекция. Решение задач. Работа в группах. Формирование умений и навыков решения задач по теме.	– решить задачи (ауд. СРС)	2
3.3 Исследование обобщенных циклотомических последовательностей.	Информационная лекция. Решение задач. Работа в группах. Самообразовательная деятельность.	– решить задачи (ауд. СРС)	2

Теоретические вопросы к индивидуальным домашним заданиям

1. Сравнения и их свойства.
2. Первообразные корни и циклотомические классы.
3. Разностные множества.
4. Циклотомические числа и их свойства.
5. Обобщенное правило кодирования последовательностей на основе циклотомических классов.
6. Последовательности Лежандра, Холла.
7. Последовательности Сидельникова.
8. Обобщенные циклотомические последовательности.
9. Циклотомические числа и автокорреляционные свойства циклотомических последовательностей.
10. Методы анализа линейной сложности циклотомических последовательностей.

А.2 Методические рекомендации по практическим занятиям

Цель практических занятий – закрепление теоретического материала и выработка у студентов умения решать задачи по практическим аспектам дисциплины.

На практических занятиях студентам предлагаются задачи и вопросы по пройденному разделу дисциплины. На занятиях преподаватель проверяет выполнение домашних заданий, разбирает вместе со всеми нерешенные дома задачи.

Практические занятия строятся следующим образом:

- 20% аудиторного времени отводится на объяснение решения типовой задачи у доски;
- 70% аудиторного времени – самостоятельное решение задач студентами;

– 10% аудиторного времени в конце текущего занятия – разбор типовых ошибок при решении задач.

При подготовке к практическим занятиям студент должен изучить лекционный материал, в случае необходимости обратиться к соответствующим разделам рекомендованной литературы и методическим пособиям, разработанным на кафедре ПМИ. При изучении материала необходимо отметить вызывающие затруднения вопросы для получения консультации у преподавателя. К практическим занятиям по конкретной теме студент обязан знать основные понятия, определения, формулировки теорем и свойства. На практических занятиях необходимо иметь конспект лекций по изучаемой теме.

Демонстрационные варианты контрольных работ.

Раздел 1 Контрольная работа по теме “Специальные разделы теории чисел и алгебры ”.

1. Вычислить: $\left(\frac{5}{19}\right), \left(\frac{2}{83}\right)$.

2. Проверить, что множество {1, 7, 9, 10, 12, 16, 26, 33, 34} является разностным с параметрами (37, 9, 2).

3. Доказать, что *D*= {0, 1, 2, 3, 4, 5, 6, 7, 9, 11, 12, 15, 16, 19, 23, 24, 29, 30, 32, 35, 37, 39} - разностное множество, сбалансированное на 2 уровня с параметрами (45, 22, 10, 22).

4. Записать разбиение группы Z_{11}^* на 5 классов смежности по подгруппе $H = \{1,10\}$.

5. Найти все образующие мультипликативной группы поля $GF(3^2)$, $p(x) = x^2 + 1$.

6. Вычислить циклотомические числа $(0, j)_4$, $j = 0, 1, 2, 4$ для $p = 41$.

Раздел 2 Контрольная работа по теме “ Математический аппарат для синтеза и формирования последовательностей ”.

1. Сформировать бинарную последовательность, соответствующую разностному множеству биквадратичных вычетов для $p = 37$.

2. Сформировать последовательность Лежандра для $p = 17$.

3. Найти ПАКФ характеристической последовательности разностного множества {0, 1, 3, 9} с параметрами (13, 4, 1).

4. Найти пары двоичных последовательностей X, Y, сформированных на циклотомических классах шестого порядка, с одноуровневой ПВКФ.

Раздел 3 Контрольная работа по теме “ Математический аппарат для анализа последовательностей ”.

1. Показать, что не существует двоичных последовательностей, сформированных на основе одного циклотомического класса пятого порядка, с одноуровневой ПАКФ.

2. Показать, что двоичная последовательность, сформированная на основе одного циклотомического класса восьмого порядка, имеет одноуровневую ПАКФ тогда и только тогда, когда $p = 3^2 + 64u^2 = 1^2 + 8g^2$, где u, g – целые числа.

3. Применяя циклотомические числа шестого порядка, вычислить ПАКФ последовательностей Холла.

Приведенные примеры позволяют студентам оценить степень сложность заданий, которые им предстоит выполнить на практическом занятии и во время контрольных работах.

А.4 Методические рекомендации по самостоятельной работе студентов

Для подготовки к практическим занятиям, контрольной работе, и экзамену рекомендуется пользовать основной и дополнительной учебно-методической литературой, представленной в карте учебно-методического обеспечения. Для закрепления темы студенту выдаются индивидуальные домашние задания (ИДЗ) для самостоятельной работы. Они выполняются на отдельных листах и защищаются во время аудиторной СРС. ИДЗ выдаётся на первом практическом занятии по разделу и выполняется по мере изучения материала. При их выполнении рекомендуется использовать проработанный в аудитории материал и обратиться к задачникам, в которых разобраны типовые примеры с решениями стандартных задач. Таким образом, после каждого практического занятия студент закрепляет пройденный материал.

Демонстрационные варианты индивидуальных домашних заданий

ИДЗ №1 по теме “Специальные разделы теории чисел и алгебры ”.

1. Найти: $\left(\frac{3}{7}\right), \left(\frac{10}{7}\right), \left(\frac{5}{7}\right), \left(\frac{5}{11}\right), \left(\frac{7}{13}\right), \left(\frac{5}{17}\right), \left(\frac{10}{17}\right)$.

2. Проверить, что множество {0, 1, 3, 9} является разностным с параметрами (13, 4, 1).

3. Доказать, что *D*= {0, 1, 2, 3, 4, 5, 6, 8, 13, 14, 18, 20, 22, 25, 28, 29} - разностное множество, сбалансированное на 2 уровня с параметрами (33, 16, 7, 16).

4. Записать разбиение группы Z_{15}^* на классы смежности по подгруппе третьего порядка.

5. Найти все образующие мультипликативной группы поля $GF(2^2)$.

6. Вычислить таблицы циклотомических чисел второго и четвертого порядков для $p = 17$ и $g = 5$.

ИДЗ №2 по теме “ Математический аппарат для синтеза и формирования последовательностей ”.

1. Сформировать бинарную последовательность, соответствующую разностному множеству биквадратичных вычетов и нуля для $p = 13$.

2. Сформировать последовательность Сидельникова, используя конечное поле восьмого порядка.

3. Найти ПАКФ характеристической последовательности разностного множества {1, 7, 9, 10, 12, 16, 26, 33, 34} с параметрами (37, 9, 2).

4. Найти пары уравновешенных троичных последовательностей X, Y, сформированных по обобщенному правилу кодирования на циклотомических классах четвертого порядка, с ПВКФ: $\left|r_{X,Y}(\tau)\right| \le 1, \tau = 0,1,..., p-1$.

ИДЗ №3 по теме “ Математический аппарат для анализа последовательностей ”.

1. Показать, что не существует двоичных последовательностей, сформированных на основе одного циклотомического класса шестого порядка с одноуровневой ПАКФ.

2. Найти необходимые условия существования ДП, сформированной на основе одного циклотомического класса, с двухуровневой ПАКФ.

3. Найти необходимые условия существования почти сбалансированных БП, с двухуровневой ПАКФ.

4. Найти необходимые условия существования почти уравновешенной БП, сформированной по ПК (5.1.1), с одноуровневой ПАКФ.

Приложение Б
(обязательное)

Технологическая карта
дисциплины «Прикладные задачи теории чисел»
семестр – 8, ЗЕ – 2, вид аттестации – зачет, акад.часов – 72, баллов рейтинга – 100

№ и наименование раздела учебного модуля, КП/КР	№ недели сем.	Трудоемкость, ак.час					Форма текущего контроля успев. (в соотв. с паспортом ФОС)	Максим. кол-во баллов рейтинга
		Аудиторные занятия				СРС		
		ЛЕК	ПЗ	ЛР	АСРС			
Раздел 1 **Специальные разделы теории чисел и алгебры**	1-6 8семестр	5	6		4	12	ИДЗ№1 СР	30
Раздел 2 **Математический аппарат для синтеза и формирования последовательностей**	7-12 8семестр	5	7		4	12	ИДЗ№2 КР	30
Раздел 3 **Математический аппарат для анализа последовательностей**	12-18 8семестр	5	7		4	13	ИДЗ№3 СР	40
Рубежная аттестация	сессия						зачет	
Итого:		15	20		12	37		100

Критерии оценки качества освоения студентами дисциплины (в соответствии с Положением «Об организации учебного процесса по основным образовательным программам высшего профессионального образования» от 27.09.2011г. № 32):

- пороговый (оценка «удовлетворительно») – от 50 до 74 баллов
- стандартный (оценка «хорошо») – от 75 до 89 баллов
- эталонный (оценка «отлично») – от 90 до 100 баллов

Приложение Г (обязательное)

Карта учебно-методического обеспечения

дисциплины **«Прикладные задачи теории чисел»**

Направление (специальность) 010400.62 Прикладная математика и информатика

Формы обучения очная Курс 4 Семестр 8

Часов**:** всего 72, лекций 15, практ. зан. 20, лаб. раб. 0, СРС 37

Обеспечивающая кафедра ПМИ

Таблица Г.1- Обеспечение учебного модуля учебными изданиями

Библиографическое описание издания (автор, наименование, вид, место и год издания, кол. стр.)	Кол. экз. в библ. НовГУ	Наличие в ЭБС
Учебники и учебные пособия		
1. Едемский В.А. Математический аппарат для анализа, синтеза и формирования троичных последовательностей: учеб. Пособие / В.А. Едемский, В.Е. Гантмахер; НовГУ им. Ярослава Мудрого. – Великий Новгород, 2014. - 205с.	40(каф.)	
2 Гантмахер В. Е. Специальные разделы математики (Теория чисел, теория групп и полей Галуа, корреляционный анализ, автономные линейные последовательные машины) : учеб. пособие / В. Е. Гантмахер ; Новгород. гос. ун-т им. Ярослава Мудрого. - Великий Новгород, 2000.96с. Ф1-8	8	
Учебно-методические издания		
2. Рабочая программа модуля с приложениями «Прикладные задачи теории чисел» /Авт.-сост. В.А. Едемский; НовГУ. – В.Новгород, 2014. – 12 с.		

Таблица Г.2 – Информационное обеспечение учебного модуля

Название программного продукта, интернет-ресурса	**Электронный адрес**	**Примечание**
электронная библиотека учебников Мех-Мата МГУ,	***http://poiskknig.ru***	электронная библиотека учебников Мех-Мата МГУ, Москва
общероссийский математический портал	***http://www.mathnet.ru.ru/***	
электронная библиотека механико-математического факультета Московского государственного университета	***http://www.lib.mexmat.ru***	**электронная библиотека** Мех-Мата МГУ
научные журналы издательства Wiley&Sons	***http://onlinelibrary.wiley.com***	
научные журналы издательства Elsevier	***http://www.sciencedirect.com/***	•
Сайт информационных технологий	***http://inftech.webservis.ru/it/conference/isanditc/2000/section3/rus/arrus16.html***	
MathemLib.ru: Библиотека по математике	***http://mathemlib.ru/about***	включает накопленный за советский период опыт в виде книг изданных в СССР и дополнена современными новостными статьями.

Действительно для учебного года _____/_____
Зав. кафедрой _____ Б.И. Селезнев
_____ _____ 20 г.

СОГЛАСОВАНО
НБ НовГУ: _____ _____ _____
должность подпись расшифровка