

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ИНГУШСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

ФИЗИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

КАФЕДРА «Математический анализ»

СОГЛАСОВАНА

Руководитель образовательной программы

_____/проф. И.А.Танкиев

от «27» февраля 2025г.

УТВЕРЖДАЮ

Декан физико-математического факультета

_____/Б.С. Кульбужев

от «14» марта 2025г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.07.01. Теория чисел

Направление подготовки

44.03.01. Педагогическое образование

Направленность (профиль подготовки)

Математика

Квалификация выпускника

БАКАЛАВР

Форма обучения

Очная

Магас, 2025г

1. Цели освоения дисциплины

Дисциплина базируется на знании основных понятий делимости целых чисел (делимое, делитель, частное и остаток), теории колец (идеал кольца, факторкольцо, обратимый элемент кольца) и многочленов (степень, корень многочлена, деление многочленов с остатком, теорема Безу и схема Горнера).

Перечень профессиональных стандартов, обобщенных трудовых функций и трудовых функций, соответствующих профессиональной деятельности выпускников

Код и наименование профессионального стандарта	Обобщенные трудовые функции			Трудовые функции		
	Код	наименование	Уровень квалификации	наименование	код	Уровень (подуровень) квалификации
01.001 «Педагог (педагогическая деятельность в сфере дошкольного, Начального общего, основного общего, среднего общего образования) (воспитатель, учитель)»	А	Педагогическая деятельность по проектированию и реализации образовательного процесса в образовательных организациях дошкольного, начального общего, основного общего, среднего общего образования	6	Общепедагогическая функция. Обучение	А/01.6	6
			6	Воспитательная деятельность	А/02.6	6
			6	Развивающая деятельность	А/03.6	6
	В	Педагогическая деятельность по проектированию и реализации основных общеобразовательных программ	5-6	Педагогическая деятельность по реализации программ дошкольного образования	В/01.5	5
			5-6	Педагогическая деятельность по реализации программ начального общего образования	В/02.6	6

Место дисциплины в структуре ОПОП бакалавриата

Дисциплина относится к блоку «Дисциплины по выбору». Читается в 3 семестре. Находится под индексом Б1.В.ДВ.07.01.

3. Результаты освоения дисциплины (модуля) теория чисел

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО по данному направлению:

Код компетенции	Наименование компетенции	Индикатор достижения компетенции (закрепленный за дисциплиной)
УК-3	Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	<p>УК-3.1. Определяет свою роль в социальном взаимодействии и командной работе, исходя из стратегии сотрудничества для достижения поставленной цели;</p> <p>УК-3.2. При реализации своей роли в социальном взаимодействии и командной работе учитывает особенности поведения и интересы других участников;</p> <p>УК-3.3. Анализирует возможные последствия личных действий в социальном взаимодействии и командной работе, и строит продуктивное взаимодействие с учетом этого;</p> <p>УК-3.4. Осуществляет обмен информацией, знаниями и опытом с членами команды; оценивает идеи других членов команды для достижения поставленной цели;</p> <p>УК-3.5. Соблюдает нормы и установленные правила командной работы; несет личную ответственность за результат.</p>
ПК-1	Способность разрабатывать и реализовывать программ учебных дисциплин в соответствии с требованиями федеральных государственных образовательных стандартов	<p>ПК.-1.1. Проводит анализ требований федеральных государственных образовательных стандартов к реализации программ учебной дисциплины</p> <p>ПК.-1.2. Разрабатывает структуру программы учебной дисциплины с учетом требований к ней</p> <p>ПК.-1.3. Планирует учебные занятия и самостоятельную работу учащихся по учебной дисциплине</p> <p>ПК.-1.4. Выстраивает индивидуальные образовательные маршруты по дисциплине</p> <p>ПК.-1.5. Реализует программы учебных дисциплин и оценивает результаты собственной деятельности</p>
ПК-2	Способность математически корректно ставить	<p>ПК-2.1: Знает способы определения видов и типов профессиональных задач, структурирования задач различных групп.</p>

												Зачет	+
												Зачет с оценкой	-
												Экзамен	-

4.2. Содержание дисциплины (модуля)

Раздел 1. Делимость целых чисел, НОД и его свойства.

Тема 1.1. Делимость целых чисел, свойства делимости. Частное и остаток. Наибольший общий делитель и алгоритм Евклида. Свойства НОД и взаимно простых чисел. Наименьшее общее кратное и его свойства.

Раздел 2. Простые числа.

Тема 2.1. Простые числа. Свойства простых чисел. Бесконечность множества простых чисел. Решето Эратосфена. Неравенства Чебышева. Каноническое разложение натурального числа.

Раздел 3. Теоретико-числовые функции.

Тема 3.1. Целая и дробная части действительного числа. Число делителей и сумма делителей натурального числа.

Раздел 4. Теория сравнений.

Тема 4.1. Сравнения. Свойства сравнений. Полная система вычетов. Признак полной системы вычетов. Приведенная система вычетов. Признак приведенной системы вычетов. Функция Эйлера. Теоремы Эйлера и Ферма. Сравнения первой степени с одним неизвестным.

Раздел 5. Непрерывные дроби.

Тема 5.1. Представление действительных чисел непрерывными дробями. Подходящие дроби и их свойства. Теорема Лежандра о квадратичной иррациональности.

Раздел 6. Решение сравнений.

Тема 6.1. Решение в целых числах уравнения $ax + by = c$. Сравнение по простому модулю. Число решений сравнения по простому модулю. Теорема Вильсона.

Раздел 7. Первообразные корни и индексы.

Тема 7.1. Показатель числа по модулю, свойства показателя. Первообразные корни. Существование первообразных корней по простому модулю. Индексы и их свойства.

Раздел 8. Приложения теории сравнений.

Тема 8.1. Системы счисления, арифметические операции над числами в заданной системе счисления. Перевод чисел из одной системы счисления в другую. Признаки делимости.

Тема 8.2. Признак Паскаля. Десятичные дроби. Конечные, чистые периодические и смешанные периодические десятичные дроби.

Темы лабораторных работ (Лабораторный практикум)

Не предусмотрены учебным планом ООП

Примерная тематика курсовых работ

Не предусмотрены учебным планом ООП

5. Образовательные технологии

Активные и интерактивные формы: лекции, практические занятия, контрольные работы, коллоквиумы, зачеты и экзамены. В течение семестров студенты решают задачи, указанные преподавателем.

6. Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

6.1. План самостоятельной работы студентов

№ п/п	Наименование раздела (темы)	Вид самостоятельной работы	Трудоемкость (в академических часах)
Раздел 1	Делимость целых чисел, НОД и его свойства.		
1.1	Делимость целых чисел, свойства делимости. Частное и остаток. Наибольший общий делитель и алгоритм Евклида. Свойства НОД и взаимно простых чисел. Наименьшее общее кратное и его свойства.	Аудиторная работа	4
Раздел 2	Простые числа.		
2.1	Простые числа. Свойства простых чисел. Бесконечность множества простых чисел. Решето Эратосфена. Неравенства Чебышева. Каноническое разложение натурального числа.	Теоретический тест	4
Раздел 3	Теоретико-числовые функции.		
3.1	Целая и дробная части действительного числа. Число делителей и сумма делителей натурального числа.	Аудиторная работа	4
Раздел 4	Теория сравнений.		
4.1	Сравнения. Свойства сравнений. Полная система вычетов. Признак полной системы вычетов. Приведенная система вычетов. Признак приведенной системы вычетов. Функция Эйлера. Теоремы	Контрольная работа	4

	Эйлера и Ферма. Сравнения первой степени с одним неизвестным.		
Раздел 5	Непрерывные дроби.		
5.1	Представление действительных чисел непрерывными дробями. Подходящие дроби и их свойства. Теорема Лежандра о квадратичной иррациональности.	Аудиторная работа	4
Раздел 6	Решение сравнений.		
6.1	Решение в целых числах уравнения $ax + by = c$. Сравнение по простому модулю. Число решений сравнения по простому модулю. Теорема Вильсона.	Контрольная работа	4
Раздел 7	Первообразные корни и индексы.		
7.1	Показатель числа по модулю, свойства показателя. Первообразные корни. Существование первообразных корней по простому модулю. Индексы и их свойства.	Аудиторная работа	6
Раздел 8	Приложения теории сравнений.		
8.1	Системы счисления, арифметические операции над числами в заданной системе счисления. Перевод чисел из одной системы счисления в другую. Признаки делимости.	Аудиторная работа	2
8.2	Признак Паскаля. Десятичные дроби. Конечные, чистые периодические и смешанные периодические десятичные дроби.	Контрольная работа	4

Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Критерии оценки промежуточной аттестации в форме зачета

Оценка	Характеристика требований к результатам аттестации в форме зачета
«Зачтено»	Теоретическое содержание курса освоено полностью без пробелов или в целом, или большей частью, необходимые практические навыки работы с освоенным материалом сформированы или в основном сформированы, все или большинство предусмотренных рабочей программой учебных заданий выполнены, отдельные из выполненных заданий содержат ошибки.
«Не зачтено»	Теоретическое содержание курса освоено частично, необходимые навыки работы не сформированы или сформированы отдельные из них, большинство предусмотренных рабочей учебной программой заданий не выполнено либо выполнено с грубыми ошибками, качество их выполнения оценено числом баллов, близким к минимуму.

Критерии оценки промежуточной аттестации в форме экзамена

Оценка	Характеристика требований к результатам аттестации в форме экзамена
«Отлично»	Теоретическое содержание курса освоено полностью без пробелов, системно и глубоко, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные рабочей учебной программой учебные задания выполнены безупречно, качество их выполнения оценено числом баллов, близким к максимуму.
«Хорошо»	Теоретическое содержание курса освоено в целом без пробелов, необходимые практические навыки работы с освоенным материалом в основном сформированы, предусмотренные рабочей учебной программой учебные задания выполнены с отдельными неточностями, качество выполнения большинства заданий оценено числом баллов, близким к максимуму.
«Удовлетворительно»	Теоретическое содержание курса освоено большей частью, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных рабочей учебной программой учебных заданий выполнены, отдельные из выполненных заданий содержат ошибки.

«Неудовлетворительно»	Теоретическое содержание курса освоено частично, необходимые навыки работы не сформированы или сформированы отдельные из них, большинство предусмотренных рабочей учебной программой учебных заданий не выполнено либо выполнено с грубыми ошибками, качество их выполнения оценено числом баллов, близким к минимуму.
-----------------------	--

6.2. Методические указания по организации самостоятельной работы студентов

Самостоятельная работа является одним из видов учебной деятельности обучающихся, способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Аудиторная самостоятельная работа по учебной дисциплине осуществляется на учебных занятиях под непосредственным руководством преподавателя и по его заданию.

Внеаудиторная самостоятельная работа выполняется по заданию преподавателя без его непосредственного участия.

Виды заданий для внеаудиторной самостоятельной работы, их характер, учитывать специфику изучаемой учебной дисциплины, индивидуальные особенности обучающегося.

Контроль самостоятельной работы и оценка ее результатов организуется как единство двух форм:

1. самоконтроль и самооценка обучающегося;
2. контроль и оценка со стороны преподавателя.

Организация и руководство аудиторной самостоятельной работы

Аудиторная самостоятельная работа по дисциплине выполняется на учебных занятиях под непосредственным руководством преподавателя и по его заданию.

Основными видами аудиторной работы самостоятельной работы являются:

- выполнение лабораторных и практических работ осуществляется на лабораторных и практических занятиях в соответствии с графиком учебного процесса. Для обеспечения самостоятельной работы преподавателями разрабатываются методические указания по выполнению лабораторной /практической работы.

Работа с литературой, другими источниками информации, в т.ч. электронными, может реализовываться на семинарских и практических занятиях. Данные источники информации могут быть представлены на бумажном и/или электронном носителях, в том числе, в сети Интернет.

Преподаватель формулирует цель работы с данным и источником информации, определяет время на проработку документа и форму отчетности.

Само и взаимопроверка выполненных заданий чаще всего используется на семинарском, практическом и других видах занятий. Проблемная /ситуационная задача должна иметь четкую формулировку, к ней должны быть поставлены вопросы, ответы на которые необходимо найти и обосновать. Критерии оценки правильности решения проблемной/ситуационной задачи должны быть известны всем обучающимся.

Организация и руководство внеаудиторной работы

Внеаудиторная самостоятельная работа выполняется по заданию преподавателя, но без его непосредственного участия.

При предъявлении видов заданий на внеаудиторную самостоятельную работу рекомендуется использовать дифференцированный подход к уровню подготовленности обучающегося. Перед выполнением внеаудиторной самостоятельной работы преподаватель проводит консультацию с определением цели задания, его содержания, сроков выполнения, ориентировочного объема работы, основных требований к результатам работы, критериев оценки, форм контроля и перечня литературы. В процессе консультации преподаватель предупреждает о возможных типичных ошибках, встречающихся при выполнении задания.

Для методического обеспечения и руководства самостоятельной работой в образовательном учреждении разрабатываются учебные пособия, методические рекомендации по самостоятельной подготовке к различным видам занятий с учетом специальности учебной дисциплины, особенностей контингента студентов, объема и содержания самостоятельной работы, форм контроля и т.п.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня подготовленности обучающихся.

Видами заданий для внеаудиторной самостоятельной работы могут быть:

- для овладения знаниями: чтения текста; составления плана текста; графическое изображение структуры текста; конспектирование текста; выписки из текста; работа со словарями и справочникам; учебно-исследовательская работа; использование аудио и видеозаписей, компьютерной техники и Интернет ресурсов и др.;

- для закрепления и систематизации знаний: работа с конспектом лекции; повторная работа над учебным материалом; составление плана, тезисов ответа; составление таблиц, ребусов, кроссвордов, глоссария для систематизации учебного материала; изучение словарей, справочников; ответы на контрольные вопросы; аналитическая обработка текста; подготовка сообщений к выступлению на семинаре, конференции; подготовка

рефератов, докладов; составление биографий, заданий в тестовой форме и др.

- для формирования умений: решение задач и упражнений по образцу; решение вариативных задач и упражнений; составление схем; решение ситуационных производственных задач; подготовка к деловым и ролевым играм; проектирование и моделирование разных видов и компонентов профессиональной деятельности, подготовка презентаций, творческих проектов; подготовка курсовых и выпускных работ; опытно-экспериментальная работа; проектирование и моделирование разных видов и компонентов профессиональной деятельности и др.

Для обеспечения внеаудиторной самостоятельной работы по дисциплине преподавателем разрабатывается перечень заданий для самостоятельной работы, который необходим для эффективного управления данным видом учебной деятельности обучающихся.

Преподаватель осуществляет управление самостоятельной работой, регулирует ее объем на одно учебное занятие и осуществляет контроль выполнения всеми студентами группы. Для удобства преподаватель может вести ведомость учета выполнения минимума заданий, необходимы для допуска к итоговой аттестации по дисциплине.

В процессе самостоятельной работы студент приобретает навыки самоорганизации, самоконтроля, самоуправления и становится активным самостоятельным субъектом учебной деятельности.

Студент самостоятельно определяет режим своей внеаудиторной работы и меру труда, затрачиваемого на овладение знаниями и умениями по каждой дисциплине, выполняет внеаудиторную работу по индивидуальному плану, в зависимости от собственной подготовки, бюджета времени и других условий.

Ежедневно студент должен уделять выполнению внеаудиторной самостоятельной работы в среднем не менее 3 часов.

При выполнении внеаудиторной самостоятельной работы студент имеет право обращаться к преподавателю за консультацией с целью уточнения задания, формы контроля выполненного задания.

6.3. Материалы для проведения текущего и промежуточного контроля знаний студентов

Контрольная работа № 1.

1. Найти НОД (6188,4709).
2. Разложить в непрерывную дробь $\alpha \equiv \frac{125}{92}$.
3. Найти каноническое разложение числа 125!
4. Вычислить $\tau(\alpha)$ и $S(\alpha)$, $\alpha = 2800$.

5. Найти $\varphi(5040)$, $\mu(147)$ и $\mu(143)$.

Контрольная работа № 2.

1. Решить сравнение $256x \equiv 179 \pmod{337}$.
2. Решить систему сравнений
 $x \equiv 3 \pmod{8}$, $x \equiv 11 \pmod{20}$, $x \equiv 1 \pmod{15}$.
3. Решить сравнение $9x^2 + 29x + 62 \equiv 0 \pmod{64}$.

Контрольная работа № 3.

Указать число решений сравнения:

- a) $x^2 \equiv 5 \pmod{73}$,
- б) $x^2 \equiv 3 \pmod{75}$,
- в) $x^2 \equiv 226 \pmod{563}$,
- г) $x^2 \equiv 429 \pmod{563}$.

Контрольная работа № 4.

- 1) Доказать, что $(4n + 15n - 1) \approx 9$ при $\forall n \in \mathbb{N}$;
- 2) Найти НОД чисел 529, 1541 и 1817.
- 3) Найти НОК чисел 684 и 3131.
- 4) Простым или составным является число 1897?
- 5) С каким показателем степени входит 3 в каноническое разложение числа 40! ?

Контрольная работа № 5.

- 1) Решить сравнение $14x \equiv 7 \pmod{101}$.
- 2) Найти остаток, получаемый при делении 53 117 на 11.
- 3) Найти двузначное число, сравнимое с 2 по модулям 3 и 7 и с (-2) по модулю 11.
- 4) Решить в целых числах: $53x + 17y = 25$
- 5) Доказать, что $(2 \cdot 5^n - 1) \approx 31$ при $\forall n \in \mathbb{N}$.

Вопросы к зачету:

1. Отношение делимости. Свойства делимости.
2. Теорема о делении с остатком.
3. Наибольший общий делитель. Алгоритм Евклида.
4. Свойства НОД. Линейная форма НОД. НОД нескольких чисел.
5. Взаимно простые числа. Свойства взаимно простых чисел.

6. Наименьшее общее кратное. Свойства НОК. Наименьшее общее кратное нескольких чисел.
7. Простые числа. Свойства простых чисел.
8. Решето Эратосфена. Бесконечность множества простых чисел.
9. Основная теорема арифметики.
10. Теоретико-числовые функции.
11. Непрерывные дроби.
12. Подходящие дроби. Свойства подходящих дробей.
13. Сравнения. Свойства сравнений.
14. Полная система вычетов.
15. Приведенная система вычетов.
16. Функция Эйлера.
17. Теоремы Эйлера и Ферма.
18. Сравнения первой степени.
19. Сравнения высших степеней.
20. Решение неопределенных уравнений.
21. Показатель числа. Свойства показателя.
22. Первообразные корни по простому модулю.
23. Индексы и их свойства.
24. Признаки делимости.
25. Системы счисления. Систематические числа.

Контроль освоения компетенций

№ п\п	Вид контроля	Контролируемые разделы	Компетенции, компоненты которых контролируются
1	Аудиторная контр.работа(проверка и оценка)	Раздел 1- Раздел 8	ОПК-1, ПК-2
2	Теоретический тест	Раздел 2	ОПК-1, ПК-2
3	Самостоятельное решение практических заданий (аудиторная)	Раздел 1- Раздел 8	ОПК-1, ПК-2
5	Зачет во 2 семестре	Раздел 1 - Раздел 8	ОПК-1, ПК-2

7. Учебно-методическое и материально-техническое обеспечение дисциплины (модуля) теория чисел

Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля) теория чисел.

К основной (обязательной) литературе относятся учебники, учебные пособия, учебно-методическая литература и монографии, изучение которых является обязательным для овладения знаниями в полном объеме по дисциплине в соответствии с данной программой. К основной, прежде всего, относится литература, имеющая гриф Министерства образования и науки Российской Федерации или Учебно-методического объединения, рекомендующих издание к использованию в учебном процессе. В списке основной литературы указывается не более пяти источников, имеющих в достаточном количестве в фонде библиотеки. Если доступна электронная версия учебников, учебных пособий и т.д., следует указать для них режим доступа.

К дополнительной относится литература, рекомендуемая бакалаврам, магистрам для самостоятельного изучения при выполнении курсового проекта (работы), учебной научно-исследовательской работы, при написании рефератов, для подготовки к семинарам, практическим занятиям, лабораторным работам и другим учебным занятиям, а также для углубления и расширения знаний по данной дисциплине.

Все источники в основной и дополнительной литературе даются с полными библиографическими описаниями в соответствии с российским или западным стандартами оформления.

Для магистратуры обязательно наличие литературы на английском языке.

7.1. Учебная литература:

Основная литература:

1. Алгебра и теория чисел. ЧЗ [Текст]: учебное пособие для студентов-заочников пед. ин-тов / под редакцией Н.Я. Виленкина. – Просвещение, 2004. – 192 с.
2. Виноградов И.М. Основы теории чисел [Текст] / И.М. Виноградов. – 10-е изд., стер. – СПб.: Лань, 2006. – 176 с.
3. Грибанов В.У. Сборник упражнений по теории чисел [Текст]: учеб. пособие для пед. ин-тов / В.У. Грибанов, П.И. Титов. – М.: Просвещение, 2005. – 144 с.
4. Ильиных А.П. Теория чисел [Текст]: учебное пособие / А.П. Ильиных; Урал. гос. пед. ун-т. – Екатеринбург. [б.и.], 2003. – 148 с.
5. Кудреватов Г.А. Сборник задач по теории чисел [Текст]: учеб. пособие для вузов. / Г.А. Кудреватов. – М.: Просвещение, 2000. – 128 с.

Дополнительная литература:

1. Борович З.И. Теория чисел [Текст] / З.И. Борович, И.Р. Шафаревич. – М., Наука, 2001. – 496 с.
2. Бухштаб А.А. Теория чисел [Текст]: учеб. пособие для физ.-мат. фак. пед. ин-тов / А.А. Бухштаб. – М.: Просвещение, 2006. – 384 с.
3. Девенпорт Г. Высшая арифметика [Текст] / Г. Девенпорт. – М., Наука, 2008.
5. Карацуба А. А. Основы аналитической теории чисел [Текст] / А.А. Карацуба. – М., Наука, 2003. –
6. Кочева А. А. Задачник-практикум по алгебре и теории чисел [Текст]: учебное пособие для студентов- заочников 2 курса физ.-мат. фак. пед. ин-тов / А.А. Кочева. – М., Просвещение, 2000.

7.2. Интернет-ресурсы

Поскольку в настоящее время при работе с информацией широко используются ресурсы телекоммуникационной сети «Интернет» (далее — сеть «Интернет»), то следует указать перечень сайтов, использующихся для получения дополнительных знаний по изучаемой дисциплине. Также следует указать адрес сайта, содержащего учебную информацию по курсу (при его наличии), принципы размещения в нем информации и способы работы с сайтом.

№	Название	Электронный адрес	Содержание
---	----------	-------------------	------------

1.	<u>Exponenta</u>.ru	www.exponenta.ru	На сайте размещены электронные учебники, справочники, статьи, примерами применения математических пакетов в образовательном процессе, демо-версии по популярным математических пакетов, электронные книги и свободно распространяемые программы.
2.	<u>Math</u>.ru	www.math.ru	Математический сайт для школьников, студентов, учителей и всех, кто интересуется математикой.
3.	Математика	www.mathematics.ru	Учебный материал по различным разделам математики.
4.	Математика для студентов и прочее.	www.xplusy.isnet.ru	Содержит большое количество видеолекций для школьников, абитуриентов и студентов по математике и физике.
5.	Российское образование.	www.edu.ru	Федеральный образовательный портал: учреждения, программы, стандарты, ВУЗы, тесты ЕГЭ.

7.3. Программное обеспечение:

1. Microsoft Excel
2. Microsoft Word
3. Microsoft PowerPoint

7.4. Материально-техническое обеспечение

В организации учебного процесса необходимыми являются средства, обеспечивающие аудиовизуальное восприятие учебного материала (специализированное демонстрационное оборудование):

1. Доска и мел (или более современные аналоги)
2. компьютерные и мультимедийные технологии
3. микрофон и соответствующие установки (для работы в больших аудиториях с многочисленными группами студентов)

Рабочая программа по дисциплине «Теория чисел» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 44.03.01 Педагогическое образование Математика

Программу составил:

Ст. преподаватель кафедры «Математический анализ» Оздоева Ева Висхаевна

Программа одобрена на заседании кафедры «Математический анализ»

Протокол №6 от «27» февраля 2025г

Программа одобрена Учебно-методическим советом физико-математического факультета

Протокол № 7 от «13» марта 2025 г.

Приложение №1

Оценочные материалы по дисциплине «Теория чисел»

1. Оценочные материалы для текущего контроля

1.1. Оценочные материалы для входного контроля

1. Сколько имеется точек, в которых производная функции $\frac{\ln^2 x}{x}$ обращается в нуль?

1. 1

2. 2

3. 3

4. больше 3

2. Выбрать уравнение касательной к графику функции $\ln^2 x$ в точке с абсциссой 1.

1. $y = x$

2. $y = x - 1$

3. $y = 1$

4. $y = 0$

3. Производной какой функции является функция $x^{\cos x} \frac{\cos x}{x} - \sin x \cdot \ln x$?

1. $(\cos x)^{\cos x}$

2. $x^{\cos x}$

3. $(\sin x)^{\cos x}$

4. $(\sin x)^x$

4. Указать правильную формулу производной функции $y = \frac{f(\sin x)}{x}$

$\frac{x f'(\sin x) - f(\sin x)}{x^2}$

1.

$\frac{\cos x f'(\sin x) - f(\sin x)}{x^2}$

2.

$\frac{x \cos x f'(\sin x) - f(\sin x)}{x^2}$

3.

$\frac{x \cos x f'(\sin x) + f(\sin x)}{x^2}$

4.

5. Пусть $f(x) = x^2$; $g(x) = x^3$. Указать правильно вычисленные производные

1. $(f(x) + g(x))' = 3x + 2x^2$

2. $(f(x) \cdot g(x))' = 5x^4$

3. $\left(\frac{f(x)}{g(x)}\right)' = \frac{1}{x^2}$

4. $(f(g(x)))' = 6x^5$

6. Пусть $f(x) = x^2$; $g(x) = \sqrt{x}$. Указать правильно вычисленные производные

1. $(f(x) + g(x))' = 2x + \frac{1}{2\sqrt{x}}$

2. $(f(x) \cdot g(x))' = 5x^4$

$$3. \left(\frac{f(x)}{g(x)} \right)' = \frac{1}{x^2}$$

$$4. (f(g(x)))' = 1$$

7. Пусть $f(x) = \sin x$; $g(x) = \arcsin x$. Указать правильно вычисленные производные

$$1. (f(x) + g(x))' = \cos x + \frac{1}{\sqrt{x}}$$

$$2. (f(x) \cdot g(x))' = \cos x \cdot \arcsin x + \frac{\sin x}{\sqrt{1-x^2}}$$

$$3. \left(\frac{f(x)}{g(x)} \right)' = \frac{\cos x \cdot \arcsin x + \frac{\sin x}{\sqrt{1-x^2}}}{(\arcsin x)^2}$$

$$4. (f(g(x)))' = 1$$

8. Пусть $f(x) = \operatorname{tg} x$; $g(x) = \operatorname{arctg} x$. Указать правильно вычисленные производные

$$1. (f(x) + g(x))' = \frac{1}{\cos^2 x} + \frac{1}{1+x^2}$$

$$2. (f(x) + g(x))' = \frac{1}{\cos^2 x} \operatorname{arctg} x + \frac{1}{1+x^2} \operatorname{ctg} x$$

$$3. (f(x) + g(x))' = \frac{\cos^2 x \operatorname{arctg} x - \frac{1}{1+x^2} \operatorname{tg} x}{\operatorname{arctg}^2 x}$$

$$4. (f(g(x)))' = x$$

Критерий выставления оценок

Количество правильных ответов	Количество баллов
три и менее правильных ответа	0 баллов
Решено четыре задания	1 балл
Решено шесть ответов	2 балла
Решено восемь ответов	3 балла

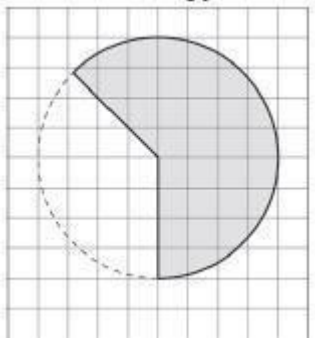
Вариант №2

1 В квартире, где проживает А, установлен прибор учета расхода горячей воды (счётчик). 1 марта счётчик показывал расход 896 куб.м воды, а 1 апреля - 907 куб.м. Какую сумму должен заплатить А за горячую воду за март, если цена за 1 куб.м горячей воды составляет 81 р.? Ответ дайте в рублях.

2 На рисунке жирными точками показан курс китайского юаня, установленный Центробанком РФ, во все рабочие дни с 23 сентября по 23 октября 2010 года. По горизонтали указываются числа месяца, по вертикали - цена китайского юаня в рублях. Для наглядности жирные точки на рисунке соединены линией. Определите по рисунку наименьший курс китайского юаня за указанный период. Ответ дайте в рублях.



- 3 Площадь закрашенного сектора, изображенного на клетчатой бумаге равна 22,5. Найдите площадь круга.



- 4 Автомобильный журнал определяет рейтинги автомобилей на основе оценок безопасности S, комфорта C, функциональности F, качества Q и дизайна D. Каждый отдельный показатель оценивается читателями журнала по 5-ти бальной шкале. Рейтинг R вычисляется по формуле:

$$R = \frac{3S + 2C + 2F + 2Q + D}{50}$$

В таблице даны оценки каждого показателя для трех моделей автомобилей. Определите, какой автомобиль имеет наивысший рейтинг. В ответ запишите значение этого рейтинга.

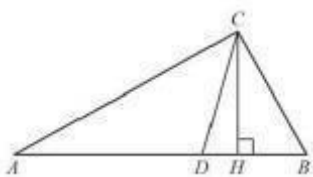
Модель	Безопасность	Комфорт	Функциональность	Качество	Дизайн
А	3	3	2	1	5
Б	5	3	4	3	4
В	1	2	2	1	4

- 5 Решите уравнение

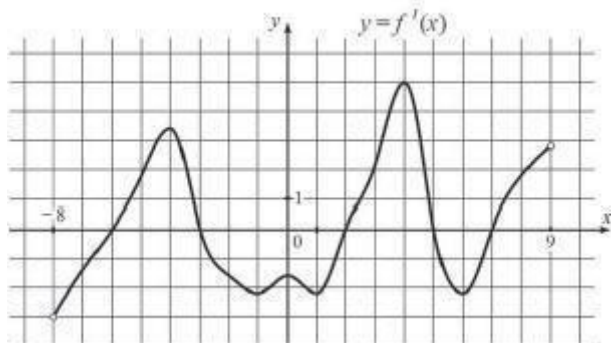
$$\frac{x-1}{5x+8} = \frac{x-1}{4x+3}$$

Если уравнение имеет более одного корня, в ответе запишите больший из корней.

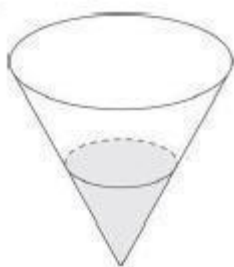
- 6 Острые углы прямоугольного треугольника равны 85° и 5° . Найдите угол между высотой и биссектрисой, проведенными из вершины прямого угла. Ответ дайте в градусах.



- 7 На рисунке изображен график производной $y = f'(x)$ функции $f(x)$, определенной на интервале $(-8;9)$. Найдите количество точек минимума функции $f(x)$, принадлежащих отрезку $[-4;8]$.



- 8 В сосуд, имеющий форму конуса, налили 30 мл жидкости, до половины высоты сосуда. Сколько миллилитров жидкости нужно долить в сосуд, чтобы заполнить его доверху?



Критерий выставления оценок

Количество правильных ответов					Количество баллов
три	и	менее	правильных	ответа	0 баллов
Решено		четыре		задания	1 балл
Решено		шесть		ответов	2 балла
Решено		восемь		ответов	3 балла

1.2. Вопросы для собеседования (доклада, сообщения)

- Новое о системах счисления.
- Деление с остатком (арифметика гауссовых чисел).
- Занимательные дроби (бесконечные цепные дроби, загадка Архимеда, загадка Григория XIII).
- Пифагоровы треугольники.
- Решение уравнений в целых числах (китайская теорема с остатком, уравнение Пелля).
- Точки с целочисленными координатами.
- Обобщение теоремы Вильсона.
- Числа Кармайкла.
- Критерий Клемента (простые числа-близнецы).
- Критерий Люка.
- Теорема Поклингтона.

12. Теорема Прота.
13. Числа Мерсенна. Совершенные числа.
14. Теорема Диомитко.
15. Метод Маурера.
16. Метод Полларда (критерий, алгоритм).
17. Функция Мебиуса, свойства.
18. Логарифмическое свойство $\pi(x)$ и утверждение о p_n .
19. Квадратичные вычеты и невычеты.
20. Символ Лежандра.
21. Обобщенная функция Эйлера. Теорема Эйлера.
22. Преставление чисел квадратичными формами.
23. Представление чисел в виде суммы двух квадратов и в виде $x^2 + 2y^2$.
24. Числа Фибоначчи.
25. Фареевы дроби.
26. Видоизменения решета Эратосфена.
27. Детерминированный алгоритм получения простых чисел.
28. Мультипликативные функции, свойства.
29. Распределение простых чисел.
30. Разложение числа «e» в цепную дробь.
31. Криптосистема RSA.
32. Криптосистема Эль Гамала.
33. Электронная подпись.
34. Сложность арифметических операций с целыми числами. Алгоритм умножения Карацубы-Офмана.
35. Сложность алгоритма Евклида. Алгоритм обращения и нахождения НОД.
36. Сложность вычислений в кольце вычетов. Модульная арифметика. Метод Монтгомери.
37. Решение систем линейных уравнений в целых числах.
38. Псевдопростые числа.
39. Частные Ферма, Вильсона и другие.
40. Магические квадраты из простых чисел.

Критерии оценки:

3 балла за каждое собеседование – дан полный, развернутый ответ на поставленный вопрос; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений; знание по предмету демонстрируются на фоне понимания его в системе данной науки и междисциплинарных связей; ответы на дополнительные вопросы четкие, краткие.

2 балла за каждое собеседование – дан полный, развернутый ответ на поставленный вопрос, показано умение выделять существенные и несущественные признаки, причинно-следственные связи; рассказ недостаточно логичен с единичными ошибками в частностях, исправленные студентом с помощью преподавателя; единичные ошибки в специальной терминологии; ответы на дополнительные вопросы правильные, недостаточно полные и четкие.

1 балл за каждое собеседование – ответ не полный, с ошибками в деталях, умение раскрыть значение обобщённых знаний не показано, речевое оформление требует поправок, коррекции; логика и последовательность изложения имеют нарушения, студент не способен самостоятельно выделить существенные и несущественные признаки и причинно-следственные связи; ошибки в раскрываемых понятиях, терминах; студент допускает серьезные ошибки; студент не может ответить на большую часть дополнительных вопросов.

0 баллов за каждое собеседование – ответ представляет собой разрозненные знания с существенными ошибками по вопросу; присутствуют фрагментарность, нелогичность изложения, студент не осознает связь обсуждаемого вопроса с другими объектами дисциплины, речь неграмотная; незнание терминологии; ответы на дополнительные вопросы неправильные.

1.3. Критерии оценки домашнего задания

Домашняя работа №1. Отношение делимости и его свойства

1. Что означает высказывание: «целое число, а делится на целое число b »? Истинно ли оно если $a = 275, b = 1$; $a = 1, b = 275$? Сформулируйте отрицание этого высказывания?

2. Сформулируйте основные свойства делимости целых чисел.

3. Докажите, что произведение трех последовательных натуральных чисел делится на 6.

4. Определить, при каких натуральных n $(n^3 + 14) : (n + 2)$

5. Определить, при каких целых n $(n^3 + 4n^2 - 3) : (n + 2)$

6. Доказать, что при любом натуральном n $(10^{3^n} - 1) : 3^{n+2}$

7. Доказать, что $(n^5 - 5n^2 + 4n) : 120$ при любом натуральном n .

8. Доказать, что если $(a^2 + b^2) : 7$ то $ab : 49$

Домашняя работа №2. Деление целых чисел с остатком

1. Сформулируйте основную теорему о делении целых чисел с остатком.

2. Пусть $a = -1284, b = 148$. Укажите такое q , что $bq < a < b(q + 1)$.

3. Пусть $a = -135, b = 14$. Укажите такое r , что $0 \leq r < |b|$ и $(a - r) : b$

4. Укажите частное и остаток от деления 5 на 7, 120 на 13, -529 на -23, -410 на 47, 256 на -15.

5. Сколько существует классов $(x)_6$, таких, что $(3)_6 \cdot (x)_6 = (3)_6$?

6. Найти наименьший положительный вычет класса по модулю $m = 10$, которому принадлежит 19^{321} .

7. На какую цифру оканчивается $7^{4k}, 7^{4k+1}, 7^{4k+2}, 7^{4k+3}$?

8. Было 7 листов бумаги. Некоторые из них разделили на 7 кусков. Затем некоторые из получившихся кусков снова разрезали на 7 кусков. Так сделали несколько раз. Могло ли в результате получиться 1973 куска?

Домашняя работа №3. НОД И НОК целых чисел

1. Что называется, НОД двух целых чисел?

2. Пользуясь определителем, установить, чему равен НОД (15,0)?

3. Как найти НОД двух целых чисел с помощью алгоритма Евклида?

4. Укажите основные свойства НОД.

5. Почему процесс последовательного деления в алгоритме Евклида конечен?

6. Как понимать, НОД двух целых чисел является их линейной комбинацией?

7. С помощью алгоритма Евклида найти НОД (299,391,667).

8. Найти НОД $(6, k^3 - 3k^2 + 2k + 1)$, $k \in \mathbb{N}$.

9. На какие числа может быть сократима дробь

$$\frac{12n+5}{6n+3}, n \in \mathbb{N}?$$

10. Решить в целых числах уравнение $8x + 5y = 49$.

11. Какое число называется общим кратным целых чисел?

12. Что называется, наименьшим общим кратным двух целых чисел, нескольких чисел?

13. Чему равен НОД двух чисел? 14. Найти НОК (299,391,667).

14. Найти наименьшее натуральное число, делящееся на 5, которое при делении на 3,4,5,6,7,8 дает остаток 2.

Домашняя работа №4. Взаимно простые числа. Простые числа.

1. Какие числа называются взаимно простыми?
2. Перечислите свойства взаимно простых чисел?
3. Какая разница между понятиями «взаимно простые числа» и «попарно взаимно простые числа»?
4. Какое из понятий «взаимно простые числа» и «попарно взаимно простые числа» являются следствием другого? В каком случае два понятия совпадают?
5. Докажите, что если простое число взаимно просто с каждым сомножителем, то оно взаимно просто и с их произведением, т. е. если $\text{НОД}(a,c)=1$, $\text{НОД}(b,c)=1$, то $\text{НОД}(a \cdot b, c)=1$.
6. Докажите, что $(a^4 - 1) : 10$, если $\text{НОД}(a, 10)=1$.
7. Какие числа называются простыми? Составными?
8. Являются ли 1 простым числом? Составным числом?
9. Может ли простое число быть четным?
10. Число 30 не делится на простое число 13. Чему равен НОД (30,13), НОК (30,13)?
11. Исследуется вопрос: является ли простым число 1093? Уже проверено, что оно не делится ни на одно из чисел: 2, 3, 5, 7, 11, 13, 17, 19, 23, 31, 37. Следует ли продолжать проверку? Почему?
12. С помощью решета Эратосфена найти все простые числа от 1 до 100. Известны ли вам модификации решета Эратосфена?
13. Можно ли назвать самое большое простое число?
14. Могут ли в натуральном ряду быть идущими подряд 1000000 составных чисел?
15. Определить, какие числа между 2680 и 2710 простые?
16. С помощью канонического разложения найти НОД (18, 72, 136) и НОК (18, 72, 136)?

Домашняя работа №5. Сравнения. Свойства сравнений. Полная и приведенная системы вычетов по модулю m . Теорема Эйлера и Ферма.

1. Что означает запись $a \equiv b \pmod{m}$?
2. Какое условие является необходимым и достаточным для того, чтобы два числа были сравнимы по модулю m ?
3. Установить, сравнимы ли числа 726 и 162 по модулю 5, пользуясь: а) определением; б) признаком сравнимости чисел по модулю.
4. Сформулируйте свойства сравнения, отличные от свойств равенства.
5. Сформулируйте свойства сравнения, аналогичные свойствам равенства.
6. В каком случае можно разделить на одно и тоже число: а) обе части сравнения и модуль; б) обе части сравнения, не изменяя модуля?
7. Классы вычетов по модулю m .
8. Какое условие является необходимым и достаточным для того, чтобы два числа принадлежали одному и тому же классу по модулю m ?

9. Напишите 4 числа из класса $\bar{3}$ по модулю 6.
10. Как определяются операции сложения и умножения классов? Найдите $\bar{5} + \bar{7}$ и $\bar{5} - \bar{8}$, если $m = 9$.
11. Приведите пример кольца классов вычетов с делителями нуля и без делителей нуля.
12. Всегда ли кольцо классов вычетов без делителей нуля является полем?
13. Как получить полную систему вычетов по модулю m ?
14. Напишите наиболее употребительную и произвольную систему вычетов по модулю $m=8$.
15. Сформулируйте определение и основное свойство приведенной системы вычетов по модулю m .
16. Найдите наиболее употребительную и произвольную приведенную систему вычетов по модулю $m = 8$.
17. Какие из полей $\mathbb{Z}_5, \mathbb{Z}_8, \mathbb{Z}_{11}$ являются полями?
18. Дайте определение функции Эйлера. Что означает символ $\varphi(m)$?
19. Какими свойствами обладает функция Эйлера? Напишите выражение для $\varphi(m)$ по каноническому разложению числа m .

Домашняя работа №6. Сравнения первой степени с одним неизвестным.

Системы линейных сравнений с одним неизвестным. Сравнения n -ой степени.

1. Каково условие разрешимости сравнения первой степени с одним неизвестным?
2. Сколько решений имеет сравнение $ax \equiv b \pmod{m}$ в случае его неразрешимости?
3. Как найти решение сравнения $ax \equiv b \pmod{m}$ при условии что $\text{НОД}(a, m) = d = 1$, если известно одно решение этого сравнения?
4. Сформулируйте алгоритм решения системы линейных сравнений с одним неизвестным?
5. Найти числа, которые при делении на 13, 5 и 12 дают соответственно в остатке 5, 1 и 7?
6. Что называется, сравнением n -ой степени с неизвестной величиной?
7. Почему сравнение $f(x) \equiv b \pmod{m}$ имеет не более чем m решений. Почему при решении этого сравнения достаточно ограничиться испытанием чисел $0, 1, 2, \dots, (m-1)$?
8. Какие сравнения называется равносильным?
9. Всегда ли при умножении обеих частей сравнения с неизвестной величиной на целое число получается равносильное сравнение?
10. Получим ли равносильное сравнение при умножении обеих частей сравнения и модуль на целое число?
11. Чему равна степень сравнения $7x^9 + 14x^5 + 3x^2 + 1 \equiv 0 \pmod{7}$?
12. Может ли сравнение $4x^5 + 2x^3 + 3x^2 + 1 \equiv 0 \pmod{41}$ иметь 7 корней?
13. Решить сравнение
14. $6x^9 - 5x^8 + 4x^7 + x^5 - 2x^2 + x - 3 \equiv 0 \pmod{7}$, заменив его равносильным сравнением, степень которого меньше модуля.

Домашняя работа №7. Показатель числа по данному модулю.

Первообразные корни. Индексы

1. Дайте определение порядка класса вычетов по модулю m .
2. Какие значения могут принимать порядки классов вычетов по модулю 13?

3. Класс вычетов 4 имеет порядок по модулю 11. Найдите четыре класса вычетов по модулю 11, имеющих порядок 5.
4. Могут ли существовать классы вычетов порядка 7 по модулю 26?
5. Какое число называется первообразным корнем по модулю p .
6. Достаточно ли выполнимости сравнения $a^{\varphi(p)} \equiv 1 \pmod{p}$ для того, чтобы утверждать, что a - первообразный корень по модулю p ?
7. Чему равно число первообразных корней по простому модулю p ? Сколько их в случае $p = 17$?
8. Что называется индексом числа a по простому модулю p при основании g ?
9. На основании чего можно утверждать, что всякое число a , взаимно простое с p , имеет единственный индекс γ , меньший p ?
10. Зная индекс γ числа a по простому модулю p , укажите все индексы данного числа a . По какому модулю они образуют класс чисел?
11. Перечислите основные свойства индексов.
12. К решению какого сравнения первой степени сводится решение сравнения
13. $ax^n \equiv b \pmod{p}, (a, p) = 1$?
14. При каком условии сравнение $ax^n \equiv b \pmod{p}$ не имеет решений, при каком условии имеет и сколько?
15. Найти показатель, которому принадлежит 25 по модулю 31.
16. Зная, что 2 является первообразным корнем по модулю 19, составьте приведенную систему вычетов по модулю 19 при помощи степеней числа 2.
17. При помощи таблиц индексов решите сравнения: $x^{16} \equiv 3 \pmod{37}$, $17 \equiv 7^x \pmod{53}$.

Критерии оценки:

- 5 баллов получает студент, если правильно выполнено более 50% заданий;
- 0 баллов выставляется студенту, если правильно выполнено менее 50% заданий.

1.4. Критерии оценки творческих заданий

Решить поставленные задачи с использованием СКА.

1. Среди чисел 217, 42, 182, 241 найти все пары чисел, сравнимых между собой по модулю 12.
2. Даны три числа: 137, 343, 633. Какие из данных чисел сравнимы с числом 13 по модулю 31?
3. Даны три числа: 217, 201, 186. Какие из них сравнимы с числом 11 по модулю 19?
4. Даны три числа: 234, 634, 104. Какие из этих чисел сравнимы с числом 9 по модулю 25?
5. Показать, что сравнения:
 - а) $11^{207} \equiv 6 \pmod{27}$,
 - б) $6^{89} \equiv 7 \pmod{16}$,
 - в) $13^{25} \equiv 5 \pmod{30}$,
 - г) $7^{101} \equiv 3 \pmod{35}$,
 - д) $8^{107} \equiv 7 \pmod{14}$
 не имеют места.
6. Написать полную систему наименьших положительных вычетов по модулям: а) 6, б) 11, в) 9, г) 13, д) 15.
7. Написать полную систему наименьших неотрицательных вычетов по модулям: а) 5, б) 7, в) 11, г) 12, д) 14.
8. Написать полную систему абсолютно наименьших вычетов по модулям: а) 11, б) 9,

- в) 7, г) 8, д) 12.
9. Написать приведенную систему вычетов по модулям:
а) 5, б) 7, в) 9, г) 11, д) 12, е) 14, ж) 15.
10. Найти наименьшие положительные вычеты:
а) чисел 113, 127, 41, 47, 53 по модулю 11,
б) чисел 84, 123, 71, 83, 101 по модулю 13,
в) чисел 75, 83, 103, 117, 201 по модулю 15,
г) чисел 63, 88, 97, 105, 136 по модулю 12,
д) чисел 107, 121, 132, 150, 161 по модулю 17.
11. Найти наименьшие неотрицательные вычеты:
а) чисел 115, 131, 57, 48, 83 по модулю 9,
б) чисел 82, 127, 73, 89, 107 по модулю 11,
в) чисел 87, 131, 97, 103, 111 по модулю 12,
г) чисел 69, 93, 100, 123, 141 по модулю 13,
д) чисел 75, 89, 102, 137, 151 по модулю 15.
12. Найти абсолютно наименьшие вычеты:
а) чисел 108, 123, 201, 75, 83 по модулю 10,
б) чисел 97, 138, 61, 87, 151 по модулю 11,
в) чисел 81, 102, 94, 107, 203 по модулю 13,
г) чисел 57, 115, 138, 69, 107 по модулю 12,
д) чисел 41, 87, 105, 13, 127 по модулю 14,
е) чисел 77, 91, 138, 121, 101 по модулю 17.
13. Найти количество натуральных чисел, меньших чисел:
а) 101, б) 131, в) 270, г) 341, д) 600 и взаимно простых с ними.
14. Найти количество натуральных чисел, не превышающих числа:
а) 103, б) 144, в) 152, г) 160, д) 720 и взаимно простых с ними.
15. Найти остаток от деления: а) числа 11^{1201} на число 1000, б) числа 7^{1199} на число 1000, в) числа 3^{157} на число 100.
16. Найти число, составленное тремя цифрами младших разрядов числа 3^{798} .
17. Найти две последние цифры чисел: а) 17^{61} , б) 19^{79} , в) 7^{114} , г) 11^{203} , д) 7^{302} .
18. Используя соответствующие признаки делимости, установить делимость
а) числа 9633 на число 39,
б) числа 8918 на число 7,
в) числа 29148 на число 7,
г) числа 7493 на число 59,
д) числа 9633 на число 13.

Критерии оценки:

- 5 баллов выставляется, если студент выполнил задание полностью, при этом дав полную аргументацию своего мнения, корректно использовал терминологию, учел все требования, поставленные в условии задачи.

- 0 баллов выставляется, если студент выполнил задание менее чем на 50%, не может обосновать свою точку зрения, некорректно использует терминологию.

1.5. Критерии оценки доклада (сообщения)

Сообщение (доклад) оценивается баллами от 1 до 8:

- 8 баллов выставляется студенту, если сообщение (доклад) полностью раскрывает заявленную тему; список использованных источников включает научную, популярную, методическую литературу и Интернет-ресурсы; доклад сопровождается презентацией; текст оформлен в соответствии с требованиями, само выступление презентативно и содержит информацию, выходящую за рамки изученного материала;

- 1 балл выставляется студенту, если сообщение (доклад) раскрывает заявленную тему; однако список использованных источников не полон; доклад не сопровождается презентацией; в оформлении текста имеются отклонения от требований, выступление не содержит информации, выходящей за рамки изученного материала.

1.6. Критерии оценки презентации

Элементы оценки	максимальное количество баллов
титульный слайд с заголовком	0,5
дизайн слайдов	1
использование дополнительных эффектов (смена слайдов, звук, графика, анимация)	0,5
список источников информации	0,5
широта кругозора	0,5
логика изложения материала	1
текст хорошо написан и сформированные идеи ясно изложены и структурированы	1
слайды представлены в логической последовательности	0,5
грамотное создание и сохранение документов в папке рабочих материалов	0,5
слайды распечатаны в форме заметок	0,5
средняя оценка:	

2. Оценочные материалы для промежуточной аттестации

2.1. Примерный перечень вопросов для зачета.

1. Отношение делимости. Свойства делимости.
2. Теорема о делении с остатком.
3. Наибольший общий делитель. Алгоритм Евклида.
4. Свойства НОД. Линейная форма НОД. НОД нескольких чисел.
5. Взаимно простые числа. Свойства взаимно простых чисел.
6. Наименьшее общее кратное. Свойства НОК. Наименьшее общее кратное нескольких чисел.
7. Простые числа. Свойства простых чисел.
8. Решето Эратосфена. Бесконечность множества простых чисел.
9. Основная теорема арифметики.

10. Теоретико-числовые функции.
11. Непрерывные дроби.
12. Подходящие дроби. Свойства подходящих дробей.
13. Сравнения. Свойства сравнений.
14. Полная система вычетов.
15. Приведенная система вычетов.
16. Функция Эйлера.
17. Теоремы Эйлера и Ферма.
18. Сравнения первой степени.
19. Сравнения высших степеней.
20. Решение неопределенных уравнений.
21. Показатель числа. Свойства показателя.
22. Первообразные корни по простому модулю.
23. Индексы и их свойства.
24. Признаки делимости.
25. Системы счисления. Систематические числа.

2.2. Типовые задачи (практические задания)

Делимость чисел

Задача №1. Найти целые числа, дающие при делении на 7 частное 5.

Решение. Искомые числа можно представить в виде $n = 7 \cdot 5 + r$, где $0 \leq r < 7$, т.е. r может принимать значения 0,1,2,3,4,5,6. Поэтому искомыми числами являются 35,36,37,38,39, 40,41.

Ответ: 35,36,37,38,39, 40,41.

Задача №2. Найти делитель и остаток, если делимое равно 25, а частное равно 3.

Решение. Из соотношений $25 = b \cdot 3 + r$ и $0 \leq r \leq (b-1)$ следует двойное неравенство $3b \leq 25 \leq 4b - 1$. Отсюда получаем границы для делителя: $6\frac{1}{2} \leq b \leq 8\frac{2}{3}$.

Поэтому делитель может принимать значения 7 и 8, а остаток, соответственно, 4 и 1.

Ответ.

b	7	8
r	4	1

Задача №3. Доказать, что сумма квадратов двух последовательных натуральных чисел при делении на 4 дает остаток 1.

Решение. Возьмем два последовательных натуральных числа n и $n+1$. Одно из них четное, а другое нечетное. Найдем сумму S их квадратов: $S = n^2 + (n+1)^2 = 2n^2 + 2n + 1 = 2n(n+1) + 1$. Если разделить S на 4, то в частном будет натуральное число $\frac{n(n+1)}{2}$, а в остатке 1.

Простые числа: решето Эратосфена; теорема Евклида о бесконечности множества простых чисел.

Задача №1. Найти натуральное число n такое, что числа n , $n+10$, $n+14$ - простые.

Решение. Если $n > 3$, то при делении на 3 в остатке может быть 1 или 2. Если $n = 3q + 1$, то $n + 14 = 3q + 15$ - не простое число, т.к. делится на 3. Если $n = 3q + 2$, то $n + 10 = 3q + 12$ - также не простое число. Поэтому $n = 3$, $n + 10 = 13$, $n + 14 = 17$.

Задача №2. Если $p > 3$ - простое число, то его можно представить в виде $6n + 1$ или $6n - 1$, где n - натуральное число.

Решение. Разделим p на 6 с остатком: $p = 6q + r$. Поскольку p простое число, то остаток не может быть равен 2, 3 и 4. Остаются две возможности: $r = 1$ и $r = 5$. В первом случае $p = 6n + 1$, где $n = q$, а во втором случае $p = 6n - 1$, где $n = q + 1$.

Задача №3. Доказать, что среди чисел вида $2p + 1$, где p - простое число, только одно является точным кубом.

Решение. Данное число нечетное, поэтому оно является кубом нечетного числа: $2p + 1 = (2n + 1)^3$. Раскрывая это соотношение, получаем $p = n(4n^2 + 6n + 3)$. Так как p - простое число, то $n = 1$ и $p = 13$.

Задача №4. Доказать, что при $n > 2$ между числами n и $n!$ содержится по крайней мере одно простое число.

Решение. Если это утверждение неверно, то все простые числа, меньшие $n!$, будут также не больше, чем n . Рассмотрим число $n! - 1$. Оно составное и поэтому должно делиться на простые числа, которые не превосходят n . На эти же простые числа делится $n!$. Но два последовательных натуральных числа не могут иметь общих простых делителей, т.к. они взаимно простые.

Задача №5. Доказать, что если натуральные числа при делении на m дают остаток 1, то их произведение при делении на m также дает остаток 1.

Решение. Достаточно доказать это для произведения двух чисел. Пусть $a = m \cdot s + 1$ и $b = m \cdot t + 1$. Тогда $a \cdot b = (m \cdot s + 1) \cdot (m \cdot t + 1) = m \cdot (m \cdot s \cdot t + s + t) + 1$, т.е. частным от деления числа $a \cdot b$ на m будет $(m \cdot s \cdot t + s + t)$, а остатком 1.

Задача №6. Доказать, что в числовой последовательности $\{3n + 2\}$, где n - натуральное число, имеется бесконечно много простых чисел.

Решение. Допустим, что в этой последовательности существует конечное число простых чисел. Одно из них равно 2, и, кроме того, k нечетных: $p_1 = 3q_1 + 2, p_2 = 3q_2 + 2, \dots, p_k = 3q_k + 2$. Рассмотрим число $A = 3p_1 p_2 \dots p_k + 2$. Это нечетное число. Оно не может быть простым, т.к. принадлежит той же последовательности, но больше, чем p_1, p_2, \dots, p_k . Оно не делится на числа p_1, p_2, \dots, p_k , поэтому в его разложение на простые множители входят только числа, которые при делении на 3 дают остаток 1. Но произведение таких чисел тоже дает остаток 1, тогда как число $A = 3p_1 p_2 \dots p_k + 2$ дает остаток 2.

Задача №7. Доказать, что в числовой последовательности $\{3n + 2\}$, где n - натуральное число, нет точных квадратов.

Решение. В данной числовой последовательности все числа при делении на 3 дают остаток 2, а квадрат любого натурального числа при делении на 3 дает остаток 0 или 1.

Задача №8. В прямоугольном треугольнике длины всех сторон являются целыми числами. Доказать, что длина хотя бы одного катета делится на 3.

Решение. Пусть длины катетов равны a и b , а длина гипотенузы равна c . По теореме Пифагора $a^2 + b^2 = c^2$. Рассуждая так же, как и в предыдущей задаче, находим, что остаток от деления на 3 правой части этого соотношения равен 0 или 1. Остаток левой

части может быть равен 0 только в том случае, когда оба числа a и b делятся на 3. Аналогично, остаток левой части может быть равен 1 только в том случае, когда одно из чисел a или b делится на 3, а другое не делится. Если же оба числа a и b не делятся на 3, то остаток левой части равен 2, и поэтому соотношение $a^2 + b^2 = c^2$ невозможно.

НОД и НОК. Алгоритм Евклида

Задача №1. Найти наибольший общий делитель чисел 385 и 132.

Решение. Применим алгоритм Евклида к данным числам

$$385 = 132 \cdot 2 + 121$$

$$132 = 121 \cdot 1 + 11$$

$$121 = 11 \cdot 11$$

и оформим его в виде таблицы деления «столбиком», при этом частные записываем в верхнюю строку:

	2	1	11
385	132	121	11
—	—	—	
264	121	121	
—	—	—	
121	11	0	

Последний ненулевой остаток 11 есть наибольший общий делитель.

Ответ: НОД(385,132)=11.

Задача №2. Дробь $\frac{a}{b}$ несократима. Будет ли несократимой дробь $\frac{a}{a+b}$?

Решение. Пусть d - наибольший общий делитель чисел a и $a+b$. Тогда d является также делителем их разности, т.е. числа b . Но a и b - взаимно простые числа.

Значит $d = 1$, и дробь $\frac{a}{a+b}$ несократима.

Практическое занятие №3. Оценки Чебышева для функции числа простых чисел, не превосходящих x .

Задача №1. Найти количество натуральных чисел, не превосходящих 1600 и взаимно простых с 45.

Решение. Поскольку $45 = 3^2 \cdot 5$, взаимно простыми числами с 45 являются те, которые не делятся ни на 3, ни на 5. Количество чисел, не превосходящих 1600 и делящихся на 3, равно $\left\lfloor \frac{1600}{3} \right\rfloor = 533$, а делящихся на 5 равно $\left\lfloor \frac{1600}{5} \right\rfloor = 320$.

Количество чисел, не превосходящих 1600 и делящихся и на 3 и на 5, равно $\left\lfloor \frac{1600}{15} \right\rfloor = 106$. Поэтому количество чисел, не превосходящих 1600 и делящихся либо на

3, либо на 5, равно $533 + 320 - 106 = 747$. Остальные числа не делятся ни на 3, ни на 5, т.е. они взаимно просты с числом 1600. Их количество равно $1600 - 747 = 853$.

Ответ: 853

Задача №2. Сколькими нулями оканчивается число 2012!?

Решение. Надо вычислить, сколько раз это число делится на 10. Для этого надо найти, с каким показателем степени входят числа 2 и 5 в разложение числа 2012! Показатель степени для 2 равен

$$\left\lfloor \frac{2012}{2} \right\rfloor + \left\lfloor \frac{2012}{4} \right\rfloor + \left\lfloor \frac{2012}{8} \right\rfloor + \left\lfloor \frac{2012}{16} \right\rfloor + \left\lfloor \frac{2012}{32} \right\rfloor + \left\lfloor \frac{2012}{64} \right\rfloor + \left\lfloor \frac{2012}{128} \right\rfloor + \left\lfloor \frac{2012}{256} \right\rfloor + \left\lfloor \frac{2012}{512} \right\rfloor + \left\lfloor \frac{2012}{1024} \right\rfloor = 1006 + 503 + 251 + 125 + 62 + 31 + 15 + 7 + 3 + 1 = 2004.$$

$$\left\lfloor \frac{2012}{2} \right\rfloor + \left\lfloor \frac{2012}{4} \right\rfloor + \left\lfloor \frac{2012}{8} \right\rfloor + \left\lfloor \frac{2012}{16} \right\rfloor + \left\lfloor \frac{2012}{32} \right\rfloor + \left\lfloor \frac{2012}{64} \right\rfloor + \left\lfloor \frac{2012}{128} \right\rfloor + \left\lfloor \frac{2012}{256} \right\rfloor + \left\lfloor \frac{2012}{512} \right\rfloor + \left\lfloor \frac{2012}{1024} \right\rfloor = 402 + 80 + 16 + 3 = 501.$$

Поэтому 2012! делится на 10 в степени 501, т.е. оканчивается 501 нулем.

Ответ: 2012! оканчивается 501 нулем.

Задача №3. Найти наибольшее натуральное число n , при котором дробь $101 \cdot 102 \cdot \dots \cdot 1000$

$A = \frac{1000!}{7^n}$ является целым числом.

Решение. Данную дробь можно представить в виде $\frac{1000!}{7^n \cdot 100!}$.

$$\left\lfloor \frac{1000}{7} \right\rfloor + \left\lfloor \frac{1000}{49} \right\rfloor + \left\lfloor \frac{1000}{343} \right\rfloor = 142 + 20 + 2 = 164, \text{ а в разложение } 100! \text{ с показателем}$$

$$\left\lfloor \frac{100}{7} \right\rfloor + \left\lfloor \frac{100}{49} \right\rfloor = 14 + 2 = 16. \text{ Таким образом, для того, чтобы дробь } A \text{ была целым}$$

числом, наибольшее возможное значение n должно быть равно $n = 164 - 16 = 48$.

Ответ: $n = 48$.

Задача №4. Решить уравнение $\left\lfloor \frac{x}{n} \right\rfloor = \left\lfloor \frac{x}{n+1} \right\rfloor$, где n - натуральное число, и найти

количество целочисленных решений.

Решение. При $x > 0$ имеет место неравенство $\frac{x}{n+1} < \frac{x}{n}$. Пусть $\left\lfloor \frac{x}{n} \right\rfloor = k \geq 0$. Тогда

из условия задачи получаем неравенство $k \leq \frac{x}{n+1} < \frac{x}{n} < k+1$, из которого следует

$k \cdot (n+1) \leq x < n \cdot (k+1)$. Последнее неравенство возможно только при $k < n$.

Рассмотрим решение этого неравенства при различных значениях числа k .

k	x	Целочисленные решения	Кол-во целочисленных решений
0	$0 \leq x < n$	$0, 1, 2, \dots, n-1$	n
1	$n+1 \leq x < 2n$	$n+1, n+2, \dots, 2n-1$	$n-1$
2	$2n+2 \leq x < 3n$	$2n+2, 2n+3, \dots, 3n-1$	$n-2$
.....
$n-2$	$n^2 - n - 2 \leq x < n^2 - n$	$n^2 - n - 2, n^2 - n - 1$	2
$n-1$	$n^2 - 1 \leq x < n^2$	$n^2 - 1$	1

$$\lceil x \rceil = k < 0.$$

Пусть теперь $\lceil \frac{x}{n} \rceil = k < 0$. Тогда из условия задачи получаем неравенство $k \leq \frac{x}{n} < k+1$, из которого следует $k \cdot n \leq x < (k+1) \cdot (n+1)$. Последнее неравенство возможно только при $k > -(n+1)$.

Рассмотрим решение этого неравенства при отрицательных значениях числа k .

k	x	Целочисленные решения	Кол-во целочисленных решений
-1	$-n \leq x < 0$	$-n, -n+1, \dots, -1$	n
-2	$-2n \leq x < -(n+1)$	$-2n, -2n+1, \dots, -(n+2)$	$n-1$
.....
$-n+1$	$n^2 + n \leq x < -n^2 + n + 2$	$-n^2 + n, -n^2 + n + 1$	2
$-n$	$-n^2 \leq x < n^2 + 1$	$-n^2$	1

В итоге общее количество целочисленных решений равно $n(n+1)$.

Ответ. Количество целочисленных решений равно $n(n+1)$.

Задача №5. Вычислить значения функции Эйлера для чисел $n=1000, 125, 360$.

Решение. Для решения надо воспользоваться свойством мультипликативности функции Эйлера и формулой её значения для степени простого числа:

$$\varphi(p^k) = (p^k - p^{k-1}).$$

Отсюда получаем:

$$\varphi(1000) = \varphi(2^3 \cdot 5^3) = \varphi(2^3) \cdot \varphi(5^3) = (2^3 - 2^2) \cdot (5^3 - 5^2) = 4 \cdot 100 = 400,$$

$$\varphi(125) = \varphi(5^3) = (5^3 - 5^2) = 100,$$

$$\varphi(360) = \varphi(2^3 \cdot 3^2 \cdot 5) = \varphi(2^3) \cdot \varphi(3^2) \cdot \varphi(5) = (2^3 - 2^2) \cdot (3^2 - 3) \cdot (5 - 1) = 4 \cdot 6 \cdot 4 = 96.$$

Задача №6. Найти значение $\varphi(2m)$, если известно значение $\varphi(m)$.

Решение. Если число m нечетное, то в силу мультипликативности функции Эйлера $\varphi(2m) = \varphi(2) \cdot \varphi(m) = 1 \cdot \varphi(m) = \varphi(m)$. Если же число m четное, $m = 2^k \cdot n$, где n - нечетное, то $\varphi(2m) = \varphi(2^{k+1} \cdot n) = \varphi(2^{k+1}) \cdot \varphi(n) = (2^{k+1} - 2^k) \cdot \varphi(n) = 2^k \cdot \varphi(n)$.

Но $\varphi(m) = \varphi(2^k \cdot n) = \varphi(2^k) \cdot \varphi(n) = (2^k - 2^{k-1}) \cdot \varphi(n) = 2^{k-1} \cdot \varphi(n)$. Таким образом, в этом случае $\varphi(2m) = 2 \cdot \varphi(m)$.

Конечные цепные дроби

Задача №1. Разложить число $\frac{45}{16}$ в цепную дробь.

Решение. Применим алгоритм Евклида

	2	1	4	3
45	16	13	3	1
—	—	—	—	
32	13	12	3	
13	3	1	0	

Элементы верхней строки (неполные частные алгоритма Евклида) являются элементами искомой цепной дроби.

45
Ответ: $\frac{45}{16} = \langle 2, 1, 4, 3 \rangle$.

Задача №2. Найти число, представимое цепной дробью $\alpha = \langle 2, 1, 4, 7, 3 \rangle$, и подходящие дроби.

Решение. Составим таблицу для нахождения подходящих дробей. Для этого возьмем заготовку таблицы.

*					
1					
0	1				

Далее в верхнюю строку вставим элементы цепной дроби.

*	2	1	4	7	3
1					
0	1				

Второй элемент средней строки равен второму элементу верхней строки.

*	2	1	4	7	3
1	2				
0	1				

Пустые клетки заполняем по порядку слева направо по следующей схеме: число в верхней клетке умножаем на число в левой клетке и прибавляем число из предыдущей левой клетки.

*	2	1	4	7	3
1	2	3	14	101	317
0	1	1	5	36	113

Элементы средней строки являются числителями подходящих дробей, а элементы нижней строки – знаменателями. Последняя подходящая дробь является искомым числом.

Ответ: $\alpha = \frac{2}{1}, \alpha = \frac{3}{1}, \alpha = \frac{14}{5}, \alpha = \frac{101}{36}, \alpha = P = \frac{317}{113}$.

Задача №3. Дробь $\alpha = \frac{1261}{881}$ заменить подходящей дробью с возможно меньшими

знаменателями так, чтобы погрешность не превосходила 10^{-4} .

Решение. Разложим данную дробь в цепную дробь

	1	2	3	7	8	2
1261	881	380	121	17	2	1
—	—	—	—	—	—	

881	760	363	119	16	2
380	121	17	2	1	0

Отсюда получаем разложение $\alpha = \langle 1, 2, 3, 7, 8, 2 \rangle$. Найдем подходящие дроби

*	1	2	3	7	8	2
1	1	3	10	73	594	1261
0	1	2	7	51	415	881

Подходящие дроби $\alpha_0 = \frac{1}{1}, \alpha_1 = \frac{3}{2}, \alpha_2 = \frac{10}{7}, \alpha_3 = \frac{73}{51}, \alpha_4 = \frac{594}{415}, \alpha_5 = \frac{1261}{881}$. По формуле

оценки погрешности $|\alpha - \alpha_n| < \frac{1}{Q_n \cdot Q_{n+1}}$, где Q_n и Q_{n+1} - знаменатели n -ой и $(n+1)$ -ой подходящих дробей. Решением поставленной задачи является подходящая дробь

$\alpha = \frac{73}{51}$, т.к. $|\alpha - \alpha_3| < \frac{1}{51 \cdot 415} = \frac{1}{21165} < 10^{-4}$.

Практическое занятие №4. Некоторые частные случаи теоремы Дирихле о бесконечности множества простых чисел в арифметической прогрессии.

Бесконечные цепные дроби. Разложение квадратичных иррациональностей в цепные дроби

Задача №1. Разложить в бесконечную цепную дробь число $\alpha = \sqrt{7}$.

Решение. Найдем целую и дробную части данного числа: $q_0 = \left[\sqrt{7} \right] = 2, \left\{ \sqrt{7} \right\} = \sqrt{7} - 2$. Обозначим дробную часть как $\frac{1}{\beta_1}$. Тогда

$\beta_1 = \frac{1}{\sqrt{7} - 2} = \frac{\sqrt{7} + 2}{3}$. Аналогично для числа β_1 найдем целую и дробную части:

$q_1 = \left[\beta_1 \right] = 1, \left\{ \beta_1 \right\} = \frac{\sqrt{7} - 1}{3}$. Обозначим дробную часть как $\frac{1}{\beta_2}$. Тогда

$\beta_2 = \frac{3}{\sqrt{7} - 1} = \frac{\sqrt{7} + 1}{2}$. Далее также находим целую часть числа β_2 :

$q_2 = \left[\beta_2 \right] = 1, \left\{ \beta_2 \right\} = \frac{\sqrt{7} - 1}{2}$. Обозначим дробную часть как $\frac{1}{\beta_3}$. Тогда

$\beta_3 = \frac{2}{\sqrt{7} - 1} = \frac{\sqrt{7} + 1}{3}$. Далее также находим целую часть числа β_3 :

$q_3 = \left[\beta_3 \right] = 1, \left\{ \beta_3 \right\} = \frac{\sqrt{7} - 2}{3}$. Обозначим дробную часть как $\frac{1}{\beta_4}$. Тогда

$\beta_4 = \frac{3}{\sqrt{7} - 2} = \frac{\sqrt{7} + 2}{1}$. Далее также находим целую часть числа β_4 :

$q_4 = [\sqrt{\beta_4}] = 4, \{\sqrt{\beta_4}\} = \frac{\sqrt{7}-2}{1}$. Обозначим дробную часть как $\frac{1}{\beta_5}$. Тогда

$\beta_5 = \frac{1}{\frac{1}{\sqrt{7}-2}} = \frac{\sqrt{7}+2}{3}$. Очевидно, что $\beta_5 = \beta_1$, поэтому далее элементы цепной дроби

будут повторяться: $\alpha = \sqrt{7} = \langle 2, 1, 1, 1, 4, 1, 1, 1, 4, 1, 1, 1, 4, \dots \rangle = \langle 2, (1, 1, 1, 4) \rangle$.

Ответ: $\sqrt{7} = \langle 2, (1, 1, 1, 4) \rangle$.

Задача №2. Найти число, представимое бесконечной чисто периодической дробью $\langle (2, 1, 3, 4) \rangle$

Решение. Число $\alpha = \langle (2, 1, 3, 4) \rangle$ можно представить в виде конечной дроби $\alpha = \langle 2, 1, 3, 4, \alpha \rangle$. Составим и заполним таблицу для обращения цепной дроби в обыкновенную:

*	2	1	3	4	α
1	2	3	11	47	$47\alpha + 11$
0	1	1	4	17	$17\alpha + 4$

Искомое число равно последней подходящей дроби: $\alpha = \frac{47\alpha + 11}{17\alpha + 4}$. Отсюда

находим квадратное уравнение для α : $17\alpha^2 - 43\alpha - 11 = 0$. Решая это уравнение,

находим $\alpha = \frac{43 + \sqrt{2597}}{34}$.

Ответ: $\alpha = \frac{43 + \sqrt{2597}}{34}$.

Задача №3. Найти число, представимое бесконечной смешанной периодической дробью $\beta = \langle 3, 5, (2, 1, 3, 4) \rangle$.

Решение. Пусть $\alpha = \langle (2, 1, 3, 4) \rangle$ - число, найденное в предыдущей задаче. Тогда число β можно представить в виде конечной цепной дроби $\beta = \langle 3, 5, \alpha \rangle$. Составим и заполним таблицу для обращения цепной дроби в обыкновенную:

*	3	5	α
1	3	16	$16\alpha + 3$
0	1	5	$5\alpha + 1$

Число β равно последней подходящей дроби: $\beta = \frac{16\alpha + 3}{5\alpha + 1}$. Подставляя значение

$\alpha = \frac{43 + \sqrt{2597}}{34}$ и преобразуя, находим $\beta = \frac{5525 - 17\sqrt{2597}}{1462}$.

Ответ: $\beta = \frac{5525 - 17\sqrt{2597}}{1462}$.

Элементы теории сравнений. Поле классов вычетов

Задача №1. Найти две последние цифры числа 17^{2012} .

Решение. Две последние цифры числа показывает остаток от деления на 100. Возводя число 17 в различные натуральные степени, и находя остатки по модулю 100, мы обнаружим, что показателем числа 17 по модулю 100 является 20: $17^{20} \equiv 1 \pmod{100}$. Поскольку $2012 = 20 \cdot 100 + 12$, то $17^{2012} = (17^{20})^{100} \cdot 17^{12} \equiv 17^{12} \equiv 61 \pmod{100}$.

Ответ: Две последние цифры числа 17^{2012} будут 6 и 1.

Задача №2. При каких n число $2^n - 1$ делится на 7?

Решение. Сравнение $2^n \equiv 1 \pmod{7}$ возможно тогда и только тогда, когда n делится на показатель числа 2 по модулю 7. Этот показатель равен 3.

Ответ: При n кратном 3.

Задача №3. Доказать, что число $2^{2^n} + 1$ оканчивается цифрой 7 при любом натуральном $n > 1$.

Решение. Утверждение задачи означает, что $2^{2^n} + 1 \equiv 7 \pmod{10}$ или $2^{2^n} \equiv 6 \pmod{10}$. При $n = 2$ это очевидно. Далее применяем метод математической индукции. Если для некоторого натурального числа n имеет место сравнение $2^{2^n} \equiv 6 \pmod{10}$, то возводя его в квадрат, получим $2^{2^{n+1}} \equiv 36 \pmod{10} \equiv 6 \pmod{10}$. Это означает, что $2^{2^{n+1}} + 1$ также оканчивается цифрой 7.

Задача №4. Составить таблицы сложения и умножения в поле классов вычетов по модулю 11.

Решение. Возьмем полную систему вычетов по модулю 11: $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

Выполняя обычные операции сложения и умножения над вычетами, берем остаток от деления результата операции на 11.

Таблица сложения

+	0	1	2	3	4	5	6	7	8	9	10
0	0	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10	0
2	2	3	4	5	6	7	8	9	10	0	1
3	3	4	5	6	7	8	9	10	0	1	2
4	4	5	6	7	8	9	10	0	1	2	3
5	5	6	7	8	9	10	0	1	2	3	4
6	6	7	8	9	10	0	1	2	3	4	5
7	7	8	9	10	0	1	2	3	4	5	6
8	8	9	10	0	1	2	3	4	5	6	7
9	9	10	0	1	2	3	4	5	6	7	8
10	10	0	1	2	3	4	5	6	7	8	9

Таблица умножения

×	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10

2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

Задача №5. В поле классов вычетов по модулю 11 решить систему уравнений методом Крамера.

$$\begin{cases} 5x + 3y = 7 \\ 7x + 9y = 2 \end{cases}$$

Решение. Вычисляем главный и вспомогательные определители, пользуясь таблицами сложения и умножения из предыдущей задачи:

$$\Delta = \begin{vmatrix} 5 & 3 \\ 7 & 9 \end{vmatrix} = 45 - 21 = 24 = 2,$$

$$\Delta_x = \begin{vmatrix} 7 & 3 \\ 2 & 9 \end{vmatrix} = 63 - 6 = 57 = 2,$$

$$\Delta_y = \begin{vmatrix} 5 & 7 \\ 7 & 2 \end{vmatrix} = 10 - 49 = -39 = 5.$$

$$x = \frac{\Delta_x}{\Delta} = \frac{2}{2} = 1, y = \frac{\Delta_y}{\Delta} = \frac{5}{2} = 8.$$

Ответ: $x=1, y=8$.

Сравнения 1-ой степени

Задача №1. Решить сравнение $17x \equiv 13 \pmod{23}$.

Решение. Решать сравнение будем четырьмя разными способами.

1-й способ: подбор. В отличие от уравнений сравнения можно решать методом подбора, поскольку неизвестное x может принимать конечное число значений. Перебирая наименьшие неотрицательные вычеты из всех классов вычетов по модулю 23, находим $x \equiv 17 \pmod{23}$.

2-й способ: теорема Эйлера. Решение сравнения $ax \equiv b \pmod{m}$ основано на применении теоремы Эйлера $x^{\varphi(m)} \equiv 1 \pmod{m}$, откуда следует, что $x \equiv b \cdot a^{\varphi(m)-1} \pmod{m}$. В данном случае $x \equiv 13 \cdot 17^{\varphi(23)-1} \pmod{23} \equiv 13 \cdot 17^{21} \pmod{23}$. Вычисляя значения степеней числа 17 по модулю 23, находим, что $17^{21} \equiv 19 \pmod{23}$ и $13 \cdot 19 \equiv 17 \pmod{23}$, т.е. $x \equiv 17 \pmod{23}$.

3-й способ: цепные дроби. Для решения сравнения $ax \equiv b \pmod{m}$ надо дробь $\frac{m}{a}$ разложить в цепную дробь и найти числитель предпоследней подходящей дроби.

Разложим обыкновенную дробь $\frac{23}{17}$ в цепную дробь: $\frac{23}{17} = \langle 1, 2, 1, 5 \rangle$. Длина полученной цепной дроби равна $n = 3$. Найдем подходящие дроби:

*	1	2	1	5
1	1	3	4	23
0	1	2	3	17

Числитель предпоследней подходящей дроби равен 4. Решение сравнения находим по формуле:

$$x \equiv (-1)^n \cdot b \cdot P_{n-1}(\text{mod } m) \equiv (-1)^3 \cdot 13 \cdot 4(\text{mod } 23) \equiv -6(\text{mod } 23) \equiv 17(\text{mod } 23)$$

4-й способ: изменение коэффициентов. Преобразуем сравнение, заменяя коэффициенты на другие, сравнимые с ними по данному модулю. Затем применяем свойство сравнений: обе части сравнения можно делить на число, взаимно простое с модулем.

$$17x \equiv 13(\text{mod } 23),$$

$$40x \equiv -10(\text{mod } 23),$$

$$4x \equiv -1(\text{mod } 23),$$

$$4x \equiv 22(\text{mod } 23),$$

$$2x \equiv 11(\text{mod } 23),$$

$$2x \equiv 34(\text{mod } 23),$$

$$x \equiv 17(\text{mod } 23).$$

Ответ: $x \equiv 17(\text{mod } 23)$.

Задача №2. Решить систему сравнений

$$\begin{cases} x \equiv 5(\text{mod } 7) \\ x \equiv 3(\text{mod } 11) \end{cases}$$

Решение.

1-й способ. Перейдем от сравнения к равенству, введя новую переменную: $x = 5 + 7y$.

Подставим это выражение во второе сравнение системы и преобразуем.

$$5 + 7y \equiv 3(\text{mod } 11),$$

$$7y \equiv -2(\text{mod } 11),$$

$$-4y \equiv -2(\text{mod } 11),$$

$$2y \equiv 1(\text{mod } 11),$$

$$2y \equiv 12(\text{mod } 11),$$

$$y \equiv 6(\text{mod } 11),$$

$$y = 6 + 11z,$$

$$x = 5 + 7(6 + 11z) = 47 + 77z,$$

$$x \equiv 47(\text{mod } 77).$$

2-й способ: китайская теорема об остатках. Рассмотрим вспомогательные сравнения:

$$11y \equiv 1(\text{mod } 7) \text{ и } 7y \equiv 1(\text{mod } 11).$$

Их решения: $y \equiv 2 \pmod{7}$ и $y \equiv 8 \pmod{11}$. Возьмем $y_1 = 2$ и $y_2 = 8$. Тогда по китайской теореме об остатках получаем

$$x \equiv 11 \cdot 5 \cdot 2 + 7 \cdot 3 \cdot 8 \pmod{77} \equiv 278 \pmod{77} \equiv 47 \pmod{77}.$$

Ответ: $x \equiv 47 \pmod{77}$.

Неопределенные уравнения

Задача №1. Решить неопределенное уравнение $5x + 11y = 13$.

Решение. Найдем сначала частное решение, перейдя от уравнения к вспомогательному сравнению:

$$5x \equiv 13 \pmod{11},$$

$$5x \equiv 35 \pmod{11},$$

$$x \equiv 7 \pmod{11}.$$

Отсюда получаем

$$x_0 = 7, \quad y_0 = \frac{13 - 5 \cdot 7}{11} = -2.$$

Общее решение неопределенного уравнения теперь имеет вид

$$\begin{cases} x = 7 - 11t \\ y = -2 + 13t \end{cases}, \quad t \in \mathbf{Z}.$$

Ответ: $\begin{cases} x = 7 - 11t \\ y = -2 + 13t \end{cases}, \quad t \in \mathbf{Z}.$

Задача №2. На почте продаются марки ценой по 3 рубля и по 11 рублей. Сколько марок можно купить на 100 рублей?

Решение. Составляем неопределенное уравнение $3x + 11y = 100$, где x и y - количества марок 1-го и 2-го типов соответственно. Находим частное решение:

$x_0 = 4, \quad y_0 = 8$. Общее решение имеет вид

$$\begin{cases} x = 4 - 11t \\ y = 8 + 3t \end{cases}, \quad t \in \mathbf{Z}.$$

По смыслу задачи неизвестные x и y должны быть неотрицательны. Это дает двойное неравенство для переменной t : $-\frac{8}{3} \leq t \leq \frac{4}{11}$. Целочисленная переменная t

принимает значения $t_1 = -2, t_2 = -1, t_3 = 0$. Им соответствуют решения уравнения

$$x_1 = 26, \quad y_1 = 2,$$

$$x_2 = 15, \quad y_2 = 5,$$

$$x_3 = 4, \quad y_3 = 8.$$

Ответ: $x_1 = 26, \quad y_1 = 2; \quad x_2 = 15, \quad y_2 = 5; \quad x_3 = 4, \quad y_3 = 8$.

Задача №3. Найти все числа, на которые может быть сократима дробь $\frac{7n+5}{5n+2}$. При каких значениях числа n дробь будет сократимой?

Решение. Дробь сократима, когда наибольший общий делитель числителя и знаменателя больше 1. Если $d = \text{НОД}(7n+5, 5n+2)$, то $\begin{cases} 7n+5 = d \cdot x \\ 5n+2 = d \cdot y \end{cases}$. Исключая из этой системы число n , получим $d \cdot (5x-7y) = 11$. Поскольку число 11 простое, то $d=11$ и $(5x-7y)=1$. Решая последнее неопределенное уравнение, получим $\begin{cases} x = 3 + 7t \\ y = 2 + 5t \end{cases}, t \in \mathbb{Z}$. Из этого решение находим, при каких значениях n дробь сократима: $n = 4 + 11t, t \in \mathbb{Z}$.

Ответ: Дробь может быть сократима только на 11 при $n = 4 + 11t, t \in \mathbb{Z}$.

Первообразные корни и индексы

Задача №1. Найти первообразный корень по модулю 17.

Решение. Проверим число 2:

$$2^2 \equiv 4(\text{mod } 17), 2^3 \equiv 8(\text{mod } 17), 2^4 \equiv 16(\text{mod } 17), 2^5 \equiv 15(\text{mod } 17), \\ 2^6 \equiv 13(\text{mod } 17), 2^7 \equiv 9(\text{mod } 17), 2^8 \equiv 1(\text{mod } 17).$$

Это означает, что показатель числа 2 по модулю 17 равен 8, и число 2 не является первообразным корнем по модулю 17.

Проверим число 3:

$$3^2 \equiv 9(\text{mod } 17), 3^3 \equiv 10(\text{mod } 17), 3^4 \equiv 13(\text{mod } 17), 3^5 \equiv 5(\text{mod } 17), 3^6 \equiv 15(\text{mod } 17), \\ 3^7 \equiv 11(\text{mod } 17), 3^8 \equiv 16(\text{mod } 17), 3^9 \equiv 14(\text{mod } 17), 3^{10} \equiv 8(\text{mod } 17), 3^{11} \equiv 7(\text{mod } 17), \\ 3^{12} \equiv 4(\text{mod } 17), 3^{13} \equiv 12(\text{mod } 17), 3^{14} \equiv 2(\text{mod } 17), 3^{15} \equiv 6(\text{mod } 17), 3^{16} \equiv 1(\text{mod } 17).$$

Показатель числа 3 по модулю 17 равен 16, поэтому число 3 является первообразным корнем по модулю 17.

Задача №2. На циферблате часов расставить числа 1,2,3,...,12 так, чтобы для любых трех чисел a, b, c , стоящих подряд, число $b^2 - a \cdot c$ делилось на 13.

Решение. Число 13 – простое. Возьмем любой первообразный корень по модулю 13, например 2. Выпишем его двенадцать степеней: 2,4,8,16,32,64,128,256,512,1024,2048,4096.

Это геометрическая прогрессия. По свойству геометрической прогрессии квадрат любого члена равен произведению двух соседних членов: $b^2 = a \cdot c$. Если числа прогрессии заменить их остатками при делении на 13:

$$2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1,$$

то полученная последовательность будет удовлетворять условию задачи. Эти числа можно расставить на циферблате начиная с любого места. Кроме того, можно двигаться как по часовой стрелке, так и против часовой стрелки.

Степенные и показательные сравнения

Задача №1. Решить сравнение $7x^3 \equiv 3(\text{mod } 11)$.

Решение. Число 2 является первообразным корнем по модулю 11. Составим таблицу индексов по модулю 11 и основанию 2.

$$2^1 \equiv 2(\text{mod } 11), 2^2 \equiv 4(\text{mod } 11), 2^3 \equiv 8(\text{mod } 11), 2^4 \equiv 5(\text{mod } 11), 2^5 \equiv 10(\text{mod } 11), \\ 2^6 \equiv 9(\text{mod } 11), 2^7 \equiv 7(\text{mod } 11), 2^8 \equiv 3(\text{mod } 11), 2^9 \equiv 6(\text{mod } 11), 2^{10} \equiv 1(\text{mod } 11).$$

x	1	2	3	4	5	6	7	8	9	10
-----	---	---	---	---	---	---	---	---	---	----

$ind(x)$	0	1	8	2	4	9	7	3	6	5
----------	---	---	---	---	---	---	---	---	---	---

Проиндексируем данное сравнение и получим новое сравнение по модулю $\varphi(11)=10$. Введём новую переменную $y = ind(x)$:

$$ind(7) + 3ind(x) \equiv ind(3)(\text{mod}10),$$

$$7 + 3y \equiv 8(\text{mod}10),$$

$$3y \equiv 1(\text{mod}10),$$

$$3y \equiv 21(\text{mod}10),$$

$$y \equiv 7(\text{mod}10).$$

По таблице индексов находим $x \equiv 7(\text{mod}11)$.

Ответ: $x \equiv 7(\text{mod}11)$.

Задача №2. Решить показательное сравнение $5 \cdot 8^x \equiv 3(\text{mod}11)$.

Решение. Проиндексируем данное сравнение, воспользовавшись таблицей индексов из предыдущего примера:

$$ind(5) + x \cdot ind(8) \equiv ind(3)(\text{mod}10)$$

$$4 + 3x \equiv 8(\text{mod}10)$$

$$3x \equiv 4(\text{mod}10)$$

$$x \equiv 8(\text{mod}10)$$

Ответ: $x \equiv 8(\text{mod}10)$.

Задача №3. Решить сравнение $x^2 + 7x + 5 \equiv 0(\text{mod}13)$.

Решение. Преобразуем сравнения путем замены коэффициентов на другие, сравнимые с ними по модулю 13:

$$x^2 - 6x + 5 \equiv 0(\text{mod}13),$$

$$x^2 - 6x + 9 \equiv 4(\text{mod}13),$$

$$(x - 3)^2 - 2^2 \equiv 0(\text{mod}13),$$

$$(x - 1)(x - 5) \equiv 0(\text{mod}13),$$

$$x_1 \equiv 1(\text{mod}13), x_2 \equiv 5(\text{mod}13).$$

Таким образом, сравнение имеет два решения.

Ответ: $x_1 \equiv 1(\text{mod}13), x_2 \equiv 5(\text{mod}13)$.

Символ Лежандра

Задача №1. Вычислить символ Лежандра $\left(\frac{26}{43}\right)$.

$$\begin{aligned} \text{Решение. Воспользуемся свойствами символа Лежандра:} \\ \left(\frac{26}{43}\right) &= \left(\frac{2 \cdot 13}{43}\right) = \left(\frac{2}{43}\right) \cdot \left(\frac{13}{43}\right) = (-1)^{\frac{43^2-1}{8}} \cdot (-1)^{\frac{43-1}{2} \cdot \frac{13-1}{2}} \cdot \left(\frac{43}{13}\right) = \\ &= (-1)^{231} \cdot (-1)^{21 \cdot 6} \cdot \left(\frac{43}{13}\right) = -\left(\frac{43}{13}\right) = -\left(\frac{4}{13}\right) = -\left(\frac{2^2}{13}\right) = -1. \end{aligned}$$

Задача №2. Доказать, что произведение двух последовательных натуральных чисел при делении на 17 не может давать в остатке 1.

Решение. Пусть произведение двух последовательных натуральных чисел x и $x+1$ при делении на 17 дает в остатке 1. Тогда имеет место сравнение $x \cdot (x+1) \equiv 1 \pmod{17}$. Преобразуем, пользуясь свойствами сравнений:

$$x^2 + x \equiv 1 \pmod{17},$$

$$4x^2 + 4x \equiv 4 \pmod{17},$$

$$4x^2 + 4x + 1 \equiv 5 \pmod{17},$$

$$(2x + 1)^2 \equiv 5 \pmod{17}.$$

Последнее сравнение возможно, если число 5 является квадратичным вычетом по модулю 17. Проверим с помощью символа Лежандра.

$$\left(\frac{5}{17}\right) = (-1)^{\frac{(5-1)(17-1)}{2}} \cdot \left(\frac{17}{5}\right) = \left(\frac{17}{5}\right) = \left(\frac{2}{5}\right) = \left(\frac{-}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1$$

Это означает, что число 5 является квадратичным невычетом по модулю 17, поэтому сравнение $(2x+1)^2 \equiv 5 \pmod{17}$ не имеет решения.

Задача №3. Доказать, что простое число вида $p = 4n + 3$ нельзя представить в виде суммы квадратов двух натуральных чисел.

Решение. Допустим, что $p = a^2 + b^2$. Тогда $a^2 + b^2 \equiv 0 \pmod{p}$. Отсюда получаем $a^2 \equiv -b^2 \pmod{p}$. Числа a и b взаимно просты с p . Возьмем число c такое, что $b \cdot c \equiv 1 \pmod{p}$. Тогда $(a \cdot c)^2 \equiv -1 \pmod{p}$. Это означало бы, что число (-1) является квадратичным вычетом по модулю p . Но значение символа Лежандра для числа (-1) равно $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{2n+1} = -1$, т.е. (-1) является квадратичным невычетом по модулю $p = 4n + 3$.

Задача №4. Числа a и b можно представить в виде суммы квадратов двух целых чисел. Доказать, что их произведение также можно представить в виде суммы квадратов двух целых чисел.

Решение. Пусть $a = x^2 + y^2$ и $b = z^2 + t^2$. Тогда

$$ab = (x^2 + y^2)(z^2 + t^2) = x^2z^2 + x^2t^2 + y^2z^2 + y^2t^2 = (xz + yt)^2 + (xt - yz)^2.$$

Задача №5. Доказать, что число $(1+a_1^2) \cdot (1+a_2^2) \cdot \dots \cdot (1+a_n^2)$ является суммой квадратов двух целых чисел, где a_1, a_2, \dots, a_n - целые числа.

Решение следует из предыдущей задачи применением метода математической индукции.

Критерии оценки

Зачёт по дисциплине без прохождения итогового контроля выставляется студенту при условии успешного прохождения им точек рубежного контроля в семестре и при количестве набранных баллов не менее 80 в соответствии с рейтинговой системой учета учебных достижений студентов.

Зачёт проводится в устной форме.

В ходе ответа студента преподаватель имеет право задавать дополнительные вопросы по материалу, вынесенному на зачет. Во время сдачи зачёта с оценкой студентам запрещается:

1. Пользоваться средствами мобильной связи и иными средствами хранения и передачи информации.
2. Вести переговоры и осуществлять иные контакты с другими студентами с целью сдачи зачета.
3. Выходить из аудитории, где проводится зачет, до получения оценки.
4. Задерживать сдачу листа ответа после объявления преподавателем об окончании времени подготовки.
5. Выносить лист ответа из аудитории после окончания зачета.

Оценка «**зачтено**» ставится в том случае, когда студент демонстрирует полное знание учебного материала, демонстрирует систематический характер знаний по дисциплине. Ответ полный и правильный, подтвержден примерами; но их обоснование не аргументировано, отсутствует собственная точка зрения. Материал изложен в определенной логической последовательности, могут быть допущены 2-3 несущественные погрешности, исправленные по требованию преподавателя. Студент может испытывать незначительные трудности в ответах на дополнительные вопросы. Материал изложен осознанно, самостоятельно, с использованием современных научных терминов, математическим языком.

Оценка «**незачтено**» выставляется студенту, когда он демонстрирует пробелы в знаниях основного учебного материала по дисциплине. При ответе обнаружено непонимание студентом основного содержания теоретического материала или допущен ряд существенных ошибок, которые студент не может исправить при наводящих вопросах преподавателя, затрудняется в ответах на вопросы. Студент подменил научное обоснование проблем рассуждением бытового плана. Ответ носит поверхностный характер; наблюдаются неточности в использовании научной терминологии.

Сведения об утверждении программы на очередной учебный год и регистрации изменений

Учебный год	Решение кафедры (№ протокола, дата)	Внесенные изменения	Подпись зав. кафедрой

