Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Механико-математический факультет

УТВЕРЖДЕНО:
Декан ММФ ТГУ
Л.В.Гензе

Оценочные материалы по дисциплине

Теория чисел

по направлению подготовки

01.03.01 Математика
02.03.01 Математика и компьютерные науки

Направленность (профиль) подготовки
Основы научно-исследовательской деятельности в области математики
Основы научно-исследовательской деятельности в области математики и компьютерных наук

Форма обучения
Очная

Квалификация
Бакалавр

Год приема
2023

СОГЛАСОВАНО:
Руководитель ОП
Л.В.Гензе

Председатель УМК
Е.А.Тарасов

Томск – 2023

1. Компетенции и индикаторы их достижения, проверяемые данными оценочными материалами

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-1 Способен применять фундаментальные знания в области математического анализа, комплексного и функционального анализа, алгебры, аналитической геометрии, дифференциальной геометрии и топологии, дифференциальных уравнений, дискретной математики и математической логики, теории вероятностей, математической статистики и случайных процессов, численных методов, теоретической механики как для использования в профессиональной деятельности, так и для консультирования.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК 1.1 Демонстрирует навыки работы с профессиональной литературой по основным естественнонаучным и математическим дисциплинам

ИОПК 1.2 Демонстрирует навыки выполнения стандартных действий, решения типовых задач с учетом основных понятий и общих закономерностей, формулируемых в рамках базовых математических и естественнонаучных дисциплин

ИОПК 1.3 Владеет фундаментальными знаниями, полученными в области математических и (или) естественных наук

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:

- тест №1 «Основы теории чисел»;
- тест №2;
- контрольные работы №1-№3;
- рефераты «Основоположники теории чисел», «работы П.Л. Чебышева в теории чисел», «Примеры применения теории чисел в криптографии». «работы К.Ф. Гаусса в теории чисел».

Тест №1 (ИОПК-1.2).

Примеры задач.

1) Выберите верные утверждения:

а) Тернарная проблема Гольдбаха решена в 2013 г.

б) Неизвестно, бесконечно ли множество простых чисел Мерсенна.

в) Найдено несколько десятков простых чисел Ферма.

Ответ: а), б).

2) Выберите верные утверждения:

а) По модулю n существует первообразный корень $\Leftrightarrow$ $n = 2,4,p^a,2p^a$, где a из $\mathbb{N}$, а p – нечетное простое натуральное число.

б) По модулю n существует первообразный корень $\Leftrightarrow$ $n = 2,4,p^a$, где a из $\mathbb{N}$, а p – нечетное простое натуральное число.

в) По модулю n существует первообразный корень $\Leftrightarrow$ $n = 2,4,p$, где p – нечетное простое натуральное число.

г) По модулю n существует первообразный корень $\Leftrightarrow$ $n = 2,p^a$, где a из $\mathbb{N}$, а p – нечетное простое натуральное число.

Ответ: а).

Тест с ограничением по времени – 90 минут и одна попытка. Всего в тесте предложено 14 задач с оценкой от 1 до 10 баллов. Максимальная оценка за тест 44 балла. Тест считается пройденным, если учащийся получил не менее 22 балла.

Тест №2 (ИОПК-1.2, 1.3). Более сложный, требующий не только владения основными понятиями, но и их применения на практике, решение задач.

Примеры задач.

1) Пусть 1, 1 + p, … - арифметическая прогрессия, где p – простое натуральное число. Выберите верные утверждения:

а) В этой прогрессии содержится бесконечное множество простых чисел.

б) каждое простое натуральное число содержится в подобной прогрессии при некотором p.

в) При фиксированном натуральном p подобная прогрессия содержит все множество простых натуральных чисел.

Ответ: а), б).

2) Укажите последнюю цифру числа 7^{2023}.

а) 1; б) 9; в) 7; г) 3; д) 2; е) 5.

Ответ: в).

Тест с ограничением по времени – 80 минут и одна попытка. Всего в тесте предложено 22 задачи с оценкой 2 балла. Максимальное количество баллов по тесту 44. Тест считается пройденным, если учащийся получил не менее 22 балла.

Примерные темы рефератов (ИОПК 1.1): «Методы теории чисел в криптосиситеме RSA», «Основоположники теории чисел», «Работы П.Л. Чебышева в теории чисел», «Примеры применения теории чисел в криптографии». «Работы К.Ф. Гаусса в теории чисел».

Контрольные работы (ИОПК 1.3). Предусмотрены 3 контрольные работы, которые необходимо выполнить самостоятельно в течении семестра.

Примеры задач.

1) Найдите сумму и число всех натуральных делителей следующих чисел:

а) 365; б) 870; в) 1061.

Ответ. а) 4, 444. б) 16, 2160. в) 2, 1062.

2) Решить уравнение 417x-22y=378 при помощи а) сравнений и б) цепных дробей.

Ответ: x=18+22t, y=324+417t, где $t \in \mathbb{Z}$.

3) Разложите в непрерывную дробь число $\frac{2+\sqrt{5}}{3}$.

Ответ [1,(2,2,2,1,12,1)].

За решение задач начисляются баллы от 0 до 100.

Оценка «отлично» выставляется за при 81-100 баллов, «хорошо» выставляется при получении 61-80 баллов, «удовлетворительно» выставляется за 45-60 баллов, «неудовлетворительно» выставляется при получении менее 44 баллов.

3. Оценочные материалы итогового контроля (промежуточной аттестации) и критерии оценивания

Зачет в шестом семестре проводится в письменной форме по билетам. Билет содержит теоретический вопрос и две задачи. Продолжительность зачета 1,5 часа.

Примерный перечень теоретических вопросов

1. Вопрос 1. Мультипликативность функции $\tau(n)$. Доказать, что если $n = p^{\alpha}\dots q^{\gamma}$ – каноническое разложение числа n, то $\tau(n) = (\alpha + 1)\dots(\gamma + 1)$.

2. Вопрос 2. Докажите теорему о разрешимости в $\mathbb{Z}$ уравнения $ax + by = c$, где a,b,c – целые числа и $ab \neq 0$

3. Вопрос 3. Докажите, что если a – квадратичный вычет по модулю p, то

$a^{(p-1)/2} \equiv 1 \pmod{p}$.

Вопрос 4. Теория чисел и криптосистема RSA.

Примеры задач:

1. Найдите двузначное число, сравнимое с 2 по модулю 3 и 7, и с -2 по модулю 11.
2. Решите сравнение $2x - 3y \equiv 4 \pmod 5$.
3. Разложите число 539/103 в цепную дробь.
4. Исследовать, какие из чисел между 2320 и 2350 являются простыми.

Вид оцениваемой работы:	*Удельный вес указанного вида работы в итоговой оценке (в процентах)*	В течение семестра/в конце семестра	*Критерии оценивания указанного вида работы*
Инд. задание в системе Moodle.	20%	В течение семестра	По 100 бальной системе.
Тесты в системе Moodle.	30%	В течение семестра	Максимальное использование возможностей программы
Зачет	50%	В конце семестра	Студент допускается до зачета только при наличии выполненных индивидуального задания и теста. 1) Полный ответ, изложенный кратко и ясно – «зачет». 2) Ответ неполный (но > 50%), пояснения логически непротиворечивы – «зачет». 3) Ответ неполный (< 50%), отсутствие логики в пояснениях – «незачет». 4) Ответ по сути отсутствует – «незачет».

Студенты, не выполнившие тесты или контрольные работы получают дополнительно идентичные задачи и вопросы, после их решения и положительного ответа получают билет для зачета.

4. Оценочные материалы для проверки остаточных знаний (сформированности компетенций)

Тест (ИОПК-1.2, 1.3)

1) Решением в $\mathbb{N}$ уравнения $x^y = y^x$ являются только следующие наборы натуральных чисел:

а) (1,1), (2,4), (4,2).

б) (a,a), (2,4), (4,2), где a из $\mathbb{N}$.

в) (a,a), $(2b,4b)$, $(4b,2b)$, где $a \in \mathbb{N}$, а $b = 1$ или $b = 2$.

г) в) (a,a), $(b,2b)$, $(2b,b)$, где a,b из $\mathbb{N}$.

Ответ: б).

2) Теорема Чебышева формулируется так:

а) Для любого натурального числа $n \geq 6$ между числами n и $2n$ существуют по крайней мере два простых числа.

б) Для любого натурального числа $n \geq 6$ между числами n и $2n$ существует хотя бы одно простое число.

в) Для любого натурального числа $n \geq 28$ между числами n и $2n$ существуют по крайней мере три простых числа.

Ответ: а).

Задачи (ИОПК 1.2)

1) Вычислить символы Лежандра: (166/229) и (41/617)

Ответ. -1 и 1.

2) Являются ли 2, 7, 11 и 13 первообразными корнями по модулю 61?
Ответ. 2 и 7 – первообразные, 11 нет, так как $11^4 = 1$ mod(61).

3) Решить в $\mathbb{N}$ уравнение $x! + y! = z!!$. Здесь $z!!$ – произведение натуральных чисел, не превосходящих числа z и имеющие с ним одинаковую четность.
Ответ. (1,1,2), (2,1,3), (1,2,3).

Теоретические вопросы (ИОПК 1.3)

1) Мультипликативность функции $\tau(n)$. Доказать, что если $n = p^{\alpha}\ldots q^{\gamma}$ – каноническое разложение числа n, то $\tau(n) = (\alpha + 1)\ldots(\gamma + 1)$.

2) Пусть p – нечетное простое число. Доказать, что сравнение $x^2 \equiv -1 \pmod p$ разрешимо тогда и только тогда, когда $p \equiv 1 \pmod 4$.

3) Докажите формулу для функции Эйлера $\varphi(n)$.

Ответы на вопросы должны содержать определения соответствующих понятий, пояснение необходимых для доказательства свойств, само доказательство должно быть полным и безукоризненным с точки зрения логики

Информация о разработчиках

Чехлов Андрей Ростиславович, д.ф.-м.н., доцент, профессор каф. алгебры ТГУ.