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 дисциплины

Избранные вопросы теории чисел

по направлению подготовки

01.04.01 Математика

Направленность (профиль) подготовки:
Фундаментальная математика

Форма обучения
Очная

Квалификация
Магистр

Год приема
2023

СОГЛАСОВАНО:
Руководитель ОП
П.А. Крылов

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 формулировать и решать актуальные и значимые проблемы математики.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК 1.1 Формулирует поставленную задачу, пользуется языком предметной области, обоснованно выбирает метод решения задачи.

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:

– тесты;
– контрольная работа;
– рефераты.

Примеры тестовых вопросов (ИОПК 1.1).

А) Выберите правильный ответ. Алгоритм Монтгомери является алгоритмом:

1) модульного умножения в кольце вычетов;
2) разложения многочленов в произведение неприводимых многочленов;
3) проверки простоты чисел.

Ключ: 1).

Б) Доказано, что вероятность правильного ответа в тест Миллера-Рабина

1) $\geq 4/5$; 2) $\geq 3/4$; 3) $\geq 9/10$.

Ключ: 2).

В) Студент на экзамене дает следующее определение: «дискретным логарифмом элемента h группы G по основанию $g \in G$ называется число x являющееся решением уравнения $g^x = h$». Спохватившись, студент пытается поправить определение. Выберите правильное дополнение:

1) число x должно быть натуральным;
2) группа G должна быть конечной;
3) группа G должна быть циклической конечного порядка m, а $x \in \{0,1,\ldots,m\text{-}1\}$.

Ключ: 3).

Примеры задач на контрольной работе (ИОПК 1.1).

1) Воспользовавшись бинарный алгоритм возведения в степень, найдите x^{80}.

2) С помощью расширенного алгоритма Евклида найдите обратный элемент 96^{-1} в кольце вычетов $\mathbb{Z}_{127}$.

3) Пусть $f(x) = x^3 - x^2 + 2x + 1$, найти корни этого многочлена в $\mathbb{Z}_k$ при $k = 3^4$.

Ответ: 74.

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

Экзамен в третьем семестре проводится в письменной форме по билетам. Экзаменационный билет состоит из трех частей. Продолжительность экзамена 1,5 часа.

Примерный перечень теоретических вопросов первой части.

Вопрос. Алгоритм Монтгомери относится к алгоритмам:

а) нахождения первообразных корней по модулю;

б) модульной арифметики;

в) проверки простоты натуральных чисел;

г) факторизации;

д) дискретного логарифмирования.

Примерный перечень теоретических вопросов второй части.

Вопрос 1. Доказать теорему Поклингтона о виде простых делителей числа N, для которого известно частичное разложение на множители числа N-1.

Вопрос 2. Обосновать принципиальное отличие теста Миллера-Рабина проверки простоты числа от теста Соловея-Штрассена.

Вопрос 3. Докажите, что множество вычетов по модулю N, относительно которых N является эйлеровым псевдопростым, образует подгруппу.

Примерный перечень задач из третьей части. Решение при помощи инженерного калькулятора.

Задача 1. При помощи алгоритма Чипполы найти квадратный корень из a по модулю p, если $p = 19$, $a = 13$.

Задача 2. Решить сравнение $x^7 = -88 \bmod 841$.

Задача 3. Решить сравнение $11^x = 19 \bmod 529$.

Результаты экзамена определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Инд. задание в системе Moodle.	20%	В течение семестра	По 100 бальной системе.
Тесты в системе Moodle.	20%	В течение семестра	Максимальное использование возможностей программы
Экзамен	60%	В конце семестра	Студент допускается до экзамена только при наличии выполненных индивидуального задания и теста. 1) Полный ответ, изложенный кратко и ясно – «отлично». 2) Ответ неполный (но > 70%), пояснения логически непротиворечивы – «хорошо». 3) Ответ неполный (но >50%), отсутствие логики в пояснениях – «удовлетворительно». 4) Ответ неполный (<50%), отсутствие логики в пояснениях или по сути отсутствует – «неудовлетворительно».

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

Примеры тестовых вопросов (ИОПК 1.1).

А) Выберите правильные ответы.

1) Тесты Миллера-Рабина, Соловея-Штрассена и Люка-Лемера относятся к вероятностным тестам проверки простоты чисел.

2) К вероятностным тестам проверки простоты чисел относятся тесты Миллера-Рабина и Соловея-Штрассена, а алгоритм Люка-Лемера является полиномиальным, детерминированным и безусловным тестом простоты для чисел Мерсенна.

3) Поклингтон доказал теорему, позволяющую проверять простоту числа N, зная только частичное разложение на множители числа N-1.

Ключ: 2), 3).

Б) Выберите правильные ответы.

1) Малая теорема Ферма утверждает, что если число N простое, то $a^{N-1} \equiv 1 \bmod N$ для всякого натурального числа a, взаимно простого с N.

2) Малая теорема Ферма утверждает, что если число N простое, то $a^{N-1} \equiv 1 \bmod N$ для всякого натурального числа a.

3) Малая теорема Ферма утверждает, что число N простое тогда и только тогда, когда $a^{N-1} \equiv 1 \bmod N$ для всякого натурального числа a, взаимно простого с N.

Ключ: 1).

Примеры задач (ИОПК 1.1).

1) Вычислить $x = (\log_2 15)_{61}$.

Ответ: $(\log_2 15)_{61} = 28$.

2) Покажите, что число 25 является эйлеровым псевдопростым по основанию 7.

3) Решить сравнение $5^x \equiv 13 \bmod 32$.

Ответ: по модулю 32 сравнение имеет решения: 7, 15, 23, 31.

4) Тестом Соловея-Штрассена проверить на простоту число $N = 8651$.

Ответ: число составные $8651 = 41 \cdot 21$.

5) Найдите квадратный корень из 65 по модулю 67.

Ответ: 20 и 47.

Информация о разработчиках

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