

Документ подписан простой электронной подписью
 Информация о владельце:
 ФИО: ЧУМАЧЕНКО ТАТЬЯНА АЛЕКСАНДРОВНА
 Должность: РЕКТОР
 Дата подписания: 31.08.2022 11:48:32
 Уникальный программный ключ:
 9c9f7aaffa4840d284abe156657b8f85432bdb16




МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ
ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУнГГПУ»)

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
(ОЦЕНОЧНЫЕ СРЕДСТВА)



| | |
|------|----------------------------------|
| Шифр | Наименование дисциплины (модуля) |
| Б1.В | Компьютерная алгебра |

| | |
|---|---|
| Код направления подготовки | 09.03.02 |
| Направление подготовки | Информационные системы и технологии |
| Наименование (я) ОПОП (направленность / профиль) | Информационные технологии в образовании |
| Уровень образования | бакалавр |
| Форма обучения | очная |

Разработчики:

| Должность | Учёная степень, звание | Подпись | ФИО |
|-----------|--------------------------------------|--|------------------------------|
| Доцент | кандидат педагогических наук, доцент |  | Поднебесова Галина Борисовна |

Рабочая программа рассмотрена и одобрена (обновлена) на заседании кафедры (структурного подразделения)

| Кафедра | Заведующий кафедрой | Номер протокола | Дата протокола | Подпись |
|--|------------------------------|-----------------|----------------|---|
| Кафедра информатики, информационных технологий и методики обучения информатике | Рузаков Андрей Александрович | 10 | 13.06.2019 |  |
| Кафедра информатики, информационных технологий и методики обучения информатике | Рузаков Андрей Александрович | 1 | 10.09.2020 |  |
| | | | | |
| | | | | |

Раздел 1. Компетенции обучающегося, формируемые в результате освоения образовательной программы с указанием этапов их формирования

Таблица 1 - Перечень компетенций, с указанием образовательных результатов в процессе освоения дисциплины (в соответствии с РПД)

| Формируемые компетенции | | | |
|---|---|---|--|
| Индикаторы ее достижения | Планируемые образовательные результаты по дисциплине | | |
| | знать | уметь | владеть |
| ПК-1 способность проводить исследования на всех этапах жизненного цикла программных средств | | | |
| ПК.1.1 Знать современные методики проведения исследований на всех этапах жизненного цикла программных средств | 3.1 характеристику числовых систем; 3.2 определение основных понятий абстрактной и компьютерной алгебры; 3.3 способы кодирования информации; 3.4 алгоритмы компьютерной алгебры для анализа результатов профессиональных исследований. | | |
| ПК.1.2 Уметь проводить исследования на всех этапах жизненного цикла программных средств | | У.1 выполнять операции на множестве целых и комплексных чисел при разработке информационных систем; У.2 применять алгоритмы компьютерной алгебры для вычислений. | |
| ПК.1.3 Иметь навыки владения современным программным обеспечением для проведения исследований на всех этапах жизненного цикла программных средств | | | В.1 методами описания алгоритмов компьютерной алгебры для решения практических задач; В.2 основными алгоритмами компьютерной алгебры для программирования вычислительного блока систем. |

Компетенции связаны с дисциплинами и практиками через матрицу компетенций согласно таблице 2.

Таблица 2 - Компетенции, формируемые в результате обучения

| Код и наименование компетенции | |
|--|--|
| Составляющая учебного плана (дисциплины, практики, участвующие в формировании компетенции) | Вес дисциплины в формировании компетенции (100 / количество дисциплин, практик) |
| ПК-1 способность проводить исследования на всех этапах жизненного цикла программных средств | |
| Теория алгоритмов | 25,00 |
| Компьютерная алгебра | 25,00 |
| Проектирование информационных систем в образовании | 25,00 |
| Машинное обучение | 25,00 |

Таблица 3 - Этапы формирования компетенций в процессе освоения ОПОП

| Код компетенции | Этап базовой подготовки | Этап расширения и углубления подготовки | Этап профессионально-практической подготовки |
|------------------------|--------------------------------|--|---|
|------------------------|--------------------------------|--|---|

| | | | |
|------|--|-------------------|--|
| ПК-1 | Теория алгоритмов, Компьютерная алгебра, Проектирование информационных систем в образовании | Машинное обучение | |
|------|--|-------------------|--|

Раздел 2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Таблица 4 - Показатели оценивания компетенций на различных этапах их формирования в процессе освоения учебной дисциплины (в соответствии с РПД)

| № | Раздел | |
|---|---|------------------------------|
| Формируемые компетенции | | |
| Показатели сформированности (в терминах «знать», «уметь», «владеть») | | Виды оценочных средств |
| 1 | Аналитические вычисления на компьютере | |
| ПК-1 | | |
| Знать определение основных понятий абстрактной и компьютерной алгебры; | | Кейс-задачи |
| 2 | Кольцо целых чисел | |
| ПК-1 | | |
| Знать характеристику числовых систем; Знать способы кодирования информации; | | Отчет по лабораторной работе |
| Уметь выполнять операции на множестве целых и комплексных чисел при разработке информационных систем; | | Отчет по лабораторной работе |
| Владеть методами описания алгоритмов компьютерной алгебры для решения практических задач; | | Отчет по лабораторной работе |
| 3 | Полиномы от одной и нескольких переменных | |
| ПК-1 | | |
| Уметь применять алгоритмы компьютерной алгебры для вычислений. | | Тест |
| Владеть основными алгоритмами компьютерной алгебры для программирования вычислительного блока систем. | | Тест |
| 4 | Интегрирование и дифференцирование | |
| ПК-1 | | |
| Знать алгоритмы компьютерной алгебры для анализа результатов профессиональных исследований. | | Отчет по лабораторной работе |
| Уметь применять алгоритмы компьютерной алгебры для вычислений. | | Отчет по лабораторной работе |
| Владеть основными алгоритмами компьютерной алгебры для программирования вычислительного блока систем. | | Отчет по лабораторной работе |

Таблица 5 - Описание уровней и критериев оценивания компетенций, описание шкал оценивания

| Код | Содержание компетенции | | | |
|-----------------------------|---|---|---|---------------------------------|
| Уровни освоения компетенции | Содержательное описание уровня | Основные признаки выделения уровня (критерии оценки сформированности) | Пятибалльная шкала (академическая оценка) | % освоения (рейтинговая оценка) |
| ПК-1 | ПК-1 способность проводить исследования на всех этапах жизненного цикла программных средств | | | |

Раздел 3. Типовые контрольные задания и (или) иные материалы, необходимые для оценки планируемых результатов обучения по дисциплине (модулю)

1. Оценочные средства для текущего контроля

Раздел: Аналитические вычисления на компьютере

Задания для оценки знаний

1. Кейс-задачи:

Разработать кейс по одной из систем компьютерной математики.

Кейс должен включать:

1. Функциональное назначение;
2. Тип архитектуры;
3. Средства реализации;
4. Области применения;
5. Примеры (принтскрины);
6. Интегральные оценки качества.

Аналитик-С – среда аналитических вычислений

Официальный сайт проекта:

http://www.sgau.ru/analitik_c/

Основные характеристики:

Язык реализации – PHP

Платформа реализации – сервер Apache

Открытый исходный код

Синтаксис и функциональность языка Аналитик:

Поддержка символов латиницы, кириллицы и греческих

Двуязычность ключевых слов: пусть(let), вычислить(calculate) и т.п.

Базовые функции - комбинаторика, полиномы, матрицы, дифференциалы, интегралы, тригонометрия, графика)
+ специальные расширения (управление в технических системах).

Коллектив разработчиков: аспиранты и студенты СГТУ и СГАУ.

Задания для оценки умений

Задания для оценки владений

Раздел: Кольцо целых чисел

Задания для оценки знаний

1. Отчет по лабораторной работе:

Восстановить произведение двух целых чисел по их модулярным компонентам:

В 1. $n_1=3$ $n_2=7$ $n_3=13$ $n_4=17$,

$x_1=2$ $x_2=2$ $x_3=0$ $x_4=14$,

$x_1=0$ $x_2=1$ $x_3=10$ $x_4=2$.

В 2. $n_1=3$ $n_2=7$ $n_3=13$ $n_4=17$

$x_1=2$ $x_2=2$ $x_3=0$ $x_4=14$

$x_1=0$ $x_2=1$ $x_3=10$ $x_4=2$

В 3. $n_1=3$ $n_2=11$ $n_3=13$ $n_4=17$

$x_1=1$ $x_2=4$ $x_3=11$ $x_4=3$

$x_1=0$ $x_2=1$ $x_3=0$ $x_4=10$

В 4. $n_1=3$ $n_2=7$ $n_3=11$ $n_4=13$

$x_1=0$ $x_2=2$ $x_3=6$ $x_4=7$

$x_1=2$ $x_2=0$ $x_3=2$ $x_4=9$

В 5. $n_1=3$ $n_2=7$ $n_3=13$ $n_4=17$

$x_1=2$ $x_2=6$ $x_3=10$ $x_4=11$

$x_1=0$ $x_2=3$ $x_3=6$ $x_4=11$

- В 6. $n_1=3$ $n_2=7$ $n_3=13$ $n_4=17$
 $x_1=0$ $x_2=0$ $x_3=11$ $x_4=12$
 $x_1=0$ $x_2=0$ $x_3=3$ $x_4=8$
- В 7. $n_1=3$ $n_2=7$ $n_3=13$ $n_4=17$
 $x_1=0$ $x_2=0$ $x_3=6$ $x_4=16$
 $x_1=0$ $x_2=0$ $x_3=6$ $x_4=11$
- В 8. $n_1=3$ $n_2=7$ $n_3=13$ $n_4=17$
 $x_1=2$ $x_2=6$ $x_3=5$ $x_4=15$
 $x_1=1$ $x_2=3$ $x_3=0$ $x_4=1$
- В 9. $n_1=7$ $n_2=11$ $n_3=13$ $n_4=17$
 $x_1=2$ $x_2=6$ $x_3=7$ $x_4=4$
 $x_1=5$ $x_2=3$ $x_3=8$ $x_4=13$
- В 10. $n_1=3$ $n_2=7$ $n_3=11$ $n_4=13$
 $x_1=0$ $x_2=5$ $x_3=9$ $x_4=10$
 $x_1=0$ $x_2=1$ $x_3=3$ $x_4=10$
- В 11. $n_1=3$ $n_2=7$ $n_3=13$ $n_4=17$
 $x_1=2$ $x_2=0$ $x_3=12$ $x_4=9$
 $x_1=0$ $x_2=4$ $x_3=0$ $x_4=5$
- В 12. $n_1=3$ $n_2=7$ $n_3=13$ $n_4=17$
 $x_1=1$ $x_2=1$ $x_3=12$ $x_4=13$
 $x_1=2$ $x_2=0$ $x_3=9$ $x_4=1$

Задания для оценки умений

1. Отчет по лабораторной работе:

Восстановить произведение двух целых чисел по их модулярным компонентам:

- В 1. $n_1=3$ $n_2=7$ $n_3=13$ $n_4=17$,
 $x_1=2$ $x_2=2$ $x_3=0$ $x_4=14$,
 $x_1=0$ $x_2=1$ $x_3=10$ $x_4=2$.
- В 2. $n_1=3$ $n_2=7$ $n_3=13$ $n_4=17$
 $x_1=2$ $x_2=2$ $x_3=0$ $x_4=14$
 $x_1=0$ $x_2=1$ $x_3=10$ $x_4=2$
- В 3. $n_1=3$ $n_2=11$ $n_3=13$ $n_4=17$
 $x_1=1$ $x_2=4$ $x_3=11$ $x_4=3$
 $x_1=0$ $x_2=1$ $x_3=0$ $x_4=10$
- В 4. $n_1=3$ $n_2=7$ $n_3=11$ $n_4=13$
 $x_1=0$ $x_2=2$ $x_3=6$ $x_4=7$
 $x_1=2$ $x_2=0$ $x_3=2$ $x_4=9$
- В 5. $n_1=3$ $n_2=7$ $n_3=13$ $n_4=17$
 $x_1=2$ $x_2=6$ $x_3=10$ $x_4=11$
 $x_1=0$ $x_2=3$ $x_3=6$ $x_4=11$
- В 6. $n_1=3$ $n_2=7$ $n_3=13$ $n_4=17$
 $x_1=0$ $x_2=0$ $x_3=11$ $x_4=12$
 $x_1=0$ $x_2=0$ $x_3=3$ $x_4=8$
- В 7. $n_1=3$ $n_2=7$ $n_3=13$ $n_4=17$
 $x_1=0$ $x_2=0$ $x_3=6$ $x_4=16$
 $x_1=0$ $x_2=0$ $x_3=6$ $x_4=11$
- В 8. $n_1=3$ $n_2=7$ $n_3=13$ $n_4=17$
 $x_1=2$ $x_2=6$ $x_3=5$ $x_4=15$
 $x_1=1$ $x_2=3$ $x_3=0$ $x_4=1$
- В 9. $n_1=7$ $n_2=11$ $n_3=13$ $n_4=17$
 $x_1=2$ $x_2=6$ $x_3=7$ $x_4=4$
 $x_1=5$ $x_2=3$ $x_3=8$ $x_4=13$
- В 10. $n_1=3$ $n_2=7$ $n_3=11$ $n_4=13$
 $x_1=0$ $x_2=5$ $x_3=9$ $x_4=10$
 $x_1=0$ $x_2=1$ $x_3=3$ $x_4=10$
- В 11. $n_1=3$ $n_2=7$ $n_3=13$ $n_4=17$
 $x_1=2$ $x_2=0$ $x_3=12$ $x_4=9$
 $x_1=0$ $x_2=4$ $x_3=0$ $x_4=5$
- В 12. $n_1=3$ $n_2=7$ $n_3=13$ $n_4=17$
 $x_1=1$ $x_2=1$ $x_3=12$ $x_4=13$
 $x_1=2$ $x_2=0$ $x_3=9$ $x_4=1$

Задания для оценки владений

1. Отчет по лабораторной работе:

Восстановить произведение двух целых чисел по их модулярным компонентам:

В 1. $n_1=3$ $n_2=7$ $n_3=13$ $n_4=17$,

$x_1=2$ $x_2=2$ $x_3=0$ $x_4=14$,

$x_1=0$ $x_2=1$ $x_3=10$ $x_4=2$.

В 2. $n_1=3$ $n_2=7$ $n_3=13$ $n_4=17$

$x_1=2$ $x_2=2$ $x_3=0$ $x_4=14$

$x_1=0$ $x_2=1$ $x_3=10$ $x_4=2$

В 3. $n_1=3$ $n_2=11$ $n_3=13$ $n_4=17$

$x_1=1$ $x_2=4$ $x_3=11$ $x_4=3$

$x_1=0$ $x_2=1$ $x_3=0$ $x_4=10$

В 4. $n_1=3$ $n_2=7$ $n_3=11$ $n_4=13$

$x_1=0$ $x_2=2$ $x_3=6$ $x_4=7$

$x_1=2$ $x_2=0$ $x_3=2$ $x_4=9$

В 5. $n_1=3$ $n_2=7$ $n_3=13$ $n_4=17$

$x_1=2$ $x_2=6$ $x_3=10$ $x_4=11$

$x_1=0$ $x_2=3$ $x_3=6$ $x_4=11$

В 6. $n_1=3$ $n_2=7$ $n_3=13$ $n_4=17$

$x_1=0$ $x_2=0$ $x_3=11$ $x_4=12$

$x_1=0$ $x_2=0$ $x_3=3$ $x_4=8$

В 7. $n_1=3$ $n_2=7$ $n_3=13$ $n_4=17$

$x_1=0$ $x_2=0$ $x_3=6$ $x_4=16$

$x_1=0$ $x_2=0$ $x_3=6$ $x_4=11$

В 8. $n_1=3$ $n_2=7$ $n_3=13$ $n_4=17$

$x_1=2$ $x_2=6$ $x_3=5$ $x_4=15$

$x_1=1$ $x_2=3$ $x_3=0$ $x_4=1$

В 9. $n_1=7$ $n_2=11$ $n_3=13$ $n_4=17$

$x_1=2$ $x_2=6$ $x_3=7$ $x_4=4$

$x_1=5$ $x_2=3$ $x_3=8$ $x_4=13$

В 10. $n_1=3$ $n_2=7$ $n_3=11$ $n_4=13$

$x_1=0$ $x_2=5$ $x_3=9$ $x_4=10$

$x_1=0$ $x_2=1$ $x_3=3$ $x_4=10$

В 11. $n_1=3$ $n_2=7$ $n_3=13$ $n_4=17$

$x_1=2$ $x_2=0$ $x_3=12$ $x_4=9$

$x_1=0$ $x_2=4$ $x_3=0$ $x_4=5$

В 12. $n_1=3$ $n_2=7$ $n_3=13$ $n_4=17$

$x_1=1$ $x_2=1$ $x_3=12$ $x_4=13$

$x_1=2$ $x_2=0$ $x_3=9$ $x_4=1$

Раздел: Полиномы от одной и нескольких переменных

Задания для оценки знаний

Задания для оценки умений

1. Тест:

Задания для подготовки к тесту:

1. Неравенство Ландау-Миньотта позволяет:

- 1) оценить старшие коэффициенты полиномов;
- 2) найти границу для коэффициентов НОД двух полиномов;
- 3) определить количество итераций для вычисления НОД.

2. Алгоритмом Евклида используется для:

- 1) вычисления полинома;
- 2) разложения на множители;
- 3) нахождения НОД двух полиномов.

3. Если полином имеет положительную степень и обладает только тривиальными делителями, то он называется:

- 1) простым;
- 2) составным;
- 3) приводимым.

4. По формуле $pp(p)=p/\text{cont}(p)$ определяется

- 1) содержание полинома p ;
- 2) примитивная часть полинома p ;
- 3) НОД всех коэффициентов полинома p .

5. Произведение всех переменных двух полиномов p и q , каждая в степени, равная максимуму ее степеней в этих членах и коэффициентов этих членов – это:

- 1) редуцированный полином;
- 2) S -полином полиномов p и q ;
- 3) наименьшее общее кратное двух полиномов.

6. Алгоритм вычисления НОД двух полиномов от нескольких переменных опирается на:

- 1) лемму Гаусса;
- 2) теорему Дирихле;
- 3) теорему Ламе.

Приложение 1

1. Поставить в соответствие.

- 1) прямой метод;
- 2) метод Эрмита.
- a) представляет остающийся после вычисления интеграл в виде суммы логарифмов;
- b) использует разложение дроби q/r на простейшие дроби;
- c) позволяет определить рациональную часть интеграла рациональной функции без использования дополнительных величин.

2. Восстановить правильную последовательность в алгоритме вычисления НОД двух полиномов:

- 1) то $c := \text{модулярный_НОД}(a, b, p)$;
- 2) $p := \text{найти_большое_простое}(2 * m)$;
- 3) $m := \text{граница_Ландау_Миньотта}(a, b)$;
- 4) то выход c ;
- 5) цикл до бесконечности;
- 6) если $\text{степень_остатка}(p, a)$ или $\text{степень_остатка}(p, b)$;
- 7) если делит (c, a) и делит (c, b) ;
3. Для полинома $x^2 + 2xy + y^2 + x + y + 1$ выбрать рекурсивную форму записи:
- 1) $(x+y)^2 + (x+y) + 1$;
- 2) $(x^2 + 2xy + y^2) + x + y + 1$;
- 3) $x^2 + x(2y+1) + (y^2 + y + 1)$.

4. Переход от набора значений к его коэффициентам называется:

- 1) сверткой;
- 2) интерполяцией;
- 3) преобразованием Фурье.
5. Быстрый алгоритм интерполяции имеет сложность:
- 1) $O(n)$;
- 2) $O(n^2)$;
- 3) $O(n^3)$.

Задания для оценки владений

1. Тест:

Задания для подготовки к тесту:

1. Неравенство Ландау-Миньотта позволяет:
- 1) оценить старшие коэффициенты полиномов;
- 2) найти границу для коэффициентов НОД двух полиномов;
- 3) определить количество итераций для вычисления НОД.
2. Алгоритмом Евклида используется для:
- 1) вычисления полинома;
- 2) разложения на множители;
- 3) нахождения НОД двух полиномов.
3. Если полином имеет положительную степень и обладает только тривиальными делителями, то он называется:
- 1) простым;
- 2) составным;
- 3) приводимым.
4. По формуле $pp(p)=p/\text{cont}(p)$ определяется
- 1) содержание полинома p ;
- 2) примитивная часть полинома p ;

- 3) НОД всех коэффициентов полинома p .
5. Произведение всех переменных двух полиномов p и q , каждая в степени, равная максимуму ее степеней в этих членах и коэффициентов этих членов – это:
 - 1) редуцированный полином;
 - 2) S-полином полиномов p и q ;
 - 3) наименьшее общее кратное двух полиномов.
6. Алгоритм вычисления НОД двух полиномов от нескольких переменных опирается на:
 - 1) лемму Гаусса;
 - 2) теорему Дирихле;
 - 3) теорему Ламе.

Приложение 1

1. Поставить в соответствие.
 - 1) прямой метод;
 - 2) метод Эрмита.
 - а) представляет остающийся после вычисления интеграл в виде суммы логарифмов;
 - б) использует разложение дроби q/r на простейшие дроби;
 - с) позволяет определить рациональную часть интеграла рациональной функции без использования дополнительных величин.
2. Восстановить правильную последовательность в алгоритме вычисления НОД двух полиномов:
 - 1) то $c := \text{модулярный_НОД}(a, b, p)$;
 - 2) $p := \text{найти_большое_простое}(2^*m)$;
 - 3) $m := \text{граница_Ландау_Миньотта}(a, b)$;
 - 4) то выход c ;
 - 5) цикл до бесконечности;
 - 6) если $\text{степень_остатка}(p, a)$ или $\text{степень_остатка}(p, b)$;
 - 7) если делит (c, a) и делит (c, b) ;
3. Для полинома $x^2 + 2xy + y^2 + x + y + 1$ выбрать рекурсивную форму записи:
 - 1) $(x+y)^2 + (x+y) + 1$;
 - 2) $(x^2 + 2xy + y^2) + x + y + 1$;
 - 3) $x^2 + x(2y+1) + (y^2 + y + 1)$.
4. Переход от набора значений к его коэффициентам называется:
 - 1) сверткой;
 - 2) интерполяцией;
 - 3) преобразованием Фурье.
5. Быстрый алгоритм интерполяции имеет сложность:
 - 1) $O(n)$;
 - 2) $O(n^2)$;
 - 3) $O(n^3)$.

Раздел: Интегрирование и дифференцирование

Задания для оценки знаний

1. Отчет по лабораторной работе:

Зашифровать следующие аббревиатуры, используя систему RSA:

| | |
|----------------------|----------------------|
| Вариант 1 | Вариант 2 |
| ASD ($p=13, q=73$) | FOP ($p=17, q=61$) |
| Вариант 3 | Вариант 4 |
| TIR ($p=23, q=67$) | DGA ($p=13, q=71$) |
| Вариант 5 | Вариант 6 |
| PTE ($p=19, q=47$) | SPO ($p=11, q=71$) |
| Вариант 7 | Вариант 8 |
| KOL ($p=19, q=61$) | QFI ($p=23, q=89$) |
| Вариант 9 | Вариант 10 |
| GYZ ($p=7, q=47$) | PON ($p=19, q=53$) |
| Вариант 11 | Вариант 12 |
| RET ($p=17, q=59$) | RUS ($p=21, q=41$) |

Задания для оценки умений

1. Отчет по лабораторной работе:

Зашифровать следующие аббревиатуры, используя систему RSA:

| | |
|----------------------|----------------------|
| Вариант 1 | Вариант 2 |
| ASD ($p=13, q=73$) | FOP ($p=17, q=61$) |
| Вариант 3 | Вариант 4 |
| TIR ($p=23, q=67$) | DGA ($p=13, q=71$) |
| Вариант 5 | Вариант 6 |
| PTE ($p=19, q=47$) | SPO ($p=11, q=71$) |
| Вариант 7 | Вариант 8 |
| KOL ($p=19, q=61$) | QFI ($p=23, q=89$) |
| Вариант 9 | Вариант 10 |
| GYZ ($p=7, q=47$) | PON ($p=19, q=53$) |
| Вариант 11 | Вариант 12 |
| RET ($p=17, q=59$) | RUS ($p=21, q=41$) |

Задания для оценки владений

1. Отчет по лабораторной работе:

Зашифровать следующие аббревиатуры, используя систему RSA:

| | |
|----------------------|----------------------|
| Вариант 1 | Вариант 2 |
| ASD ($p=13, q=73$) | FOP ($p=17, q=61$) |
| Вариант 3 | Вариант 4 |
| TIR ($p=23, q=67$) | DGA ($p=13, q=71$) |
| Вариант 5 | Вариант 6 |
| PTE ($p=19, q=47$) | SPO ($p=11, q=71$) |
| Вариант 7 | Вариант 8 |
| KOL ($p=19, q=61$) | QFI ($p=23, q=89$) |
| Вариант 9 | Вариант 10 |
| GYZ ($p=7, q=47$) | PON ($p=19, q=53$) |
| Вариант 11 | Вариант 12 |
| RET ($p=17, q=59$) | RUS ($p=21, q=41$) |

2. Оценочные средства для промежуточной аттестации

1. Экзамен

Вопросы к экзамену:

1. Арифметические вычисления и операции.
2. Представление целых чисел в компьютере.
3. Умножение длинных целых чисел. Длинная арифметика.
4. Представление математических объектов в системах компьютерной математики.
5. Представление полиномов.
6. Представление рациональных, алгебраических и трансцендентных чисел.
7. Система компьютерной алгебры Mathematica.
8. Развитие систем компьютерной алгебры.
9. Алгебры. Основные алгебраические структуры.
10. Элементы теории делимости в кольце целых чисел.
11. Основная теорема арифметики. Теорема Ламе.
12. Теорема Евклида. Алгоритм Евклида.
13. Позиционные системы счисления.
14. Элементы теории сравнений в кольце целых чисел.
15. Расширенный алгоритм Евклида.
16. Функция Эйлера. Теоремы Эйлера и Ферма.
17. Китайская теорема об остатках (для двух и более элементов).
18. Модулярная арифметика.
19. Сравнение двух целых чисел по их модулярным компонентам.
20. Кольцо полиномов от одной переменной.
21. Полиномы над полем.
22. Вычисление полиномов.
23. Обобщенная схема Горнера.
24. Китайская теорема об остатках для полиномов.

25. Нахождение НОД полиномов от одной переменной.
26. Неравенство Ландау-Миньотта. Следствие.
27. Алгоритм вычисления НОД полиномов.
28. Анализ Фурье. Методы анализа Фурье.
29. Быстрое преобразование Фурье.
30. Применение преобразования Фурье.
31. Кольцо полиномов от нескольких переменных.
32. Упрощение полиномиальных уравнений.
33. Системы записи полиномов.
34. Вычисление НОД от нескольких переменных.
35. Задача интегрирования. Интегрирование рациональных функций.
36. Дифференцирование. Алгоритмы. Примеры.
37. Кодирование информации.
38. Криптография. Системы с открытым ключом.
39. Криптография. Системы с закрытым ключом.
40. Криптосистема RSA.

Раздел 4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

1. Для текущего контроля используются следующие оценочные средства:

1. Кейс-задачи

Кейс – это описание конкретной ситуации, отражающей какую-либо практическую проблему, анализ и поиск решения которой позволяет развивать у обучающихся самостоятельность мышления, способность выслушивать и учитывать альтернативную точку зрения, а также аргументировано отстаивать собственную позицию.

Рекомендации по работе с кейсом:

1. Сначала необходимо прочитать всю имеющуюся информацию, чтобы составить целостное представление о ситуации; не следует сразу анализировать эту информацию, желательно лишь выделить в ней данные, показавшиеся важными.
2. Требуется охарактеризовать ситуацию, определить ее сущность и отметить второстепенные элементы, а также сформулировать основную проблему и проблемы, ей подчиненные. Важно оценить все факты, касающиеся основной проблемы (не все факты, изложенные в ситуации, могут быть прямо связаны с ней), и попытаться установить взаимосвязь между приведенными данными.
3. Следует сформулировать критерий для проверки правильности предложенного решения, попытаться найти альтернативные способы решения, если такие существуют, и определить вариант, наиболее удовлетворяющий выбранному критерию.
4. В заключении необходимо разработать перечень практических мероприятий по реализации предложенного решения.
5. Для презентации решения кейса необходимо визуализировать решение (в виде электронной презентации, изображения на доске и пр.), а также оформить письменный отчет по кейсу.

2. Отчет по лабораторной работе

При составлении и оформлении отчета следует придерживаться рекомендаций, представленных в методических указаниях по выполнению лабораторных работ по дисциплине.

3. Тест

Тест это система стандартизированных вопросов (заданий), позволяющих автоматизировать процедуру измерения уровня знаний и умений обучающихся. Тесты могут быть аудиторными и внеаудиторными. Преподаватель доводит до сведения студентов информацию о проведении теста, его форме, а также о разделе (теме) дисциплины, выносимой на тестирование.

При самостоятельной подготовке к тестированию студенту необходимо:

- проработать информационный материал по дисциплине. Проконсультироваться с преподавателем по вопросу выбора учебной литературы;
- выяснить все условия тестирования заранее. Необходимо знать, сколько тестов вам будет предложено, сколько времени отводится на тестирование, какова система оценки результатов и т.д.
- работая с тестами, внимательно и до конца прочесть вопрос и предлагаемые варианты ответов; выбрать правильные (их может быть несколько); на отдельном листке ответов выписать цифру вопроса и буквы, соответствующие правильным ответам. В случае компьютерного тестирования указать ответ в соответствующем поле (полях);
- в процессе решения желательно применять несколько подходов в решении задания. Это позволяет максимально гибко оперировать методами решения, находя каждый раз оптимальный вариант.
- решить в первую очередь задания, не вызывающие трудностей, к трудному вопросу вернуться в конце.
- оставить время для проверки ответов, чтобы избежать механических ошибок.

2. Описание процедуры промежуточной аттестации

Оценка за зачет/экзамен может быть выставлена по результатам текущего рейтинга. Текущий рейтинг – это результаты выполнения практических работ в ходе обучения, контрольных работ, выполнения заданий к лекциям (при наличии) и др. видов заданий.

Результаты текущего рейтинга доводятся до студентов до начала экзаменационной сессии.

Экзамен преследует цель оценить работу обучающегося за определенный курс: полученные теоретические знания, их прочность, развитие логического и творческого мышления, приобретение навыков самостоятельной работы, умения анализировать и синтезировать полученные знания и применять их для решения практических задач.

Экзамен проводится в устной или письменной форме по билетам, утвержденным заведующим кафедрой (или в форме компьютерного тестирования). Экзаменационный билет включает в себя два вопроса и задачи. Формулировка вопросов совпадает с формулировкой перечня вопросов, доведенного до сведения обучающихся не позднее чем за один месяц до экзаменационной сессии.

В процессе подготовки к экзамену организована предэкзаменационная консультация для всех учебных групп.

При любой форме проведения экзаменов по билетам экзаменатору предоставляется право задавать студентам дополнительные вопросы, задачи и примеры по программе данной дисциплины. Дополнительные вопросы также, как и основные вопросы билета, требуют развернутого ответа.