



1920

Кафедра функционального анализа и алгебры

Магистратура: 2 курс

Билет № 1

Дополнительные главы фундаментальной математики

1. Решение систем линейных уравнений над полем. Алгоритм Гаусса.
2. Основные алгебраические конструкции пакета Nemo языка программирования Julia.
3. Найти группу обратимых элементы кольца \mathbb{Z}_{16}

Заведующий кафедрой



1920

Кафедра функционального анализа и алгебры

Магистратура: 2 курс

Билет № 2

Дополнительные главы фундаментальной математики

1. Второе раундовое преобразование шифра AES. Нахождение жордановой формы матрицы линейного преобразования.
2. Линейные отображения векторных пространств. Матричная запись
3. В кольце \mathbb{Z}_{16} решить уравнение $4x = 2$.

Заведующий кафедрой



1920

Кафедра функционального анализа и алгебры

Магистратура: 2 курс

Билет № 3

Дополнительные главы фундаментальной математики

1. Собственные и корневые вектора. Определение и свойства.
2. Симметрический многочлен. Основная теорема о симметрических многочленах. Симметрический многочлен однозначно выражается через элементарные симметрические многочлены.
3. Найти примитивный элемент поля \mathbb{Z}_{13} .

Заведующий кафедрой



1920

Кафедра функционального анализа и алгебры

Магистратура: 2 курс

Билет № 4

Дополнительные главы фундаментальной математики

1. Многочлен как функция – интерполяционная формула Лагранжа.
2. Алгоритм нахождения собственных векторов: вычисление определителя, задающего характеристический многочлен; для каждого корня нахождение собственных векторов

3. Над полем \mathbb{Z}_5 решить систему
$$\begin{cases} 2x - 3y + 3z = 3 \\ x + y - z = 3 \\ 3x + 2y + 4z = 3 \end{cases}$$

Заведующий кафедрой



1920

Кафедра функционального анализа и алгебры

Магистратура: 2 курс

Билет № 5

Дополнительные главы фундаментальной математики

1. Китайская теорема об остатках.
2. Алгоритм нахождения жордановой формы над полем комплексных чисел и над полем разложения характеристического многочлена в случае полей Галуа.

3. Решить систему
$$\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 5 \pmod{7} \\ x \equiv 7 \pmod{9} \end{cases}$$

Заведующий кафедрой



1920

Кафедра функционального анализа и алгебры

Магистратура: 2 курс

Билет № 6

Дополнительные главы фундаментальной математики

1. Алгоритм решение систем линейных уравнений над кольцом целых чисел.
2. Алгоритм нахождения обратных элементов в поле Галуа.
3. Методом Евклида решить уравнение $7x \equiv 8 \pmod{123}$.

Заведующий кафедрой



1920

Кафедра функционального анализа и алгебры

Магистратура: 2 курс

Билет № 7

Дополнительные главы фундаментальной математики

1. Алгоритм быстрого возведения в степень.
2. Определение и примеры евклидовых колец: кольцо целых чисел и кольцо многочленов над полем $P[x]$.
3. Разложить в сумму простейших дробей $\frac{8}{35}$.

Заведующий кафедрой



1920

Кафедра функционального анализа и алгебры

Магистратура: 2 курс

Билет № 8

Дополнительные главы фундаментальной математики

1. Существование НОД и НОК в евклидовых кольцах.
2. Описание алгоритма AES и его анализ.
3. Разложить в сумму простейших в кольце $\mathbb{R}[x]$ дробь $\frac{2x+4}{x^3-1}$.

Заведующий кафедрой



1920

Кафедра функционального анализа и алгебры

Магистратура: 2 курс

Билет № 9

Дополнительные главы фундаментальной математики

1. Описание алгоритма RSA и его анализ.
2. Алгоритм Евклида деления с остатком. Нахождение НОД, как последнего ненулевого остатка.
3. Существует ли дифференцирование в кольце $\mathbb{Z}_{12}[x]$, такое, что $d(2x^3) = 6x^4$.

Заведующий кафедрой



1920

Кафедра функционального анализа и алгебры

Магистратура: 2 курс

Билет № 10

Дополнительные главы фундаментальной математики

1. Решение систем линейных уравнений по разным модулям.
2. Следствие из алгоритма Евклида, нахождение обратного элемента по модулю натурального числа.
3. Найти $\text{НОД}(1234, 2345)$.

Заведующий кафедрой



1920

Кафедра функционального анализа и алгебры

Магистратура: 2 курс

Билет № 11

Дополнительные главы фундаментальной математики

1. Кольцо вычетов по модулю n . Решение линейных уравнений в кольце Z_n .
2. Квадратичный закон взаимности – формулировка и примеры применения
3. Найти $\text{НОД}(x^4 + x^3 - 3x^2 - 4x - 1, x^3 + x^2 - x - 1)$ над $\mathbb{R}[x]$

Заведующий кафедрой



1920

Кафедра функционального анализа и алгебры

Магистратура: 2 курс

Билет № 12

Дополнительные главы фундаментальной математики

1. Линейные регистры сдвига с обратной связью.
2. Кольцо вычетов по простому модулю. Проверка, что $Z_p \cong GF(p)$ - поле, простое поле Галуа.
3. Используя производную найти кратные множители многочлена $x^6 - 6x^4 - 4x^3 + 9x^2 + 12x + 4$ над \mathbb{R} .

Заведующий кафедрой



1920

Кафедра функционального анализа и алгебры

Магистратура: 2 курс

Билет № 13

Дополнительные главы фундаментальной математики

1. Линейные регистры сдвига – характеристический многочлен. Явная формула для n -го члена регистра, выраженная через корни характеристического многочлена.
2. Расширение полей Галуа. Расширение, как поле разложения неприводимого многочлена.
3. Найти все неприводимые многочлены третьей степени в кольце $\mathbb{Z}_2[x]$.

Заведующий кафедрой



1920

Кафедра функционального анализа и алгебры

Магистратура: 2 курс

Билет № 14

Дополнительные главы фундаментальной математики

1. Башня расширений полей Галуа.
2. Линейные регистры сдвига – матричная запись. Импульсная функция.
3. Построить поле разложения многочлена $x^2 + x + 1 \in \mathbb{Z}_2[x]$.

Заведующий кафедрой



1920

Кафедра функционального анализа и алгебры

Магистратура: 2 курс

Билет № 15

Дополнительные главы фундаментальной математики

1. Линейные регистры сдвига с обратной связью над полями Галуа. Определение и оценка минимального периода.
2. След и норма элементов в поле Галуа.
3. Является ли отображение линейным $(x_1, x_2, x_3) \rightarrow (x_1 + 2, x_2 + 1, x_3 + 3)$, если да, то найти его матрицу в стандартном базисе, над полем $\text{GF}(5)$

Заведующий кафедрой



1920

Кафедра функционального анализа и алгебры

Магистратура: 2 курс

Билет № 16

Дополнительные главы фундаментальной математики

1. Связь корней неприводимого многочлена степени n над полем Галуа характеристики p :

$$\alpha_1 = \alpha; \alpha_2 = \alpha^p; \dots; \alpha_n = \alpha^{p^{n-1}}.$$

2. Операция сложения на эллиптической кривой над полем Галуа.

3. Найти все неприводимые многочлены второй степени в кольце $\mathbb{Z}_3[x]$.

Заведующий кафедрой



1920

Кафедра функционального анализа и алгебры

Магистратура: 2 курс

Билет № 17

Дополнительные главы фундаментальной математики

1. Подсчет числа точек эллиптической кривой над полем Галуа.

2. Логарифм Якоби в поле Галуа и его нахождение.

3. Построить поле разложения многочлена $x^2 + x + 2 \in \mathbb{Z}_3[x]$.

Заведующий кафедрой



1920

Кафедра функционального анализа и алгебры

Магистратура: 2 курс

Билет № 18

Дополнительные главы фундаментальной математики

1. Алгоритм нахождения примитивного элемента и логарифма Галуа.

2. Эллиптическая кривая над полем Галуа. Приведение к каноническому виду.

3. Является ли отображение линейным $(x_1, x_2, x_3) \rightarrow (x_1 + 1, x_2 + 2, 2x_3)$, если да, то найти его матрицу в стандартном базисе над полем $\text{GF}(7)$.

Заведующий кафедрой
