

МИНОБРНАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ

Директор института прикладной
математики и компьютерных наук


А.В. Замятин

« 02 » июля 2021 г.

Фонд оценочных средств по дисциплине

Теория чисел

Специальность

10.05.01 Компьютерная безопасность

код и наименование специальности

Анализ безопасности компьютерных систем

наименование специализации

ФОС составил(и):

канд. физ.-мат. наук, доцент
доцент кафедры компьютерной безопасности



М.А. Приходовский

Рецензент:

канд. тех. наук, доцент
заведующий кафедрой компьютерной безопасности



С.А. Останин

Фонд оценочных средств одобрен на заседании учебно-методической комиссии
института прикладной математики и компьютерных наук (УМК ИПМКН)

Протокол от 17 июня 2021 г. № 05

Председатель УМК ИПМКН,
д-р техн. наук, профессор



С.П. Сущенко

Фонд оценочных средств (ФОС) является элементом системы оценивания сформированности компетенций у обучающихся в целом или на определенном этапе ее формирования.

ФОС разрабатывается в соответствии с рабочей программой (РП) дисциплины и включает в себя набор оценочных материалов для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине.

1. Компетенции и результаты обучения, формируемые в результате освоения дисциплины

Компетенция	Индикатор компетенции	Код и наименование результатов обучения (планируемые результаты обучения, характеризующие этапы формирования компетенций)	Критерии оценивания результатов обучения			
			Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
ОПК-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	ИОПК-3.1 Демонстрирует навыки выполнения стандартных действий, решения типовых задач, формулируемых в рамках базовых математических дисциплин; ИОПК-3.2 Осуществляет применение основных понятий, фактов, концепций, принципов математики и информатики для решения задач профессиональной деятельности; ИОПК-3.3 Выявляет научную сущность проблем, возникающих в ходе профессиональной деятельности, и применяет соответствующий	ОР-1.1.1. <i>Обучающийся сможет:</i> Знать: базовые понятия, идеи и методы теории чисел и их место, и роль в математическом знании Уметь: выбирать оптимальную методику и подбирать алгебраический аппарат для решения задач профессиональной деятельности, излагать содержание математической теории с необходимым уровнем строгости и доступности, основываясь на теоретических принципах и методов теории чисел. Владеть: алгебраическими методами и возможностью эффективно использовать фундаментальные знания в	Знать идеи и приемы доказательств теорем теории чисел; методы решения задач, сформулированных в теоретико-числовой терминологии Уметь формулировать и доказывать известные теоремы теории чисел, формулировать следствия теорем для отдельных случаев их применения, уметь обосновывать ход решения задач	Знать: базовые понятия, идеи и методы теории чисел и их место, и роль в математическом знании Уметь: выбирать оптимальную методику и подбирать алгебраический аппарат для решения задач профессиональной деятельности, излагать содержание математической теории с необходимым уровнем строгости	Знать терминологию и формулировки теорем теории чисел Уметь формулировать постановку задачи в терминах теории чисел, подбирать метод решения Владеть способностью к определению общих форм и закономерностей теории и методов теории чисел.	Не знать терминологию теории чисел Не уметь решать задачи Не владеть навыками решения задач

	<p>математический аппарат для их формализации, анализа и выработки решения.</p>	<p><i>области теории чисел в будущей профессиональной деятельности</i></p>	<p>теоретическими фактами Владеть способностью строго доказывать формулировать теоретико-числовые результаты, видеть следствия полученных результатов, применять их при решении математических задач</p>	<p>и доступности, основываясь на теоретических принципах и методов теории чисел. Владеть: алгебраическими методами и возможностью использовать фундаментальные знания в области теории чисел в будущей профессиональной деятельности</p>		
--	---	--	---	---	--	--

2. Этапы формирования компетенций и виды оценочных средств

№	Этапы формирования компетенций (разделы дисциплины)	Код и наименование результатов обучения	Вид оценочного средства (тесты, задания, кейсы, вопросы и др.)
1.	<i>Делимость и простые числа. Теорема о делении с остатком. НОД чисел. Алгоритм Евклида. Простые числа. Основная теорема арифметики.</i>	ОР-1.1.1.	Контрольные задания, тесты, экзамен
2.	<i>Арифметические функции. Мультипликативные функции и их примеры.</i>	ОР-1.1.1.	Контрольные задания, тесты, экзамен
3.	<i>Цепные дроби.</i>	ОР-1.1.1.	Контрольные задания, тесты, экзамен
4.	<i>Сравнения 1-й степени</i>	ОР-1.1.1.	Контрольные задания, тесты, экзамен
5.	<i>Сравнения n-степени.</i>	ОР-1.1.1.	Контрольные задания, тесты, экзамен
6.	<i>Сравнения 2-степени</i>	ОР-1.1.1.	Контрольные задания, тесты, экзамен
7.	<i>Первообразные корни и индексы.</i>	ОР-1.1.1.	Контрольные задания, тесты, экзамен

3. Типовые контрольные задания или иные материалы, необходимые для оценки образовательных результатов обучения

3.1. Типовые задания для проведения текущего контроля успеваемости по дисциплине

Вариант 1

1. Методом решета все простые числа между 118 и 131.
2. При каких натуральных n числа n , $n + 13$, $n + 17$ являются простыми?
3. Пусть $a = 248$, $b = 182$. При помощи расширенного алгоритма Евклида найти их НОД.
4. Найдите сумму и число всех натуральных делителей следующих чисел:
1) 165; 2) 270; 3) 363.

Вариант 2

1. Методом решета все простые числа между 870 и 900.
2. Сколько натуральных чисел ≤ 210 , не делящихся ни на 3, ни на 5?
3. Пусть $a = 138$, $b = 162$. При помощи расширенного алгоритма Евклида найти их НОД.
4. Найдите каноническое разложение числа $30!$

Вариант 3

1. Методом решета все простые числа между 110 и 130.
2. При каких натуральных n числа n , $n + 5$, $n + 9$, $n + 19$ являются простыми?
3. Разложите в непрерывную дробь: $-15/57$ и $-\sqrt{15}$.
4. Вычислить символы Лежандра: $(18/29)$ и $(13/41)$.

Вариант 4

1. Решите уравнение $\varphi(2x) = x/2$.
2. Пусть $a = 108$, $b = 112$. При помощи расширенного алгоритма Евклида найти их НОД.
3. Вычислить символы Лежандра: $(13/19)$ и $(17/31)$.
4. Является ли 5 первообразным корнем по модулю 31?

Вариант 5

1. Решите уравнение $\varphi(3x) = x/3$.
2. Пусть $a = 106$, $b = 118$. При помощи расширенного алгоритма Евклида найти их НОД.
3. Вычислить символы Лежандра: $(12/19)$ и $(15/37)$.
4. Является ли 7 первообразным корнем по модулю 19?

Вариант 6

1. Найдите все классы квадратичных вычетов по модулям 11.
2. Решите сравнение $5x = 9 \pmod{17}$.
3. Найдите остатки от деления 528^{180} на 43.
4. Найдите остаток от деления $2021^7 - 7$ на 11.

Вариант 7

1. Решите сравнение $1287x = 447 \pmod{516}$.
2. Найти последнюю цифру 17^{2132} .
3. Найдите корни многочлена $2x^3 + 5x^2 + 7x + 21 = 0 \pmod{131}$.
4. Вычислить символ Якоби $(219/323)$.

Вариант 8

1. Решите сравнение $12x = 6 \pmod{18}$.
2. Является ли 7 первообразным корнем по модулю 53?

3. Найдите сумму и число всех натуральных делителей 1244.

4. Вычислить символ Лежандр $(15/131)$.

Вариант 9

1. Решите сравнение $111x = 75 \pmod{321}$.

2. Является ли 11 первообразным корнем по модулю 47?

3. Вычислить символ Лежандра $(21/101)$.

4. Разложите в непрерывную дробь: -8.91 и $312/456$.

Вариант 10

1. Решите сравнение $27x = 611 \pmod{1021}$.

2. Является ли 11 первообразным корнем по модулю 94?

3. Вычислить символ Лежандра $(27/131)$.

4. Разложите в непрерывную дробь $-\sqrt{17}$.

Ответы

Вариант 1. 1. 127 и 131. 2. Таких чисел нет. 3. НОД = 2. 4. 1) Сумма и число всех натуральных делителей у 165 соответственно равны 288 и 8. 2) Сумма и число всех натуральных делителей у 270 соответственно равны 720 и 16. 3) Сумма и число всех натуральных делителей у 363 соответственно равны 532 и 6.

Вариант 2. 1. 877 и 879. 2. 112. 3. 6. 4. $30! = 2^{26} \cdot 3^{14} \cdot 5^7 \cdot 7^4 \cdot 11^2 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23 \cdot 29$.

Вариант 3. 1. 113 и 127. 2. Нет таких чисел. 3. $[-1, 2, 2, 1, 4]$ и $[-4, 7, (1, 6)]$.

Вариант 4. 1. Нет решений. 2. 4. 3. $(13/19) = -1$ и $(17/31) = -1$. 4. Нет.

Вариант 5. 1. Нет решений. 2. 2. 3. $(12/19) = -1$ и $(15/37) = -1$. 4. Нет.

Вариант 6. 1. 1, 3, 4, 5, 9 mod 11. 2. $x = 12 \pmod{17}$. 3. Остаток равен 11. 4. Остаток равен 6.

Вариант 7. 1. $x = 109; 281; 453 \pmod{516}$. 2. 1. 3. $x = 117 \pmod{131}$. 4. 1.

Вариант 8. 1. $x = 2; 5; 8; 11; 14; 17 \pmod{18}$. 2. Нет. 3. Сумма и число всех натуральных делителей у 1244 соответственно равны 2184 и 6. 4. $(15/131) = 1$.

Вариант 9. 1. $x = 99; 206; 313 \pmod{321}$. 2. Да. 3. $(21/101) = 1$. 4. $-8.91 = [-9; 11, 9]$ и $312/456 = [0; 1, 2, 6]$.

Вариант 10. 1. $x = 968 \pmod{1021}$. 2. Да. 3. $(27/131) = 1$. 4. $-\sqrt{17} = [-5; 1, 7, (8)]$.

3.2. Типовые задания для проведения промежуточной аттестации по дисциплине

- 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) Мультипликативность функции $\sigma(n)$. Доказать, что если $n = p^\alpha \dots q^\gamma$ – каноническое разложение числа n , то $\sigma(n) = [(p^\alpha - 1) \dots (q^\gamma - 1)] / [(p - 1) \dots (q - 1)]$.
- 3) Примеры совершенных чисел. Доказать, что четное число n является совершенным тогда и только тогда, когда $n = 2^{a-1}(2^a - 1)$, где $a \geq 2$ и $2^a - 1$ – простое число.
- 4) Доказать, что если $2^a - 1$ – простое число, то число a также простое.
- 5) Докажите мультипликативность функции Мебиуса $\mu(n)$.
- 6) Докажите формулу для функции Эйлера $\varphi(n)$.
- 7) Докажите теорему о разрешимости в \mathbb{Z} уравнения $ax + by = c$, где a, b, c – целые числа и $ab \neq 0$.
- 8) Докажите, что если $[a_0, \dots, a_n]$ – цепная дробь, то для каждого $k \leq n$ справедливо равенство $P_k Q_{k-1} - Q_k P_{k-1} = (-1)^{k-1}$, где $P_0 = a_0, P_1 = a_0 a_1 + 1, \dots$, а $P_k = P_{k-1} a_k + P_{k-2}, Q_k = Q_{k-1} a_k + Q_{k-2}$ при $2 \leq k \leq n$.
- 9) Докажите китайскую теорему об остатках.
- 10) Докажите мультипликативность функции Эйлера $\varphi(n)$.
- 11) Докажите, что:
если a – квадратичный вычет по модулю p , то $a^{(p-1)/2} \equiv 1 \pmod{p}$;
если a – квадратичный невычет по модулю p , то $a^{(p-1)/2} \equiv -1 \pmod{p}$
- 12) Докажите, что число 3 является первообразным корнем по модулю 7, а по модулю 8 первообразных корней нет.
- 13) Докажите, что если число Мерсенна $2^n - 1$ является простым, то и число n также простое.
- 14) Докажите, что если a, b – взаимно простые натуральные числа и $ab = c^n$, где $n \geq 2$, $c \in \mathbb{Z}$, то $a = x^n, b = y^n$ для некоторых целых чисел x, y .
- 15) Приведите, по крайней мере, два различных доказательства теоремы Евклида о бесконечности множества простых чисел.
- 16) Докажите, что $\sum \mu(d) = 1$, если $n = 1$ и $\sum \mu(d) = 0$, если $n > 1$, где d пробегает все натуральные делители числа n .
- 17) Докажите, что для всякого натурального числа справедлива формула $n = \sum \varphi(d)$, где d пробегает все натуральные делители числа n .
- 18) Докажите, что если $x > 0$ – действительное число, то число всех целых чисел в интервале $[1, x]$, делящихся на d , равно целой части числа x/d .
- 19) Используя теорему Чебышева, докажите, что если $n \geq 2$, то $p_n + p_{n+1} > p_{n+2}$, где p_n – n -ое простое число.

- 20) Пусть p, q – различные простые числа и e, f – такие целые числа, что $ef \equiv 1 \pmod{\varphi(pq)}$. Докажите, что $a^{ef} \equiv a \pmod{pq}$ для любого целого числа a .
- 21) Докажите, что для любого нечетного числа $n \geq 1$ число $2^{n!} - 1$ делится на n .
- 22) Методом Б. Паскаля выведите признак делимости на 3.
- 23) Докажите, что 561 является числом Р. Кармайкла (R. Carmichael).
- 24) Докажите, что если δ – показатель числа a по модулю n , то число δ делит $\varphi(n)$.
- 25) Докажите теорему Вильсона: если p – простое число, то $(p - 1)! + 1 \equiv 0 \pmod{p}$.
- 26) Докажите, что не существует натурального числа n такого, что число $1 + 2 + \dots + n$ оканчивается цифрой 7.
- 27) Докажите, что парабола $5x^2 - 11y = 7$ не содержит точек с целыми координатами.
- 28) Пусть p – нечетное простое число. Докажите, что сравнение $x^2 \equiv -1 \pmod{p}$ разрешимо тогда и только тогда, когда $p \equiv 1 \pmod{4}$.

4. Методические материалы, определяющие процедуры оценивания образовательных результатов обучения

4.1. Методические материалы для оценки текущего контроля успеваемости по дисциплине.

Порядок формирования оценки при использовании балльно-рейтинговой системы; критерии оценивания теоретических вопросов и практических заданий;

- 1) Полный ответ, изложенный кратко и ясно – «отлично».
- 2) Ответ неполный (но $> 80\%$), пояснения логически непротиворечивы – «хорошо».
- 3) Ответ неполный (но $> 50\%$), есть проблемы в логике и пояснениях – «удовлетворительно».
- 4) Ответ неполный ($< 50\%$), отсутствие логики в пояснениях – «неудовлетворительно».

4.2. Методические материалы для проведения промежуточной аттестации по дисциплине.

- 1) Полный ответ, изложенный кратко и ясно – «отлично».
- 2) Ответ неполный (но $> 80\%$), пояснения логически непротиворечивы – «хорошо».
- 3) Ответ неполный (но $> 50\%$), есть проблемы в логике и пояснениях – «удовлетворительно».
- 4) Ответ неполный ($< 50\%$), отсутствие логики в пояснениях – «неудовлетворительно».