Приложение к рабочей программе дисциплины

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Наименование дисциплины	Теоретико-числовые функции
Направление подготовки / Специальность	01.03.01 Математика
Направленность (профиль) /Специализация	Вещественный, комплексный и функциональный анализ
Форма обучения	очная
Разработчик	Девятков А. П., доцент кафедры фундаментальной математики и механики

1. Темы дисциплины для самостоятельного освоения обучающимися
   Отсутствуют.
2. План самостоятельной работы

№ п/п	Учебные встречи	Виды самостоятельной работы	Форма отчетности / контроля	Количество баллов	Рекомендуемый бюджет времени на выполнение (ак.ч.)
1	2	3	4	5	6
1	Теория делимости	Изучение лекционного материала	Решение задач по теме лекции, выполнение контрольной работы	0	2
2	Теория делимости	Решение задач по теме лекции	Защита решения перед преподавателем	5	6
3	Арифметические функции	Изучение лекционного материала	Решение задач по теме лекции, выполнение контрольной работы	0	4
	Арифметические функции	Решение задач по теме лекции	Защита решения перед преподавателем	5	6
4	Мультипликативные функции	Решение задач по теме лекции	Защита решения перед преподавателем	5	6
5	Умножение Дирихле	Решение задач по теме лекции	Защита решения перед преподавателем	5	6
6	Теория сравнений	Изучение лекционного материала	Решение задач по теме лекции, выполнение контрольной работы	0	4
7	Теория сравнений	Решение задач по теме лекции	Защита решения перед преподавателем	5	8
8	Теория сравнений	Подготовка к контрольной работе	Решение демоверсии контрольной работы	0	6
9	Элементы теории групп	Изучение лекционного материала	Решение задач по теме лекции, выполнение контрольной работы	0	2
10	Элементы теории групп	Решение задач по теме лекции	Защита решения перед преподавателем	5	6
11	Конечные абелевы группы и их характеры	Изучение лекционного материала	Решение задач по теме лекции, выполнение контрольной работы	0	2
12	Конечные абелевы группы и их характеры	Решение задач по теме лекции	Защита решения перед преподавателем	5	6
13	Первообразные корни и индексы	Изучение лекционного	Решение задач по теме лекции,	0	2

		материала	выполнение контрольной работы		
14	Первообразные корни и индексы	Решение задач по теме лекции	Защита решения перед преподавателем	5	6
15	Первообразные корни и индексы	Подготовка к контрольной работе	Решение демоверсии контрольной работы	0	6
16	Квадратичный закон взаимности	Изучение лекционного материала	Решение задач по теме лекции, выполнение контрольной работы	0	2
17	Подготовка к дифференцированному зачету	Повторение лекционного материала и решение задач с практических занятий	Дифференцированный зачет	0	6
18			Итого	40	86

3. Требования и рекомендации по выполнению самостоятельных работ обучающихся, критерии оценивания.

Изучение лекционного материала

Рекомендации по выполнению.

Помимо записей лекций, рекомендуется обратиться к следующим учебникам:

1) Виноградов И. М. Основы теории чисел. М.: Наука, 1972.
2) Бухштаб А. А. Теория чисел. М.: Просвещение, 1966.
3) Чандрасекхаран К. Введение в аналитическую теорию чисел. М.: Мир, 1974.
4) Нестеренко Ю. В. Теория чисел. М.: Академия, 2008.
5) Мальцев Ю. Н., Монастырева А. С., Петров Е. П. Теория чисел. Барнаул: Изд-во Алт. ун-та. 2023.
6) Айерлэнд К., Роузен М. Классическое введение в современную теорию чисел. М.: Мир, 1987.
7) Винберг Э. Б. Курс алгебры. М.: МЦНМО, 2019.

Распределение учебников по темам:

Теория делимости

[1] – глава первая; [2] – главы 1,2,3; [3] – глава I; [4] – глава 1, разделы 2.1., 2.2. главы 2; [5] – глава 1; [6] – глава 1 (также на более абстрактном уровне рассматривается делимость в областях главных идеалов).

Арифметические функции

[1] – глава вторая; [3] – глава VI; [4] – глава 3; [5] – глава 2; [6] – глава 2.

Теория сравнений

[1] – главы третья, четвертая; [2] – главы 7,8,9,10,11,12,13,14,15,16; [3] – глава II; [4] – главы 4,5, раздел 1.4. глава 1 (решение линейных уравнений в целых числах); [5] – главы 4,5; [6] – глава 3.

Квадратичный закон взаимности

[1] – глава пятая; [2] – главы 21, 22; [3] – главы VI, V; [4] – глава 6; [5] – глава 6; [6] – глава 5.

Элементы теории групп

[7] – глава 4; глава 9, §1.

Конечные абелевы группы и их характеры

[3] – глава 10, §2, §3.

Первообразные корни и индексы

[1] – главы шестая, седьмая; [2] – главы 18, 19; [6] – главы 4.

При проработке теоретического материала необходимо параллельно решать задачи по данной теме, предложенные преподавателем для самостоятельного решения.

Решение задач по теме лекции

Задачи предназначены для самостоятельного решения студентами в течение семестра. При решении задач можно пользоваться любыми источниками, помощью одногруппников и так далее. Решенные задачи нужно показать (и объяснить решение) преподавателю, который ведет практические занятия. При полном корректном решении задачи и при условии ответов студента на все вопросы преподавателя по представленному решению, за задачу дается указанное количество баллов. При недочетах в решении или при отсутствии ответов на вопросы по решению, на выбор студента: либо задача не засчитывается и может быть сдана позднее, либо за неё ставится меньшее количество баллов на усмотрение преподавателя.

Примерные задания по темам.

Теория делимости

1) Рациональное число a/b для которого $(a, b) = 1$ называется *приведенной дробью*. Докажите, что если сумма двух приведенных дробей есть целое число, $a/b + c/d = n$, то $|b| = |d|$.
2) Применяя алгоритм Евклида, найти НОК(1403,1058,3266).
3) Докажите, что если числа $a_1,...,a_n$ попарно взаимно просты, то $[a_1,...,a_n] = a_1...a_n$, то есть наименьшее общее кратное этих чисел равно их произведению.
4) Докажите утверждения, или приведите соответствующий контрпример:
   - если $a^n \mid b^n$, то $a|b$;
   - если $n^n|m^m$, то $n|m$;
   - если $a^n|2b^n$ и $n > 1$, то $a|b$.
5) Докажите, что если $(a, b) = 1$ и $ab = c^n$, то $a = x^n$ и $b = y^n$ для некоторых целых x, y.
6) Докажите, что при $n > 1$ число $\sum_{k=1}^{\infty} 1/k$ не является целым.

Рекомендации по выполнению:

- Изучить лекционный материал: понятия делимости, наибольшего общего делителя, наименьшего общего кратного, их свойства, алгоритм Евклида, понятие простого и составного числа, теорему об однозначном разложении на простые множители.
- Разобрать доказательства теорем.
- Внимательно разобрать примеры решения, рассмотренные на практических занятия, и примеры, разобранные в учебниках.

Арифметические функции, Мультипликативные функции, Умножение Дирихле

1) Пусть при $m > 0$ $\tau_m(a)$ обозначает число решений неопределённого уравнения $x_1x_2...x_m = a$ ($x_1, x_2,..., x_m$ независимо друг от друга пробегают целые положительные числа). В частности, $\tau_1(a) = u(a) = 1$, $\tau_2(a) = \tau(a)$ - число делителей a.

а) Докажите, что $\tau_{m+n} = \tau_m * \tau_n$ для всех $m, n > 0$ (звездочка означает умножение Дирихле);

б) Докажите, что функция $\tau_m(a)$ мультипликативна;

в) Докажите, что для простого p, целого $\alpha \geq 0$ и $m > 1$ имеем

$$\tau_m(p^\alpha) = \frac{(\alpha+1)(\alpha+2)...(\alpha+m-1)}{(m-1)!}$$

г) Докажите, что $\sum_{0<a\leq n} \tau_m(a)$ выражает число решений неравенства $x_1x_2...x_m \leq n$ в целых

положительных $x_1, x_2, ..., x_m$.

д) Пусть $s = \sigma + it$. При $\sigma > 1$ полагаем $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$. Докажите, что при всех $m = 1, 2, ...$

$$\left(\zeta(s)\right)^m = \sum_{n=1}^{\infty} \frac{\tau_m(n)}{n^s}$$

2) Пусть функция f вполне мультипликативна. Докажите, что

$$f \cdot (g * h) = (f \cdot g) * (f \cdot h)$$

для любых арифметических функций g и h, где $f \cdot g$ обозначает обычное произведение функций, $(f \cdot g)(n) = f(n)g(n)$.

3) Докажите, что если $a \mid b$, то $\varphi(a) \mid \varphi(b)$.

4) В таблице задано несколько первых значений арифметической функции $f(n)$. Найдите несколько первых значений обратной по Дирихле функции $f^{-1}(n)$.

n	1	2	3	4	5	6	7	8	9	10
$f(n)$	1	-1	0	2	3	-2	1	1	0	2
$f^{-1}(n)$										

Проверьте, что $(f * f^{-1})(n) = I(n)$.

5) *Функция Лиувилля* λ определяется следующим образом: $\lambda(1) = 1$, и если $n = p_1^{\alpha_1} ... p_k^{\alpha_k}$, то $\lambda(n) = (-1)^{\alpha_1 + ... + \alpha_k}$. Докажите, что функция λ вполне мультипликативна.

6) Докажите, что для любого простого p выполнено

$$\sum_{d|n} \mu(d)\mu((p,d)) = \begin{cases} 1, & \text{если } n = 1 \\ 2, & \text{если } n = p^\alpha, \alpha > 0 \\ 0, & \text{иначе} \end{cases}$$

7) Пусть $\varphi_\alpha(n) = \sum_{\substack{k=1 \\ (k,n)=1}}^{n} k^\alpha$. В частности, $\varphi_0(n) = \varphi(n)$.

а) Докажите, что

$$\sum_{d|n} \frac{\varphi_\alpha(d)}{d^\alpha} = \frac{1^\alpha + ... + n^\alpha}{n^\alpha}$$

б) Используя формулу обращения Мёбиуса, докажите, что при $n > 1$

$$\varphi_1(n) = \frac{1}{2} n\varphi(n), \; \varphi_2(n) = \frac{1}{3} n^2 \varphi(n) + \frac{n}{6} \prod_{p|n} (1 - p).$$

в) Выведите соответствующую формулу для $\varphi_3(n)$.

8) Пусть функция f мультипликативна. Докажите, что

а) $f^{-1}(n) = \mu(n) f(n)$ для каждого свободного от квадратов n.

б) $f^{-1}(p^2) = f(p)^2 - f(p^2)$ для каждого простого p.

9) Пусть $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$, где $\operatorname{Re} s > 1$, – дзета-функция Римана; $\mu(n)$ – функция Мёбиуса; $\varphi(n)$ – функция Эйлера; $\Lambda(n)$ – функция Мангольдта; $\lambda(n)$ – функция Лиувилля; $\omega(n) = \sum_{p|n} 1$ – количество различных простых множителей в каноническом разложении числа n; $\sigma_\alpha(n) = \sum_{d|n} d^\alpha$ – сумма α-степеней положительных делителей числа n; $\tau(n) = \sigma_0(n)$ – количество положительных делителей числа n; $\sigma(n) = \sigma_1(n)$ – сумма положительных делителей числа n.

Докажите, что в подходящей полуплоскости $\operatorname{Re} s > c$ выполнены равенства а) $\dfrac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \dfrac{\mu(n)}{n^s}$;

б) $\dfrac{\zeta(s-1)}{\zeta(s)} = \sum_{n=1}^{\infty} \dfrac{\varphi(n)}{n^s}$;

в) $\zeta(s)\zeta(s-\alpha) = \sum_{n=1}^{\infty} \dfrac{\sigma_\alpha(n)}{n^s}$;

г) $\zeta^2(s) = \sum_{n=1}^{\infty} \dfrac{\tau(n)}{n^s}$;

д) $\dfrac{\zeta^3(s)}{\zeta(2s)} = \sum_{n=1}^{\infty} \dfrac{\tau(n^2)}{n^s}$;

е) $\dfrac{\zeta^4(s)}{\zeta(2s)} = \sum_{n=1}^{\infty} \dfrac{\tau^2(n)}{n^s}$;

ж) $\ln\zeta(s) = \sum_{n=2}^{\infty} \dfrac{\Lambda(n)}{\ln n} \dfrac{1}{n^s}$;

з) $-\zeta'(s) = \sum_{n=2}^{\infty} \dfrac{\ln n}{n^s}$;

и) $\dfrac{\zeta'(s)}{\zeta(s)} = -\sum_{n=1}^{\infty} \dfrac{\Lambda(n)}{n^s}$;

к) $\dfrac{\zeta(2s)}{\zeta(s)} = \sum_{n=1}^{\infty} \dfrac{\lambda(n)}{n^s}$;

л) $\dfrac{\zeta(s)}{\zeta(2s)} = \sum_{n=1}^{\infty} \dfrac{|\mu(n)|}{n^s}$;

м) $\dfrac{\zeta^2(s)}{\zeta(2s)} = \sum_{n=1}^{\infty} \dfrac{2^{\omega(n)}}{n^s}$.

Рекомендации по выполнению:

- Изучить лекционный материал: понятия мультипликативной и вполне мультипликативной функции, их свойства, основные теоретико-числовые функции – функция Эйлера, функция Мёбиуса, функция суммы делителей, понятие умножения (свертки) Дирихле и его свойства, связь умножения Дирихле с формальными рядами Дирихле, формулы обращения Мёбиуса, функция $[x]$ (целая часть числа) и её свойства.
- Разобрать доказательства теорем.
- Внимательно разобрать примеры решения, рассмотренные на практических занятиях, и примеры, разобранные в учебниках.

Теория сравнений

1) Указать общее решение для системы сравнений
$$x \equiv b_1 \pmod{25},\ x \equiv b_2 \pmod{27},\ x \equiv b_3 \pmod{59}.$$
2) Решить систему сравнений
$$x \equiv 3 \pmod 8,\ x \equiv 11 \pmod{20},\ x \equiv 1 \pmod{15}.$$
3) Какому сравнению степени ниже 5 равносильно сравнение
$$3x^{14} + 4x^{13} + 3x^{12} + 2x^{11} + x^9 + 2x^8 + 4x^7 + x^6 + 3x^4 + x^3 + 4x^2 + 2x \equiv 0 \pmod 5$$
4) Пусть m – целое, $m > 0$, a – целое, x пробегает полную систему вычетов по модулю m. Доказать, что
$$\sum e^{2\pi i \frac{ax}{m}} = \begin{cases} m, & \text{если } a \text{ кратно } m, \\ 0 & \text{в противном случае.} \end{cases}$$
5) Найдите все положительные целые n, для которых $(n-1)!+1$ является степенью n.
6) Решить сравнение $x^4 + 4x^3 + 2x^2 + 2x + 12 \equiv 0 \pmod{625}$.
7) Найдите все положительные целые n, для которых $n^{17} \equiv n \pmod{4080}$.
8) а) докажите, что если $n = 4$ или $n = p^\alpha$, где p – простое, $p \equiv 3 \pmod 4$, $\alpha > 0$, то $\varphi(n) \equiv 2 \pmod 4$;

   б) Найдите все n, для которых $\varphi(n) \equiv 2 \pmod 4$.

Рекомендации по выполнению:

- Изучить лекционный материал: понятия сравнения по модулю, свойства сравнений, понятие полной и приведенной системы вычетов, теоремы Эйлера и Ферма, свойства сравнений по простому модулю, китайскую теорему об остатках.
- Разобрать доказательства теорем.
- Внимательно разобрать примеры решения, рассмотренные на практических занятия, и примеры, разобранные в учебниках.

Квадратичный закон взаимности

1) Пусть p – нечетное простое. Пользуясь свойствами символа Лежандра
   а) найти решения сравнения (в случае его возможности)
   $$x^2 \equiv a \pmod{p}; \ \ p = 4m + 3.$$
   б) указать способ разыскания решений сравнения
   $$x^2 \equiv a \pmod{p}; \ \ p = 8m + 5.$$
   в) указать возможно более простой способ разыскания решений сравнений вида
   $$x^2 \equiv a \pmod{p}; \ \ p = 8m + 1$$
   случае, когда известен некоторый квадратичный вычет N по модулю p.
   г) пользуясь теоремой Вильсона, доказать, что решения сравнения
   $$x^2 + 1 \equiv 0 \pmod{p}; \ \ p = 4m + 1.$$
   будут
   $$x = \pm 1 \cdot 2 \cdot \dots 2m \pmod{p}.$$
2) Доказать бесконечность простых чисел вида $4m + 1$.
3) Доказать, что число представлений целого $m > 1$ в виде
   $$m = x^2 + y^2, \qquad (x, y) = 1, \qquad x > 0, y > 0$$
   равно числу решений сравнения $z^2 + 1 \equiv 0 \pmod{m}$.

Рекомендации по выполнению:
- Изучить лекционный материал: понятия квадратичного вычета и невычета, свойства символа Лежандра, квадратичный закон взаимности, символ Якоби и его свойства.
- Разобрать доказательства теорем.
- Внимательно разобрать примеры решения, рассмотренные на практических занятия, и примеры, разобранные в учебниках.

Элементы теории групп

1) Пусть группа G конечна. Докажите, что непустое множество $H \subset G$ является подгруппой группы G тогда и только тогда, когда из $a, b \in H$ следует $a \cdot b \in H$ для любых $a, b \in G$. Приведите пример бесконечной группы G и подмножества $H \subset G$, замкнутого относительно операции, но не являющегося подгруппой.
2) Пусть A, B – подгруппы группы G. Докажите, что множество $AB = \{ab \mid a \in A, b \in B\}$ является подгруппой тогда и только тогда, когда $AB = BA$.
3) Докажите, что если в группе G любой элемент удовлетворяет уравнению $x^2 = e$, то группа G абелева.
4) Докажите, что если N – нормальная подгруппа, а H – любая подгруппа группы G, то множество NH – подгруппа.
5) а) Докажите, что отображение $\sigma_g(x) = gxg^{-1}$ является автоморфизмом группы G для любого $g \in G$; б) докажите, что отображение g а σ_g является гомоморфизмом группы G в группу $\operatorname{Aut} G$ всех автоморфизмов группы G; в) что является ядром этого гомоморфизма?
6) Докажите, что если A, B – подгруппы группы G такие, что $A \cap B = \{e\}$, то $|AB| = |A| \cdot |B|$.
7) Найдите все порождающие элементы циклической группы C_m. Сколько их?
8) Опишите все гомоморфизмы из циклической группы C_m в произвольную группу G.
9) Опишите все гомоморфизмы из C_m в C_n. Сколько их?
10) Найдите порядок подстановки $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 7 & 4 & 8 & 3 & 2 & 1 \end{pmatrix}$ в группе S_8.

Рекомендации по выполнению:
- Изучить лекционный материал: понятие группы, подгруппы, нормальной подгруппы, гомоморфизма, фактор-группы, теорема Лагранжа, теорема о ядре гомоморфизма, циклические групп и их свойства.

- Разобрать доказательства теорем.
- Внимательно разобрать примеры решения, рассмотренные на практических занятиях, и примеры, разобранные в учебниках.

Конечные абелевы группы и их характеры

1) Докажите, что группа $\mathbf{Z}/m_1\mathbf{Z}\times\ldots\times\mathbf{Z}/m_k\mathbf{Z}$ является циклической тогда и только тогда, когда числа $m_1,\ldots,m_k$ попарно взаимно просты.
2) (*внутреннее прямое произведение*) Пусть $G_1,G_2,\ldots,G_k$ – подгруппы группы G. Докажите, что отображение
$$G_1\times G_2\times\ldots\times G_k\to G,\ (g_1,g_2,\ldots,g_k)\mapsto g_1g_2\ldots g_k$$
является изоморфизмом тогда и только тогда, когда
   1) любой элемент $g\in G$ единственным образом представим в виде $g=g_1g_2\ldots g_k$, где $g_i\in G_i$ для всех $i=1,\ldots,k$;
   2) подгруппа G_i нормальна в G для всех $i=1,\ldots,k$.

   В этом случае говорят, что группа G *раскладывается в прямое произведение своих подгрупп* $G_1,G_2,\ldots,G_k$.
3) Опишите строение группы $(\mathbf{Z}/600\mathbf{Z})^*$. Чему равен показатель этой группы?
4) Разложить группу $(\mathbf{Z}/m\mathbf{Z})^*$ в прямое произведение своих циклический подгрупп для модуля m, равного а) 15, 24, 35, б) 75, 90, 96, в) 105, 110, 120, г) 124, 210, 328, 380, 10976. Для каждой подгруппы указать образующую и её порядок. Например, $(\mathbf{Z}/35\mathbf{Z})^*=\langle\overline{22}\rangle_4\times\langle\overline{31}\rangle_6$.
5) Найдите все характеры по модулю 5. Представьте функцию $f(n)$, равную остатку от деления числа n на 5, в виде линейной комбинации характеров по модулю 5, $f=\sum_\chi \hat{f}(\chi)\chi$.

Рекомендации по выполнению:
- Изучить лекционный материал: теорема о строении конечнопорожденных абелевых групп, понятие характера конечной абелевой группы, теорема об ортогональности характеров, естественный изоморфизм между группой и её второй группой характеров.
- Разобрать доказательства теорем.
- Внимательно разобрать примеры решения, рассмотренные на практических занятиях, и примеры, разобранные в учебниках.

Первообразные корни и индексы

1) Найдите первообразные корни (по одной штуке) по модулям а) 11, 19, 31, 41, б) 81, 101, 121, в) 250, 343.
2) Найдите наименьший первообразный корень по модулю 242.
3) Составьте таблицы индексов по модулю 23.
4) Пользуясь таблицей индексов (И. М. Виноградов Основы теории чисел), указать число решений сравнений а) $x^{60}\equiv 79 \pmod{97}$ б) $x^{55}\equiv 17 \pmod{97}$ в) $x^{15}\equiv 46 \pmod{97}$
5) Указать число решений сравнений а) $3x^{12}\equiv 31 \pmod{41}$ б) $7x^7\equiv 11 \pmod{41}$ в) $5x^{30}\equiv 37 \pmod{41}$.
6) Решить сравнения а) $23x^5\equiv 15 \pmod{73}$ б) $37x^6\equiv 69 \pmod{73}$ в) $44x^{21}\equiv 53 \pmod{73}$
7) Среди вычетов приведенной системы вычетов по модулю 19 указать а) квадратичные вычеты б) кубические вычеты.
8) Среди вычетов приведенной системы вычетов по модулю 37 указать а) вычеты степени 15 б) вычеты степени 8.
9) Среди вычетов приведенной системы вычетов по модулю 43 указать а) числа, показатель которых равен 6 б) первообразные корни.

10) Среди вычетов приведенной системы вычетов по модулю 61 указать а) числа, показатель которых равен 10 б) первообразные корни.
11) Составить таблицы индексов по модулям а) 2, 4, 10, б) 12, 15, 16, 25.

Рекомендации по выполнению:
- Изучить лекционный материал: понятие первообразного корня, признаки первообразного корня, строение группы $(\mathbb{Z}/m\mathbb{Z})^*$, случаи, когда эта группа является циклической, понятие индекса и его свойства.
- Разобрать доказательства теорем.
- Внимательно разобрать примеры решения, рассмотренные на практических занятиях, и примеры, разобранные в учебниках.

<u>Подготовка к контрольной работе</u>
В течение семестра проводятся две аудиторные контрольные работы, каждая на 30 баллов – 6 задач по 5 баллов каждая. Время выполнения работы – 2 академических часа (90 минут).
Примерное задание. Решить тестовую контрольную работу. Тестовая контрольная работа является инструментом текущего контроля знаний, умений и навыков обучающего по группам тем дисциплины.
Примерные варианты контрольных работ

Контрольная работа № 1

1. Пусть $m = ax + by$, $n = cx + dy$, где $ad - bc = \pm 1$. Докажите, что $(m, n) = (x, y)$. Все числа целые.
2. Применяя алгоритм Евклида, найти [1403,1058,3266].
3. Пусть функция f вполне мультипликативна. Докажите, что
$$f \cdot (g * h) = (f \cdot g) * (f \cdot h)$$
для любых арифметических функций g и h, где $f \cdot g$ обозначает обычное произведение функций, $(f \cdot g)(n) = f(n)g(n)$, а $g * h$ обозначает свёртку Дирихле.
4. В таблице задано несколько первых значений арифметической функции $f(n)$. Найдите несколько первых значений обратной по Дирихле функции $f^{-1}(n)$.

n	1	2	3	4	5	6	7	8	9	10
$f(n)$	1	-3	0	1	4	-6	1	1	-2	1
$f^{-1}(n)$										

5. Докажите, что в подходящей полуплоскости $\operatorname{Re} s > c$ выполнено равенство
$$\frac{\zeta(s-1)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s},$$
где φ – функция Эйлера.
6. Пусть m – целое, $m > 0$, a – целое, x пробегает полную систему вычетов по модулю m. Доказать, что
$$\sum e^{2\pi i \frac{ax}{m}} = \begin{cases} m, & \text{если } a \text{ кратно } m, \\ 0 & \text{в противном случае.} \end{cases}$$

Контрольная работа № 2

1. Найдите все порождающие элементы циклической группы C_{20}.
2. Опишите все гомоморфизмы из C_{20} в C_7.
3. Найдите какой-нибудь первообразный корень по модулю 41.
4. Разложить группу $(\mathbf{Z}/m\mathbf{Z})^*$ в прямое произведение своих циклический подгрупп для модуля m, равного 105. Для каждой подгруппы указать образующую и её порядок. Пример разложения: $(\mathbf{Z}/35\mathbf{Z})^* = \langle \overline{22} \rangle_4 \times \langle \overline{31} \rangle_6$.
5 Проверить справедливость представления группы $(\mathbf{Z}/m\mathbf{Z})^*$ в виде прямого произведения циклических подгрупп и представить заданное число a в виде

произведения некоторых степеней образующих этих подгрупп, если $(\mathbf{Z}/24\mathbf{Z})^* = \langle\overline{7}\rangle\times\langle\overline{13}\rangle\times\langle\overline{17}\rangle$, $a = 5$.

6. Пользуясь таблицей индексов, решить сравнение $x^{55} \equiv 17 \pmod{97}$

Критерии оценивания:
5 баллов – обосновано получен верный ответ, названы используемые в решении теоретические утверждения, все вычисления проведены верно.
4 балла – получен верный ответ, но не названы используемые в решении теоретические утверждения; в вычислениях может быть допущена арифметическая ошибка.
3 балла – в целом верный ход решения, но присутствует грубая ошибка в вычислениях.
2 балл – названы теоретические утверждения, необходимые для решения задачи; присутствуют вычисления, имеющие отношения к задаче, но они не завершены.
1 балла – названы теоретические утверждения, необходимые для решения задачи; вычисления либо отсутствуют, либо не имеют отношения к задаче.

Рекомендации по самоподготовке к промежуточной аттестации по дисциплине

Оценка студента в рамках модульно-рейтинговой системы оценок является интегрированной оценкой выполнения студентом заданий во время практических занятий, домашних заданий, контрольных работ. Эта оценка характеризует уровень сформированности практических умений и навыков, приобретенных студентом в ходе изучения дисциплины:
61 - 75 баллов - удовлетворительно;
76 - 90 баллов - хорошо;
91 -100 баллов - отлично.
Неуспевающие студенты или студенты, желающие повысить оценку, на зачете должны написать письменную работу. Билеты для зачета включают: теоретический вопрос по курсу дисциплины и две задачи из числа разобранных на семинарах и предлагавшихся на контрольных работах.
Вопросы к дифференцированному зачёту

1. Теорема о делении с остатком.
2. Свойства делимости в кольце Z.
3. НОД. Алгоритм Евклида.
4. Теорема о линейном представлении НОД.
5. Взаимно простые числа. Их свойства.
6. НОК и его свойства.
7. Простые и составные числа и их свойства.
8. Теорема о факториальности кольца целых чисел и следствия из нее.
9. Теорема о бесконечности множества простых.
10. Распределение простых чисел в натуральном ряду.
11. Сравнения в кольце целых чисел. Различные определения и их равносильность.
12. Свойства сравнений.
13. Кольцо классов вычетов.
14. Полная и приведенная система вычетов.
15. Теоремы о вычетах линейной формы.
16. Функция Эйлера и ее свойства Теоремы Эйлера и Ферма
17. Числовые функции.
18. Порядок числа и класса вычетов.
19. Определение и свойства индексов.
20. Применение индексов к решению двучленных сравнений.
21. Приложение теории сравнений к выводу признаков делимости.
22. Теорема о гомоморфизмах групп.
23. Теорема о строении конечно порожденных абелевых групп.
24. Строение группы обратимых элементов кольца классов вычетов. Первообразные корни и индексы.

25. Группа характеров конечной абелевой группы. Ортогональность характеров. Преобразование Фурье на конечной абелевой группы.
26. Теорема Дирихле о простых числах в арифметической прогрессии.