

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»**

**Методические указания
по выполнению практических работ
по дисциплине «Теория чисел»
для студентов направления подготовки
01.03.02 «Прикладная математика и информатика»**

Ставрополь 2026 г

СОДЕРЖАНИЕ

Введение
1. Делимость в кольце целых чисел
2. Арифметические функции и их приложения
3. Конечные цепные дроби
4. Числовые сравнения
5. Сравнения и системы сравнений первой степени. Методы их решения.
6. Сравнения второй степени.
7. Первообразные корни и индексы. Степенные вычеты.
8. Арифметические приложения теории сравнений.

Введение

Теория чисел является наукой о числовых системах с их связями и законами. В первую очередь уделяется внимание числам натурального ряда, которые являются основой для построения других числовых систем. Теория чисел изучает числа с точки зрения их строения и внутренних связей, рассматривает возможности представить одни числа через другие, более простые по своим свойствам. Учитывая, что в последнее время бурно развиваются области математики, требующие глубокого анализа дискретного, то интерес к теории чисел возрастает, т.к. большинство её утверждений относятся к дискретной математике.

Цель дисциплины «Теория чисел» состоит в формировании профессиональных компетенций будущего бакалавра по направлению подготовки 01.03.02 – Прикладная математика и информатика.

К числу задач освоения курса можно отнести

- формирование теоретико-числовой культуры студента;
- освоение методов исследования и решения уравнений в целых числах;
- изучение свойств простых и составных чисел, законов распределения простых чисел в натуральном ряде и арифметических прогрессиях;
- рассмотрение структуры колец классов вычетов по натуральному модулю и овладение методами решения сравнений;
- изучение арифметики в полях алгебраических чисел, ее применений к решению уравнений в целых числах, исследованию свойств неалгебраических чисел;
- освоение методов приближения действительных чисел рациональными дробями и методов построения наилучших приближений.

В результате освоения дисциплины студент должен:

Знать: определение общих форм и закономерностей теории чисел; свойства делимости целых чисел; теорему о делении с остатками; свойства простых и составных чисел; теорему о бесконечности множества простых чисел; основную теорему арифметики; способы нахождения наибольшего общего делителя (НОД) и наименьшего общего кратного (НОК) натуральных чисел; взаимосвязь между НОДом и НОКом двух чисел; основные арифметические функции и их приложения; определение и свойства цепных дробей; определение и свойства числовых сравнений; теоремы Эйлера и Ферма; теорему о числе решений линейного сравнения и методы их нахождения; Китайскую теорему об остатках и способы решения системы 4 линейных сравнений; способы определения разрешимости сравнений второй степени; связь между сравнением и неопределенным уравнением; теорему о существовании первообразных корней; определение индексов и их свойства; понятия алгебраических и трансцендентных чисел.

Уметь: находить наибольший общий делитель двух чисел с помощью алгоритма Евклида; находить НОД и НОК чисел, зная их канонические раз-

ложения; с помощью решета Эратосфена находить простые числа на заданном интервале; вычислять и использовать числовые функции для решения практических задач; применять теоремы Эйлера и Ферма для нахождения остатков от деления; разлагать обыкновенные дроби в непрерывные; представлять квадратичные иррациональности в виде бесконечных цепных дробей; использовать аппарат цепных дробей в приближенных вычислениях; находить полную и приведенную системы вычетов; решать линейные сравнения различными методами; решать диофантовы уравнения первой степени; находить решение системы линейных сравнений; вычислять символы Лежандра и Якоби; решать линейные, степенные и показательные сравнения с помощью индексирования; строго доказывать и формулировать результаты в области теории чисел; доказывать трансцендентность чисел Π и e .

Владеть: методами решения задач на делимость; методами решения уравнений и неравенств в целых числах; аппаратом цепных дробей; методами решения линейных сравнений; навыками доказательств и формулировки утверждений в области теории чисел; доказательствами основных теорем курса.

Цель данного практикума – описание последовательности, основного содержания, методики выполнения практических (семинарских) занятий по учебному курсу и (или) самостоятельной подготовки к ним.

Тема 1. Делимость в конце целых чисел.

Цель занятия. Формирование понятийного аппарата теории делимости и навыков решения задач на делимость.

Знания и умения, приобретаемые обучающимся в результате освоения темы, в рамках формируемых компетенций или их части

Знать: свойства делимости целых чисел, способы нахождения наибольшего общего делителя (НОД) и наименьшего общего кратного (НОК) натуральных чисел; взаимосвязь между НОДом и НОКом двух чисел.

Уметь: находить наибольший общий делитель двух чисел с помощью алгоритма Евклида; находить НОД и НОК чисел, зная их канонические разложения.

Владеть: методами решения задач на делимость.

Актуальность темы. Тема делимость в кольце целых чисел важна для формирования умений и навыков решения олимпиадных задач.

Теоретическая часть

Пусть a и b целые числа, причем $b \neq 0$. Говорят, что целое число a делится на целое число b (без остатка), если существует целое число q , такое, что $a = bq$

Говорят, что целое число a делится на целое число b , отличное от нуля, с остатком, если существуют такие целые числа q и r , что $a = bq + r$ и $0 \leq r < |b|$.

В этом случае называют a - делимое, b - делитель, q - неполное частное, r - остаток. Если $r = 0$, то получаем случай делимости нацело. Таким образом, кратность есть частный случай деления с остатком.

Теорема (о делении с остатком). Для любых целых чисел a и b , причем $b \neq 0$, всегда возможно и притом единственным способом деление с остатком.

Натуральное число d называется наибольшим общим делителем чисел a и b , если

- 1) d - общий делитель чисел a и b ($a:b \wedge b:d$);
- 2) d делится на любой общий делитель δ чисел a и b .

Обозначают $\text{НОД}(a;b)$ или просто $(a;b)$.

Теорема (Алгоритм Евклида). НОД чисел a и b равен последнему отличному от нуля остатку в системе равенств (9), т.е. $(a;b) = r_n$.

Наименьшим общим кратным (НОК) чисел a и b называется такое число m , что

- 1) $m:a \wedge m:b$;
- 2) для любого общего кратного чисел a и b и числа M выполняется условие $M:m$.

Вопросы к занятию:

1. Дайте определение отношению делимости в кольце Z . Приведите примеры;

2. Сформулируйте и докажите основные свойства отношения делимости;
3. Дайте понятие операции деления с остатком. Приведите примеры;
4. Сформулируйте и докажите теорему о делении с остатком;
5. Введите понятия общего делителя чисел, наибольшего общего делителя (НОД) чисел;
6. Перечислите способы отыскания НОДа. Укажите свойства НОДа;
7. В чём заключается алгоритм Евклида, докажите эту теорему;
8. Введите понятия взаимно простых и попарно взаимно простых чисел, приведите примеры;
9. Что такое общее кратное чисел? Дайте определение наименьшего общего кратного (НОК) чисел;
10. Перечислите свойства НОК и докажите их; Какова связь между НОК и НОД двух чисел?
11. Расскажите, как в школьном курсе находят НОД и НОК чисел;
12. Докажите, что если $a = cq + r$ и $b = cq_1 + r_1$, где a, b, q, q_1, r, r_1 - целые неотрицательные числа и c - целое положительное число, то $(a, b, c) = (c, r, r_1)$. Сформулируйте вытекающее отсюда правило нахождения (a, b, c) . Обобщите это правило на случай n чисел;

Задания, решаемые в аудитории

1. Число $a=42157$ при делении на некоторое целое положительное число b даёт в частном $q=231$. Найдите делитель b и остаток r
2. Делимое 100, остаток 6. Найдите делитель b и частное q .
3. При делении a на b получается частное q и ненулевой остаток r . На какое натуральное число n нужно умножить a , чтобы при делении на b частное увеличилось в n раз?
4. Докажите, что из трёх последовательных натуральных чисел одно делится на 3, а их произведение делится на 6.
5. Покажите, что $n(n^2 + 5)$, где $n \in \mathbb{N}$, делится на 6.
6. Докажите, что сумма квадратов пяти последовательных чисел не может быть точным квадратом.
7. Между цифрами числа 16 вписывают 15, в середину числа 1156 опять вписывают 15 и т.д. Докажите, что все полученные числа будут точными квадратами.
8. Найдите все натуральные n , при которых сократите дробь
$$\frac{7n^2 + 11n + 4}{6n^2 + 5n}.$$
9. С помощью алгоритма Евклида найдите наибольший общий делитель чисел и его линейное представление
 - а) 546 и 231;
 - б) 6919 и 1443.
10. Найдите наименьшее общее кратное чисел из задачи №9.
11. Найдите НОД и НОК чисел
 - а) 819, 702, 689;
 - б) 279, 372, 1395.

12. Найдите два числа, зная, что сумма частных от деления каждого из них на их НОД равна 18 и НОК их равно 975.

Задания для самостоятельной работы дома

1. При делении целого числа a на 13 получается неполное частное 17. Найдите наибольшее значение делимого a .
2. Делимое равно 371, частное 14. Найдите делители b и соответствующие им остатки r .
3. Докажите, что из двух последовательных чётных чисел одно делится на 4, а из пяти последовательных натуральных чисел одно делится на 5.
4. Докажите, что если $mn + pq$ делится на $m - p$, то и $mq + np$ делится на $m - p$, где m, n, p, q – целые числа.
5. Покажите, что $m^2 - m$, где $m \in \mathbb{N}$, делится на 30.
6. Докажите, что если остаток от деления некоторого числа на 9 есть одно из чисел 2, 3, 5, 6, 8, то это число не может быть точным квадратом.
7. Покажите, что числа 48, 4488, 444888, ... могут быть представлены в виде произведения двух последовательных чётных чисел.
8. Найдите четырёхзначное число $\overline{xu}$, которое делится на произведение двух двузначных чисел xu , где x – две первые цифры этого числа, а u – две последние.
9. С помощью алгоритма Евклида найдите наибольший общий делитель чисел и его линейное представление
 - а) 903 и 731;
 - б) 4543 и 885.
10. Найдите наименьшее общее кратное чисел из задачи №9.
11. Найдите НОД и НОК чисел 3059, 2737, 943.
12. Сумма двух чисел 667, а отношение НОК к их НОД равно 120. Найдите эти числа.

Тема 2. Арифметические функции и их приложения.

Тема занятия. Арифметические функции и их приложения

Цель занятия. Научить студентов вычислять основные арифметические функции и применять их в решении задач.

Знания и умения, приобретаемые обучающимся в результате освоения темы, в рамках формируемых компетенций или их части

Знать: основные арифметические функции и их приложения;

Уметь: вычислять и использовать числовые функции для решения практических задач;

Владеть: навыками доказательств и формулировки утверждений в области теории чисел; доказательствами основных теорем курса.

Актуальность темы. Вычисление арифметических функций важно для решения ряда задач на делимость, а так же теории сравнений.

Теоретическая часть

Функция $f(n)$, определенная на множестве N и отличная от нуля хотя бы для одного числа, называется **мультипликативной** если для любых взаимно простых натуральных чисел a и b выполняется условие

$$f(a \cdot b) = f(a) \cdot f(b).$$

Целой частью действительного числа x (обозначается $[x]$) называется наибольшее целое число k , не превосходящее x , т.е. $k \leq x < k + 1$.

Дробной частью действительного числа x (обозначается $\{x\}$) называется разность $x - [x]$.

Свойства $[x]$.

1⁰. Если $x > 0$, то количество натуральных чисел a , не превосходящих x и делящихся на n , равно $\left[\frac{x}{n} \right]$

$$2^0. \left[\frac{[x]}{n} \right] = \left[\frac{x}{n} \right].$$

3⁰. Для любого действительного числа x $[x] - 2 \cdot \left[\frac{x}{2} \right] = 0$ или $[x] - 2 \cdot \left[\frac{x}{2} \right] = 1$.

Если $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$, то все делители числа m могут быть получены по формуле

$$d = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_k^{\beta_k} = \prod_{i=1}^k p_i^{\beta_i}, \text{ где } 0 \leq \beta_i \leq \alpha_i \text{ (} i=1,2,\dots,k \text{)}.$$

Функция $\tau(n) = \sum_{d \mid n} 1$ определяется как число положительных делителей натурального числа n .

Функция $S(n) = \sum_{d \mid n} d$ определяется как сумма положительных делителей натурального числа n .

Если $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$,
то $\tau(n) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \dots \cdot (\alpha_k + 1)$.

Если $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$, то $S(n) = \prod_{i=1}^k \frac{p_i^{\alpha_i + 1} - 1}{p_i - 1}$.

Функцией Эйлера $\varphi(m)$ называется число натуральных чисел, не превосходящих m и взаимно простых с m . По определению считают $\varphi(1) = 1$.

Если $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$,
то $\varphi(m) = m \cdot (1 - \frac{1}{p_1}) \cdot (1 - \frac{1}{p_2}) \cdot \dots \cdot (1 - \frac{1}{p_k})$

Если $(a, m) = 1$, то остаток от деления $a^{\varphi(m)}$ на m равен 1.

Вопросы и задания

Вопросы к занятию:

1. Введите понятие арифметической функции;
2. Какая функция называется мультипликативной; вполне мультипликативной?
3. Введите понятие целой части действительного числа $[x]$. Приведите примеры. Постройте график функции $y = [x]$;
4. Дайте определение дробной части действительного числа $\{x\}$. Приведите примеры. Постройте график функции $y = \{x\}$.
5. Перечислите и докажете свойства функции целая часть числа.
6. Как разложить число $n!$ на простые множители;
7. Что Вы можете рассказать о суммах, распространённых на все делители числа. Приведите примеры таких сумм;
8. Выведите формулу для нахождения числа положительных делителей натурального числа $\tau(n)$;
9. Выведите формулу для нахождения суммы положительных делителей натурального числа $s(n)$;
10. Введите понятие дружественных и совершенных чисел. Приведите примеры. Что Вы можете о них рассказать? Какие проблемы в теории чисел связаны с этими числами?
11. Дайте определение функции Эйлера $\varphi(m)$;
12. Выведите формулу для нахождения $\varphi(m)$. Чему равна функция Эйлера от простого числа?

Задания, решаемые в аудитории

1. Найдите $[-3]$; $[5,4]$; $\left[-\frac{7}{9}\right]$; $[\sqrt{31}]$; $[\sqrt{715}+1]$; $\left[4+\cos\frac{101\pi}{204}\right]$; $[2+\lg 0,3]$.
2. Найдите $\{-3\}$; $\{5,4\}$; $\left\{-\frac{7}{9}\right\}$; $\{-10,2\}$.
3. Найдите показатель степени числа 17 в каноническом разложении числа 500!
4. Найдите каноническое разложение 40!
5. Сколькими нулями оканчивается 200!
6. Найдите количество целых положительных чисел, не превосходящих 180 и не делящихся ни на одно из простых чисел 5, 7, 11.
7. Найдите количество целых положительных чисел, не превосходящих 1000 и не взаимно простых с числом 363.
8. Найдите все делители чисел 360; 957.
9. Найдите число и сумму всех натуральных делителей чисел 360; 957; 1200.
10. $N = p^\alpha \cdot q^\beta$, где p и q – простые неравные между собой числа. N^2 имеет 15 различных делителей. Сколько делителей имеет N^3 ?
11. У натурального числа ровно 9 натуральных делителей. Сумма этих делителей равна 741. Найдите это число.
12. Сколько чисел в интервале от 1 до 120 не взаимно простых с числом 30?
13. Дано $\varphi(a) = 3600$ и $a = 3^\alpha \cdot 5^\beta \cdot 7^\gamma$. Найдите a .
14. Найдите количество правильных несократимых дробей со знаменателем 16.
15. Найдите количество натуральных чисел, меньших числа 300 и имеющих с ним НОД равный 20.

Задания для самостоятельной работы дома

1. Найдите $\left[\frac{8}{3}\right]$; $[-2,7]$; $[\sqrt{15}]$; $[\sqrt[4]{200}]$; $\left[\frac{\sqrt{542}+2}{3}\right]$; $[2-\lg 2512]$; $[1+\ln 50]$.
2. Найдите $\left\{\frac{8}{3}\right\}$; $\{-2,7\}$; $\{0,4\}$; $\{-6\}$.
3. Найдите показатель степени числа 13 в каноническом разложении числа 1000!
4. Найдите каноническое разложение 54!
5. Сколькими нулями оканчивается 250!
6. Найдите количество целых положительных чисел, не превосходящих 2311 и не делящихся ни на одно из чисел 5, 7, 13, 17.
7. Найдите количество целых положительных чисел, не превосходящих 12317 и взаимно простых с числом 1575.

8. Найдите все делители чисел 375; 988.
9. Найдите число и сумму всех натуральных делителей чисел 375; 988; 1500; 4320.

Тема 3. Цепные дроби.

Тема занятия. Конечные цепные дроби

Цель занятия. Показать возможность представления рациональных чисел в виде цепных дробей.

Знания и умения, приобретаемые обучающимся в результате освоения темы, в рамках формируемых компетенций или их части

Знать: определение и свойства цепных дробей;

Уметь: разлагать обыкновенные дроби в непрерывные;

Владеть: аппаратом цепных дробей.

Актуальность темы. Цепные дроби важны в приближённых вычислениях, для решения линейных сравнений и неопределённых уравнений.

Теоретическая часть

Представление дроби $w = \frac{a}{b}$ в виде

$$\frac{a}{b} = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \ddots + \frac{1}{q_{n-1} + \frac{1}{q_n}}}}}$$

где $q_0 \in \mathbb{Z}$, $q_i \in \mathbb{N}$ ($i = \overline{1, n}$), называется правильной (конечной) цепной или правильной непрерывной дробью.

Всякая конечная цепная дробь есть рациональное число.

Дроби вида $q_0, q_0 + \frac{1}{q_1}, q_0 + \frac{1}{q_1 + \frac{1}{q_2}}, \dots, q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \ddots + \frac{1}{q_n}}}}$ называются

подходящими дробями соответственно нулевого, первого, второго, и n -го порядков и обозначаются соответственно $\frac{P_0}{Q_0}, \frac{P_1}{Q_1}, \frac{P_2}{Q_2}, \dots, \frac{P_n}{Q_n}$.

P_i - называется числителем подходящих дробей,

Q_i - называются знаменателями подходящих дробей.

Теорема 1. Для вычисления числителя и знаменателя подходящих дробей справедливы рекуррентные формулы:

$$P_0 = q_0, Q_0 = 1 \quad (6)$$

$$P_1 = q_0 q_1 + 1, Q_1 = q_1 \quad (7)$$

$$P_k = P_{k-1} q_k + P_{k-2}, Q_k = Q_{k-1} q_k + Q_{k-2} \quad (k = \overline{2, n}) \quad (8)$$

Замечание. Формулы (6)-(8) легко запомнить, пользуясь таблицей.

n			0	1	2	3	...	n
q_n			q_0	q_1	q_2	q_3		q_n
P_n	0	1	$P_0 = q_0$	$P_1 = q_0 q_1 + 1$	$P_2 = P_1 q_2 + P_0$	$P_3 = P_2 q_3 + P_1$		$P_n = P_{n-1} q_n + P_{n-2}$
Q_n	1	0	$Q_0 = 1$	$Q_1 = q_1$	$Q_2 = Q_1 q_2 + Q_0$	$Q_3 = Q_2 q_3 + Q_1$		$Q_n = Q_{n-1} q_n + Q_{n-2}$

Для числа w и его подходящих дробей справедливы соотношения:

$$\left| w - \frac{P_k}{Q_k} \right| < \frac{1}{Q_k^2},$$

$$\left| w - \frac{P_k}{Q_k} \right| \leq \frac{1}{Q_{k+1} \cdot Q_k}.$$

Вопросы и задания

Вопросы к занятию:

1. Дайте определение конечной цепной (правильной, непрерывной) дроби;
2. Как получить разложение рационального числа в цепную дробь? В чём особенность представления отрицательного числа цепной дробью?
3. Докажите, что конечная цепная дробь есть рациональное число;
4. Введите понятие подходящих дробей;
5. Введите формулы для нахождения числителей и знаменателей подходящих дробей;
6. Сформулируйте теоремы, выражающие свойства подходящих дробей, и докажите их;
7. Как сократить дробь с помощью подходящих дробей?
8. Чем определяется точность приближения рационального числа подходящих дробей?

Задания, решаемые в аудитории

1. Разложите данные обыкновенные дроби в непрерывные. Замените полученные дроби подходящими дробями четвертого порядка и определите погрешность замены

а) $\frac{163}{159}$; б) $\frac{1882}{1651}$

2. По данным конечным непрерывным дробям найдите соответствующие им обыкновенные дроби

а) (0; 4, 1, 3, 1, 2, 1); б) (-1; 2, 3, 1, 2, 1, 3, 1, 2, 3)

Найдите подходящую дробь, которая бы приближала полученное число с точностью 0, 01; 0, 001 и 0, 0005.

3. Сократите с помощью разложения в непрерывную дробь следующие обыкновенные дроби

$$\text{а) } \frac{3587}{2743}; \quad \text{б) } \frac{11281}{6583}.$$

4. С помощью непрерывных дробей решите диофантовы уравнения

а) $38x + 117y = 209$;

б) $119x - 68y = 34$.

Задания для самостоятельной работы дома

1. Разложите данные обыкновенные дроби в непрерывные. Какой подходящей дробью можно заменить данную обыкновенную дробь с погрешность не более 0,001

$$\text{а) } \frac{385}{648}; \quad \text{б) } \frac{2341}{1721}; \quad \text{в) } -\frac{313}{57}.$$

2. По данным конечным непрерывным дробям найдите соответствующие им обыкновенные дроби

а) (2; 1, 1, 5, 1, 7);

б) (-3; 2, 1, 5, 4, 1, 2);

в) (0; 1, 1, 2, 2, 3, 3).

С какой погрешностью подходящие дроби 3-го порядка приближают полученные дроби?

3. Сократите с помощью разложения в непрерывную дробь следующие обыкновенные дроби: а) $\frac{1043}{3427}$; б) $\frac{3653}{3107}$; в)

$$\frac{7093}{11111}.$$

4. С помощью непрерывных дробей решите следующие неопределённые уравнения

а) $122x + 129y = 2$;

б) $258x - 175y = 113$;

в) $41x + 114y = 5$.

5. С помощью непрерывных дробей найдите линейное представление НОДа чисел 285 и 786.

Тема 4. Числовые сравнения

Тема занятия. Числовые сравнения

Цель занятия. Формирование понятия сравнимых чисел.

Знания и умения, приобретаемые обучающимся в результате освоения темы, в рамках формируемых компетенций или их части

Знать: определение и свойства числовых сравнений; теоремы Эйлера и Ферма;

Уметь: применять теоремы Эйлера и Ферма для нахождения остатков от деления; находить полную и приведенную системы вычетов;

Владеть: навыками доказательств и формулировки утверждений в области теории чисел; доказательствами основных теорем курса

Актуальность темы. Числовые сравнения важны для изучения сравнений с неизвестной величиной.

Теоретическая часть

Числа a и b называются сравнимыми по модулю m , если их разность делится на m . Этот факт обозначается следующим образом:

$a \equiv b \pmod{m}$. Таким образом, $a \equiv b \pmod{m} \Leftrightarrow (a - b) : m$.

Теорема. Два числа a и b сравнимы по модулю m тогда и только тогда, когда они дают одинаковые остатки при делении на m .

Отношение сравнимости, как всякое отношение эквивалентности, порождает разбиение множества целых чисел на классы. При делении на m целое число может давать остатки $0, 1, 2, \dots, m-1$.

Если из каждого класса по модулю m взять по одному представителю, то полученную систему чисел называют полной системой вычетов по модулю m .

Наиболее часто используют

- полную систему наименьших неотрицательных вычетов: $0, 1, 2, \dots, m-1$;
- полную систему наименьших положительных вычетов: $1, 2, 3, \dots, m$;
- полную систему наименьших по абсолютной величине вычетов:

$0, \pm 1, \pm 2, \dots, \pm \frac{m-1}{2}$, если m – нечётное,

$0, \pm 1, \pm 2, \dots, \pm \frac{m-2}{2}, \frac{m}{2}$, если m – чётное.

Теорема (признак полной системы вычетов). Система из m не сравнимых между собой по модулю m чисел образует полную систему вычетов.

Если из полной системы вычетов выбрать числа, взаимно простые с модулем, то полученная система называется приведённой системой вычетов.

В зависимости от того, из какой полной системы выбираются числа, взаимно простые с модулем, различают

- приведённую систему наименьших положительных вычетов;
- приведённую систему наименьших по абсолютной величине вычетов.

Число чисел приведённой системы вычетов определяется функцией Эйлера, т.к. функция Эйлера $\varphi(m)$ означает количество чисел, не превосходящих m и взаимно простых с m .

Любые $\varphi(m)$ чисел, попарно несравнимых и взаимно простых с модулем m , образуют приведённую систему вычетов.

Теорема (Эйлера). Если $(a, m) = 1$, то $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Вопросы и задания

Вопросы к занятию:

1. Дайте определение сравнимых чисел;
2. Докажите эквивалентность отношения сравнимости чисел по модулю m и отношения давать одинаковые остатки при делении на m ;
3. Сформулируйте и докажите основные свойства сравнений;
4. Введите определения вычета, класса вычетов;
5. Определите операции над классами вычетов;
6. Докажите, что множество классов вычетов по составному модулю относительно операций сложения и умножения классов образуют кольцо, а по простому модулю – поле;
7. Дайте определение полной системы вычетов. Сформулируйте признак полной системы вычетов;
8. Какие виды полных систем вычетов Вы знаете? Приведите примеры;
9. Сформулируйте и докажите теоремы о полной системе вычетов;
10. Дайте определение приведённой системы вычетов. Какие Вы знаете приведённые системы, приведите примеры;
11. Как определить число чисел приведённой системы?
12. Сформулируйте и докажите теоремы о приведённой системе вычетов.
13. Сформулируйте и докажите теорему Эйлера;
14. Сформулируйте и докажите малую теорему Ферма.

Задания, решаемые в аудитории

1. Запишите в виде сравнений условия:
 - а) -38 и -3 дают при делении на 7 одинаковые остатки;
 - б) при делении на 6 число 52 даёт остаток 4 ;
 - в) $a^3 + b^3$ делится на $a + b$;
 - г) $a^2 + ab + b^2$ при делении на $a - b$ даёт остаток $3ab$.
2. Покажите, что если n – нечётное число, то $n^2 - 1 \equiv 0 \pmod{8}$.
3. Докажите, что если $3^n \equiv -1 \pmod{10}$, то $3^{n+4} \equiv -1 \pmod{10}$.
4. Найдите остаток от деления $1532^5 - 1$ на 9 .
5. Известно, что $a^{100} \equiv 2 \pmod{73}$ и $a^{101} \equiv 69 \pmod{73}$. Найдите остаток от деления числа a на 73 .
6. Запишите основные виды полной и приведённой систем вычетов по модулю

- а) $m=8$; б) $p=7$.
7. Покажите, что числа 30; -11; 13; 40; -20; 28; 4 образуют полную систему вычетов по модулю $m=7$.
8. Покажите, что числа 23; -33; 9; -19 составляют приведённую систему вычетов по модулю $m=10$.
9. С помощью теорем Эйлера и Ферма найдите остатки от деления
а) 383^{175} на 45; б) 66^{17} на 7; в) $5^{80} + 7^{100}$ на 13.
10. Найдите последние две цифры числа 541^{101} .
11. Охарактеризуйте сравнениями числа следующего вида
а) чётные; б) нечётные; в) кратные 6; г) $4k+3$; д) $9k-1$.
12. Покажите, что если $100a + 10b + c \equiv 0 \pmod{21}$, то
 $a - 2b + 4c \equiv 0 \pmod{21}$.
13. Докажите, что $2^{1131} \equiv 2 \pmod{11 \cdot 31}$.
14. Проверьте, что $3^{14} \equiv -1 \pmod{29}$.
15. Дано, что выражение $\frac{11a + 2b}{19}$ есть целое число. Докажите, что тогда и $\frac{18a + 5b}{19}$ тоже целое число.
16. Запишите основные виды полной и приведённой систем вычетов по модулю
а) $m=12$; б) $p=13$.
17. Покажите, что числа 26; -19; 17; 47; -20; 19; 38; -16 составляют полную систему вычетов по модулю $m=8$. Запишите полную систему вычетов по этому модулю с помощью чисел кратных 3.
18. Покажите, что числа 19; -9; 17; -11 составляют приведённую систему вычетов по модулю $m=8$.
19. Найдите остатки от деления

- а) 439^{291} на 60; б) 117^{53} на 11;
в) $5^{50} + 5^{60} + 5^{70}$ на 18; г) $3 \cdot 5^{75} + 4 \cdot 7^{100}$ на 132.

20. Найдите последние три цифры числа 521^{302} .

21. Докажите, что числа p и $8p^2 + 1$ могут быть одновременно простыми только при $p=3$.

22. Докажите, что $a^{12} - b^{12}$ делится на 65, если $(a, 65)=1$ и $(b, 65)=1$.

Тема 5. Сравнения и системы сравнений первой степени. Методы их решения.

Тема занятия. Сравнения и системы сравнений первой степени и методы их решения

Цель занятия. Овладение методами решения линейных сравнений и их систем.

Знания и умения, приобретаемые обучающимся в результате освоения темы, в рамках формируемых компетенций или их части

Знать: теорему о числе решений линейного сравнения и методы их нахождения; КТО

Уметь: решать линейные сравнения различными методами;

Владеть: методами решения линейных сравнений; навыками доказательств и формулировки утверждений в области теории чисел; доказательствами основных теорем курса.

Актуальность темы. Решение линейных сравнений важно для решения систем линейных сравнений и для представления информации в системе остаточных классов.

Теоретическая часть

Сравнение вида

$$f(x) \equiv 0 \pmod{m} \quad (1)$$

называется сравнением с одной неизвестной x степени n , если $f(x)$ – многочлен с целыми коэффициентами, причём $a_n \not\equiv 0 \pmod{m}$.

, сравнение первой степени имеет вид $a_1x + a_0 \equiv 0 \pmod{m}$ или будем записывать его в виде

$$ax \equiv b \pmod{m}$$

Теорема (о числе решений линейного сравнения). Если в сравнении $ax \equiv b \pmod{m}$ $(a, m) = d$ и $b : d$, то сравнение имеет d решений, если же $b \nmid d$, то сравнение (4) решений не имеет. Метод подбора заключается в использовании в качестве решений чисел полной системы вычетов. Заметим, что метод целесообразно применять, если модуль сравнения не очень большой. На практике для небольших модулей m целесообразнее, используя свойства сравнений, преобразовать коэффициенты так, чтобы правую часть можно было бы разделить на коэффициент у неизвестного x . Преобразованиям можно подвергать a или b , а также a и b сразу.

Наиболее часто выполняют следующие преобразования:

- замена коэффициентов абсолютно наименьшими вычетами;
- прибавление к b числа, кратного модулю;
- переход от a и b к сравнимым с ними числам, у которых есть общий делитель.

Теорема. При $(a, m) = 1$ решением сравнения $ax \equiv b \pmod{m}$ является класс $x \equiv a^{\varphi(m)-1} b \pmod{m}$. При решении линейных сравнений, особенно для больших модулей, является эффективным метод цепных дробей, основанный на следующей теореме:

Теорема. Если $\frac{P_0}{Q_0}, \frac{P_1}{Q_1}, \dots, \frac{P_{n-1}}{Q_{n-1}}, \frac{P_n}{Q_n} = \frac{m}{a}$ последовательность подходящих дробей разложения $\frac{m}{a}$ в цепную дробь и $(a, m) = 1$, то решением сравнения $ax \equiv b \pmod{m}$ является класс $x \equiv (-1)^n \cdot P_{n-1} \cdot b \pmod{m}$.

Неопределённое уравнение $ax + by = c$ можно свести к линейному сравнению $ax \equiv c \pmod{b}$ или $by \equiv c \pmod{a}$.

Теорема. Если модули $m_1, m_2, \dots, m_k$ попарно взаимно-просты, то система сравнений (2) имеет единственное решение по модулю $M = m_1 \cdot m_2 \cdot \dots \cdot m_k$, которое находится по формуле $x \equiv \sum_{i=1}^k M_i \xi_i b_i \pmod{M}$, где

$$M_i = \frac{M}{m_i}; M_i \xi_i \equiv 1 \pmod{m_i}, i = 1, \bar{k}.$$

теорема носит название китайской теоремы об остатках. Она выражает условие известной старинной китайской задачи о нахождении числа по его остаткам от деления на заданные числа.

Вопросы и задания

Вопросы к занятию:

1. Введите определения понятий сравнения с одной неизвестной и его решения, эквивалентных сравнений, тождественного сравнения, степени сравнения;
2. Перечислите преобразования, приводящие к эквивалентному сравнению;
3. Дайте определение линейного сравнения;
4. Сформулируйте и докажите теорему о числе решений линейного сравнения;
5. Расскажите о методе подбора при решении линейного сравнения;
6. Как решить линейное сравнение с помощью преобразования коэффициентов?
7. Расскажите о методе Эйлера и методе цепных дробей решения линейного сравнения.
8. Дайте определение системы линейных сравнений с одним неизвестным;
9. По какому модулю будет решение совместной системы линейных сравнений $x \equiv b_i \pmod{m_i}$, где $i = 1, 2, \dots, n$;

10. Сформулируйте и докажите Китайскую теорему об остатках. Какова её роль в решении систем линейных сравнений?
11. Сформулируйте и докажите условие совместности системы линейных сравнений $x \equiv b_i \pmod{m_i}$, где $i=1, 2, \dots, n$;
12. Расскажите о путях решения системы $x \equiv b_i \pmod{m_i}$, где $i=1, 2, \dots, n$;

Задания, решаемые в аудитории

- Для каждого из приведённых сравнений выясните вопрос о числе его решений
 - $35x \equiv 12 \pmod{14}$; б) $18x \equiv 28 \pmod{27}$
 - $16x \equiv 14 \pmod{34}$; г) $12x \equiv 16 \pmod{25}$.
- Решите сравнения путём испытания полной системы вычетов
 - $4x \equiv 5 \pmod{7}$; б) $2x \equiv -3 \pmod{6}$;
 - $5x \equiv 4 \pmod{6}$; г) $4x \equiv 6 \pmod{10}$.
- С помощью преобразования коэффициентов найдите решения сравнений
 - $3x \equiv 7 \pmod{13}$; б) $7x \equiv 15 \pmod{21}$; в) $16x \equiv 12 \pmod{28}$. Решите сравнения из №1.
- С помощью метода Эйлера решите сравнения
 - $8x \equiv 18 \pmod{10}$; б) $25x \equiv 4 \pmod{28}$.
- Решите сравнения методом цепных дробей
 - $124x \equiv 32 \pmod{216}$; б) $543x \equiv 421 \pmod{635}$; в) $361x \equiv 38 \pmod{541}$.
- Решите системы сравнений

а) $\begin{cases} x \equiv 6 \pmod{15} \\ x \equiv 18 \pmod{21} \\ x \equiv 3 \pmod{12} \end{cases}$	б) $\begin{cases} x \equiv 1 \pmod{25} \\ x \equiv 2 \pmod{4} \\ x \equiv 3 \pmod{7} \\ x \equiv 4 \pmod{9} \end{cases}$;	в) $\begin{cases} 4x \equiv 3 \pmod{7} \\ 5x \equiv 4 \pmod{11} \\ 11x \equiv 8 \pmod{13} \end{cases}$.
--	--	--

Задания для самостоятельной работы дома

- Для каждого из приведённых сравнений выясните вопрос о числе его решений
 - $34x \equiv 28 \pmod{44}$; б) $26x \equiv 65 \pmod{88}$
 - $26x \equiv 65 \pmod{91}$; г) $45x \equiv 27 \pmod{58}$.
- Решите сравнения путём испытания полной системы вычетов
 - $2x \equiv 7 \pmod{9}$; б) $7x \equiv 12 \pmod{13}$;
 - $8x \equiv 10 \pmod{14}$; г) $3x \equiv 5 \pmod{9}$.
- С помощью преобразования коэффициентов найдите решения сравнений
 - $11x \equiv 15 \pmod{18}$; б) $24x \equiv 36 \pmod{54}$; в) $15x \equiv 17 \pmod{21}$. Решите сравнения из №1.

4. С помощью метода Эйлера решите сравнения

а) $16x \equiv 4 \pmod{25}$; б) $18x \equiv 26 \pmod{42}$.

5. Решите сравнения методом цепных дробей

а) $37x \equiv 25 \pmod{117}$; б) $91x \equiv 143 \pmod{222}$;

6. Решите системы сравнений

а) $\begin{cases} x \equiv 4 \pmod{5} \\ x \equiv 1 \pmod{12} \\ x \equiv 7 \pmod{14} \end{cases}$; б) $\begin{cases} 5x \equiv 1 \pmod{12} \\ 5x \equiv 2 \pmod{8} \\ 7x \equiv 3 \pmod{11} \end{cases}$; в) $\begin{cases} 2x \equiv 7 \pmod{13} \\ 5x \equiv 8 \pmod{17} \\ 3x \equiv 7 \pmod{31} \\ 14x \equiv 35 \pmod{19} \end{cases}$.

7. При каких значениях параметра a система совместна

$$\begin{cases} x \equiv 3 \pmod{11} \\ x \equiv 11 \pmod{20} \\ x \equiv 1 \pmod{15} \\ x \equiv a \pmod{18} \end{cases}.$$

8. Припишите справа к числу 523 такие три цифры, чтобы полученное шестизначное число делилось на 7, 8 и 9.

Тема 6. Сравнения второй степени.

Тема занятия. Сравнения второй степени.

Цель занятия. Освоить решение сравнений второй степени.

Знания и умения, приобретаемые обучающимся в результате освоения темы, в рамках формируемых компетенций или их части

Знать: способы определения разрешимости сравнений второй степени; связь между сравнением и неопределённым уравнением;

Уметь: вычислять символы Лежандра и Якоби; строго доказывать и формулировать результаты в области теории чисел;

Владеть: навыками доказательств и формулировки утверждений в области теории чисел; доказательствами основных теорем курса

Актуальность темы. Тема важна для формирования теоретико-числовой культуры.

Теоретическая часть

Сравнением второй степени называется сравнение вида

$$Ax^2 + Bx + C \equiv 0 \pmod{M} \quad (1).$$

Сравнение второй степени (1) равносильно неопределённому уравнению второй степени вида

$$Ax^2 + Bx + C = My \quad (2).$$

Двучленным сравнением второй степени называется сравнение вида

$$x^2 \equiv a \pmod{m} \quad (3).$$

Если сравнение (3) разрешимо, то a называется квадратичным вычетом по модулю m . Если сравнение (3) неразрешимо, то a называется квадратичным невычетом по модулю m .

Рассмотрим двучленное сравнение по нечётному простому модулю.

Пусть дано сравнение:

$$x^2 \equiv a \pmod{p}, \quad (6)$$

где $(a, p) = 1, (2, p) = 1$.

Тогда решение этого сравнения следует искать среди чисел приведённой системы вычетов по модулю p .

Для отыскания решений достаточно подставлять в (6) только положительные значения $1; 2; \dots; \frac{p-1}{2}$.

При этом в левой части получаются числа

$$1^2; 2^2; 3^2; \dots; \left(\frac{p-1}{2}\right)^2 \quad (7)$$

Разрешимыми будут только такие сравнения (6), в которых число a сравнимо с одним из чисел ряда (7). Таким образом, ряд (7) состоит из квадратичных вычетов по $\text{mod } p$. Таким образом, количество квадратичных выче-

тов из разных классов по модулю p равно $\frac{p-1}{2}$. Очевидно, число квадратичных невычетов тоже равно $\frac{p-1}{2}$.

Теорема (критерий Эйлера) Число a , которое не делится на нечётное простое число p , является квадратичным вычетом по модулю p тогда и только тогда, когда

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}, \quad (8)$$

и квадратичным невычетом тогда и только тогда, когда

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \quad (9)$$

Эффективным способом выяснения будет ли число a квадратичным вычетом или невычетом является символ Лежандра.

Пусть p - нечётное простое число и a не делится на p . Символ Лежандра называется символ вида

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{если } a - \text{квадратичный вычет по mod } p, \\ -1, & \text{если } a - \text{квадратичный невычет по mod } p. \end{cases} \quad (10)$$

Читается $\left(\frac{a}{p}\right)$ - «символ Лежандра a по отношению к p », a - числитель, p - знаменатель символа.

Свойства символа Лежандра:

$$1^0. \text{ Если } a \equiv b \pmod{p}, \text{ то } \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

2⁰. $\left(\frac{1}{p}\right) = 1$, т.е. 1 – квадратичный вычет для любого нечётного простого p , т.к. сравнение $x^2 \equiv 1 \pmod{p}$ всегда разрешимо.

$$3^0. \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

$$\textbf{Следствие.} \left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{если } p \equiv 1 \pmod{4} \\ -1, & \text{если } p \equiv 3 \pmod{4}. \end{cases}$$

$$4^0. \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$$

$$\textbf{Следствие.} \left(\frac{a^2}{p}\right) = 1, \left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right).$$

$$5^0. \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Следствие. Если $p = 8m \pm 1$, то

$$\frac{p^2 - 1}{8} = \frac{(8m \pm 1)^2 - 1}{8} = \frac{64m^2 \pm 16m}{8} = 8m^2 \pm 2m \equiv 0 \pmod{2}.$$

Если $p = 8m \pm 3$, то

$$\frac{p^2 - 1}{8} = \frac{(8m \pm 3)^2 - 1}{8} = \frac{64m^2 \pm 48m + 8}{8} = 8m^2 \pm 6m + 1 \equiv 1 \pmod{2}.$$

Поэтому $\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{для } p = 8m \pm 1, \\ -1, & \text{для } p = 8m \pm 3. \end{cases}$

6⁰. (Закон взаимности) Если p и q нечётные простые числа, то, или

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

Или

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot \left(\frac{p}{q}\right).$$

(11)

Следствие. Если хотя бы одно из чисел p или q имеет форму $4m+1$, то показатель в правой части (11) чётный, и $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$.

Если и p или q имеет форму $4m+3$, то показатель в правой части (11) нечётный, и $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$.

Вопросы и задания

Вопросы к занятию:

1. Запишите сравнение n -ой степени по простому модулю. Сформулируйте и докажите теоремы об эквивалентных преобразованиях этого сравнения;
2. Сформулируйте и докажите теорему о числе решений сравнения n -ой степени по простому модулю. В каком случае это сравнение будет иметь n решений?
3. Сформулируйте и докажите теорему Вильсона. Какова её роль?
4. Как привести сравнение по составному модулю к системе сравнений?
5. Введите понятие сравнения второй степени. Как это сравнение привести к двучленному сравнению?
6. Дайте определения квадратичного вычета и квадратичного невычета;
7. Критерий Эйлера для определения квадратичного вычета по нечётному простому модулю. Докажите эту теорему;
8. Определите символ Лежандра и укажите его свойства;
9. Дайте определение символу Якоби и укажите его свойства;
10. Расскажите о решении сравнения второй степени по составному модулю.

Задания, решаемые в аудитории

1. С помощью критерия Эйлера установите, какие числа из приведённой системы наименьших положительных вычетов по модулю 11 являются квадратичными вычетами по этому модулю.
2. Вычислите символ Лежандр
а) $\left(\frac{63}{131}\right)$; б) $\left(\frac{257}{571}\right)$.
3. С помощью символа Лежандра установите, имеют ли сравнения решения
а) $x^2 \equiv 6 \pmod{7}$; б) $x^2 \equiv 10 \pmod{13}$; в) $x^2 \equiv 13 \pmod{17}$.
4. Решите сравнения, предварительно приведя их к двучленным
а) $3x^2 + 7x + 8 \equiv 0 \pmod{17}$; б) $5x^2 + x + 4 \equiv 0 \pmod{13}$.
5. Покажите, что если p – простое число вида $4k + 3$ и a – квадратичный вычет по модулю p , то сравнение $x^2 \equiv a \pmod{p}$ имеет решения $x^2 \equiv \pm a^{k+1} \pmod{p}$. Используя этот результат решите сравнение $x^2 \equiv 2 \pmod{311}$.
6. Докажите, что уравнение $11y = 5x^2 - 7$ неразрешимо в целых числах.
7. Установите, проходит ли парабола $73y = x^2 - 37$ через целочисленные точки.

Задания для самостоятельной работы дома

1. Пользуясь критерием Эйлера, найдите классы квадратичных вычетов по модулю 17.
2. Вычислите символ Лежандр
а) $\left(\frac{35}{97}\right)$; б) $\left(\frac{47}{383}\right)$; в) $\left(\frac{734}{997}\right)$; г) $\left(\frac{324}{613}\right)$.
3. С помощью символа Лежандра установите, имеют ли сравнения решения
а) $x^2 \equiv 3 \pmod{11}$; б) $x^2 \equiv 12 \pmod{13}$; в) $x^2 \equiv 16 \pmod{47}$.
4. Решите сравнения, предварительно приведя их к двучленным
а) $3x^2 + 4x + 7 \equiv 0 \pmod{31}$;
б) $5x^2 - 11x + 16 \equiv 0 \pmod{41}$;
в) $4x^2 - 11x - 3 \equiv 0 \pmod{23}$.
5. Покажите, что если p – простое число вида $8k + 5$ и a – квадратичный вычет по модулю p , то сравнение $x^2 \equiv a \pmod{p}$ имеет решения $x \equiv \pm a^{k+1} \cdot 2^{(2k+1)t} \pmod{p}$, где $t = 0$ и 1 .
6. Решите неопределённое уравнение $13y = x^2 - 21x + 110$.
7. Решите сравнение $5x^2 - 4x - 1 \equiv 0 \pmod{143}$.
8. Установите, проходит ли парабола $443y = x^2 - 152$ через целочисленные точки.

Тема 7. Первообразные корни и индексы. Степенные вычеты.

Тема занятия. Первообразные корни и индексы. Степенные вычеты

Цель занятия. Формирование понятий показатель числа, первообразный корень, индекс числа.

Знания и умения, приобретаемые обучающимся в результате освоения темы, в рамках формируемых компетенций или их части

Знать: теорему о существовании первообразных корней; определение индексов и их свойства;

Уметь: решать линейные, степенные и показательные сравнения с помощью индексирования;

Владеть: навыками доказательств и формулировки утверждений в области теории чисел; доказательствами основных теорем курса

Актуальность темы. Тема важна для формирования метода решения сравнений.

Теоретическая часть

Сравнение вида $a^x \equiv b \pmod{m}$ называется показательным. Изучение таких сравнений сводится к изучению сравнений вида

$$a^x \equiv 1 \pmod{m}. \quad (1)$$

Если $(a, m) = 1$, то по теореме Эйлера $a^{\varphi(m)} \equiv 1 \pmod{m}$, следовательно сравнение (1) при $(a, m) = 1$ всегда имеет решение.

Наименьшее положительное решение δ сравнения (1) называется показателем числа a по модулю m , или говорят, что число a

принадлежит показателю δ по модулю m . Записывают $a \in \delta \pmod{m}$.

Числа, принадлежащие показателю $\delta = \varphi(m)$, называются первообразными корнями по модулю m .

Показатель числа a по модулю m надо искать среди делителей $\varphi(m)$.

Замечание. Первообразные корни существуют только по модулям, $m = 2, 4, p^\alpha, 2p^\alpha$, где p – простое нечётное число, $\alpha \geq 1$.

Первообразные корни по модулям p^α и $2p^\alpha$ можно находить, пользуясь теоремой:

Теорема. Пусть $c = \varphi(m)$ и $g_1, g_2, \dots, g_k$ – различные простые делители числа c . Для того, чтобы число g , взаимно простое с модулем m , было первообразным корнем по модулю m , необходимо и достаточно, чтобы это g не удовлетворяло ни одному из сравнений

$$g^{\frac{c}{q_1}} \equiv 1 \pmod{m}, g^{\frac{c}{q_2}} \equiv 1 \pmod{m}, \dots, g^{\frac{c}{q_k}} \equiv 1 \pmod{m}. \quad (6)$$

Пусть g – первообразный корень по простому модулю p , тогда числа $g^0, g^1, \dots, g^{p-2}$ представляют собой приведённую систему вычетов по

модулю p .

Так как для любого простого p существуют первообразные корни, то приведённую систему вычетов можно составить указанным способом. Таким образом, для любого числа a , взаимно простого с p , найдётся единственное число g^k , принадлежащее тому же классу по модулю p , что и a , т.е.

$$g^k \equiv a \pmod{p}, \text{ где } 0 \leq k \leq p-2. \quad (7)$$

Пусть $(a, p)=1$, g – первообразный корень по модулю p . Если выполняется сравнение (7), то число k называется индексом числа a по модулю p при основании g и обозначается $k = \text{ind}_g a$.

Свойства индексов.

$$1^0. \text{ind}_g(ab) \equiv \text{ind}_g a + \text{ind}_g b \pmod{p-1}.$$

$$2^0. \text{ind}_g a^k \equiv k \cdot \text{ind}_g a \pmod{p-1}.$$

$$3^0. \text{ind}_g \frac{a}{b} \equiv \text{ind}_g a - \text{ind}_g b \pmod{p-1}.$$

$$4^0. \text{ind}_g g \equiv 1 \pmod{p-1}, g - \text{первообразный корень}.$$

$$5^0. \text{ind}_g 1 \equiv 0 \pmod{p-1}.$$

$$6^0. \text{Если } a \equiv b \pmod{p}, g - \text{первообразный корень, то } \text{ind}_g a \equiv \text{ind}_g b \pmod{p-1}.$$

Двучленным сравнением называется сравнение вида $Ax^n \equiv B \pmod{m}$.

Это сравнение всегда можно привести к виду $x^n \equiv a \pmod{m}$. Ограничимся случаем сравнения по простому модулю

$$x^n \equiv a \pmod{p}.$$

(9)

Теорема(критерий разрешимости двучленного сравнения). Двучленное сравнение по простому модулю(9) разрешимо тогда и только тогда, когда выполняется условие

$$a^{\frac{p-1}{d}} \equiv 1 \pmod{p}, \quad (12)$$

Число a называется вычетом n -ой степени по простому модулю p , если $a \not\equiv p$ и сравнение $x^n \equiv a \pmod{p}$ имеет решения.

Число a называется невычетом n -ой степени по простому модулю, если сравнение $x^n \equiv a \pmod{p}$ не имеет решения.

Вопросы и задания

Вопросы к занятию:

1. Запишите показательное сравнение и дайте определение показателя числа по данному модулю. Как найти показатель числа?
2. Введите понятие первообразного корня по данному модулю. Как определить первообразные корни?

3. Перечислите и докажите свойства показателей;
4. Сформулируйте и докажите теорему Гаусса о существовании первообразных корней по простому модулю;
5. По каким модулям существуют первообразные корни? Расскажите о первообразных корнях по модулям p^α и $p^{2\alpha}$, где p – простое число.
6. Введите понятие индекса числа по простому модулю;
7. Перечислите и докажите свойства индексов;
8. Как составить таблицу индексов и таблицу антииндексов? Для чего эти таблицы используются?
9. По каким модулям существуют индексы?
10. Введите понятие двучленного сравнения n -ой степени;
11. Укажите критерий разрешимости двучленного сравнения n -ой степени;
12. Дайте определение степенного вычета и степенного невычета n -ой степени;
13. Как с помощью таблицы индексов найти все классы вычетов n -ой степени по простому модулю?
14. Перечислите свойства индексов;
15. Расскажите о решении линейного сравнения с помощью индексирования;
16. Расскажите о решении степенного сравнения с помощью индексирования;
17. Расскажите о решении показательного сравнения с помощью индексирования. По какому модулю получим решение в этом случае?

Задания, решаемые в аудитории

1. Найдите показатель числа a по модулю m , если
 - а) $a = 5, m = 7$; б) $a = 12, m = 17$; в) $a = 10, m = 19$.
2. Найдите все первообразные корни по модулю $p = 31$.
3. Составьте таблицу индексов и антииндексов для модуля $p = 19$.
4. Индексированием найдите показатели, которым принадлежат все числа от 2 до $p - 1$ по простым модулям
 - а) $p = 7$; б) $p = 17$.
5. Индексированием установите, являются ли первообразными корнями по модулю 59 числа
 - а) 2; б) 6; в) 12; г) 32; д) 47.
6. Найдите первообразные корни по модулям
 - а) $m = 9$; б) $m = 18$.
7. Составьте таблицу индексов по модулю $m = 18$.
8. Зная, что по модулю 73 $\text{ind}_5 54 \equiv 26 \pmod{72}$, найдите по этому же модулю $\text{ind}_{11} 54$ (11 – первообразный корень по модулю 73).

Задания для самостоятельной работы дома

1. Пользуясь критерием Эйлера и применением индексов определите, какие из чисел 12, 13, 14, 15, 16, 17, 18 являются квадратичными вычетами по модулю

- а) 19; б) 43; в) 61.
2. Пользуясь таблицами индексов найдите остаток от деления
а) 341^{245} на 89; б) $53^{29} \cdot 43^{17}$ на 37.
3. С помощью индексирования решите показательные сравнения
а) $16^x \equiv 5 \pmod{61}$; б) $12^x \equiv 40 \pmod{47}$; в)
 $19^x \equiv 27 \pmod{83}$;
г) $5^x \equiv 49 \pmod{61}$; д) $7^x \equiv 80 \pmod{97}$; е)
 $46^x \equiv 17 \pmod{53}$.
4. Методом индексирования решите линейные сравнения
а) $12x \equiv 57 \pmod{43}$; б) $42x \equiv 50 \pmod{59}$; в)
 $31x \equiv 18 \pmod{61}$;
г) $37x \equiv 82 \pmod{47}$; д) $125x \equiv 7 \pmod{79}$; е)
 $228x \equiv 317 \pmod{1517}$.
5. Решите двучленные сравнения, применяя индексирование
а) $x^{35} \equiv 17 \pmod{67}$; б) $x^{27} \equiv 39 \pmod{43}$; в) $x^9 \equiv 59 \pmod{71}$;
г) $x^2 \equiv -28 \pmod{83}$; д) $27x^{14} \equiv 15 \pmod{41}$; е)
 $8x^{26} \equiv 37 \pmod{41}$.

Тема 8. Арифметические приложения теории сравнений.

Тема занятия. Систематические числа. Нахождение остатков от деления. Вывод признаков делимости.

Цель занятия. Научить находить остатки от деления и выводить признаки делимости, опираясь на теорию сравнений.

Знания и умения, приобретаемые обучающимся в результате освоения темы, в рамках формируемых компетенций или их части

Знать: теоретическую базу для нахождения остатков от деления и признаков делимости; теоретические основы определения длины периода и предпериода систематической дроби и проверки правильности арифметических действий;

Уметь: выводить признаки делимости в различных системах счисления; проверять правильность арифметических вычислений;

Владеть: навыками доказательств и формулировки утверждений в области теории чисел; доказательствами основных теорем курса; методом определения длины периода систематической дроби.

Актуальность темы. Тема важна для развития навыков решения олимпиадных задач.

Теоретическая часть

Способ замены данного числа N другим числом, чтобы вычисления остатка от деления на m значительно упростилось был предложен французским математиком Б. Паскалем (1623-1662).

Пусть

$$N = a_n g^n + a_{n-1} g^{n-1} + \dots + a_1 g + a_0.$$

Обозначим абсолютно наименьший вычет числа g^k по модулю m через r_k , так что

$$g_k \equiv r_k \pmod{m}, k = 0, 1, \dots, n.$$

Тогда

$$N \equiv R_m \pmod{m}, \quad \text{где}$$

$$R_m = a_n r_n + a_{n-1} r_{n-1} + \dots + a_1 r_1 + a_0 r_0.$$

Отсюда следует, что число N при делении на m даёт такой же остаток, как и R_m .

Рассмотренный выше способ отыскания остатков при делении чисел может быть использован при выводе признаков делимости, так как число N делится на m , когда R_m делится на m .

Теорема1. Пусть $(m, 10) = 1, 10 \in \delta = k \pmod{m}$ и число N записано в виде (2) в десятичной системе счисления. Число N делится на m тогда и только тогда, когда на m делится сумма чисел, которые получаются при разбиении справа налево цифровой записи числа N на грани по k цифр в каждой грани.

Замечание. Сформулированный признак делимости на m всегда будет таков, что количество цифр в каждой грани не больше $\varphi(m)$. Наименее удобен этот признак, когда k максимальное.

Теорема 2. Пусть N записано в десятичной системе счисления в виде (2). Число N делится на 2^k (на 5^k) тогда и только тогда, когда на 2^k (на 5^k) делится на число, имеющее те же цифры, что и последние k цифр числа N .

Теорема 3. Пусть $(m, 10) = 1$, $10^l \equiv -1 \pmod{m}$ и N записано в десятичной системе счисления. Число N делится на m тогда и только тогда, когда на m делится сумма взятых попеременно со знаком плюс и минус чисел, которые получаются при разбиении справа налево цифровой записи числа N на грани по l цифр в каждой грани.

Замечание. Приведённые теоремы можно сформулировать для системы счисления с любым основанием g .

Пусть $w = \frac{l}{m}$, $0 < w < 1$. Запишем это число в q -чной системе счисления:

$$w = (0, a_1 a_2 \dots a_n a_{n+1} \dots)_g, \quad (4)$$

где $a_i \in \{0, 1, \dots, g-1\}$.

Найдём формулу для вычисления цифры a_n .

Умножим (4) на g^n :

$$g^n w = (a_1 a_2 \dots a_n, a_{n+1} \dots)_g \quad (5)$$

Возьмем целую часть от обеих частей равенства (5):

$$[g^n w] = (a_1 a_2 \dots a_n)_g \quad (6)$$

Аналогично

$$[g^{n-1} w] = (a_1 a_2 \dots a_{n-1})_g \quad (7)$$

Умножим (7) на g :

$$g[g^{n-1} w] = (a_1 a_2 \dots a_{n-1} 0)_g \quad (8)$$

Вычитая из (6) равенство (8), получаем формулу для вычисления цифры a_n , стоящей на n -м месте после запятой в числе w

$$a_n = [g^n w] - g[g^{n-1} w]. \quad (9)$$

Теорема (о длине периода q -чной дроби). Если $(g, m) = 1$, то длина периода получающегося при обращении рационального числа $w = \frac{l}{m}$ ($0 < w < 1$) в

q -чную дробь равна показателю δ числа g по $\text{mod } m$.

Замечание 1. Период при обращении обыкновенной дроби в систематическую зависит только от знаменателя дроби, т.е. все дроби имеющие одинаковый знаменатель имеют одинаковую длину периода при обращении в систематическую дробь.

Замечание 2. Наибольшую длину периода имеют дроби $w = \frac{l}{m}$, для которых основание системы g - первообразный корень по $\text{mod } m$.

Теория сравнения даёт удобный способ проверки правильности арифметических действий.

Пусть при сложении получено $N_1 + N_2 = N$ и $N_1 \equiv r_1 (\text{mod } m)$, $N_2 \equiv r_2 (\text{mod } m)$, $N \equiv r (\text{mod } m)$.

Если сложение выполнено правильно, то $r_1 + r_2 \equiv r (\text{mod } m)$.

Аналогично, из правильности соотношений

$$N_1 - N_2 = N \text{ следует } r_1 - r_2 \equiv r (\text{mod } m),$$

$$N_1 \cdot N_2 = N \text{ следует } r_1 \cdot r_2 \equiv r (\text{mod } m).$$

Замечание. Для проверки соотношения $\frac{N_1}{N_2} = N$ представляем его в виде $N_1 = N \cdot N_2$.

Таким образом, при проверке большие числа заменяют на небольшие, сравнимые с ними по модулю.

Применение этого способа проверки имеет смысл только тогда, когда нахождение остатков r_i по $\text{mod } m$ осуществляется легко и быстро. Поэтому в качестве модуля m выбирают число $m = 9$ или (и) $m = 11$.

Способ «Проверки с помощью девятки». Каждое число, записанное в десятичной системе счисления, сравнимо с суммой его цифр по модулю 9. Для каждого числа вычисляют остаток от деления на 9 суммы цифр. Производя действия на числами, производят такие же действия над этими остатками. Результат рассматриваемых действий над этими остатками должен отличаться от суммы цифр искомого результата на число кратное 9. Если ошибка кратна 9, то она замечена не будет.

Способ «Проверки с помощью одиннадцати». По модулю $m = 11$ каждое число, записанное в десятичной системе счисления, будет сравнимо с разностью суммы цифр, стоящих на нечётном месте, и суммы цифр, стоящих на чётном месте. Для каждого числа вычисляют остаток от деления на 11 разности между суммами цифр, стоящих на чётном и нечётном местах. Результат рассматриваемых действий над этими остатками должен отличаться

от разности сумм цифр на чётном и нечётном местах искомого результат на число кратное 11. Если ошибка кратна 11, то она не будет обнаружена.

Замечание. При сложных вычислениях имеет смысл производить две проверки с помощью $m = 9$ и с помощью $m = 11$. Тогда необнаруженными могут быть только ошибки кратные 99.

Вопросы и задания

Вопросы к занятию:

1. Дайте определение систематической записи числа;
2. Расскажите о способе нахождения остатка от деления на число, предложенном Б. Паскалем;
3. Как вывести признаки делимости, используя теорию сравнений? Какие признаки делимости Вы знаете? Выведите эти признаки;
4. Выведите функцию цифры числа;
5. Сформулируйте и докажите теорему о длине периода десятичной дроби;
6. Какие обыкновенные дроби имеют наибольшую длину периода при обращении в систематическую дробь?
7. Как используется теория сравнений для проверки правильности результатов арифметических действий?
8. Сформулируйте способы проверки арифметических действий с помощью «девятки» и с помощью «одиннадцати».

Задания, решаемые в аудитории

1. Установите признак делимости, общий для чисел 7, 11, 13.
2. Делятся ли числа
а) 973 126; б) 96 736 068; в) 385 073 689
на 7, 11 или 13.
3. Найдите остаток от деления 34521_7 на 6.
4. Для каких чисел в системе счисления с $q = 13$ признаки делимости аналогичны признакам делимости на 3 в десятичной системе счисления.
5. Определите длину периода при обращении следующих обыкновенных дробей в десятичные:
а) $\frac{1}{31}$; б) $\frac{1}{11 \cdot 13 \cdot 17}$; в) $\frac{1}{4 \cdot 53 \cdot 73}$.
6. Укажите длину периода и количество цифр перед первым периодом при обращении в десятичную дробь рационального числа со знаменателем 1150.
7. Найдите вид периодической дроби для $\frac{107}{143}$, зная, что
 $\frac{1}{11} = 0,(09)$, $\frac{1}{13} = 0,(076923)$.
8. Проверьте правильность выполнения следующих арифметических действий:

- а) $25\,041 + 91\,382 = 116\,423$;
- б) $42\,932 - 18\,265 = 24\,667$;
- в) $8\,264 \cdot 5\,201 = 42\,981\,064$;
- г) $28\,342 : 383 = 74$.

Задания для самостоятельной работы дома

1. Установите признак делимости, общий для чисел 3, 9, 37.
2. Делятся ли числа
а) 20 794; б) 11 200 122; в) 2 575 163
на 37.
3. Найдите остаток от деления на 37 чисел
а) 27 877 165; б) 2 348 544.
4. Для каких чисел в системе счисления с $q = 25$ признаки делимости аналогичны признакам делимости на 3 в десятичной системе счисления.
5. Определите длину периода при обращении следующих обыкновенных дробей в десятичные:
а) $\frac{1}{2 \cdot 11}$; б) $\frac{1}{17 \cdot 37}$; в) $\frac{1}{5 \cdot 29 \cdot 43}$.
6. Укажите длину периода и количество цифр перед первым периодом при обращении в десятичную дробь рационального числа со знаменателем 2 380.
7. Найдите вид периодической дроби для $\frac{123}{133}$, зная, что
 $\frac{1}{7} = 0,(142857)$, $\frac{1}{19} = 0,(052631578947368421)$.
8. Проверьте правильность выполнения следующих арифметических действий:
а) $208\,973 + 163\,786 = 372\,759$;
б) $13\,547 - 9\,865 = 3\,685$;
в) $3745 \cdot 8067 = 30\,210\,915$;
г) $266\,377 : 2993 = 89$.

Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

Перечень основной литературы:

1. Бухштаб А. А. Теория чисел Электронный ресурс / Бухштаб А. А.: учебное пособие для вузов. - 5-е изд., стер. - Санкт-Петербург: Лань, 2020. - 384 с. - ISBN 978-5-8114-5836-3, экземпляров неограничено
2. Виноградов И. М. Основы теории чисел Электронный ресурс / Виноградов И. М. - 14-е изд., стер. - Санкт-Петербург: Лань, 2020. - 176 с. - ISBN 978-5-8114-5329-0, экземпляров неограничено

3. Джамбетов Э. М. Теория чисел в примерах и задачах Электронный ресурс / Джамбетов Э. М., Тарамова Х. С.: учебное пособие. - Грозный: ЧГПУ, 2018. - 66 с. - ISBN 978-5-00128-100-9, экземпляров неограничено

Перечень дополнительной литературы:

1. Грибанов В. У. Сборник упражнений по теории чисел / В.У. Грибанов, П.И. Титов. - Москва: Издательство «Просвещение», 1964. - 144 с. - <http://biblioclub.ru/>, экземпляров неограничено

2. Данилова Т. В. Теория чисел: Задачи с примерами решений: учебное пособие / Т.В. Данилова; Министерство образования и науки Российской Федерации ; Северный (Арктический) федеральный университет имени М.В. Ломоносова. - Архангельск: САФУ, 2015. - 104 с. - <http://biblioclub.ru/>. - Библиогр. в кн. - ISBN 978-5-261-01004-3, экземпляров неограничено

3. Михелович Ш. Х. Теория чисел / Ш.Х. Михелович; Академия наук СССР; Институт истории естествознания и техники; отв. ред. И. Б. Погребыский. - Москва: Высшая школа, 1962. - 260 с.: ил. - <http://biblioclub.ru/>. - ISBN 978-5-4475-7997-5, экземпляров неограничено

4. Михелович Ш.Х. Теория чисел. - Изд. 2-е, перераб. и доп. - М.: Высшая школа, 1967. - 336 с., экземпляров 15

5. Нестеренко Ю. В. Теория чисел: учебник для студентов вузов / Ю. В. Нестеренко. - М.: Академия, 2008. - 266 с. - (Высшее профессиональное образование. Физико-математические науки). - Библиогр.: с. 262. - ISBN 978-5-7695-4646-4, экземпляров 15

6. Терентьев И. В. Теория чисел и ее применение. Справочник Электронный ресурс / Терентьев И. В.: учебное пособие для студентов всех специальностей. - Санкт-Петербург: СПбГЛТУ, 2010. - 142 с. - ISBN 978-5-9239-0171-9, экземпляров неограничено

Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

Перечень основной литературы:

1. Бухштаб, А. А. Теория чисел Электронный ресурс / Бухштаб А. А. : учебное пособие для вузов. - 5-е изд., стер. - Санкт-Петербург: Лань, 2020. - 384 с. - ISBN 978-5-8114-5836-3, экземпляров неограничено
2. Виноградов, И. М. Основы теории чисел Электронный ресурс / Виноградов И. М. - 14-е изд., стер. - Санкт-Петербург : Лань, 2020. - 176 с. - ISBN 978-5-8114-5329-0, экземпляров неограничено
3. Джембетов, Э. М. Теория чисел в примерах и задачах Электронный ресурс / Джембетов Э. М., Тарамова Х. С. : учебное пособие. - Грозный : ЧГПУ, 2018. - 66 с. - ISBN 978-5-00128-100-9, экземпляров неограничено

Перечень дополнительной литературы:

1. Грибанов, В. У. Сборник упражнений по теории чисел / В.У. Грибанов, П.И. Титов. - Москва : Издательство «Просвещение», 1964. - 144 с. - <http://biblioclub.ru/>, экземпляров неограничено
2. Данилова, Т. В. Теория чисел: Задачи с примерами решений : учебное пособие / Т.В. Данилова ; Министерство образования и науки Российской Федерации ; Северный (Арктический) федеральный университет имени М.В. Ломоносова. - Архангельск : САФУ, 2015. - 104 с. - <http://biblioclub.ru/>. - Библиогр. в кн. - ISBN 978-5-261-01004-3, экземпляров неограничено
3. Михелович, Ш. Х. Теория чисел / Ш.Х. Михелович ; Академия наук СССР ; Институт истории естествознания и техники ; отв. ред. И. Б. Погребысский. - Москва : Высшая школа, 1962. - 260 с. : ил. - <http://biblioclub.ru/>. - ISBN 978-5-4475-7997-5, экземпляров неограничено
4. Михелович, Ш.Х. Теория чисел. - Изд. 2-е, перераб. и доп. - М. : Высшая школа, 1967. - 336 с., экземпляров 15
5. Нестеренко, Ю. В. Теория чисел : учебник для студентов вузов / Ю. В. Нестеренко. - М. : Академия, 2008. - 266 с. - (Высшее профессиональное образование. Физико-математические науки). - Библиогр.: с. 262. - ISBN 978-5-7695-4646-4, экземпляров 15
6. Терентьев, И. В. Теория чисел и ее применение. Справочник Электронный ресурс / Терентьев И. В. : учебное пособие для студентов всех специальностей. - Санкт-Петербург : СПбГЛТУ, 2010. - 142 с. - ISBN 978-5-9239-0171-9, экземпляров неограничено

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»**

Методические указания
для обучающихся по организации и проведению самостоятельной работы
по дисциплине «Теории чисел»
для студентов направления подготовки
01.03.02 «Прикладная математика и информатика»

СОДЕРЖАНИЕ

Введение	61
Технологическая карта самостоятельной работы обучающихся	64
План-график выполнения студентами выполнения студентами самостоятельной работы	65
Методические указания по изучению дисциплины для студентов	66

Введение

Самостоятельная работа – планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль за работой студента).

Самостоятельная работа студента является важным видом учебной и научной деятельности студента. Федеральным государственным образовательным стандартом предусматривается значительный объем времени из общей трудоемкости дисциплины на самостоятельную работу. В связи с этим, обучение включает в себя две, практически одинаковые по объему и взаимовлиянию части – процесса обучения и процесса самообучения. Поэтому самостоятельная работа должна стать эффективной и целенаправленной работой студента.

Концепцией модернизации российского образования определены основные задачи профессионального образования – подготовка квалифицированного работника соответствующего уровня и профиля, конкурентоспособного на рынке труда, компетентного, ответственного, свободно владеющего своей профессией и ориентированного в смежных областях деятельности, способного к эффективной работе по специальности на уровне мировых стандартов, готового к постоянному профессиональному росту, социальной и профессиональной мобильности.

Решение этих задач невозможно без повышения роли самостоятельной работы студентов над учебным материалом, усиления ответственности преподавателей за развитие навыков самостоятельной работы, за стимулирование профессионального роста студентов, воспитание творческой активности и инициативы.

Самостоятельная работа студента предполагает, прежде всего, его научно-исследовательскую и практическую деятельность, поскольку именно эти виды учебной работы в первую очередь готовят к самостоятельному выполнению профессиональных задач. Конечной целью самостоятельной работы является организация самостоятельной познавательной деятельности, формирование умения самостоятельно анализировать информацию, выделять главное и второстепенное.

Ведущая цель организации и осуществления СРС должна совпадать с целью обучения студента – подготовкой бакалавра с высшим образованием. При организации СРС важным и необходимым условием становятся формирование умения самостоятельной работы для приобретения знаний, навыков и возможности организации учебной и научной деятельности.

Целью самостоятельной работы студентов является овладение фундаментальными знаниями, профессиональными умениями и навыками деятель-

ности по профилю, опытом творческой, исследовательской деятельности. Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Задачами СРС являются:

- систематизация и закрепление полученных теоретических знаний и практических умений студентов;
- углубление и расширение теоретических знаний;
- формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развитие исследовательских умений;
- использование материала, собранного и полученного в ходе самостоятельных занятий на семинарах, на практических и лабораторных занятиях, при написании курсовых и выпускной квалификационной работ, для эффективной подготовки к итоговым зачетам и экзаменам.

Самостоятельная работа включает в себя:

подготовку к аудиторным занятиям (лекциям, практическим занятиям) и выполнение соответствующих заданий;

самостоятельную работу над отдельными модулями (темами) дисциплины в соответствии с рабочей программой;

написание рефератов, докладов;

подготовку к практическим занятиям и выполнение предусмотренных ими заданий;

подготовку ко всем видам аттестаций;

подготовку презентаций по темам (части темы).

В результате освоения дисциплины студент должен:

Знать: определение общих форм и закономерностей теории чисел; свойства делимости целых чисел; теорему о делении с остатками; свойства простых и составных чисел; теорему о бесконечности множества простых чисел; основную теорему арифметики; способы нахождения наибольшего общего делителя (НОД) и наименьшего общего кратного (НОК) натуральных чисел; взаимосвязь между НОДом и НОКом двух чисел; основные арифметические функции и их приложения; определение и свойства цепных дробей; определение и свойства числовых сравнений; теоремы Эйлера и Ферма; теорему о числе решений линейного сравнения и методы их нахождения; Китайскую теорему об остатках и способы решения системы линейных сравнений;

способы определения разрешимости сравнений второй степени; связь между сравнением и неопределенным уравнением; теорему о существовании первообразных корней; определение индексов и их свойства; понятия алгебраических и трансцендентных чисел.

Уметь: находить наибольший общий делитель двух чисел с помощью алгоритма Евклида; находить НОД и НОК чисел, зная их канонические разложения; с помощью решета Эратосфена находить простые числа на заданном интервале; вычислять и использовать числовые функции для решения практических задач; применять теоремы Эйлера и Ферма для нахождения остатков от деления; разлагать обыкновенные дроби в непрерывные; представлять квадратичные иррациональности в виде бесконечных цепных дробей; использовать аппарат цепных дробей в приближенных вычислениях; находить полную и приведенную системы вычетов; решать линейные сравнения различными методами; решать диофантовы уравнения первой степени; находить решение системы линейных сравнений; вычислять символы Лежандра и Якоби; решать линейные, степенные и показательные сравнения с помощью индексирования; строго доказывать и формулировать результаты в области теории чисел; доказывать трансцендентность чисел π и e .

Владеть: методами решения задач на делимость; методами решения уравнений и неравенств в целых числах; аппаратом цепных дробей; методами решения линейных сравнений; навыками доказательств и формулировки утверждений в области теории чисел; доказательствами основных теорем курса.

Технологическая карта самостоятельной работы обучающегося

Коды реализуемых компетенций, индикатора(ов)	Вид деятельности студентов	Средства и технологии оценки	Объем часов, в том числе		
			СРС	Контактная работа с преподавателем	Всего
3 семестр					
ПК-1 ИД-1 ПК-1 ИД-2 ПК-1 ИД-3	Подготовка к коллоквиуму 1	Коллоквиум	10.13	0.37	10.50
ПК-1 ИД-1 ПК-1 ИД-2 ПК-1 ИД-3	Подготовка к коллоквиуму 2	Коллоквиум	11.26	0.74	12.00
ПК-1 ИД-1 ПК-1 ИД-2 ПК-1 ИД-3	Подготовка индивидуальных проектов	Индивидуальный проект	7.12	0.38	7.5
ПК-1 ИД-1 ПК-1 ИД-2 ПК-1 ИД-3	Подготовка к лабораторному занятию	Собеседование	17.8	0.95	18.75
ПК-1 ИД-1 ПК-1 ИД-2 ПК-1 ИД-3	Решение разноуровневых заданий	Индивидуальное задание	17.8	0.95	18.75
Итого за 3 семестр			64.11	3.39	67.50
Итого			64.13	3.38	67.50

ПЛАН-ГРАФИК ВЫПОЛНЕНИЯ СТУДЕНТАМИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Вид деятельности студентов	Итоговый продукт самостоятельной работы	Средства и технологии оценки	Время сдачи
Подготовка к коллоквиуму 1	Ответы на вопросы коллоквиума 1	Коллоквиум	занятие 7
Самотестирование, подготовка к тестированию	тестирование	Тестирование	занятие 13
Подготовка к коллоквиуму 2	Ответы на вопросы коллоквиума 2	Коллоквиум	занятие 18
Выполнение разноразрядных заданий, решение разноразрядных задач. Тема «Делимость в кольце целых чисел»	решение комплекта заданий 1	Индивидуальное задание	занятие 1
Выполнение разноразрядных заданий, решение разноразрядных задач. Тема «Простые и составные числа»	решение комплекта заданий 2	Индивидуальное задание	занятие 2
Выполнение разноразрядных заданий, решение разноразрядных задач. Тема «Методы решения линейных сравнений»	решение комплекта заданий 3	Индивидуальное задание	занятие 8
Выполнение разноразрядных заданий, решение разноразрядных задач. Тема «Решение систем сравнений первой степени»	решение комплекта заданий 4	Индивидуальное задание	занятие 10
Выполнение разноразрядных заданий, решение разноразрядных задач. Тема «Первообразные корни и индексы»	решение комплекта заданий 5	Индивидуальное задание	занятие 13

Вид деятельности студентов	Итоговый продукт самостоятельной работы	Средства и технологии оценки	Время сдачи
Подготовка индивидуального проекта	Проект	Индивидуальное задание	Занятия 7,13,18 (в зависимости от темы проекта)

Методические указания по изучению дисциплины для студентов

Изучение дисциплины следует начинать с проработки рабочей программы, особое внимание, уделяя целям и задачам, структуре и содержанию курса.

При подготовке к занятиям студент должен просмотреть конспекты лекций, рекомендованную литературу по данной теме; подготовиться к ответу на контрольные вопросы.

Успешное изучение курса требует от студентов посещения лекций, активной работы на практических занятиях, выполнения всех учебных заданий преподавателя, ознакомления основной и дополнительной литературой.

Запись лекции – одна из форм активной самостоятельной работы студентов, требующая навыков и умения кратко, схематично, последовательно и логично фиксировать основные положения, выводы, обобщения, формулировки. Культура записи лекции – один из важнейших факторов успешного и творческого овладения знаниями. Последующая работа над текстом лекции воскрешает в памяти ее содержание, позволяет развивать аналитическое мышление. В конце лекции преподаватель оставляет время (5-10 минут) для того, чтобы студенты имели возможность задать уточняющие вопросы по изучаемому материалу.

Лекции имеют в основном обзорный характер и нацелены на освещение наиболее трудных и дискуссионных вопросов, а также призваны способствовать формированию навыков работы с научной литературой. Предполагается также, что студенты приходят на лекции, предварительно проработав соответствующий учебный материал по источникам, рекомендуемым программой.

Работа с конспектом лекций предполагает просмотр конспекта в тот же день после занятий, пометку материала конспекта, который вызывает затруднения для понимания. Попытайтесь найти ответы на затруднительные вопросы, используя рекомендуемую литературу. Если самостоятельно не удалось разобраться в материале, сформулируйте вопросы и обратитесь за помощью к преподавателю на консультации или ближайшей лекции. Регулярно отводите время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам.

Как слушать лекцию.

1. Выделяйте основные положения. Нельзя понять и запомнить все, что говорит лектор, однако можно выделить основные моменты. Для этого необходимо обращать внимание на вводные слова, словосочетания, фразы, которые используются, как правило, для перехода к новым положениям, выводам и обобщениям.

2. Старайтесь поэтапно (в момент завершения вопроса, подвопроса, тезиса и т.п.) анализировать и обобщать материал. Это готовит базу для его экономной, свернутой записи.

3. Старайтесь опережать речь лектора, предугадать дальнейшее содержание. С каждым случаем удачи улучшается понимание и запоминание отдельных положений лекции. Даже при неудачах качество восприятия лекции повышается, т.к. вы имеете возможность сравнить ваши предложения и утверждения лектора.

4. Будьте постоянно готовы слушать лекцию до конца, не поддавайтесь соблазну «отдохнуть» на длинной лекции.

Как правильно записывать лекцию.

1. Подготовьте специальную тетрадь для записи лекций: оставьте поля (для вопросов, мелких пометок и рисунков, собственных замечаний и т.д.), оставляйте при записи между строчками интервал (для дополнений, подчеркиваний и т.п.).

2. Не пишите лекцию дословно, подробно записывайте основную информацию, а дополнительные и вспомогательные сведения - очень кратко.

3. Применяйте систему условных сокращений:

а) сокращение общепринятых вспомогательных слов: так как, например (т.к., напр.), так далее (т.д.), таким образом, главным образом (т.о., гл.обр.), смотри (см), может быть (м.б.), так называемый (т.н.), какой-либо (к-л.), который (кт. или ктр.), несколько (неск.), чтобы (чбы.) и т.д.

б) аббревиатуры для ключевых слов курса, например, теория и методика развития математических представлений у детей дошкольного возраста (ТМРМП), формирование математических представлений (ФМП) и другие.

4. При записи и работе над конспектом лекции используйте условные знаки:

I - прочитать ещё раз, Y – важно, Z - законспектировать ! – смело, ? – непонятно, S – слишком сложно, A – согласен, N - ново и др.

Как работать с книгой

При работе с книгой необходимо подобрать литературу, научиться правильно ее читать, вести записи. Для подбора литературы в библиотеке используются алфавитный и систематический каталоги.

Важно помнить, что рациональные навыки работы с книгой - это всегда большая экономия времени и сил.

Правильный подбор учебников рекомендуется преподавателем, читающим лекционный курс. Необходимая литература может быть также указана в методических разработках по данному курсу.

Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и вычисления (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода).

При изучении любой дисциплины большую и важную роль играет самостоятельная индивидуальная работа.

Особое внимание следует обратить на определение основных понятий курса. Студент должен подробно разбирать примеры, которые поясняют такие определения, и уметь строить аналогичные примеры самостоятельно. Нужно добиваться точного представления о том, что изучаешь. Полезно составлять опорные конспекты. При изучении материала по учебнику полезно в тетради (на специально отведенных полях) дополнять конспект лекций. Там же следует отмечать вопросы, выделенные студентом для консультации с преподавателем.

Выводы, полученные в результате изучения, рекомендуется в конспекте выделять, чтобы они при перечитывании записей лучше запоминались.

Опыт показывает, что многим студентам помогает составление листа опорных сигналов, содержащего важнейшие и наиболее часто употребляемые формулы и понятия. Такой лист помогает запомнить формулы, основные положения лекции, а также может служить постоянным справочником для студента.

Различают два вида чтения; первичное и вторичное. Первичное - это внимательное, неторопливое чтение, при котором можно остановиться на трудных местах. После него не должно остаться ни одного непонятого слова. Содержание не всегда может быть понятно после первичного чтения.

Задача вторичного чтения - полное усвоение смысла целого (по счету это чтение может быть и не вторым, а третьим или четвертым).

Правила самостоятельной работы с литературой.

Как уже отмечалось, самостоятельная работа с учебниками и книгами (а также самостоятельное теоретическое исследование проблем, обозначенных преподавателем на лекциях) – это важнейшее условие формирования у себя научного способа познания. Основные советы здесь можно свести к следующим:

- Составить перечень книг, с которыми Вам следует познакомиться; «не старайтесь запомнить все, что вам в ближайшее время не понадобится, – советует студенту и молодому ученому Г. Селье, – запомните только, где это можно отыскать» (Селье, 1987. С. 325).

- Сам такой перечень должен быть систематизированным (что необходимо для семинаров, что для экзаменов, что пригодится для написания курсовых и дипломных работ, а что Вас интересует за рамками официальной

учебной деятельности, то есть что может расширить Вашу общую культуру...).

- Обязательно выписывать все выходные данные по каждой книге (при написании курсовых и дипломных работ это позволит очень сэкономить время).

- Разобраться для себя, какие книги (или какие главы книг) следует прочитать более внимательно, а какие – просто просмотреть.

- При составлении перечней литературы следует посоветоваться с преподавателями и научными руководителями (или даже с более подготовленными и эрудированными сокурсниками), которые помогут Вам лучше сориентироваться, на что стоит обратить большее внимание, а на что вообще не стоит тратить время...

- Естественно, все прочитанные книги, учебники и статьи следует конспектировать, но это не означает, что надо конспектировать «все подряд»: можно выписывать кратко основные идеи автора и иногда приводить наиболее яркие и показательные цитаты (с указанием страниц).

- Если книга – Ваша собственная, то допускается делать на полях книги краткие пометки или же в конце книги, на пустых страницах просто сделать свой «предметный указатель», где отмечаются наиболее интересные для Вас мысли и обязательно указываются страницы в тексте автора (это очень хороший совет, позволяющий экономить время и быстро находить «избранные» места в самых разных книгах).

- Если Вы раньше мало работали с научной литературой, то следует выработать в себе способность «воспринимать» сложные тексты; для этого лучший прием – научиться «читать медленно», когда Вам понятно каждое прочитанное слово (а если слово незнакомое, то либо с помощью словаря, либо с помощью преподавателя обязательно его узнать), и это может занять немалое время (у кого-то – до нескольких недель и даже месяцев); опыт показывает, что после этого студент каким-то «чудом» начинает буквально заглатывать книги и чуть ли не видеть «сквозь обложку», стоящая это работа или нет...

- «Либо читайте, либо перелистывайте материал, но не пытайтесь читать быстро... Если текст меня интересует, то чтение, размышление и даже фантазирование по этому поводу сливаются в единый процесс, в то время как вынужденное скорочтение не только не способствует качеству чтения, но и не приносит чувства удовлетворения, которое мы получаем, размышляя о прочитанном», – советует Г. Селье (Селье, 1987. – С. 325-326).

- Есть еще один эффективный способ оптимизировать знакомство с научной литературой – следует увлечься какой-то идеей и все книги просматривать с точки зрения данной идеи. В этом случае студент (или молодой ученый) будет как бы искать аргументы «за» или «против» интересующей его идеи, и одновременно он будет как бы общаться с авторами этих книг по по-

воду своих идей и размышлений... Проблема лишь в том, как найти «свою» идею...

Чтение научного текста является частью познавательной деятельности. Ее цель – извлечение из текста необходимой информации. От того насколько осознанна читающим собственная внутренняя установка при обращении к печатному слову (найти нужные сведения, усвоить информацию полностью или частично, критически проанализировать материал и т.п.) во многом зависит эффективность осуществляемого действия.

Выделяют четыре основные установки в чтении научного текста:

1. информационно-поисковый (задача – найти, выделить искомую информацию)
2. усваивающая (усилия читателя направлены на то, чтобы как можно полнее осознать и запомнить как сами сведения излагаемые автором, так и всю логику его рассуждений)
3. аналитико-критическая (читатель стремится критически осмыслить материал, проанализировав его, определив свое отношение к нему)
4. творческая (создает у читателя готовность в том или ином виде – как отправной пункт для своих рассуждений, как образ для действия по аналогии и т.п. – использовать суждения автора, ход его мыслей, результат наблюдения, разработанную методику, дополнить их, подвергнуть новой проверке).

С наличием различных установок обращения к научному тексту связано существование и нескольких видов чтения:

1. библиографическое – просматривание карточек каталога, рекомендательных списков, сводных списков журналов и статей за год и т.п.;
2. просмотрное – используется для поиска материалов, содержащих нужную информацию, обычно к нему прибегают сразу после работы со списками литературы и каталогами, в результате такого просмотра читатель устанавливает, какие из источников будут использованы в дальнейшей работе;
3. ознакомительное – подразумевает сплошное, достаточно подробное прочтение отобранных статей, глав, отдельных страниц, цель – познакомиться с характером информации, узнать, какие вопросы вынесены автором на рассмотрение, провести сортировку материала;
4. изучающее – предполагает доскональное освоение материала; в ходе такого чтения проявляется доверие читателя к автору, готовность принять изложенную информацию, реализуется установка на предельно полное понимание материала;
5. аналитико-критическое и творческое чтение – два вида чтения близкие между собой тем, что участвуют в решении исследовательских задач. Первый из них предполагает направленный критический анализ, как самой информации, так и способов ее получения и подачи автором; второе – поиск тех суждений, фактов, по которым или в связи с которыми, читатель считает нужным высказать собственные мысли.

Из всех рассмотренных видов чтения основным для студентов является изучающее – именно оно позволяет в работе с учебной литературой накапливать знания в различных областях. Вот почему именно этот вид чтения в рамках учебной деятельности должен быть освоен в первую очередь. Кроме того, при овладении данным видом чтения формируются основные приемы, повышающие эффективность работы с научным текстом.

Основные виды систематизированной записи прочитанного:

1. Аннотирование – предельно краткое связное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;
2. Планирование – краткая логическая организация текста, раскрывающая содержание и структуру изучаемого материала;
3. Тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;
4. Цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;
5. Конспектирование – краткое и последовательное изложение содержания прочитанного.

Конспект – сложный способ изложения содержания книги или статьи в логической последовательности. Конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи. Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.

Методические рекомендации по составлению конспекта:

1. Внимательно прочитайте текст. Уточните в справочной литературе непонятные слова. При записи не забудьте вынести справочные данные на поля конспекта;
2. Выделите главное, составьте план;
3. Кратко сформулируйте основные определения и теоремы, определите формулы, которые надо запомнить;
4. Законспектируйте материал, четко следуя пунктам плана. Записи следует вести четко, ясно.
5. Грамотно записывайте формулировки определений и теорем.

В тексте конспекта желательно приводить не только тезисные положения, но и их доказательства. При оформлении конспекта необходимо стремиться к емкости каждого предложения. Для уточнения и дополнения необходимо оставлять поля.

Овладение навыками конспектирования требует от студента целеустремленности, повседневной самостоятельной работы.

Методические рекомендации по подготовке к лабораторным занятиям

Для того чтобы лабораторные и практические занятия приносили максимальную пользу, необходимо помнить, что упражнение и решение задач

проводятся по вычитанному на лекциях материалу и связаны, как правило, с детальным разбором отдельных вопросов лекционного курса. Следует подчеркнуть, что только после усвоения лекционного материала с определенной точки зрения (а именно с той, с которой он излагается на лекциях) он будет закрепляться на практических занятиях как в результате обсуждения и анализа лекционного материала, так и с помощью решения проблемных ситуаций, задач. При этих условиях студент не только хорошо усвоит материал, но и научится применять его на практике, а также получит дополнительный стимул (и это очень важно) для активной проработки лекции.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы (задачи), то нужно сравнить их и выбрать самый рациональный. Полезно до начала вычислений составить краткий план решения проблемы (задачи). Решение проблемных задач или примеров следует излагать подробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями, схемами, чертежами и рисунками.

Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом. Полученный ответ следует проверить способами, вытекающими из существа данной задачи. Полезно также (если возможно) решать несколькими способами и сравнить полученные результаты. Решение задач данного типа нужно продолжать до приобретения твердых навыков в их решении.

Для подготовки к занятию **дома**

1. Прочитайте конспект лекции, соответствующий теме занятия. Запомните основные определения.
2. Изучите рекомендуемую литературу по вопросам, выносимым на обсуждение.
3. Найдите ответы на теоретические задания для развития и контроля владения компетенциями. Подготовьтесь к ответам на эти вопросы на занятии.
4. Законспектируйте ответы на теоретические задания, которые не содержатся в Вашем конспекте лекции по указанной теме.
5. Изучите разобранные примеры решения типовых задач и законспектируйте их решение в рабочую тетрадь.

На занятии по указанию преподавателя

1. Дайте ответы на вопросы из теоретических заданий для развития и контроля владения компетенциями.
2. В рабочей тетради и на доске решите практические задания для развития и контроля владения компетенциями из заданий, решаемых в аудитории

Дома закрепите полученные практические умения и навыки, решая практические задания для развития и контроля владения компетенциями из заданий для самостоятельной работы дома.

Правила подготовки к зачетам и экзаменам:

- Лучше сразу сориентироваться во всем материале и обязательно расположить весь материал согласно экзаменационным вопросам (или вопросам, обсуждаемым на семинарах), эта работа может занять много времени, но все остальное – это уже технические детали (главное – это ориентировка в материале!).

- Сама подготовка связана не только с «запоминанием». Подготовка также предполагает и переосмысление материала, и даже рассмотрение альтернативных идей.

- Сначала студент должен продемонстрировать, что он «усвоил» все, что требуется по программе обучения, и лишь после этого он вправе высказать иные, желательно аргументированные точки зрения.

Чтобы выполнить весь объем самостоятельной работы, необходимо заниматься по 3 - 5 часов ежедневно. Начинать самостоятельные внеаудиторные занятия следует с первых же дней семестра, пропущенные дни будут потеряны безвозвратно, компенсировать их позднее усиленными занятиями без снижения качества работы и ее производительности невозможно. Первые дни семестра очень важны для того, чтобы включиться в работу, установить определенный порядок, равномерный ритм на весь семестр. Ритм в работе - это ежедневные самостоятельные занятия, желательно в одни и те же часы, при целесообразном чередовании занятий с перерывами для отдыха. Вначале для того, чтобы организовать ритмичную работу, требуется сознательное напряжение воли. Как только человек втянулся в работу, принуждение снижается, возникает привычка, работа становится потребностью.

Если порядок в работе и ее ритм установлены правильно, то студент изо дня в день может работать, не снижая своей производительности и не перегружая себя. Правильная смена одного вида работы другим позволяет отдыхать, не прекращая работы.

Таким образом, первая задача организации внеаудиторной самостоятельной работы – это составление расписания, которое должно отражать время занятий, их характер (теоретический курс, практические занятия, графические работы, чтение), перерывы на обед, ужин, отдых, сон, проезд и т.д. Расписание не предопределяет содержания работы, ее содержание неизбежно будет изменяться в течение семестра. Порядок же следует закрепить на весь семестр и приложить все усилия, чтобы поддерживать его неизменным (кроме исправления ошибок в планировании, которые могут возникнуть из-за недооценки объема работы или переоценки своих сил).

При однообразной работе человек утомляется больше, чем при работе разного характера. Однако не всегда целесообразно заниматься многими

учебными дисциплинами в один и тот же день, так как при каждом переходе нужно вновь сосредоточить внимание, что может привести к потере времени. Наиболее целесообразно ежедневно работать не более чем над двумя-тремя дисциплинами.

Начиная работу, не нужно стремиться делать вначале самую тяжелую ее часть, надо выбрать что-нибудь среднее по трудности, затем перейти к более трудной работе. И напоследок оставить легкую часть, требующую не столько больших интеллектуальных усилий, сколько определенных моторных действий (черчение, построение графиков и т.п.).

Самостоятельные занятия потребуют интенсивного умственного труда, который необходимо не только правильно организовать, но и стимулировать. При этом очень важно уметь поддерживать устойчивое внимание к изучаемому материалу. Выработка внимания требует значительных волевых усилий. Именно поэтому, если студент замечает, что он часто отвлекается во время самостоятельных занятий, ему надо заставить себя сосредоточиться. Подобную процедуру необходимо проделывать постоянно, так как это является тренировкой внимания. Устойчивое внимание появляется тогда, когда человек относится к делу с интересом.

Следует правильно организовать свои занятия по времени: 50 минут - работа, 5-10 минут - перерыв; после 3 часов работы перерыв - 20-25 минут. Иначе нарастающее утомление повлечет неустойчивость внимания. Очень существенным фактором, влияющим на повышение умственной работоспособности, являются систематические занятия физической культурой. Организация активного отдыха предусматривает чередование умственной и физической деятельности, что полностью восстанавливает работоспособность человека.

Самопроверка

После изучения определенной темы по записям в конспекте и учебнику, а также решения достаточного количества соответствующих задач на практических занятиях и самостоятельно студенту рекомендуется, используя лист опорных сигналов, воспроизвести по памяти определения, выводы формул, формулировки основных положений и доказательств.

В случае необходимости нужно еще раз внимательно разобраться в материале.

Иногда недостаточность усвоения того или иного вопроса выясняется только при изучении дальнейшего материала. В этом случае надо вернуться назад и повторить плохо усвоенный материал. Важный критерий усвоения теоретического материала - умение решать задачи или пройти тестирование по пройденному материалу. Однако следует помнить, что правильное решение задачи может получиться в результате применения механически заученных формул без понимания сущности теоретических положений.

Консультации

Если в процессе самостоятельной работы над изучением теоретического материала или при решении задач у студента возникают вопросы, разрешить которые самостоятельно не удастся, необходимо обратиться к преподавателю для получения у него разъяснений или указаний. В своих вопросах студент должен четко выразить, в чем он испытывает затруднения, характер этого затруднения. За консультацией следует обращаться и в случае, если возникнут сомнения в правильности ответов на вопросы самопроверки.