

Федеральное агентство по образованию
Государственное образовательное учреждение
высшего профессионального образования
«Рязанский государственный университет имени С.А.Есенина»

Согласовано:

Декан
физико-математического факультета

Кирияков Б.С.

« _____ » _____ 2009 г.

Утверждено на заседании кафедры
математики и МОМД
Протокол № 6 от «18» ноября 2009 г.
Зав. кафедрой доктор пед. н., канд. физ-мат. н.,
профессор _____ Назиев А.Х.

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ПО ДИСЦИПЛИНЕ

Теория чисел

Для специальности 032100 – математика с дополнительной специальностью

Факультет: физико-математический,

Отделение математика и информатика: курс 3, семестр 5

Отделение математика и физика: курс 3, семестр 5

Всего часов (включая самостоятельную работу) – 90

Составитель: **С.А. Моисеев**, кандидат педагогических наук, доцент

Рязань, 2009

ПРОГРАММА КУРСА

Пояснительная записка

Настоящая программа разработана в соответствии с требованиями государственного образовательного стандарта подготовки специалистов по

специальности .032100.

Основная цель курса – дать начальные представления об алгебраической и аналитической теории чисел, в результате чего будущие учителя математики получат с одной стороны строгое обоснование своим школьным представлениям об арифметике, а с другой – импульс для более углубленного и осознанного изучения предмета. Значительное внимание в каждой части курса уделяется приемам и методам, которые могут быть использованы в практике школьного преподавания.

Первая часть почти целиком посвящается развитию и обоснованию вынесенного из средней школы понятия делимости. Вопрос о распределении простых чисел – первый фрагмент аналитической теории чисел. Систематическая запись числа позволяет обосновать позиционные системы счисления. Студенты должны научиться находить НОД и НОК нескольких чисел, выражать НОД линейно, использовать свойства простых и взаимно простых чисел для решения школьных задач на делимость, свободно оперировать в системах счисления по любому основанию, уметь переходить от одной системы к другой.

Теория сравнений и ее школьные приложения – основной материал второй части. Подробное изучение кольца вычетов играет значительную роль в алгебраическом развитии студентов. Студенты должны уметь сравнивать любые целые числа по любому модулю, строить таблицы сложения и умножения в любом кольце вычетов, вычислять любое значение функции Эйлера, применять теоремы Эйлера и Ферма к решению задач на делимость, решать сравнения перебором, решать разные варианты линейных сравнений и их систем, индексировать сравнения по простому модулю и решать на этой основе степенные и показательные сравнения, определять квадратичные вычеты, определять длину периода и предпериода систематической дроби, вычислять остатки числовых алгебраических выражений при делении нацелое число, формулировать и обосновывать признаки делимости.

В третьей части развивается новый для студентов аппарат цепных дробей, который продуктивно используется в решении некоторых теоретико-числовых задач. Студенты должны уметь обращать рациональное число в конечную цепную дробь и наоборот, обращать квадратичную иррациональность в периодическую цепную дробь и наоборот, находить рациональные приближения вещественных чисел с помощью подходящих дробей.

В четвертой части рассматривается важный для мировоззрения учителя математики вопрос об алгебраических и трансцендентных числах.

Предполагается, что изучение всех разделов сопровождается рассмотрением исторических сведений о развитии теории чисел.

Предусматривается проведение двух контрольных работ. Форму контрольных работ (аудиторная, домашняя, индивидуальное задание) выбирает преподаватель.

Содержание учебной дисциплины

1. Теория делимости

Отношение делимости и его свойства. Деление с остатком. Систематическая запись натурального числа.

Наибольший общий делитель. Алгоритм Евклида. Наименьшее общее кратное. Взаимно простые числа и их свойства.

Простые числа и их свойства. Основное свойство простого числа. Основная теорема арифметики. Каноническое разложение.

Решето Эратосфена. Бесконечность множества простых чисел. Неравенство Чебышева для $\pi(x)$.

Числовые функции. Число и сумма натуральных делителей. Мультипликативные функции. Функция антье и ее применение в теории чисел.

2. Теория сравнений

Отношение сравнения по модулю m и его свойства. Классы вычетов. Кольца классов вычетов. Поля вычетов по простому модулю. Обратимые классы. Полная и приведенная системы вычетов. Функция Эйлера. Теоремы Эйлера и Ферма.

Сравнения с неизвестной величиной и их свойства. Сравнения по простому модулю. Теорема Вильсона.

Сравнения первой степени. Неопределенные уравнения первой степени. Системы сравнений первой степени.

Сравнения по степени простого числа. Редукция сравнения по составному модулю к сравнению по степени простого числа и к сравнению по простому модулю.

Показатели чисел и классов по данному модулю. Число классов с заданным показателем. Теорема о существовании первообразного корня по простому модулю. Индексы чисел и классов по данному модулю. Приложения к решению сравнений.

Квадратичные вычеты и невычеты. Символ Лежандра.

Арифметические приложения теории сравнений: систематические дроби, вычисление остатков при делении на целое число, признаки делимости.

3. Цепные дроби

Конечные цепные дроби. Подходящие дроби и их свойства. Единственность представления рационального числа в виде конечной цепной дроби.

Бесконечные цепные дроби. Существование и единственность значения бесконечной цепной дроби. Представление действительных чисел цепными дробями. Теорема Лежандра о квадратичной иррациональности.

Приближение действительных чисел подходящими дробями. Теорема Дирихле и её применение к представлению простого числа $p \equiv 1 \pmod{4}$ в виде суммы двух квадратов.

4. Алгебраические и трансцендентные числа

Алгебраические числа. Теорема Лиувилля.

Трансцендентные числа. Применение теоремы Лиувилля к построению трансцендентных чисел и к доказательству иррациональности.

Примерный тематический план

№ п/п	Раздел, тема	Всего часов	Ауд.	Лекции	Семи нар	СР
1	2	3	4	5	6	7
I.	Теория делимости 1. Отношение делимости и его свойства.					

	<p>Деление с остатком. Наибольший общий делитель. Алгоритм Евклида.</p> <p>Наименьшее общее кратное. Взаимно простые числа и их свойства.</p> <p>2. Простые числа и их свойства.</p> <p>Основное свойство простого числа.</p> <p>Основная теорема арифметики.</p> <p>Каноническое разложение.</p> <p>3. Решето Эратосфена. Бесконечность множества простых чисел. Неравенство Чебышева для $\pi(x)$.</p> <p>4. Числовые функции. Число и сумма натуральных делителей.</p> <p>Мультипликативные функции. Функция антье и ее применение в теории чисел.</p> <p>5. Систематическая запись натурального числа.</p>	6	4	3	1	2
	<p>Каноническое разложение.</p> <p>3. Решето Эратосфена. Бесконечность множества простых чисел. Неравенство Чебышева для $\pi(x)$.</p> <p>4. Числовые функции. Число и сумма натуральных делителей.</p> <p>Мультипликативные функции. Функция антье и ее применение в теории чисел.</p> <p>5. Систематическая запись натурального числа.</p>	6	4	3	1	2
	<p>4. Числовые функции. Число и сумма натуральных делителей.</p> <p>Мультипликативные функции. Функция антье и ее применение в теории чисел.</p> <p>5. Систематическая запись натурального числа.</p>	5	2	2		3
	<p>Мультипликативные функции. Функция антье и ее применение в теории чисел.</p> <p>5. Систематическая запись натурального числа.</p>	7	4	3	1	3
	<p>5. Систематическая запись натурального числа.</p>	4	2	1	1	2
II.	<p>Теория сравнений</p> <p>1. Отношение сравнимости по модулю и его свойства. Классы вычетов. Кольцо вычетов.</p> <p>2. Обратимые классы. Полная и приведенная системы вычетов. Поле вычетов по простому модулю. Функция Эйлера. Теоремы Эйлера и Ферма.</p> <p>3. Сравнения с неизвестной величиной и их свойства. Сравнения первой степени. Неопределенные уравнения первой степени. Системы сравнений первой степени.</p> <p>4. Сравнения по простому модулю. Теорема Вильсона.</p> <p>5. Сравнения по степени простого числа. Редукция сравнения по составному модулю к сравнению по степени простого числа и к сравнению по простому модулю.</p> <p>6. Показатели чисел и классов по данному модулю. Число классов с заданным показателем. Теорема о существовании первообразного корня по простому модулю. Индексы чисел и классов по данному модулю.</p> <p>Приложения к решению сравнений.</p> <p>7. Квадратичные вычеты и невычеты. Символ Лежандра.</p> <p>8. Арифметические приложения теории сравнений: систематические дроби, вычисление остатков при делении на</p>	5	3	2	1	2
	<p>2. Обратимые классы. Полная и приведенная системы вычетов. Поле вычетов по простому модулю. Функция Эйлера. Теоремы Эйлера и Ферма.</p> <p>3. Сравнения с неизвестной величиной и их свойства. Сравнения первой степени. Неопределенные уравнения первой степени. Системы сравнений первой степени.</p> <p>4. Сравнения по простому модулю. Теорема Вильсона.</p> <p>5. Сравнения по степени простого числа. Редукция сравнения по составному модулю к сравнению по степени простого числа и к сравнению по простому модулю.</p> <p>6. Показатели чисел и классов по данному модулю. Число классов с заданным показателем. Теорема о существовании первообразного корня по простому модулю. Индексы чисел и классов по данному модулю.</p> <p>Приложения к решению сравнений.</p> <p>7. Квадратичные вычеты и невычеты. Символ Лежандра.</p> <p>8. Арифметические приложения теории сравнений: систематические дроби, вычисление остатков при делении на</p>	5	3	2	1	2
	<p>3. Сравнения с неизвестной величиной и их свойства. Сравнения первой степени. Неопределенные уравнения первой степени. Системы сравнений первой степени.</p> <p>4. Сравнения по простому модулю. Теорема Вильсона.</p> <p>5. Сравнения по степени простого числа. Редукция сравнения по составному модулю к сравнению по степени простого числа и к сравнению по простому модулю.</p> <p>6. Показатели чисел и классов по данному модулю. Число классов с заданным показателем. Теорема о существовании первообразного корня по простому модулю. Индексы чисел и классов по данному модулю.</p> <p>Приложения к решению сравнений.</p> <p>7. Квадратичные вычеты и невычеты. Символ Лежандра.</p> <p>8. Арифметические приложения теории сравнений: систематические дроби, вычисление остатков при делении на</p>	8	5	2	3	3
	<p>4. Сравнения по простому модулю. Теорема Вильсона.</p> <p>5. Сравнения по степени простого числа. Редукция сравнения по составному модулю к сравнению по степени простого числа и к сравнению по простому модулю.</p> <p>6. Показатели чисел и классов по данному модулю. Число классов с заданным показателем. Теорема о существовании первообразного корня по простому модулю. Индексы чисел и классов по данному модулю.</p> <p>Приложения к решению сравнений.</p> <p>7. Квадратичные вычеты и невычеты. Символ Лежандра.</p> <p>8. Арифметические приложения теории сравнений: систематические дроби, вычисление остатков при делении на</p>	3	2	2		1
	<p>5. Сравнения по степени простого числа. Редукция сравнения по составному модулю к сравнению по степени простого числа и к сравнению по простому модулю.</p> <p>6. Показатели чисел и классов по данному модулю. Число классов с заданным показателем. Теорема о существовании первообразного корня по простому модулю. Индексы чисел и классов по данному модулю.</p> <p>Приложения к решению сравнений.</p> <p>7. Квадратичные вычеты и невычеты. Символ Лежандра.</p> <p>8. Арифметические приложения теории сравнений: систематические дроби, вычисление остатков при делении на</p>	2	1	1		1
	<p>6. Показатели чисел и классов по данному модулю. Число классов с заданным показателем. Теорема о существовании первообразного корня по простому модулю. Индексы чисел и классов по данному модулю.</p> <p>Приложения к решению сравнений.</p> <p>7. Квадратичные вычеты и невычеты. Символ Лежандра.</p> <p>8. Арифметические приложения теории сравнений: систематические дроби, вычисление остатков при делении на</p>	6	4	2	2	2
	<p>7. Квадратичные вычеты и невычеты. Символ Лежандра.</p> <p>8. Арифметические приложения теории сравнений: систематические дроби, вычисление остатков при делении на</p>	3	2	1	1	1
	<p>8. Арифметические приложения теории сравнений: систематические дроби, вычисление остатков при делении на</p>	6	4	2	2	2

	целое число, признаки делимости.					
III.	Цепные дроби 1. Цепные дроби. Подходящие дроби и их свойства. Существование и единственность значения цепной дроби. Конечные цепные дроби. 2. Представление действительных чисел цепными дробями. Теорема Лежандра о квадратичной иррациональности. Приближение действительных чисел подходящими дробями. Теорема Дирихле и ее применение к представлению простого числа $p \equiv 1 \pmod{4}$ в виде суммы двух квадратов.	7	4	3	1	3
IV.	Алгебраические и трансцендентные числа 1. Алгебраические числа. Теорема Лиувилля. 2. Трансцендентные числа. Применение теоремы Лиувилля к построению трансцендентных чисел и к доказательству иррациональности.	3	2	1	1	1
		7	4	3	1	3
	Итого:	90	54	36	18	36

Содержание практических занятий

Занятие 1. Систематические числа. Перевод из одной системы счисления в другую

[2]: С.49, №№ 20 – 25.

[6]: ИЗ 48 – ИЗ 49.

Занятие 2. Делимость целых чисел. НОД и НОК. Взаимно простые числа

[6]: ИЗ 47, ИЗ 51, ГЗ 27 – ГЗ 28АБ.

[6]: ГЗ 28 Б, ИЗ 50, ИЗ 54.

Занятие 3. Простые числа. Основная теорема арифметики. Применения числовых сравнений в арифметике

[2]: С.27, №№ 19, 20, 22.

[6]: ГЗ 28ВГД – ГЗ 30.

Занятия 4–5. Числовые функции. Функция Эйлера. Числовые сравнения

[2]: С.122, №№ 16 – 19, 24 – 26, 30 – 32.

[6]: ИЗ 56, ИЗ 57.

Занятие 6. Сравнения первой степени и неопределённые уравнения первой степени

[2]: С.138, №№ 18, 20, 24, 25, 17, 27.

[6]: ИЗ 58, ИЗ 60.

Занятие 7. Порядок элемента. Первообразные корни. Индексы

[6]: ИЗ 67, ИЗ 68.

Занятие 8–9. Конечные цепные дроби. Подходящие дроби. Их применения. Бесконечные периодические цепные дроби

[6]: ИЗ 61, ИЗ 62, ИЗ 63, ИЗ 64, ИЗ 65.

Критерии оценок знаний

Оценка «отлично» ставится при условии выполнения аудиторных контрольных работ, всех индивидуальных заданий и отчетностей, полном ответе на экзамене по билету.

Оценка «хорошо» ставится при тех же условиях и ответе на экзаменационный билет с 1–2 замечаниями не принципиального характера.

Оценка «удовлетворительно» ставится, если промежуточные отчетности и индивидуальные задания в течение семестра были выполнены с некоторыми замечаниями, а ответ на экзамене имеет существенные недостатки, при этом основные определения теории усвоены.

Перечень основных знаний, умений и навыков

В результате изучения дисциплины студент должен:

- *знать*:
- основные понятия курса теории чисел: теории делимости, теории сравнений, теории конечных и бесконечных цепных дробей;
- *уметь*:
- находить НОД и НОК нескольких чисел, выражать НОД линейно, использовать свойства простых и взаимно простых чисел для решения школьных задач на делимость;
- свободно оперировать в системах счисления по любому основанию, уметь переходить от одной системы к другой;
- сравнивать любые целые числа по любому модулю, строить таблицы сложения и умножения в любом кольце вычетов, вычислять любое значение функции Эйлера, применять теоремы Эйлера и Ферма к решению задач на делимость;
- решать сравнения перебором, решать разные варианты линейных сравнений и их систем, индексировать сравнения по простому модулю и решать на этой основе степенные и показательные сравнения, определять длину периода и предпериода систематической дроби, вычислять остатки числовых алгебраических выражений при делении на целое число, формулировать и обосновывать признаки делимости;
- обращать рациональное число в конечную цепную дробь и наоборот, обращать квадратическую иррациональность в периодическую цепную дробь

и наоборот, находить рациональные приближения вещественных чисел с помощью подходящих дробей;

- *владеть* соответствующими навыками при реализации указанных умений.

Литература

1. *Виноградов И.М.* Основы теории чисел. – М.: Наука, 1972.
2. *Казачек Н.А., Перлатов Г.Н., Виленкин Н.Я., Бородин А.И.* Алгебра и теория чисел. М.: Просвещение, 1984.
3. *Михелович Ш.Х.* Теория чисел. – М.: Высшая школа, 1967.
4. *Винберг Э.Б.* Алгебра многочленов. – М.: Просвещение, 1980.
5. *Кудреватов Г.А.* Сборник задач по теории чисел. – М.: Просвещение, 1970.
6. *Моисеев С.А., Суворов Н.М.* Задачник-практикум по алгебре и теории чисел. – Рязань: Изд-во РГПУ, 2006.

Перечень экзаменационных вопросов

1. Отношение делимости на Z . Деление с остатком.
2. НОД чисел.
3. Взаимно простые числа.
4. НОК чисел.
5. Простые числа. Основная теорема арифметики.
6. Расположение простых чисел в натуральном ряде.
7. Мультипликативные функции.
8. Функции целая и дробная часть числа.
9. Числовые сравнения.
10. Признаки делимости.
11. Кольца классов вычетов.
12. Полная и приведенная системы вычетов.
13. Функция Эйлера.
14. Теоремы Эйлера и Ферма.
15. Решение сравнений с переменной.
16. Теорема Вильсона.
17. Решение сравнений 1 степени.
18. Неопределенные уравнения 1 степени.
19. Системы линейных сравнений.
20. Сравнения степени n по составному модулю.
21. Порядок класса вычетов.
22. Первообразные корни. Индексы.
23. Обращение обыкновенных дробей в бесконечные десятичные дроби.
24. Конечные цепные дроби. Представление рационального числа в виде КЦД и его единственность.
25. Подходящие дроби.
26. Бесконечные цепные дроби.
27. Квадратические иррациональности и бесконечные периодические цепные дроби.
28. Приближение действительных чисел подходящими дробями.

Тематика контрольных работ

Темы контрольной работы № 1: свойства делимости целых чисел, НОД и НОК, числовые функции, систематические числа.

Темы контрольной работы № 2: числовые сравнения, неопределённые уравнения первой степени, теорема Эйлера и её использования в приложениях арифметики, конечные цепные дроби и их использование.

Приведём примерные задания для контрольных работ.

Контрольная работа № 1

1. Найти НОД и НОК чисел 3367 и 8099.
2. Доказать делимость в \mathbf{Z} $n^4 + 3n^3 - n^2 - 3n$ на 6.
3. Найти число и сумму натуральных делителей у данного числа 4520.
4. Выполнить действия в g -ичной системе счисления: $15(11)_{12} + 2724_{12}$.

Контрольная работа № 2

1. Решить в \mathbf{Z} неопределённое уравнение первой степени $53x + 47y = 100$.
2. Решить сравнение первой степени $8x \equiv 17 \pmod{31}$.
3. Найти остаток от деления 2^{15783} на 25.
4. Найти НОД и выразить его линейно, используя аппарат цепных дробей 3953 и 871.

Мы являемся сторонниками выполнения каждым студентом индивидуальных практических заданий. Поэтому при изучении данного курса мы заменяем контрольные работы выполнением системы индивидуальных заданий из задачника [6] (20 заданий). Это тем более необходимо, что данный курс имеет большое профессионально-педагогическое значение, в то время как объём часов, выделяемых на практические задания, явно недостаточен.

ПЛАН-КОНСПЕКТ КУРСА “ТЕОРИЯ ЧИСЕЛ”

ГЛАВА I. Теория делимости

§ 1. Отношение делимости. Деление с остатком. [1]: § 1.1, [2]: § 1.1.

Определение делимости целых чисел. $a \dot{=} b, b|a$.

Теорема 1. Свойства делимости

Для любых целых чисел имеют место следующие соотношения

$$1^\circ. a \dot{=} a.$$

$$2^\circ. a \dot{=} 1.$$

$$3^\circ. a \dot{=} b \quad \pm a \dot{=} \pm b.$$

$$4^\circ. 0 \dot{=} a;$$

$$5^\circ. a \dot{=} b \quad b \dot{=} c \quad a \dot{=} c.$$

$$6^\circ. a \dot{=} b \quad b \dot{=} c \quad ua+vb \dot{=} c.$$

$$7^\circ. a \neq 0 \quad a \dot{=} b \quad |a| \quad |b|.$$

$$8^\circ. a \neq 0 \quad b \neq 0 \quad a \dot{=} b \quad b \dot{=} a \quad a = \pm b.$$

Определение деления с остатком.

Теорема 2. О делении с остатком

Любое целое число a можно разделить с остатком на любое целое число $b \neq 0$. Это деление осуществляется единственным образом.

Определение систематического представления натурального числа.

Теорема 3. Любое целое неотрицательное число a может быть представлено, причем единственным образом, в виде

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

где $g \in \mathbb{N}, g \geq 1, 0 \leq a_k < g-1$ при всех $0 \leq k \leq n$.

Запись: $\overline{a_n a_{n-1} \dots a_1 a_0}_g$.

Таблицы сложения и умножения в g -ичной системе счисления.

Перевод из одной системы счисления в другую: правила деления и умножения.

§ 2. НОД чисел. Алгоритм Евклида. [1]: § 1.2, [2]: § 1.2.

ОД и НОД системы чисел.

Теорема 1. Единственность НОД

Любые два НОД системы чисел совпадают, с точностью до знака, если они существуют.

(a_1, a_2, \dots, a_n) .

Алгоритм Евклида: описание алгоритма, конечность алгоритма.

Теорема 2. Существование НОД двух чисел

Для любых двух целых чисел, не равных нулю одновременно, их НОД существует. Он равен последнему, отличному от нуля, остатку алгоритма Евклида для этих двух чисел.

Следствие 1. Свойства НОД

1°. С точностью до знака, $(ac, bc) = (a, b)c$.

2°. Если t – ОД(a, b), то, с точностью до знака, $\left(\frac{a}{t}, \frac{b}{t}\right) = \frac{(a, b)}{t}$.

3°. Если $d = (a, b)$, то $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

4°. Если $d = (a, b)$, то существуют числа u, v такие, что $ua + vb = d$.

5°. Наибольший по модулю общий делитель чисел a и b является их НОД.

Теорема 3. Цепное правило

НОД нескольких чисел a_1, a_2, \dots, a_n существует. Он вычисляется по правилу $((\dots ((a_1, a_2), a_3), \dots, a_{n-1}), a_n)$.

Следствие 2. Свойства НОД 1°–5° двух чисел справедливы для любого конечного количества чисел.

§ 3. Взаимно простые числа. [1]: § 1.2.

Теорема 1. Критерий взаимной простоты чисел

Числа a и b взаимно простые тогда и только тогда, когда существуют целые числа u и v такие, что $ua + vb = 1$.

Теорема 2. Свойства взаимно простых чисел

1°. $(a, c) = (b, c) = 1 \implies (ab, c) = 1$.

2°. $ab \dot{\vdash} c \implies (a, c) = 1 \implies b \dot{\vdash} c$.

3°. $a \dot{\vdash} b \implies a \dot{\vdash} c \implies (b, c) = 1 \implies a \dot{\vdash} bc$.

Обобщение результатов теорем 1 и 2 на случай n чисел.

§ 4. НОК чисел. [1]: § 1.3, [2]: § 1.3.

ОК и НОК системы чисел.

Теорема 1. Единственность НОК

Любые два НОК системы чисел совпадают, с точностью до знака, если они существуют.

$[a_1, a_2, \dots, a_n]$.

Теорема 2. Существование НОК двух чисел

Для любых двух целых чисел a и b , не равных нулю одновременно, их НОК существует. Он равен $\frac{ab}{(a, b)}$.

Следствие 1. Свойства НОК двух чисел

1°. С точностью до знака, $[ac, bc] = [a, b]c$.

2°. Если t – ОД(a, b), то, с точностью до знака, $\left[\frac{a}{t}, \frac{b}{t}\right] = \frac{[a, b]}{t}$;

3°. Наименьшее по модулю общее кратное чисел a и b является их НОК.

Теорема 3. Цепное правило

НОК нескольких чисел a_1, a_2, \dots, a_n существует. Оно вычисляется по правилу $[[\dots [[a_1, a_2], a_3], \dots, a_{n-1}], a_n]$.

Следствие 2. Свойства НОК 1°–3° двух чисел справедливы для любого конечного количества чисел.

§ 5. Простые числа. Основная теорема арифметики. [1]: § 1.5, § 1.6, [2]: § 1.4.

Простые и составные числа.

Теорема 1. Свойства простых чисел

1°. p – простое $p \mid a \iff a = 1 \vee a = p$.

2°. Если p_1, p_2 – различные простые числа, то они не делятся друг на друга.

3°. p – простое $(\forall a)(a \not\mid p \implies (a, p) = 1)$.

4°. $a_1 a_2 \dots a_n \not\mid p \iff a_1 \not\mid p \vee a_2 \not\mid p \vee \dots \vee a_n \not\mid p$.

5°. $(\forall a \neq 1)(\exists p)(p \text{ – простое } \wedge a \not\mid p)$.

6°. Если $a \neq 1$ и a не делится ни на одно простое число $p \leq \sqrt{a}$, то a – простое число.

Теорема 2. Основная Теорема Арифметики

Всякое натуральное число, отличное от единицы, либо является простым числом, либо представляется в виде произведения простых чисел, причем такое представление единственное, с точностью до порядка следования множителей.

Каноническое разложение (факторизация) натурального числа.

Следствие 1. Всякое натуральное составное число имеет единственное каноническое разложение.

Следствие 2. Если a имеет каноническое разложение $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, то $b \mid a \iff b = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}$, где $0 \leq \beta_i \leq \alpha_i$ для всех $i = \overline{1, s}$.

Следствие 3. Правила отыскания НОД и НОК

Пусть $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$ – почти канонические разложения чисел a и b , то есть для всех $i = \overline{1, s}$ $0 \leq \beta_i \leq \alpha_i$, причем одно из них > 0 . Тогда

$$1^\circ. (a, b) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_s^{\gamma_s}, \text{ где } (\forall i = \overline{1, s}) (\gamma_i = \min\{\alpha_i, \beta_i\}.$$

$$2^\circ. [a, b] = p_1^{\delta_1} p_2^{\delta_2} \cdots p_s^{\delta_s}, \text{ где } (\forall i = \overline{1, s}) (\delta_i = \max\{\alpha_i, \beta_i\}.$$

§ 6. Расположение простых чисел в натуральном ряде. [2]: § 8.4.

Теорема 1. Множество простых чисел бесконечно.

Доказательство Евклида. Доказательство Эйлера.

Простые числа-близнецы. Существование отрезков произвольной длины, состоящих из составных чисел.

$\pi(x)$ = количество простых чисел на отрезке $[1, x]$.

$$\pi(x) \sim \frac{x}{\ln x - \alpha} \text{ – Лежандр, } \alpha = 1,08366.$$

Неравенство Чебышева: для достаточно больших x выполняются неравенства

$$0,92129 < \frac{\pi(x)}{x / \ln x} < 1,10555.$$

Ж. Адамар, Ш. Валле-Пуссен (1896): $\lim_{x \rightarrow \infty} \frac{\pi(x)}{x / \ln x}$ существует.

О распределении простых чисел в арифметических прогрессиях

Лежандр (1788): в любой арифметической прогрессии вида $kx+l$, где $(k, l) = 1$, содержится бесконечно много простых чисел.

П. Лежен-Дирихле (1837): доказал это утверждение.

Бесконечность простых чисел вида $4k+3$ и $6k+5$.

§ 7. Числовые функции. [1]: § 2.1, § 2.2, [2]: §§ 8.1–8.3.

А. Мультипликативные функции

Мультипликативные и вполне мультипликативные функции.

$$f(x) = x^\alpha.$$

Теорема 1. Свойства мультипликативных функций

1°. Если f – мультипликативная функция и числа a_1, a_2, \dots, a_n – попарно взаимно простые, то $f(a_1 a_2 \dots a_n) = f(a_1) f(a_2) \dots f(a_n)$.

2°. Если $f \neq 0$, то $f(1) = 1$.

3°. Произведение двух ненулевых мультипликативных функций также является

мультипликативной функцией.

4°. Если $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ – каноническое разложение числа m , то

$\sum_{d|m} f(d) = (1+f(p_1)+\dots+f(p_1^{\alpha_1}))(1+f(p_2)+\dots+f(p_2^{\alpha_2})) \dots (1+f(p_s)+\dots+f(p_s^{\alpha_s}))$, где слева стоит сумма всех значений f от делителей числа m .

Применения свойства 4°:

I. $f(x) = 1 = x^0: \tau(m)$.

II. $f(x) = x = x^1: \sigma(m)$.

Формулы для вычисления этих функций.

Теорема 2. Функции τ и σ мультипликативные, но не вполне мультипликативные.

Совершенные числа.

Теорема 3. Теорема Евклида-Эйлера о чётных совершенных числах

Чётное число m совершенно $m = 2^{k-1}(2^k-1)$, где $(2^k-1) = p$ – число простое.
Нечётные совершенные числа.

Б. Функция антье – целая часть числа

Теорема 4. Свойства функции антье

1°. $[x+y] = [x]+[y]$.

2°. $\left[\frac{x}{n}\right] = \left[\frac{[x]}{n}\right]$, если $n \in \mathbf{N}$.

3°. Если $b \in \mathbf{N}$, $a \in \mathbf{Z}$, то неполное частное от деления a на b равно $\left[\frac{a}{b}\right]$.

4°. При разложении $n!$ на простые множители показатель степени у простого

числа p , входящего в это разложение равен $\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \dots + \left[\frac{n}{p^k}\right] + \dots$, где сумма продолжается до появления нулевого слагаемого.

ГЛАВА 2. Теория сравнений

§ 1. Числовые сравнения. [1]: §§ 3.1–3.3, [2]: § 2.2.

Примечание. Числовые сравнения – конкретизация сравнения по идеалу для произвольного кольца.

$$a \equiv b \pmod{m}.$$

Теорема 1. Следующие утверждения равносильны:

1°. $a \equiv b \pmod{m}$.

2°. $a = b + mt$, $t \in \mathbf{Z}$.

3°. a и b равноостаточны при делении на m .

Теорема 2. Свойства числовых сравнений

1°. Отношение сравнения является отношением эквивалентности.

2°. Отношение сравнения согласовано со сложением.

3°. Отношение сравнения согласовано с умножением.

4°. Сравнения можно почленно складывать.

5°. Сравнения можно почленно умножать.

6°. $a \equiv b \pmod{m} \iff d|m, d > 0 \implies a \equiv b \pmod{d}$.

7°. Если $c > 0$, то $a \equiv b \pmod{m} \iff ac \equiv bc \pmod{mc}$.

8°. $ac \equiv bc \pmod{m} \iff d = (m, c) \implies a \equiv b \pmod{\frac{m}{d}}$.

9°. $ac \equiv bc \pmod{mc} \iff (m, c) = 1 \implies a \equiv b \pmod{m}$.

10°. $a \equiv b \pmod{m} \iff (a, m) = (b, m)$.

11°. $a \equiv b \pmod{m} \implies f(x) \in \mathbb{Z}[x] \implies f(a) \equiv f(b) \pmod{m}$.

12°. $a = mq + r \implies a \equiv r \pmod{m}$.

Признаки делимости. Общий признак делимости Паскаля. Признаки делимости на $2, 2^k, 5, 5^k, 3, 9, 11$.

§ 2. Кольца классов вычетов. Полная и приведенная системы вычетов.

[1]: §§ 3.4–3.5, [2]: §§ 2.2–2.3.

$$\mathbb{Z}_m = \mathbb{Z}/(m)$$

Теорема 1. Строение колец классов вычетов

1°. Если m – число простое, то \mathbb{Z}_m – поле.

2°. Если m – число составное, то \mathbb{Z}_m содержит делители нуля.

3°. Всякий ненулевой элемент кольца \mathbb{Z}_m является либо делителем нуля, либо делителем единицы (обратимым элементом).

$$4°. G^{\mathbb{Z}_m} = \{ \bar{a} : (a, m) = 1 \}.$$

$$\varphi(m)$$

Полная и приведенная системы вычетов (ПСВ и ПрСВ).

Наиболее употребительные системы вычетов: наименьшая положительная, наименьшая неотрицательная, абсолютно наименьшая и т.д.

Теорема 2. Свойства ПСВ и ПрСВ

1°. Критерий ПСВ. Любая совокупность из m целых чисел, попарно не сравнимых по модулю m , образует ПСВ по модулю m .

2°. Если числа x_1, x_2, \dots, x_m – ПСВ по модулю m , $(a, m) = 1$, b – произвольное целое число, то числа $ax_1 + b, ax_2 + b, \dots, ax_m + b$ также составляют ПСВ по модулю m .

3°. Критерий ПрСВ. Любая совокупность, состоящая из $\varphi(m)$ целых чисел, попарно не сравнимых по модулю m и взаимно простых с модулем, образует ПрСВ по модулю m .

4°. Если числа $x_1, x_2, \dots, x_{\varphi(m)}$ – ПрСВ по модулю m , $(a, m) = 1$, то числа $ax_1, ax_2, \dots, ax_{\varphi(m)}$ также составляют ПрСВ по модулю m .

§ 3. Функция Эйлера. Теоремы Эйлера и Ферма. [1]: § 2.4, § 3.6, [2]: §§ 2.4–2.5.

Определение функции Эйлера. $\varphi(m)$.

Теорема 1. Свойства функции Эйлера

1°. Если p – простое число, то $\varphi(p) = p-1$.

2°. Если p – простое число, то $\varphi(p^k) = p^{k-1}(p-1)$.

3°. Функция φ мультипликативная.

4°. Формулы для вычисления $\varphi(m)$.

5°. Тождество Гаусса: $\sum_{m:d} \varphi(d) = m$.

Теорема 2. Теорема Эйлера

Если числа a и m взаимно простые, то $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Следствие.

1°. (Теорема Ферма). Если p – простое число и a не делится на p , то $a^{p-1} \equiv 1 \pmod{p}$.

2°. (Обобщенная теорема Ферма). Если p – простое число, то $a^p \equiv a \pmod{p}$ для любых $a \in \mathbb{Z}$.

§ 4. Решение сравнений с переменной. [1]: § 4.1, § 4.4, [2]: § 3.1.

Решение сравнений. Равносильность. Степень сравнения.

Теорема. Свойства решений сравнений

1°. Решениями сравнений являются целые классы вычетов.

2°. $(\forall k)(a_k \equiv b_k \pmod{m}) \iff k = \overline{0, n}$ сравнения $\sum_k a_k x^k \equiv 0 \pmod{m}$ и $\sum_k b_k x^k \equiv 0 \pmod{m}$ равносильны.

3°. Если обе части сравнения умножить на число, взаимно простое с модулем, то получится сравнение, равносильное исходному.

4°. Всякое сравнение по простому модулю p равносильно сравнению, степень которого не превосходит $p-1$.

5°. Сравнение $\sum_{k=0}^n a_k x^k \equiv 0 \pmod{p}$, где p – простое число, имеет не более n различных решений.

6°. (Теорема Вильсона) $(n-1)! \equiv -1 \pmod{n}$ n простое число.

§ 5. Решение сравнений первой степени. [1]: § 4.2, [2]: § 3.2.

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

Теорема. 1°. Если $(a, m) = 1$, то сравнение имеет решение, причем единственное.

2°. Если $(a, m) = d$ и b не делится на d , то сравнение не имеет решений.

3°. Если $(a, m) = d$ и b делится на d , то сравнение имеет d различных решений, которые составляют один класс вычетов по модулю $\frac{m}{d}$.

Способы решения сравнений $ax \equiv b \pmod{m}$ в случае, когда $(a, m) = 1$:

- 1) подбор (перебор элементов ПСВ);
- 2) использование теоремы Эйлера;
- 3) использование алгоритма Евклида;
- 4) вариация коэффициентов (использование свойства 2° ПСВ из Теоремы 2.2);
- 5) использование подходящих дробей (свойство 2° подходящих дробей из Теоремы 3.1.3).

§ 6. Неопределённые уравнения первой степени. [2]: § 3.4.

$$ax + by = c.$$

Теорема. Уравнение $ax + by = c$ разрешимо тогда и только тогда, когда $c \in (a, b)$.

В случае $(a, b) = 1$ все решения уравнения задаются формулами

$$\begin{cases} x = x_0 + bt, \\ y = y_0 - at, \end{cases} \quad t \in \mathbf{Z}, \text{ где } x_0 \text{ является каким-либо решением сравнения}$$

$$ax \equiv c \pmod{b}, \quad y_0 = \frac{c - ax_0}{b}.$$

§ 7. Системы линейных сравнений. [1]: § 4.3, [2]: § 3.5.

Сведение к простейшим сравнениям.

Пример решения системы сравнений без ограничений на модули.

Случай попарно взаимно простых модулей.

$$\begin{cases} x \equiv b_1 \pmod{m_1}, \\ x \equiv b_2 \pmod{m_2}, \\ \dots \dots \dots \\ x \equiv b_s \pmod{m_s}, \end{cases}$$

(1)

а) $b_1 = b_2 = \dots = b_s = b_0$.

б) В противном случае.

Теорема. Пусть m_1, m_2, \dots, m_s – попарно взаимно простые числа, $M = m_1 m_2 \dots m_s$. Пусть

числа M_k и M^{-k} определены из условий $M = M_k m_k$, $M_k M^{-k} \equiv 1 \pmod{m_k}$,

$k = \overline{1, s}$. Пусть $x_0 = M_1 M^{-1} b_1 + M_2 M^{-2} b_2 + \dots + M_s M^{-s} b_s$.

Тогда множество решений системы (1) определяется сравнением $x \equiv x_0 \pmod{M}$.

Следствие. Если b_1, b_2, \dots, b_s независимо друг от друга пробегают ПСВ по модулям m_1

- 1) $\psi(\delta)$ равняется 0 или $\varphi(\delta): x^\delta \equiv 1 \pmod{p}$;
 $\sum_{\delta} \psi(\delta) = \sum_{\delta} \varphi(\delta)$
- 2) δ .

Теорема 3. Если \bar{g} – первообразный корень по модулю простого числа p , то для любого ненулевого класса вычетов \bar{x} найдется, и только одно, число γ такое, что $\bar{x} = \bar{g}^\gamma$ и $0 \leq \gamma < p-2$.

$$\text{ind}_{\bar{g}} \bar{a}$$

Теорема 4. Свойства индексов

- 1° $\text{ind} \bar{ab} = \text{ind} \bar{a} + \text{ind} \bar{b} \pmod{p-1}$.
 2° $\text{ind} \bar{a}^k = k \text{ind} \bar{a} \pmod{p-1}$.
 3° $\text{ind} \bar{a/b} = \text{ind} \bar{a} - \text{ind} \bar{b} \pmod{p-1}$.
 4° $\text{ind} \bar{1} = 0$.
 5° $\text{ind}_{\bar{g}} \bar{g} = 1$.

Применения индексов

1. При решении сравнений.
2. При отыскании порядка элемента.

§ 10. Бесконечные десятичные дроби. [2]: § 5.2.

Бесконечные десятичные дроби. Бесконечные периодические десятичные дроби. Чисто периодические и смешанные периодические десятичные дроби.

Теорема 1. Всякое рациональное число представляется в виде конечной или бесконечной периодической десятичной дроби.

Теорема 2. Правильная несократимая дробь a/b , где $a, b \in \mathbb{N}$, представляется в виде конечной десятичной дроби тогда и только тогда, когда в разложение знаменателя на простые множители входят только числа 2 или 5.

Теорема 3. Если знаменатель правильной несократимой дроби a/b , где $a, b \in \mathbb{N}$, взаимно прост с основанием системы счисления 10, то дробь a/b представляется в виде чисто периодической десятичной дроби и длина периода дроби равна порядку числа 10 по модулю b .

Теорема 4. Если разложение знаменателя b правильной несократимой дроби a/b имеет вид

$$b = 2^\alpha 5^\beta p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s},$$

где p_1, p_2, \dots, p_s – простые числа, не делящие число 10, то дробь представляется в виде смешанной периодической дроби:

$$a/b = 0, a_1 a_2 \dots a_m (a_{m+1} a_{m+2} \dots a_{m+s}).$$

Период s этой дроби равен порядку числа 10 по модулю

$$b_1 = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_s^{\alpha_s}, \text{ а предпериод } m \text{ равен } \max\{\alpha, \beta\}$$

ГЛАВА 3. Цепные дроби

§ 1. Конечные цепные дроби. [2]: §§ 3.3–3.4.

КЦД. Определение конечной цепной дроби. $[q_1, q_2, q_3, \dots, q_n]$.

Частные, начальные отрезки и “хвосты”.

Теорема 1. Свойства цепных дробей.

1°. Всякая КЦД является рациональным числом.

2°. Всякое рациональное число представляется в виде КЦД.

3°. Всякое рациональное число единственным образом представляется в виде КЦД, при условии, что последнее неполное частное $\neq 1$.

(Идея доказательства свойства 3°: доказать, что “хвост” $\alpha = [0, q_2, q_3, \dots, q_n]$ удовлетворяет условию $0 < \alpha < 1$)

$$\text{Подходящие дроби: } \delta_k = \frac{P_k}{Q_k};$$

$$P_k = q_k P_{k-1} + P_{k-2} \text{ при } k \geq 3; P_1 = q_1, P_2 = q_1 q_2 + 1.$$

$$Q_k = q_k Q_{k-1} + Q_{k-2} \text{ при } k \geq 3; Q_1 = 1, Q_2 = q_2.$$

Теорема 2. Значение любого начального отрезка КЦД совпадает со значением подходящей дроби с тем же номером.

Теорема 3. Свойства подходящих дробей

1°. $P_k, Q_k \in \mathbf{Z}; (Q_k)$ – возрастающая последовательность натуральных чисел.

2°. Имеет место тождество: $P_k Q_{k-1} - Q_k P_{k-1} = (-1)^k$.

3°. Подходящие дроби несократимы.

4°. Подходящие дроби с нечётными номерами образуют возрастающую последовательность, подходящие дроби с чётными номерами образуют убывающую последовательность.

5°. Каждая подходящая дробь δ_{2k} больше, чем δ_{2k-1} и δ_{2k+1} .

6°. Каждая подходящая дробь δ_{2k+1} меньше, чем δ_{2k} и δ_{2k+2} .

7°. Любая подходящая дробь δ_{2k} больше любой подходящей дроби δ_{2p-1} .

8°. Если $\alpha \in \mathbf{Q}_+$, то при его разложении в цепную дробь все нечётные подходящие дроби – приближения по недостатку, а все чётные подходящие дроби – приближения по избытку, за исключением последней дроби, совпадающей с α .

9°. Если $\alpha \in \mathbf{Q}_+$ и δ_k – подходящая дробь в разложении α в цепную дробь, то $|\alpha - \delta_k| < (Q_k Q_{k+1})^{-1} < Q_k^{-2}$.

Решение сравнений первой степени с помощью конечных цепных дробей.

§ 2. Бесконечные цепные дроби. [2]: § 6.1.

БЦД. Начальные отрезки и “хвосты”. Подходящие дроби.

Определение значения БЦД.

Встают задачи:

1. Сопоставить любой БЦД действительное (иррациональное) число.
2. Представить всякое иррациональное число в виде БЦД.
3. Доказать, что значение БЦД, полученное по правилу 1, разлагается в ту же самую БЦД по правилу 2.
4. Доказать, что всякое иррациональное число единственным образом разлагается в БЦД.

Теорема 1. Всякая БЦД имеет действительное значение.

Теорема 2. Всякое иррациональное число разлагается в БЦД.

Теорема 3. Пусть $\alpha \in \mathbf{R} \setminus \mathbf{Q}$, $\alpha = [q_1, q_2, \dots, q_n, \dots]$. Тогда α лежит между двумя последовательными значениями подходящих дробей δ_k и δ_{k+1} , причем α лежит ближе к δ_{k+1} , чем к δ_k .

Следствие. Если α разлагается в БЦД, то значение этой БЦД равно α .

Теорема 4. Всякое иррациональное число единственным образом разлагается в БЦД.

§ 3. Квадратичные иррациональности и периодические бесконечные цепные дроби. [2]: § 6.3.

Квадратичные иррациональности.

Теорема 1. α – квадратичная иррациональность $\alpha = \frac{a + \sqrt{b}}{c}$, где $a, c \in \mathbf{Z}$, $b \in \mathbf{N}$ и не является полным квадратом.

Теорема 2. Иррациональное число является квадратичной иррациональностью тогда и только тогда, когда оно представляется в виде бесконечной периодической цепной дроби.

§ 4. Приближение действительных чисел подходящими дробями [2]: § 6.2.

Две задачи приближения рациональными числами.

Теорема 1. Теорема Дирихле. $(\forall \alpha \in \mathbf{R})(\forall \tau > 1)(\exists r = a/b)(b < \tau)(|\alpha - r| < \frac{1}{b\tau})$.

$(r = \delta_k = \frac{P_k}{Q_k}, \text{ где } Q_k < \tau < Q_{k+1})$

Наилучшее рациональное приближение действительного числа.

Теорема 2. Подходящие дроби δ_k , где $k \geq 2$, являются наилучшими приближениями

действительных чисел.

Следствие. Отрезки с концами, равными последовательным дробям δ_{k-1} и δ_k некоторого числа не содержат ни одного рационального числа, знаменатель которого $< Q_{k-1}$.

ГЛАВА 4. Алгебраические и трансцендентные числа

§ 1. Числа алгебраические и трансцендентные [1]: § 5.2, пп. 1, 2, [2]: §§ 7.2–7.3.

Теорема 1. Множество алгебраических чисел счётное.

Следствие. Множество трансцендентных чисел несчётное.

Теорема 2. Теорема Лиувилля

Для любого действительного алгебраического числа α степени n , где $n \geq 2$, существует $c > 0$ такое, что неравенство $\left| \alpha - \frac{p}{q} \right| \geq \frac{c}{q^n}$ выполняется для любого рационального числа $\frac{p}{q}$.

Построение конкретных трансцендентных чисел.

Итоговый тест по Теории Чисел

Структура теста по теории чисел

№ ДЕ	Наименование дидактической единицы	№ задания	Тема задания
1.	Отношение делимости. Деление с остатком	1.	Определение и свойства делимости
2.	НОД, НОК. Взаимно простые числа	2.	Деление с остатком
3.	Простые числа. Основная теорема арифметики	3.	Систематические числа
4.	Числовые функции	4.	НОД
5.	Числовые сравнения	5.	НОК
6.	Функция и теорема Эйлера	6.	Связь НОД и НОК
		7.	Взаимно простые числа
		8.	Простые числа
		9.	Свойства простых чисел
		10.	Основная теорема арифметики
		11.	Мультипликативные функции
		12.	Числовые функции σ и τ
		13.	Целая и дробная части числа
		14.	Определение отношения сравнения
		15.	Свойства числовых сравнений
		16.	Кольца классов вычетов
		17.	Полная система вычетов
		18.	Приведённая система вычетов
		19.	Определение и свойства функции Эйлера
		20.	Теоремы Эйлера и Ферма

- | | |
|--|--|
| 7. Сравнения с переменной | 21. Сравнения и системы сравнений I степени |
| 8. Порядок элемента. Первообразные корни | 22. Неопределённые уравнения I степени |
| 9. Цепные дроби | 23. Сравнения высших степеней |
| | 24. Порядок элемента |
| | 25. Первообразные корни и индексы |
| | 26. Обращение обыкновенной дроби в десятичную |
| | 27. Обращение действительного числа в цепную дробь |
| | 28. Единственность представления в цепную дробь |
| | 29. Свойства подходящих дробей |
| | 30. Теорема Лагранжа |

При ответе на каждое задание следует поставить знак + или – (плюс или минус), в зависимости от того считаете ли Вы это утверждение истинным или ложным

I вариант

1. Определение и свойства делимости.

- 1) Если a и b делятся на c , то $a + b$ тоже делится на c .
- 2) Если a и b не делятся на c , то $a + b$ тоже не делится на c .
- 3) Если a делится на c , а b не делится на c , то $a + b$ делится на c .
- 4) Если a делится на c , а b не делится на c , то $a + b$ не делится на c .

2. Деление с остатком.

Определить, может ли сумма остатков от деления двух чисел на 5 быть равна:

- 1) 9;
- 2) -2;
- 3) 0;
- 4) 5.

3. Систематические числа.

Равенство $(10)_{(10)} = 10$ выполняется в системе счисления с основанием:

- 1) 19;
- 2) 99;
- 3) нигде не выполняется;
- 4) в любой системе счисления с основанием $g > 10$.

4. НОД.

- 1) Любые два целых числа имеют единственный НОД.
- 2) Любые два целых числа имеют ровно два НОД.
- 3) Любые два НОД целых чисел совпадают.
- 4) Любые два НОД целых чисел совпадают, с точностью до знака.

5. НОК.

- 1) Всякое НОК меньше любого ОК.
- 2) Всякое НОК не превышает любого ОК.
- 3) Существует ОК, меньшее некоторого НОК.
- 4) Существует НОК, не превышающее любого ОК.

6. Связь НОД и НОК.

Известно, что $[a, b] = ab$, $d = (2a, 2b)$ Тогда:

- 1) $d = 1$;
- 2) $d = 2$;
- 3) $d = 2^\alpha$, $\alpha > 1$;
- 4) d зависит от чётности a и b .

7. Взаимно простые числа.

- 1) Любые два взаимно простых числа нечётные.
- 2) Существуют два чётных взаимно простых числа.
- 3) Любые два числа разной чётности взаимно простые.
- 4) Любые два различных простых числа взаимно простые.

8. Простые числа.

- 1) Все простые числа нечётные.
- 2) Число 1 простое.
- 3) Всякое число, не являющееся простым, – составное.
- 4) Существует целое число, не являющееся ни простым, ни составным.

9. Свойства простых чисел и их количество.

- 1) $a > 1 \rightarrow (\exists p)(p \text{ – простое } p|a)$.
- 2) $p \text{ – простое } p|a \rightarrow a \text{ – составное}$.
- 3) $(\forall a)(\exists p)(p \text{ – простое } p > a)$.
- 4) $p \text{ – простое } p \neq 2 \mid a \rightarrow a \text{ – составное}$.

10. Основная теорема арифметики.

- 1) $a^2 \mid bc \rightarrow (\exists m)(\exists n)(b = m^2 \quad c = n^2)$.
- 2) $a^n \mid m \rightarrow a^n \mid m^n$.
- 3) $m \nmid a \quad m \nmid b \rightarrow m \nmid ab$.
- 4) $p \nmid a \quad p \text{ – простое} \rightarrow p \nmid a^2$.

11. Мультипликативные функции.

Функция f является мультипликативной функцией:

- 1) $f: \mathbf{N} \rightarrow \mathbf{N}$ по правилу $f(n) = n^3$;
- 2) $f: \mathbf{N} \rightarrow \mathbf{N}$ по правилу $f(n) = 2^n$;
- 3) $f: \mathbf{Z} \rightarrow \mathbf{Z}$ по правилу $f(n) = n^5$;
- 4) $f: \mathbf{R} \rightarrow \mathbf{R}$ по правилу $f(x) = x^{12}$.

12. Числовые функции σ и τ .

Число 28 является:

- 1) избыточным;
- 2) недостаточным;
- 3) совершенным;
- 4) не является ни одним из вышеперечисленных.

13. Целая и дробная части числа.

$$\left[-5 \frac{1}{17} \right] =$$

- 1) -5 ;
- 2) -6 ;
- 3) 5 ;

4) не существует, так как данное число не является целым.

14. Определение отношения сравнения.

- 1) $7 \equiv -15 \pmod{11}$.
- 2) $83 \equiv -13 \pmod{10}$.
- 3) $13 \equiv -83 \pmod{12}$.
- 4) $-37 \equiv 93 \pmod{4}$.

15. Свойства числовых сравнений.

- 1) $m \mid m_1 \quad a \equiv b \pmod{m} \rightarrow a \equiv b \pmod{m_1}$.
- 2) $m \mid m_1 \quad a \not\equiv b \pmod{m} \rightarrow a \not\equiv b \pmod{m_1}$.
- 3) $a^2 \equiv b^2 \pmod{m} \rightarrow a \equiv b \pmod{m}$.
- 4) $a \equiv b \pmod{m} \rightarrow a^3 \equiv b^3 \pmod{m}$.

16. Кольца классов вычетов.

Кольцо \mathbf{Z}_{19} :

- 1) является полем;
- 2) содержит делители нуля;
- 3) является целостным кольцом;
- 4) не является полем.

17. Полная система вычетов.

Пусть a, b – фиксированные целые числа, $f: \mathbf{Z} \rightarrow \mathbf{Z}$ по правилу $f(n) = an+b$, m – натуральное число, отличное от 1. Тогда:

- 1) при любых a, b функция f сохраняет полную систему вычетов по модулю m ;
- 2) при $(a, m) = 1$ и любом b функция f сохраняет полную систему вычетов по модулю m ;
- 3) при $(a, m) = (b, m) = 1$ функция f сохраняет полную систему вычетов по модулю m ;
- 4) при $(b, m) = 1$ и любом a функция f сохраняет полную систему вычетов по модулю m .

18. Приведённая система вычетов.

Приведённая система элементов по модулю 30 содержит:

- 1) 29 элементов;
- 2) 15 элементов;
- 3) 5 элементов;
- 4) 8 элементов.

19. Определение и свойства функции Эйлера.

- 1) $\varphi(8) = 4$;

- 2) $\varphi(7) = 6$;
- 3) $\varphi(6) = 5$;
- 4) $\varphi(9) = 6$.

20. Теоремы Эйлера и Ферма.

- 1) Если $(a, m) = 1$, то $a^m \equiv 1 \pmod{m}$.
- 2) Если $(a, m) = 1$, то $a^{\varphi(m)} \equiv 1 \pmod{m}$
- 3) Если $(a, m) = 1$, то $a^{m-1} \equiv 1 \pmod{m}$
- 4) Если $(a, m) = 1$, то $a^m \equiv a \pmod{m}$.

21. Сравнения и системы сравнений I степени.

1) Всякая система сравнений первой степени по произвольной совокупности модулей имеет решение.

2) Не всякая система сравнений первой степени по произвольной совокупности модулей имеет решение.

3) Всякая система сравнений по произвольной совокупности попарно взаимно простых модулей имеет решение.

4) Не всякая система сравнений по произвольной совокупности попарно взаимно простых модулей имеет решение.

22. Неопределённые уравнения I степени.

Уравнение $6x + 15y = 21$ имеет в \mathbf{Z} :

- 1) 0 решений;
- 2) 1 решение;
- 3) 3 решения;
- 4) бесконечно много решений.

23. Сравнения высших степеней.

Пусть $m \in \mathbf{N}$, $m > 1$, $f(x) \in \mathbf{Z}[x]$, $f(x) \not\equiv 0 \pmod{m}$. Тогда:

- 1) всякое сравнение имеет не более $\deg f$ решений;
- 2) сравнение может иметь больше, чем $\deg f$ решений;
- 3) если m – число простое, то сравнение имеет не более $\deg f$ решений;
- 4) если m – число составное, то сравнение может иметь более $\deg f$ решений.

24. Порядок элемента. Первообразные корни.

Пусть $n = \text{ord } a \pmod{m}$. Тогда:

- 1) $n|m$;
- 2) $n|\varphi(m)$;
- 3) n – любое натуральное число, $n \leq \varphi(m)$;
- 4) $(n, m) = 1$.

25. Существование первообразных корней. Индексы.

- 1) $(\exists a)(\text{ord } a \pmod{89} = 8)$;
- 2) $(\exists a)(\text{ord } a \pmod{89} = 22)$;
- 3) $(\exists a)(\text{ord } a \pmod{89} = 23)$;

4) $(\exists a)(\text{ord } a \pmod{89} = 24)$.

26. Обращение обыкновенной дроби в десятичную.

Число $\frac{1}{1500}$ представляется в виде:

- 1) конечной десятичной дроби;
- 2) бесконечной смешанной периодической десятичной дроби;
- 3) бесконечной чисто периодической десятичной дроби;
- 4) бесконечной не периодической десятичной дроби.

27. Обращение действительного числа в цепную дробь.

Число -2009 :

- 1) представляется в виде конечной цепной дроби;
- 2) не представляется в виде бесконечной цепной дроби;
- 3) представляется в виде бесконечной цепной дроби;
- 4) не представляется в виде конечной цепной дроби;.

28. Единственность представления в цепную дробь.

1) Всякое иррациональное число единственным образом представляется в виде цепной дроби.

2) Всякое рациональное число единственным образом представляется в виде цепной дроби.

3) Всякое рациональное число не единственным образом представляется в виде цепной дроби.

4) Всякое иррациональное число не единственным образом представляется в виде цепной дроби.

29. Свойства подходящих дробей.

Пусть (δ_n) последовательность подходящих дробей для бесконечной цепной дроби α . Тогда: 1) $\delta_{273} < \delta_{32}$;

3) $\delta_{52} < \delta_{63}$;

2) $\delta_{312} < \delta_{813}$;

4) $\delta_{84} < \delta_8$.

30. Теорема Лагранжа о периодических бесконечных дробях.

Пусть $\alpha = [1; 2, (3, 4)]$. Тогда:

1) существует многочлен первой степени с целыми коэффициентами, для которого α является корнем;

2) существует неприводимый многочлен второй степени с целыми коэффициентами, для которого α является корнем;

3) существует неприводимый многочлен третьей степени с целыми коэффициентами, для которого α является корнем;

4) не существует неприводимый многочлен третьей степени с целыми коэффициентами, для которого α является корнем.

II вариант

1. Определение и свойства делимости.

- 1) Если ab делится на c , то a делится на c или b делится на c .
- 2) Если ab не делится на c , то a не делится на c или b не делится на c .
- 3) Если a не делится на c или b не делится на c , то ab не делится на c .
- 4) Если a делится на c или b делится на c , то ab делится на c .

2. Деление с остатком.

Пусть $n \in \mathbb{Z}$. Тогда остаток от деления числа $2009n - 18$ на 2009 равен:

- 1) 18;
- 2) -18 ;
- 3) 1991;
- 4) не определён: зависит от значения n .

3. Систематические числа.

Равенство $(10) + (10) = 10$ выполняется в системе счисления с основанием:

- 1) 19;
- 2) 99;
- 3) нигде не выполняется;
- 4) в любой системе счисления с основанием $g > 10$.

4. НОД.

- 1) Всякий НОД больше любого ОД.
- 2) Всякий НОД не меньше любого ОД.
- 3) Существует ОД, меньший некоторого НОД.
- 4) Существует НОД, не превышающий любого ОД.

5. НОК.

- 1) Любые два целых числа имеют единственное НОК.
- 2) Любые два целых числа имеют ровно два НОК.
- 3) Любые два НОК целых чисел совпадают.
- 4) Любые два НОК целых чисел совпадают, с точностью до знака.

6. Связь НОД и НОК.

Известно, что $(16a, 12b) = 4$, $m = [12a, 6b]$. Тогда:

- 1) $m = 3ab$;
- 2) $m = 6ab$;
- 3) m зависит от чётности a ;
- 4) $m = 12ab$.

7. Взаимно простые числа.

- 1) Любые два последовательных целых числа являются взаимно простыми.
- 2) Любые два последовательных нечётных числа являются взаимно простыми.
- 3) Любые два последовательных чётных числа являются взаимно простыми.
- 4) Любые два элемента последовательности $(10n+3)$, $n \in \mathbb{N}$, являются взаимно простыми.

8. Простые числа.

- 1) Всякое натуральное число обладает простым делителем.
- 2) Всякое целое число имеет конечное число делителей.
- 3) Существует целое число, имеющее бесконечное число делителей.
- 4) Всякое натуральное число имеет конечное число делителей.

9. Свойства простых чисел и их количество.

- 1) Если $p \mid p$ и $p \mid 1$, то p – простое число.
- 2) Если a – составное число, то $a \mid a$ и $a \mid 1$.
- 3) Если a – составное число и p – простое число, то $a \mid p$.
- 4) Если a – составное число и p – простое число, то $a > p$.

10. Основная теорема арифметики.

- 1) $a^2 \mid bc$ (b, c) = 1 $\rightarrow (\exists m)(\exists n)(b = m^2 \quad c = n^2)$.
- 2) $a^2 \mid m \rightarrow a \mid m$.
- 3) $p \nmid a \quad p \nmid b \quad p$ – простое $\rightarrow p \nmid ab$.
- 4) $a^n \mid p \quad p$ – простое $\rightarrow a^n \mid p^n$.

11. Мультипликативные функции.

- 1) Функция “Целая часть числа” является мультипликативной.
- 2) Функция “Дробная часть числа” является мультипликативной.
- 3) Функция $f(x) = ax$, где a – фиксированное натуральное число, является мультипликативной.
- 4) Функция Эйлера является мультипликативной.

12. Числовые функции σ и τ .

Пусть $a = n^2$. Тогда:

- 1) количество натуральных делителей числа a чётно;
- 2) количество натуральных делителей числа a нечётно;
- 3) чётность количества натуральных делителей числа a зависит от значения числа n ;
- 4) чётность количества натуральных делителей числа a не поддаётся никакой оценке.

13. Целая и дробная части числа.

$$\left\{ -5 \frac{1}{17} \right\} =$$

$$1) -\frac{1}{17};$$

$$2) \frac{1}{17};$$

$$3) \frac{16}{17};$$

4) не существует, т.к. данное число не входит в промежуток $[0, 1)$.

14. Определение отношения сравнения.

$$1) 2 \equiv -9 \pmod{11};$$

- 2) $-37 \equiv 7 \pmod{10}$;
- 3) $287 \equiv 412 \pmod{15}$;
- 4) $-27 \equiv 90 \pmod{13}$.

15. Свойства числовых сравнений.

- 1) Если $ac \equiv bc \pmod{m}$, то $a \equiv b \pmod{m}$.
- 2) Если $a \equiv b \pmod{m}$, то $a \equiv b \pmod{mc}$.
- 3) Если $a \not\equiv b \pmod{m}$, то $a^2 \not\equiv b^2 \pmod{m}$.
- 4) Если $a \not\equiv b \pmod{m}$, то $ac \not\equiv bc \pmod{m}$.

16. Кольца классов вычетов.

Кольцо \mathbf{Z}_{18} :

- 1) является полем;
- 2) содержит делители нуля;
- 3) является целостным кольцом;
- 4) не является полем.

17. Полная система вычетов.

- 1) Числа 2, 4, 6, 8, 10 образуют ПСВ $\pmod{5}$.
- 2) Числа 4, -4 , 3, -3 , 1, 5 образуют ПСВ $\pmod{6}$.
- 3) Числа 6, -3 , 2, 1, 0, -2 образуют ПСВ $\pmod{6}$.
- 4) Числа 1, -2 , 3, -4 , 10 образуют ПСВ $\pmod{5}$.

18. Приведённая система вычетов.

- 1) Числа 1, 3, 5 образуют ПрСВ $\pmod{6}$.
- 2) Числа 3, -5 образуют ПрСВ $\pmod{6}$.
- 3) Числа 1, -2 , 5 образуют ПрСВ $\pmod{6}$.
- 4) Числа -3 , -2 , 1, 2, -4 , 12 образуют ПрСВ $\pmod{6}$.

19. Определение и свойства функции Эйлера.

- 1) $\varphi(6) = 3$;
- 2) $\varphi(7) = 6$;
- 3) $\varphi(12) = 6$;
- 4) $\varphi(8) = 4$.

20. Теоремы Эйлера и Ферма.

- 1) $a^m \equiv a \pmod{m}$ при любых a и m .
- 2) $a^m \equiv a \pmod{m}$ при любых a и простых m .
- 3) $a^{m-1} \equiv 1 \pmod{m}$ при любых a и простых m .
- 4) $a^{m-1} \equiv 1 \pmod{m}$ при простых a и m .

21. Сравнения и системы сравнений I степени.

Сравнение $115x \equiv 46 \pmod{69}$ имеет:

- 1) 0 решений;
- 2) 1 решение;
- 3) 23 решения;

4) бесконечно много решений.

22. Неопределённые уравнения I степени.

Уравнение $12x - 20y = 34$ имеет в \mathbf{Z} :

- 1) 0 решений;
- 2) 1 решение;
- 3) 4 решения;
- 4) бесконечно много решений.

23. Сравнения высших степеней.

Следующее утверждение является формулировкой теоремы Вильсона:

- 1) m – простое число $\rightarrow (m-1)! \equiv -1 \pmod{m}$;
- 2) m – простое число $\rightarrow (m-2)! \equiv 1 \pmod{m}$;
- 3) $(m-1)! \equiv -1 \pmod{m} \rightarrow m$ – простое число;
- 4) $(m-2)! \equiv 1 \pmod{m} \rightarrow m$ – простое число.

24. Порядок элемента. Первообразные корни.

Пусть m – натуральное число, по которому существует первообразный корень.

Тогда m может быть:

- 1) простым числом;
- 2) $m = p^\alpha$, где p – простое число, $\alpha \in \mathbf{N}$;
- 3) $m = 2p^\alpha$, где p – простое нечётное число, $\alpha \in \mathbf{N}$;
- 4) произвольным нечётным числом.

25. Существование первообразных корней. Индексы.

- 1) $(\exists a)(\text{ord } a \pmod{97} = 8)$;
- 2) $(\exists a)(\text{ord } a \pmod{97} = 22)$;
- 3) $(\exists a)(\text{ord } a \pmod{97} = 23)$;
- 4) $(\exists a)(\text{ord } a \pmod{97} = 24)$.

26. Обращение обыкновенной дроби в десятичную.

$\frac{1}{27}$

Число $\frac{1}{27}$ представляется в виде:

- 1) конечной десятичной дроби;
- 2) бесконечной смешанной периодической десятичной дроби;
- 3) бесконечной чисто периодической десятичной дроби;
- 4) бесконечной не периодической десятичной дроби.

27. Обращение действительного числа в цепную дробь.

$\frac{7}{\sqrt{23}}$

Число $\frac{7}{\sqrt{23}}$:

- 1) представляется в виде конечной цепной дроби;
- 2) не представляется в виде бесконечной цепной дроби;
- 3) представляется в виде бесконечной цепной дроби;
- 4) не представляется в виде конечной цепной дроби.

28. Единственность представления в цепную дробь.

- 1) Число $\frac{712}{217}$ не единственным образом представляется в виде цепной дроби.
- 2) Число $\sqrt{3} - \sqrt{2}$ не единственным образом представляется в виде цепной дроби.
- 3) Число $\sqrt{3} - 17$ единственным образом представляется в виде цепной дроби.
- 4) Число $\frac{217}{712}$ единственным образом представляется в виде цепной дроби.

29. Свойства подходящих дробей.

—
Пусть (δ_n) — последовательность подходящих дробей для конечной цепной дроби r . Тогда:

- 1) (δ_n) — возрастающая последовательность;
- 2) (δ_n) — убывающая последовательность;
- 3) каждая δ_n является несократимой дробью;
- 4) каждая δ_n является приближением r с недостатком.

30. Теорема Лагранжа о периодических бесконечных цепных дробях.

Число $\sqrt[3]{2}$ представляется:

- 1) в виде бесконечной периодической цепной дроби;
- 2) в виде бесконечной непериодической цепной дроби;
- 3) в виде конечной цепной дроби;
- 4) не представляется в виде цепной дроби.

III вариант

1. Определение и свойства делимости.

- 1) Если $a + b$ делится на c , то a делится на c и b делится на c .
- 2) Если $a + b$ и a делятся на c , то b делится на c .
- 3) Если $a + b$ и $a - b$ делятся на c , то a и b делятся на c .
- 4) Если $a - b$ и a делятся на c , то b делится на c .

2. Деление с остатком.

Пусть $n \in \mathbf{Z}$. Тогда остаток от деления числа $2009n - 18$ на -2009 равен:

- 1) 18;
- 2) -18 ;
- 3) 1991;
- 4) не определён: зависит от значения n .

3. Систематические числа.

Равенство $10 - (10) = (10)$ выполняется в системе счисления с основанием:

- 1) 19;
- 2) 99;
- 3) нигде не выполняется;

4) в любой системе счисления с основанием $g > 10$.

4. НОД.

- 1) Если d – НОД (a, b) , то $(\exists u)(\exists v)(d = ua + vb)$.
- 2) Если $(\exists u)(\exists v)(d = ua + vb)$, то d – НОД (a, b) .
- 3) Если $(\exists u)(\exists v)(1 = ua + vb)$, то 1 – НОД (a, b) .
- 4) Среди всех данных утверждений ровно три правильные.

5. НОК.

- 1) $ab \mid \text{НОК}(a, b)$.
- 2) $ab = \text{НОК}(a, b) \quad (a, b) = 1$.
- 3) $(a, b) = 1 \quad ab = \text{НОК}(a, b)$.
- 4) $\text{НОК}(a, b) \mid ab$.

6. Связь НОД и НОК.

Известно, что $(20a, 12b) = 4, d = (a, b)$. Тогда:

- 1) $d = 1$;
- 2) $d = 4$;
- 3) $d \mid 4$;
- 4) d не определён.

7. Взаимно простые числа.

- 1) Если ни одно из чисел не делится на другое, то они взаимно простые.
- 2) Если одно из чисел равно 1, то они взаимно простые.
- 3) Если числа не имеют общего простого делителя, то они взаимно простые.
- 4) Если числа не имеют общего составного делителя, то они взаимно простые.

8. Простые числа.

- 1) p – простое $(\forall a)(p \mid a \rightarrow a = p)$ и p – взаимно простые).
- 2) p – простое $a \mid p \rightarrow a = 1$.
- 3) $(\exists p)(p$ – простое $p > 2^{1000000}$).
- 4) $(\forall a)(\exists b)(b > a \rightarrow b$ – составное).

9. Свойства простых чисел и их количество.

- 1) Если p_1 и p_2 – два различных простых числа, то $p_1 + p_2$ – число чётное.
- 2) Если p_1 и p_2 – два различных простых числа, то $p_1 \cdot p_2$ – число нечётное.
- 3) Если p_1 и p_2 – два различных простых числа, то число $p_1^2 - p_2^2$ – число составное.
- 4) Если p_1 и p_2 – два различных простых нечётных числа, то число $p_1^2 - p_2^2$ – число составное.

10. Основная теорема арифметики.

- 1) $ab \dot{\vdots} m \rightarrow a \dot{\vdots} m \wedge b \dot{\vdots} m$.
- 2) $a^2 \dot{\vdots} p \wedge p$ – простое $\rightarrow a \dot{\vdots} p$.
- 3) $a^3 \dot{\vdots} bc \wedge (b, c) = 1 \rightarrow (\exists m)(\exists n)(b = m^3 \wedge c = n^3)$.
- 4) $ab \dot{\vdots} c^2 \wedge (a, b) = 1 \rightarrow a \dot{\vdots} c^2 \wedge b \dot{\vdots} c^2$.

11. Мультипликативные функции.

Пусть $f: \mathbb{N} \rightarrow \mathbb{N}$ – мультипликативная функция. Тогда:

- 1) $f(mn) = f(m)f(n)$ для любых m и n ;
- 2) $f(m+n) = f(m)+f(n)$ для любых m и n ;
- 3) $f(mn) = f(m)f(n)$ для $(m, n) = 1$;
- 4) $f(m+n) = f(m)+f(n)$ для $(m, n) = 1$.

12. Числовые функции σ и τ .

- 1) Функция σ мультипликативная.
- 2) Функция τ мультипликативная, но не вполне мультипликативная.
- 3) Функция τ мультипликативная.
- 4) Функция σ мультипликативная, но не вполне мультипликативная.

13. Целая и дробная части числа.

$$\left[-5 \frac{1}{17} \right] + \left\{ -5 \frac{1}{17} \right\} =$$

- 1) $-5 \frac{16}{17}$;
- 2) $5 \frac{16}{17}$;
- 3) $-5 \frac{1}{17}$;
- 4) $-6 \frac{1}{17}$.

14. Определение отношения сравнения.

- 1) $-8 \equiv -37 \pmod{21}$;
- 2) $113 \equiv 11 \pmod{6}$;
- 3) $-12 \equiv 27 \pmod{5}$;
- 4) $347 \equiv 28 \pmod{11}$.

15. Свойства числовых сравнений.

- 1) Если $ac \equiv bc \pmod{m}$, то $a \equiv b \pmod{m}$.
- 2) Если $a \not\equiv b \pmod{m}$, то $a^3 \not\equiv b^3 \pmod{m}$.
- 3) Если $a^2 \not\equiv b^2 \pmod{m}$, то $a \not\equiv b \pmod{m}$.
- 4) Если $a \not\equiv b \pmod{m}$, то $ac \not\equiv bc \pmod{m}$.

16. Кольца классов вычетов.

Кольцо \mathbb{Z}_{12} :

- 1) является полем;
- 2) содержит делители нуля;
- 3) является целостным кольцом;
- 4) не является полем.

17. Полная система вычетов.

- 1) Числа $-2, -4, -6, 8, 10$ образуют полную систему вычетов по mod 5.
- 2) Числа $4, -4, 3, -3, -1, -5$ образуют полную систему вычетов по mod 6.
- 3) Числа $-6, 3, 2, 1, 0, -2$ образуют полную систему вычетов по mod 6.
- 4) Числа $-1, 2, -3, 4, -10$ образуют полную систему вычетов по mod 5.

18. Приведённая система вычетов.

- 1) Числа $2, 3, 4, 5$ образуют приведённую систему вычетов по mod 5.
- 2) Числа $4, -4, 3, -3, -1, -5$ образуют приведённую систему вычетов по mod 5.
- 3) Числа $1, -2, 3, -4$ образуют приведённую систему вычетов по mod 5.
- 4) Числа $-3, -2, 1, 2, -4$ образуют приведённую систему вычетов по mod 5.

19. Определение и свойства функции Эйлера.

Пусть $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ – каноническое разложение m . Тогда $\varphi(m)$ вычисляется по формуле:

- 1) $(p_1+1)(p_2+1) \dots (p_s+1)$;
 $\frac{1}{p_1} \frac{1}{p_2} \dots \frac{1}{p_s}$
- 2) $m(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_s})$;
- 3) $p_1^{\alpha_1-1} (p_1-1) p_2^{\alpha_2-1} (p_2-1) \dots p_s^{\alpha_s-1} (p_s-1)$;
 $\frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \dots \frac{p_s^{\alpha_s+1} - 1}{p_s - 1}$
- 4) $\frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \dots \frac{p_s^{\alpha_s+1} - 1}{p_s - 1}$.

20. Теоремы Эйлера и Ферма.

- 1) $a^{\varphi(m)} \equiv a \pmod{m}$ при $(a, m) = 1$ и любых m .
- 2) $a^m \equiv 1 \pmod{m}$ при $(a, m) = 1$ и простых m .
- 3) $a^m \equiv 1 \pmod{m}$ при любых a и простых m .
- 4) $a^{\varphi(m)-1} \equiv a \pmod{m}$ при $(a, m) = 1$ и любых m .

21. Сравнения и системы сравнений I степени.

Сравнение $81x \equiv 72 \pmod{36}$ имеет:

- 1) 0 решений;
- 2) 1 решение;
- 3) 9 решений;
- 4) бесконечно много решений

22. Неопределённые уравнения I степени.

Уравнение $37x - 11y = 224$ имеет в \mathbf{Z} :

- 1) 0 решений;
- 2) 1 решение;
- 3) 4 решения;
- 4) бесконечно много решений.

23. Сравнения высших степеней.

Степень сравнения $7x^6+14x^5+3x^2-6x+1 \equiv 0 \pmod{7}$ равна:

- 1) 7;
- 2) 6;
- 3) 2;
- 4) 1.

24. Порядок элемента. Первообразные корни.

Пусть a – первообразный корень по модулю m . Тогда:

- 1) $(a, m) = 1$;
- 2) $a|m$;
- 3) $m|a$;
- 4) a и m имеют общий простой делитель.

25. Существование первообразных корней. Индексы.

Пусть m – модуль, по которому существует первообразный корень g . Тогда:

- 1) $\text{ind}(a+b) = \text{ind } a + \text{ind } b$;
- 2) $\text{ind}(a \cdot b) = \text{ind } a + \text{ind } b$;
- 3) $\text{ind}(a/b) = \text{ind } a - \text{ind } b$;
- 4) $\text{ind}(a^k) = k \cdot \text{ind } a$.

26. Обращение обыкновенной дроби в десятичную.

$$\frac{\sqrt{3}}{27}$$

Число $\frac{\sqrt{3}}{27}$ представляется в виде:

- 1) конечной десятичной дроби;
- 2) бесконечной смешанной периодической десятичной дроби;
- 3) бесконечной чисто периодической десятичной дроби;
- 4) бесконечной не периодической десятичной дроби.

27. Обращение действительного числа в цепную дробь.

$$\frac{7}{\sqrt{23}}$$

Число $345 - \frac{7}{\sqrt{23}}$:

- 1) представляется в виде конечной цепной дроби;
- 2) не представляется в виде бесконечной цепной дроби;
- 3) представляется в виде бесконечной цепной дроби;
- 4) не представляется в виде конечной цепной дроби.

28. Единственность представления в цепную дробь.

$$-\frac{7}{27}$$

1) Число $-\frac{7}{27}$ не единственным образом представляется в виде цепной дроби.

2) Число $5\sqrt{3} - \sqrt{2}$ не единственным образом представляется в виде цепной дроби.

3) Число $\sqrt{3} - 17$ единственным образом представляется в виде цепной дроби.

4) Число $\sqrt{3} - 17$ единственным образом представляется в виде цепной дроби.

29. Свойства подходящих дробей.

Пусть (δ_n) – последовательность подходящих дробей для представления иррационального числа a в виде бесконечной цепной дроби. Тогда:

- 1) (δ_n) – возрастающая последовательность;
- 2) (δ_{2n}) – убывающая последовательность;
- 3) (δ_{2n-1}) – убывающая последовательность;
- 4) $\delta_{2010} < \delta_{2011} < \delta_{2012}$.

30. Теорема Лагранжа о периодических бесконечных цепных дробях.

Число $4\sqrt{5} - 11$ представляется:

- 1) в виде бесконечной периодической цепной дроби;
- 2) в виде бесконечной непериодической цепной дроби;
- 3) в виде конечной цепной дроби;
- 4) не представляется в виде цепной дроби.